Soluciones de nube pública e híbrida de NetApp

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Soluciones de nube pública e híbrida de NetApp . . . 1
Novedades en las soluciones de nube pública e híbrida de NetApp . . . 2
Multicloud híbrida de NetApp con soluciones VMware . . . 3
VMware para la nube pública . . . 3
Descripción general de NetApp Hybrid Multicloud con VMware . . . 3
Soluciones NetApp para VMware en hiperescaladores . . . 7
Configuraciones compatibles con NetApp Hybrid Multicloud con VMware . . . 10
VMware en la configuración de hiperescaladores . . . 10
Almacenamiento de NetApp en nubes públicas . . . 35
Resumen y conclusión: ¿Por qué NetApp Hybrid Multicloud con VMware? . . . 138
Casos de uso de la nube híbrida de VMware . . . 140
Casos de uso de NetApp Hybrid Multicloud con VMware . . . 140
Soluciones NetApp para VMware en hiperescaladores . . . 141
Soluciones de NetApp para Amazon VMware Managed Cloud (VMC) . . . 142
Soluciones NetApp para Azure VMware Solution (AVS) . . . 142
Soluciones de NetApp para Google Cloud VMware Engine (GCVE) . . . 143
NetApp para AWS/VMC . . . 143
Capacidades de NetApp para AWS VMC . . . 143
Proteja las cargas de trabajo en AWS/VMC . . . 145
Migrar cargas de trabajo en AWS/VMC . . . 262
NetApp para AWS/EVS . . . 277
Montar FSx ONTAP como almacén de datos externo para EVS . . . 277
Proteger datastore FSx ONTAP para EVS . . . 301
NetApp para Azure/AVS . . . 334
Capacidades de NetApp para Azure AVS . . . 335
Proteger las cargas de trabajo en Azure/AVS . . . 336
Migrar cargas de trabajo en Azure/AVS . . . 406
NetApp para GCP/GCVE . . . 421
Capacidades de NetApp para Google Cloud Platform GCVE . . . 421
Proteger las cargas de trabajo en GCP/GCVE . . . 422
Migrar cargas de trabajo en GCP/GCVE . . . 455
Proteja sus datos con Google Cloud NetApp Volumes en Google Cloud . . . 472
NetApp Disaster Recovery . . . 544
Protección de datos 3-2-1 para VMware con SnapCenter Plug-in y NetApp Backup and Recovery para proteger las cargas de trabajo de VMware . . . 544
NetApp Disaster Recovery . . . 580
Multicloud híbrido de NetApp con cargas de trabajo de contenedores Red Hat OpenShift . . . 622
Empezar . . . 622
Soluciones multicloud híbridas de NetApp para cargas de trabajo de contenedores Red Hat OpenShift . . . 622
Propuestas de valor de las soluciones multicloud híbridas de NetApp para cargas de trabajo de contenedores Red Hat OpenShift . . . 624
Soluciones compatibles de NetApp Hybrid Multicloud para cargas de trabajo de contenedores Red

Hat OpenShift . . . 625
Versiones de varios componentes utilizados en la validación de la solución . . . 629
Integraciones de almacenamiento de NetApp compatibles con Red Hat OpenShift Containers . . . 630
Documentación adicional . . . 634
Openshift para instalaciones locales . . . 634
Solución NetApp con cargas de trabajo de la plataforma Red Hat OpenShift Container en VMware . . . 634
Implementar y configurar la plataforma Red Hat OpenShift Container en VMware . . . 635
Protección de datos mediante Trident Protect . . . 637
Nube híbrida con componentes autogestionados . . . 638
Solución NetApp con cargas de trabajo de la plataforma Red Hat OpenShift Container en la nube híbrida . . . 638
Implementar y configurar la plataforma Red Hat OpenShift Container en AWS . . . 640
Implementar y configurar Red Hat OpenShift Container Platform en Google Cloud . . . 642
Implementar y configurar la plataforma Red Hat OpenShift Container en Azure . . . 644
Protección de datos mediante Trident Protect . . . 647
Nube híbrida con componentes administrados por el proveedor . . . 647
Solución NetApp con cargas de trabajo de la plataforma de contenedores Red Hat OpenShift administradas . . . 647
Implementar y configurar la plataforma Managed Red Hat OpenShift Container en AWS . . . 648
Implemente y configure OpenShift Dedicated en Google Cloud con Google Cloud NetApp Volumes . . . 651
Protección de datos . . . 653
Soluciones multicloud híbridas adicionales de NetApp para cargas de trabajo de Red Hat OpenShift . . . 653
Proteja sus datos con Trident Protect . . . 653
Protección de datos para Container Apps en OpenShift Container Platform usando Trident Protect . . . 653
Protege las máquinas virtuales en Red Hat OpenShift Virtualization usando Trident Protect . . . 665
Proteja las aplicaciones de contenedores mediante herramientas de terceros . . . 685
Protección de datos para aplicaciones de contenedores en OpenShift Container Platform mediante la API de OpenShift para la protección de datos (OADP) . . . 685
Instalación del operador de API de OpenShift para protección de datos (OADP) . . . 687
Creación de copias de seguridad a pedido para aplicaciones en OpenShift Container Platform . . . 696
Migrar una aplicación de un clúster a otro . . . 699
Restaurar una aplicación desde una copia de seguridad . . . 703
Eliminar copias de seguridad y restauraciones al usar Velero . . . 710
Vea videos y demostraciones sobre soluciones multicloud híbridas con NetApp . . . 712
Vea videos sobre soluciones multicloud híbridas para Amazon Web Services con NetApp . . . 712
Almacenamiento conectado para invitados . . . 712
TCO y almacenes de datos complementarios . . . 712
Flujos de trabajo de migración (HCX) . . . 712
Vea videos sobre soluciones multicloud híbridas para Azure VMware Cloud con NetApp . . . 712
Almacenes de datos complementarios . . . 712
Recuperación ante desastres . . . 712
Flujos de trabajo de migración (HCX) . . . 713
Vea videos sobre soluciones multicloud híbridas para Red Hat OpenShift con NetApp . . . 713
Instantáneas y restauración . . . 713
Integración de almacenamiento . . . 713

Conmutación por error y recuperación . . . 713
Automatización de soluciones . . . 713
Lea blogs de soluciones en la nube de expertos de NetApp . . . 714
Integración de VMware con AWS y Amazon FSx para ONTAP . . . 714
Solución VMware de Azure . . . 714
Motor VMware de Google Cloud . . . 714
Protección y gestión de datos . . . 714
NetApp para cargas de trabajo de contenedores OpenShift . . . 714
Nube soberana de VMware . . . 714
Avisos legales . . . 715
Copyright . . . 715
Marcas comerciales . . . 715
Patentes . . . 715
Política de privacidad . . . 715

Soluciones de nube pública e híbrida de NetApp

Novedades en las soluciones de nube pública e híbrida de NetApp

Conozca las novedades en soluciones de nube pública e híbrida.

[[18-august-2025]]
== 18 de agosto de 2025

El sitio de NetApp Solutions ahora es el"Familia de soluciones NetApp" , que incluye los siguientes sitios:

- "Soluciones de inteligencia artificial de NetApp"
- "Soluciones de contenedores de NetApp"
- "Soluciones de gestión de datos de NetApp"
- "Soluciones de bases de datos de NetApp"
- Soluciones de nube pública e híbrida de NetApp
- "Soluciones NetApp para SAP"
- "Soluciones de virtualización de NetApp"

Multicloud híbrida de NetApp con soluciones VMware

VMware para la nube pública

Descripción general de NetApp Hybrid Multicloud con VMware

La mayoría de las organizaciones de TI siguen el enfoque híbrido de nube primero. Estas organizaciones están en una fase de transformación y los clientes están evaluando su panorama de TI actual y luego migrando sus cargas de trabajo a la nube basándose en el ejercicio de evaluación y descubrimiento.

Los factores que llevan a los clientes a migrar a la nube pueden incluir elasticidad y expansión, salida del centro de datos, consolidación del centro de datos, escenarios de fin de vida útil, fusiones, adquisiciones, etc. El motivo de esta migración puede variar según cada organización y sus respectivas prioridades comerciales. Al migrar a la nube híbrida, elegir el almacenamiento adecuado en la nube es muy importante para liberar el poder de la implementación y la elasticidad de la nube.

Opciones de VMware Cloud en la nube pública

En esta sección se describe cómo cada uno de los proveedores de nube admite una pila VMware Software Defined Data Center (SDDC) y/o VMware Cloud Foundation (VCF) dentro de sus respectivas ofertas de nube pública.

Solución VMware de Azure

Azure VMware Solution es un servicio de nube híbrida que permite que los SDDC de VMware funcionen completamente dentro de la nube pública de Microsoft Azure. Azure VMware Solution es una solución propia totalmente administrada y respaldada por Microsoft, verificada por VMware que aprovecha la infraestructura de Azure. Esto significa que cuando se implementa Azure VMware Solution, los clientes obtienen ESXi de VMware para la virtualización informática, vSAN para el almacenamiento hiperconvergente y NSX para la red y la seguridad, todo ello mientras aprovechan la presencia global de Microsoft Azure, las instalaciones de centros de datos líderes en su clase y la proximidad al rico ecosistema de servicios y soluciones nativos de Azure.

VMware Cloud en AWS

VMware Cloud on AWS lleva el software SDDC de clase empresarial de VMware a la nube de AWS con acceso optimizado a los servicios nativos de AWS. VMware Cloud on AWS, impulsado por VMware Cloud Foundation, integra los productos de virtualización de red, almacenamiento y computación de VMware (VMware vSphere, VMware vSAN y VMware NSX) junto con la gestión de VMware vCenter Server, optimizado para ejecutarse en una infraestructura de AWS dedicada, elástica y completa.

Motor VMware de Google Cloud

Google Cloud VMware Engine es una oferta de infraestructura como servicio (IaaS) basada en la infraestructura escalable de alto rendimiento de Google Cloud y la pila VMware Cloud Foundation: VMware vSphere, vCenter, vSAN y NSX-T. Este servicio facilita una transición rápida a la nube, migrando o ampliando sin problemas las cargas de trabajo de VMware existentes desde entornos locales a Google Cloud Platform sin el coste, el esfuerzo ni el riesgo de rediseñar aplicaciones ni reestructurar operaciones. Es un servicio vendido y respaldado por Google, en estrecha colaboración con VMware.

La nube privada SDDC y la coubicación de NetApp Cloud Volumes brindan el mejor rendimiento con una latencia de red mínima.

¿Sabías?

Independientemente de la nube utilizada, cuando se implementa un VMware SDDC, el clúster inicial incluye los siguientes productos:

- Hosts VMware ESXi para virtualización informática con un dispositivo vCenter Server para administración
- Almacenamiento hiperconvergente VMware vSAN que incorpora los activos de almacenamiento físico de cada host ESXi
- VMware NSX para redes virtuales y seguridad con un clúster NSX Manager para administración

Configuración de almacenamiento

Para los clientes que planean alojar cargas de trabajo intensivas en almacenamiento y escalar en cualquier solución VMware alojada en la nube, la infraestructura hiperconvergente predeterminada dicta que la expansión debe ser tanto en los recursos de cómputo como de almacenamiento.

Al integrarse con NetApp Cloud Volumes, como Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponible en los tres hiperescaladores principales) y Google Cloud NetApp Volumes para Google Cloud, los clientes ahora tienen opciones para escalar su almacenamiento de forma independiente por separado y solo agregar nodos de cómputo al clúster SDDC según sea necesario.

Notas:

- VMware no recomienda configuraciones de clúster desequilibradas, por lo tanto, ampliar el almacenamiento significa agregar más hosts, lo que implica mayor TCO.
- Solo es posible un entorno vSAN. Por lo tanto, todo el tráfico de almacenamiento competirá directamente con las cargas de trabajo de producción.
- No existe la opción de proporcionar múltiples niveles de rendimiento para alinear los requisitos de la aplicación, el rendimiento y el costo.
- Es muy fácil alcanzar los límites de la capacidad de almacenamiento de vSAN construido sobre los hosts del clúster. Utilice NetApp Cloud Volumes para escalar el almacenamiento para alojar conjuntos de datos activos o agrupar datos más actualizados en un almacenamiento persistente.

Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponible en los tres hiperescaladores principales) y Google Cloud NetApp Volumes para Google Cloud se pueden usar junto con máquinas virtuales invitadas. Esta arquitectura de almacenamiento híbrido consta de un almacén de datos vSAN que contiene el sistema operativo invitado y los datos binarios de la aplicación. Los datos de la aplicación se conectan a la VM a través de un iniciador iSCSI basado en invitado o los montajes NFS/SMB que se comunican directamente con Amazon FSx ONTAP, Cloud Volume ONTAP, Azure NetApp Files y Google Cloud NetApp Volumes para Google Cloud respectivamente. Esta configuración le permite superar fácilmente los desafíos con la capacidad de almacenamiento, ya que con vSAN, el espacio libre disponible depende del espacio disponible y de las políticas de almacenamiento utilizadas.

Consideremos un clúster SDDC de tres nodos en VMware Cloud on AWS:

- La capacidad bruta total para un SDDC de tres nodos = 31,1 TB (aproximadamente 10 TB para cada nodo).
- El espacio libre que debe mantenerse antes de agregar hosts adicionales = 25 % = (0,25 x 31,1 TB) = 7,7

TB.

- La capacidad bruta utilizable después de la deducción del espacio libre = 23,4 TB
- El espacio libre efectivo disponible depende de la política de almacenamiento aplicada.

  Por ejemplo:

  - RAID 0 = espacio libre efectivo = 23,4 TB (capacidad bruta utilizable/1)
  - RAID 1 = espacio libre efectivo = 11,7 TB (capacidad bruta utilizable/2)
  - RAID 5 = espacio libre efectivo = 17,5 TB (capacidad bruta utilizable/1,33)

Por lo tanto, el uso de NetApp Cloud Volumes como almacenamiento conectado a invitados ayudaría a expandir el almacenamiento y optimizar el TCO y, al mismo tiempo, cumplir con los requisitos de rendimiento y protección de datos.

> El almacenamiento para invitados era la única opción disponible en el momento en que se escribió este documento.

Puntos para recordar

- En los modelos de almacenamiento híbrido, coloque cargas de trabajo de nivel 1 o de alta prioridad en el almacén de datos de vSAN para abordar cualquier requisito de latencia específico porque son parte del host mismo y están cerca. Utilice mecanismos de invitado para cualquier máquina virtual de carga de trabajo para la cual las latencias transaccionales sean aceptables.
- Utiliza la tecnología NetApp SnapMirror para replicar los datos de la carga de trabajo desde el sistema ONTAP local a Cloud Volumes ONTAP o Amazon FSx ONTAP para facilitar la migración mediante mecanismos de nivel de bloque. Esto no se aplica a Azure NetApp Files ni a Google Cloud NetApp Volumes. Para migrar datos a Azure NetApp Files o Google Cloud NetApp Volumes, usa NetApp XCP, NetApp Copy and Sync, rysnc o robocopy en función del protocolo de archivos utilizado.
- Las pruebas muestran una latencia adicional de 2 a 4 ms al acceder al almacenamiento desde los respectivos SDDC. Tenga en cuenta esta latencia adicional en los requisitos de la aplicación al asignar el almacenamiento.
- Para montar el almacenamiento conectado al invitado durante la conmutación por error de prueba y la conmutación por error real, asegúrese de que los iniciadores iSCSI estén reconfigurados, el DNS esté actualizado para los recursos compartidos SMB y los puntos de montaje NFS estén actualizados en fstab.
- Asegúrese de que las configuraciones de registro de tiempo de espera de disco, firewall y E/S multiruta de Microsoft (MPIO) en el invitado estén configuradas correctamente dentro de la máquina virtual.

> Esto se aplica únicamente al almacenamiento conectado por invitados.

Beneficios del almacenamiento en la nube de NetApp

El almacenamiento en la nube de NetApp ofrece los siguientes beneficios:

- Mejora la densidad de procesamiento y almacenamiento al escalar el almacenamiento independientemente del procesamiento.
- Le permite reducir la cantidad de hosts, lo que reduce el TCO general.
- La falla del nodo de cómputo no afecta el rendimiento del almacenamiento.
- La capacidad de remodelación de volumen y de nivel de servicio dinámico de Azure NetApp Files le permite optimizar los costos mediante el dimensionamiento para cargas de trabajo de estado estable,

evitando así el aprovisionamiento excesivo.

- Las eficiencias de almacenamiento, la organización en niveles de la nube y las capacidades de modificación del tipo de instancia de Cloud Volumes ONTAP permiten formas óptimas de agregar y escalar el almacenamiento.
- Evita el aprovisionamiento excesivo de recursos de almacenamiento y se agregan solo cuando es necesario.
- Las copias instantáneas y clones eficientes le permiten crear copias rápidamente sin ningún impacto en el rendimiento.
- Ayuda a abordar los ataques de ransomware mediante el uso de una recuperación rápida de copias instantáneas.
- Proporciona una recuperación ante desastres regional eficiente basada en transferencia de bloques incremental y un nivel de bloque de respaldo integrado en todas las regiones que brinda mejores RPO y RTO.

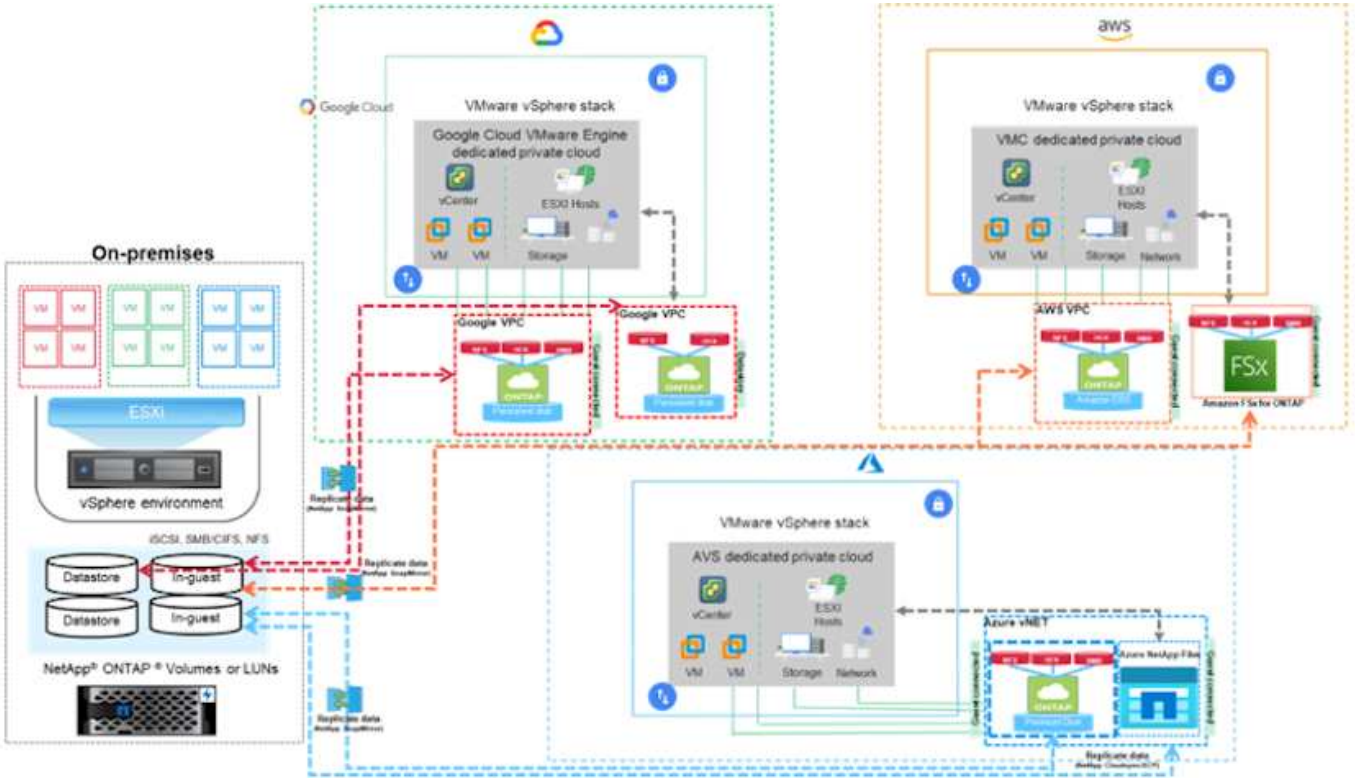
Suposiciones

- Se habilita la tecnología SnapMirror u otros mecanismos de migración de datos relevantes. Hay muchas opciones de conectividad, desde las instalaciones locales hasta cualquier nube de hiperescala. Utilice la ruta adecuada y trabaje con los equipos de redes relevantes.
- El almacenamiento para invitados era la única opción disponible en el momento en que se escribió este documento.

> Involucre a los arquitectos de soluciones de NetApp y a los respectivos arquitectos de nube de hiperescalador para planificar y dimensionar el almacenamiento y la cantidad necesaria de hosts. NetApp recomienda identificar los requisitos de rendimiento de almacenamiento antes de usar el dimensionador de Cloud Volumes ONTAP para finalizar el tipo de instancia de almacenamiento o el nivel de servicio apropiado con el rendimiento correcto.

Arquitectura detallada

Desde una perspectiva de alto nivel, esta arquitectura (que se muestra en la figura a continuación) cubre cómo lograr la conectividad multicloud híbrida y la portabilidad de aplicaciones entre múltiples proveedores de nube utilizando NetApp Cloud Volumes ONTAP, Google Cloud NetApp Volumes para Google Cloud y Azure NetApp Files como una opción de almacenamiento invitado adicional.



Soluciones NetApp para VMware en hiperescaladores

Obtenga más información sobre las capacidades que NetApp aporta a los tres (3) hiperescaladores principales: desde NetApp como un dispositivo de almacenamiento conectado invitado o un almacén de datos NFS complementario hasta la migración de flujos de trabajo, la extensión/ampliación a la nube, la copia de seguridad/restauración y la recuperación ante desastres.

¡Elige tu nube y deja que NetApp haga el resto!



Para ver las capacidades de un hiperescalador específico, haga clic en la pestaña correspondiente a ese hiperescalador.

Salte a la sección del contenido deseado seleccionando entre las siguientes opciones:

- "VMware en la configuración de hiperescaladores"
- "Opciones de almacenamiento de NetApp"
- "Soluciones en la nube NetApp /VMware"

VMware en la configuración de hiperescaladores

Al igual que en las instalaciones locales, la planificación de un entorno de virtualización basado en la nube es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

AWS/VMC

Esta sección describe cómo configurar y administrar VMware Cloud on AWS SDDC y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

El almacenamiento en el host es el único método compatible para conectar Cloud Volumes ONTAP a AWS VMC.

El proceso de configuración se puede dividir en los siguientes pasos:

- Implementar y configurar VMware Cloud para AWS
- Conecte VMware Cloud a FSx ONTAP

Ver el detalle"Pasos de configuración para VMC" .

Azure/AVS

En esta sección se describe cómo configurar y administrar Azure VMware Solution y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

El almacenamiento en el invitado es el único método compatible para conectar Cloud Volumes ONTAP a Azure VMware Solution.

El proceso de configuración se puede dividir en los siguientes pasos:

- Registrar el proveedor de recursos y crear una nube privada
- Conectarse a una puerta de enlace de red virtual ExpressRoute nueva o existente
- Validar la conectividad de la red y acceder a la nube privada

Ver el detalle"Pasos de configuración para AVS" .

GCP / GCVE

Esta sección describe cómo configurar y administrar GCVE y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

El almacenamiento en el huésped es el único método compatible para conectar Cloud

Volumes ONTAP y Google Cloud NetApp Volumes a GCVE.

El proceso de configuración se puede dividir en los siguientes pasos:

- Implementar y configurar GCVE
- Habilitar el acceso privado a GCVE

Ver el detalle"Pasos de configuración para GCVE" .

Opciones de almacenamiento de NetApp

El almacenamiento de NetApp se puede utilizar de varias maneras (ya sea como invitado conectado o como un almacén de datos NFS complementario) dentro de cada uno de los tres hiperescaladores principales.

Por favor visite"Opciones de almacenamiento de NetApp compatibles" Para más información.

AWS/VMC

AWS admite el almacenamiento de NetApp en las siguientes configuraciones:

- FSx ONTAP como almacenamiento conectado para invitados
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- FSx ONTAP como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para VMC" . Ver el detalle"Opciones de almacén de datos NFS complementario para VMC" .

Azure/AVS

Azure admite el almacenamiento de NetApp en las siguientes configuraciones:

- Azure NetApp Files (ANF) como almacenamiento conectado invitado
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- Azure NetApp Files (ANF) como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para AVS" . Ver el detalle"Opciones de almacén de datos NFS complementarias para AVS" .

GCP / GCVE

Google Cloud admite el almacenamiento de NetApp en las siguientes configuraciones:

- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- Google Cloud NetApp Volumes (NetApp Volumes) como almacenamiento conectado para invitados
- Google Cloud NetApp Volumes (NetApp Volumes) como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para GCVE" . Ver el detalle"Opciones de almacén de datos NFS suplementarias para GCVE" .

Leer más sobre"Compatibilidad del almacén de datos de Google Cloud NetApp Volumes con Google Cloud VMware Engine (blog de NetApp)" o"Cómo usar Google Cloud NetApp Volumes como almacenes de datos para Google Cloud VMware Engine (blog de Google)"

Soluciones en la nube NetApp /VMware

Con las soluciones de nube de NetApp y VMware, muchos casos de uso son fáciles de implementar en el hiperescalador que usted elija. VMware define los principales casos de uso de carga de trabajo en la nube como:

- Proteger (incluye recuperación ante desastres y copia de seguridad/restauración)
- Emigrar
- Extender

AWS/VMC

"Explorar las soluciones de NetApp para AWS/VMC"

Azure/AVS

"Explorar las soluciones de NetApp para Azure/AVS"

GCP / GCVE

"Explorar las soluciones de NetApp para Google Cloud Platform (GCP) / GCVE"

Configuraciones compatibles con NetApp Hybrid Multicloud con VMware

Comprender las combinaciones para el soporte de almacenamiento de NetApp en los principales hiperescaladores.

	Invitado conectado	Almacén de datos NFS complementario
AWS	CVO FSx ONTAP"Detalles"	FSx ONTAP"Detalles"
Azur	CVO ANF"Detalles"	ANF"Detalles"
GCP	Volúmenes CVO NetApp"Detalles"	Volúmenes de NetApp"Detalles"

VMware en la configuración de hiperescaladores

Configuración del entorno de virtualización en el proveedor de nube

Aquí se describen los detalles sobre cómo configurar el entorno de virtualización en cada uno de los hiperescaladores compatibles.

AWS/VMC

Esta sección describe cómo configurar y administrar VMware Cloud on AWS SDDC y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

El almacenamiento en el host es el único método compatible para conectar Cloud Volumes ONTAP a AWS VMC.

El proceso de configuración se puede dividir en los siguientes pasos:

- Implementar y configurar VMware Cloud para AWS

- Conecte VMware Cloud a FSx ONTAP

Ver el detalle"Pasos de configuración para VMC" .

Azure/AVS

En esta sección se describe cómo configurar y administrar Azure VMware Solution y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

> El almacenamiento en el invitado es el único método compatible para conectar Cloud Volumes ONTAP a Azure VMware Solution.

El proceso de configuración se puede dividir en los siguientes pasos:

- Registrar el proveedor de recursos y crear una nube privada
- Conectarse a una puerta de enlace de red virtual ExpressRoute nueva o existente
- Validar la conectividad de la red y acceder a la nube privada

Ver el detalle"Pasos de configuración para AVS" .

GCP / GCVE

Esta sección describe cómo configurar y administrar GCVE y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

> El almacenamiento en el huésped es el único método compatible para conectar Cloud Volumes ONTAP y Google Cloud NetApp Volumes a GCVE.

El proceso de configuración se puede dividir en los siguientes pasos:

- Implementar y configurar GCVE
- Habilitar el acceso privado a GCVE

Ver el detalle"Pasos de configuración para GCVE" .

Implementar y configurar el entorno de virtualización en AWS

Al igual que en las instalaciones locales, la planificación de VMware Cloud on AWS es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

Esta sección describe cómo configurar y administrar VMware Cloud on AWS SDDC y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

> Actualmente, el almacenamiento en el host es el único método compatible para conectar Cloud Volumes ONTAP (CVO) a AWS VMC.

El proceso de configuración se puede dividir en los siguientes pasos:

▼ **Implementar y configurar VMware Cloud para AWS**

"VMware Cloud en AWS"Proporciona una experiencia nativa de la nube 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 una nube privada virtual (VPC) de Amazon y proporciona una pila VMware completa (incluido vCenter Server), redes definidas por software NSX-T, almacenamiento definido por software vSAN y uno o más hosts ESXi que proporcionan recursos informáticos y de almacenamiento a sus cargas de trabajo.

En esta sección se describe cómo configurar y administrar VMware Cloud on AWS y usarlo en combinación con Amazon FSx ONTAP o Cloud Volumes ONTAP en AWS con almacenamiento invitado.

> Actualmente, el almacenamiento en el host es el único método compatible para conectar Cloud Volumes ONTAP (CVO) a AWS VMC.

El proceso de configuración se puede dividir en tres partes:

▼ **Regístrese para obtener una cuenta de AWS**

Regístrese para obtener una"Cuenta de Amazon Web Services" .

Necesita una cuenta de AWS para comenzar, suponiendo que aún no haya una creada. Ya sea nuevo o existente, necesitará privilegios administrativos en la cuenta para muchos pasos de este procedimiento. Mira esto"enlace" para obtener más información sobre las credenciales de AWS.

▼ **Regístrese para obtener una cuenta My VMware**

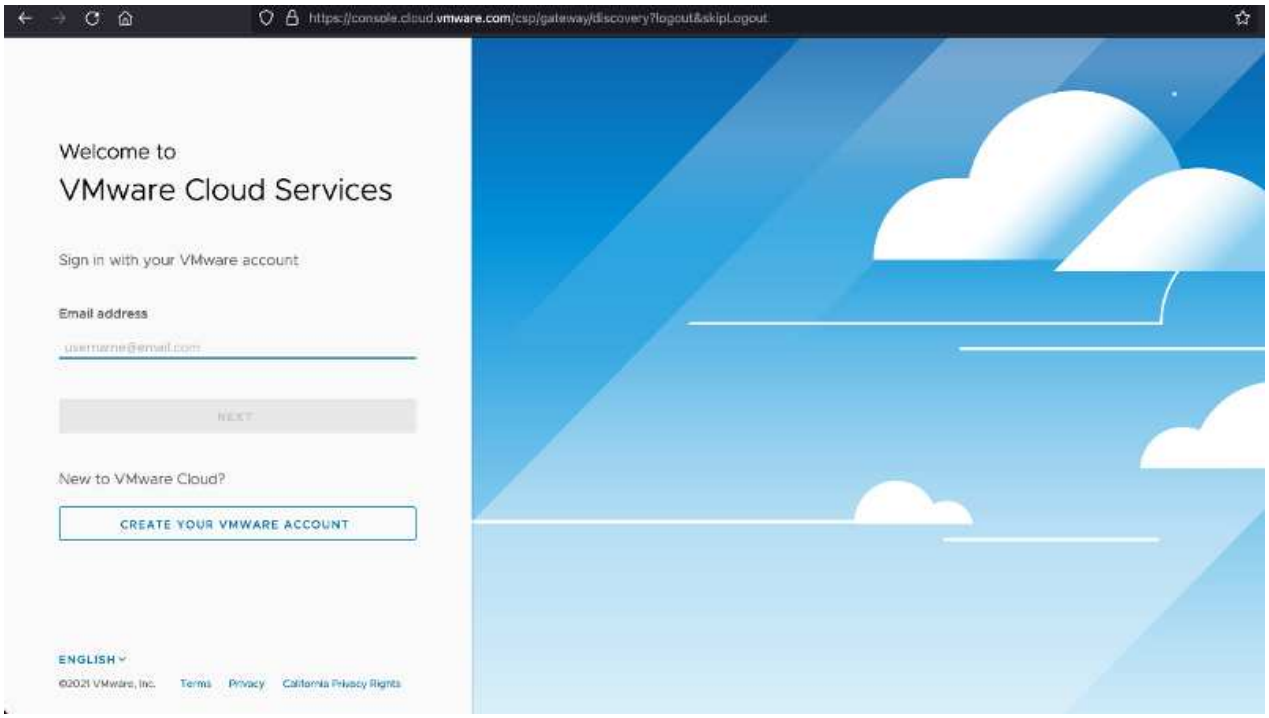
Regístrese para obtener una"Mi VMware" cuenta.

Para acceder a la cartera de nubes de VMware (incluido VMware Cloud en AWS), necesita una cuenta de cliente de VMware o una cuenta My VMware. Si aún no lo ha hecho, cree una cuenta de VMware"aquí" .

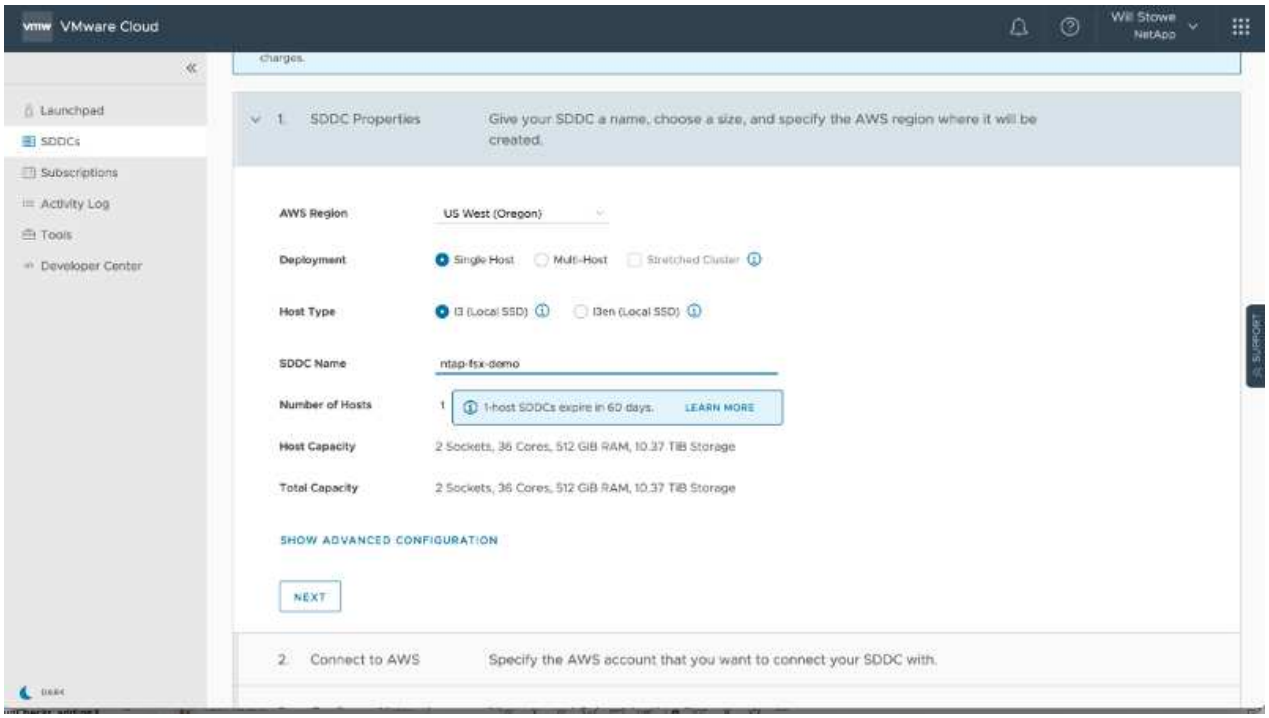
▼ **Aprovisionamiento de SDDC en VMware Cloud**

Una vez configurada la cuenta de VMware y realizada la dimensionación adecuada, la implementación de un centro de datos definido por software es el siguiente paso obvio para utilizar el servicio VMware Cloud on AWS. Para crear un SDDC, seleccione una región de AWS para alojarlo, asígnele un nombre al SDDC y especifique cuántos hosts ESXi desea que contenga el SDDC. Si aún no tiene una cuenta de AWS, puede crear un SDDC de configuración de inicio que contenga un solo host ESXi.

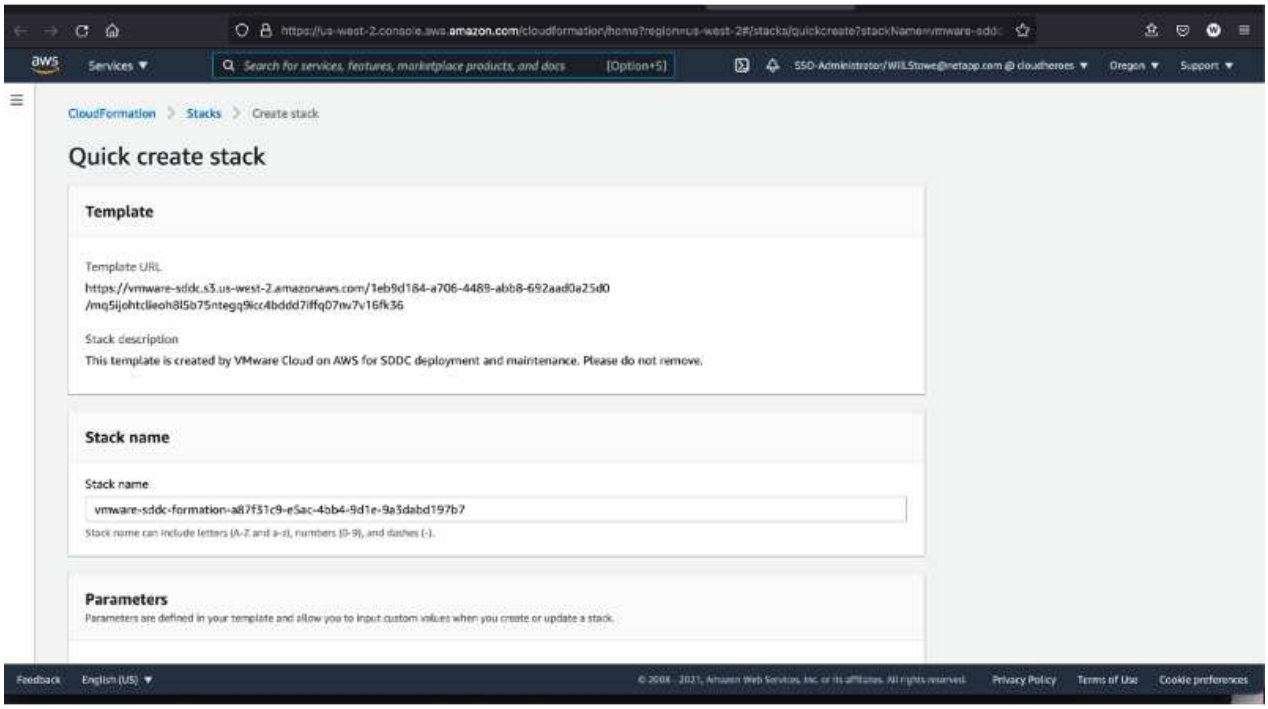
1. Inicie sesión en VMware Cloud Console utilizando sus credenciales de VMware existentes o recién creadas.

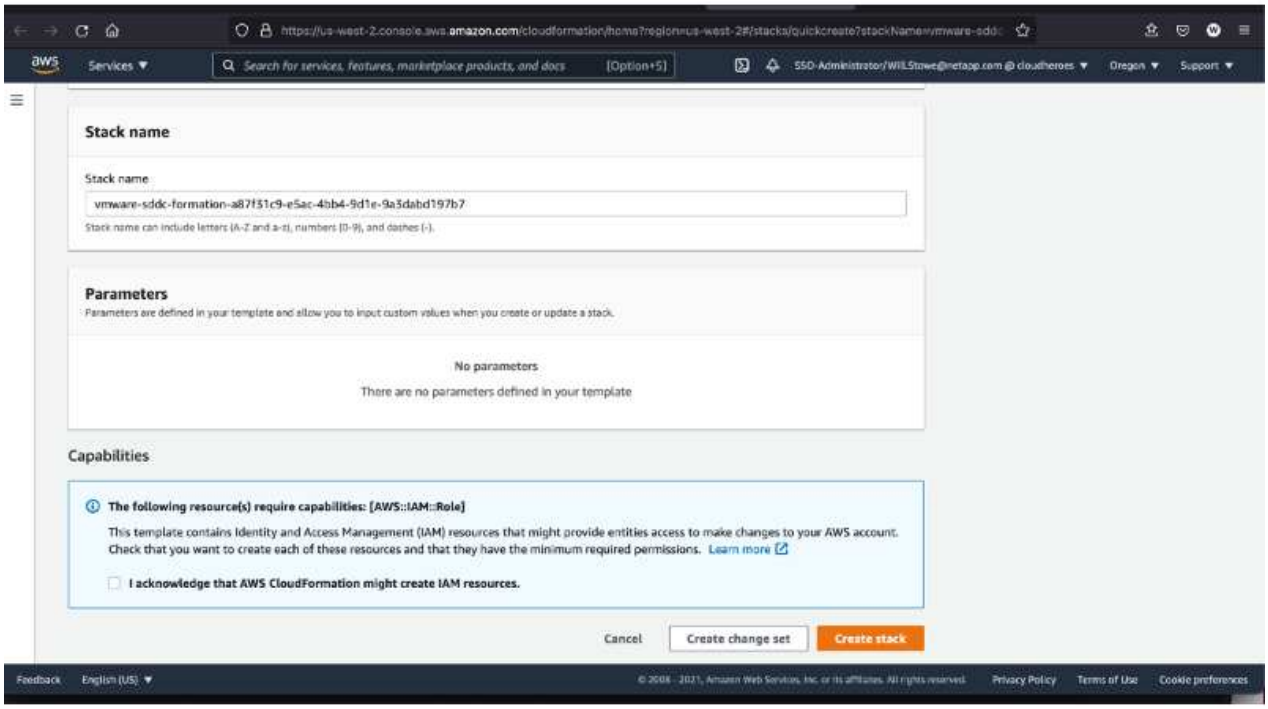


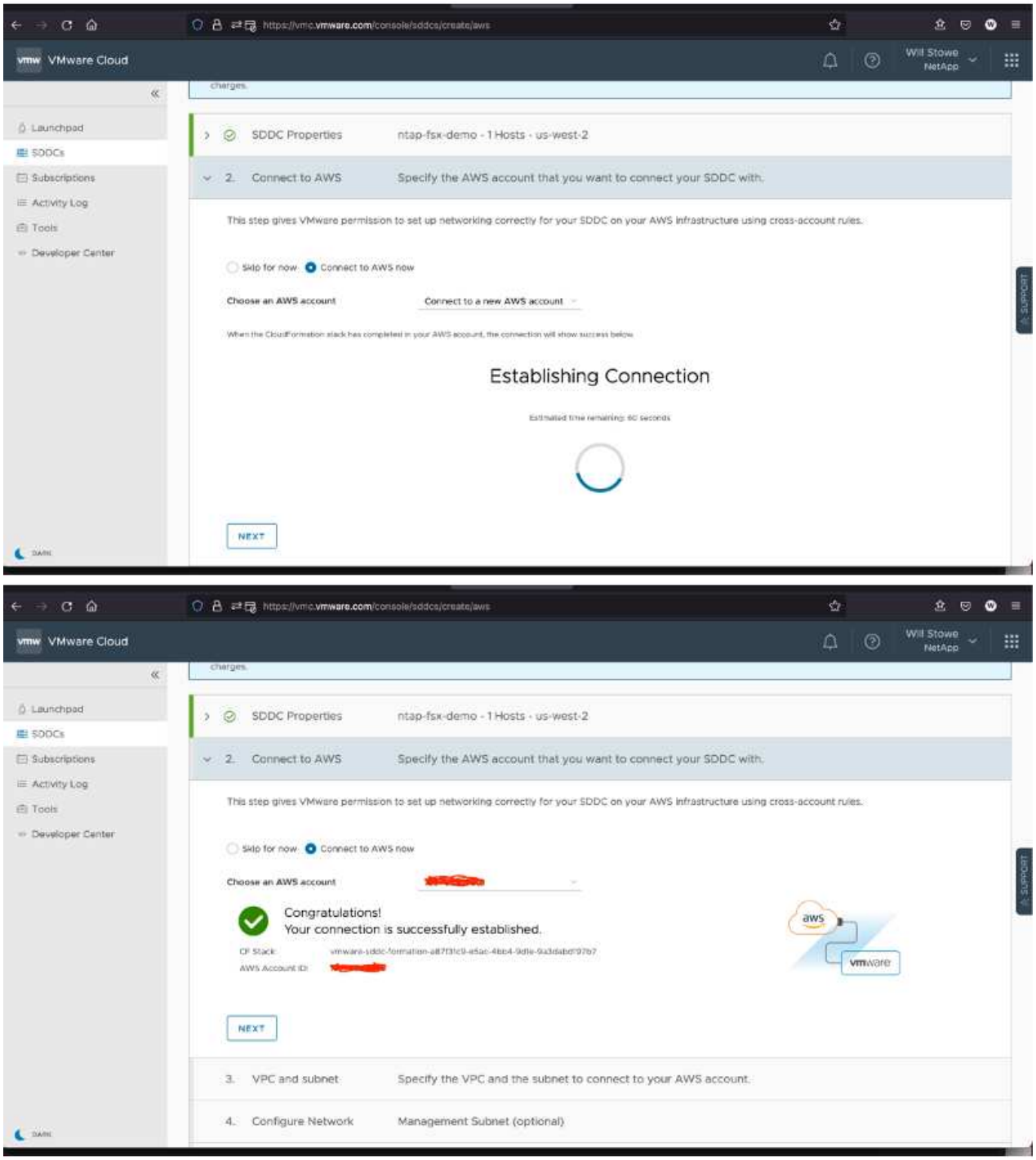
2. Configure la región de AWS, la implementación y el tipo de host y el nombre del SDDC:



3. Conéctese a la cuenta de AWS deseada y ejecute la pila AWS Cloud Formation.

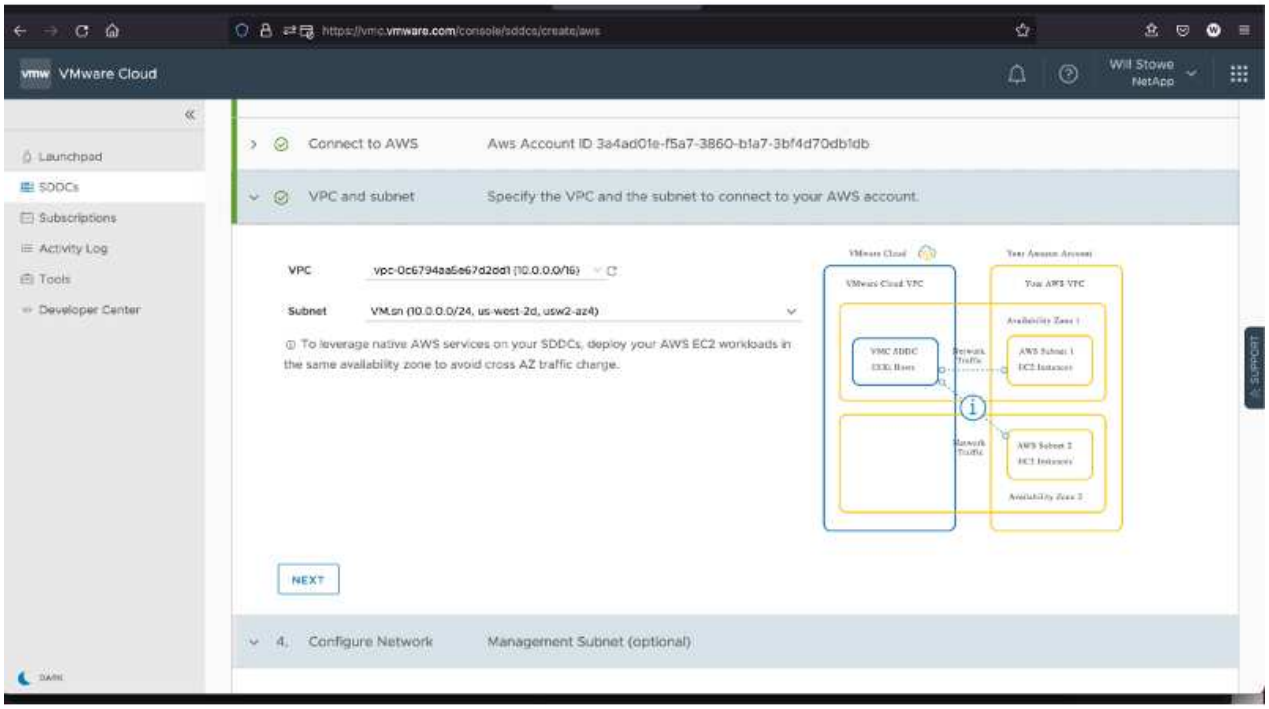

CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ljohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.


Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack

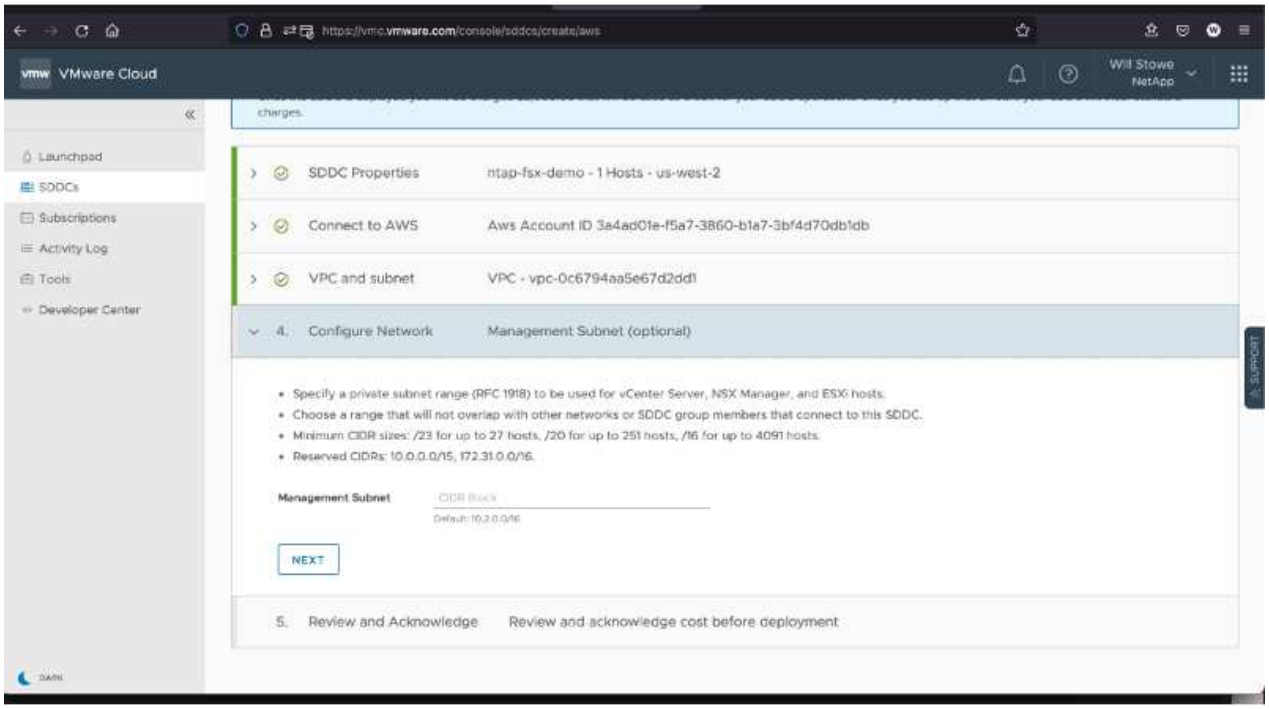


En esta validación se utiliza la configuración de host único.

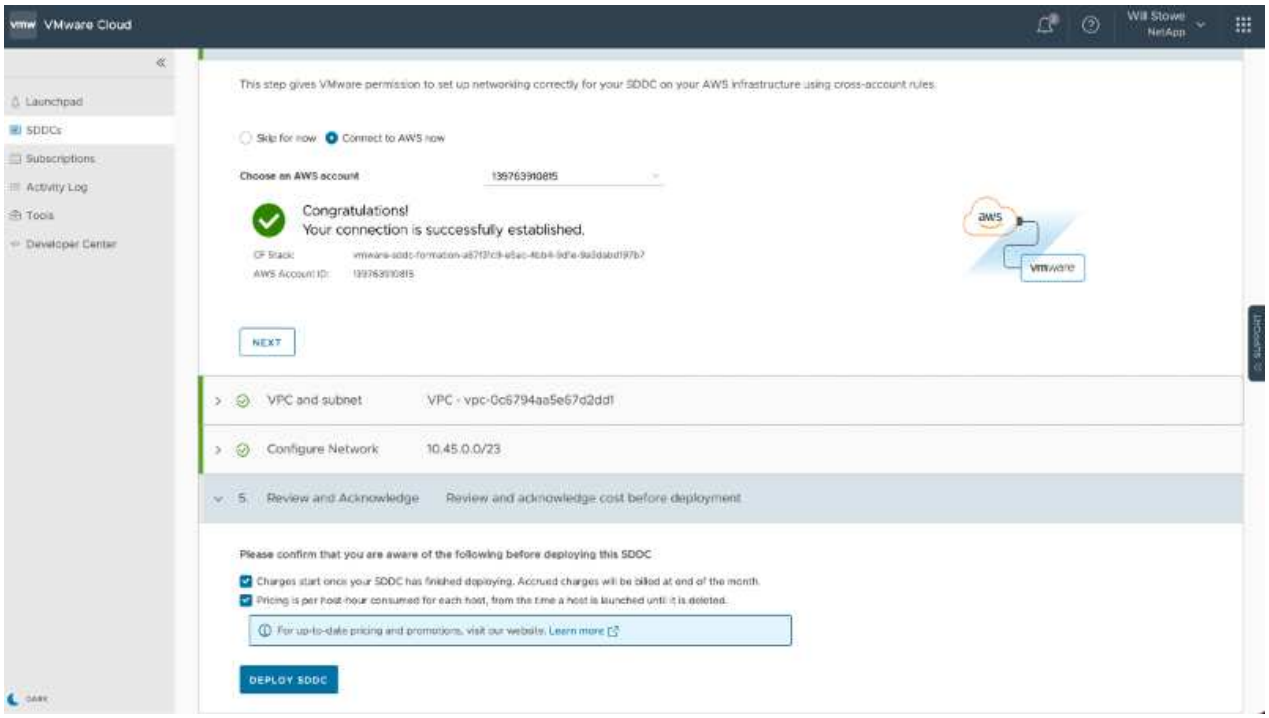
4. Seleccione la VPC de AWS deseada para conectar el entorno de VMC.



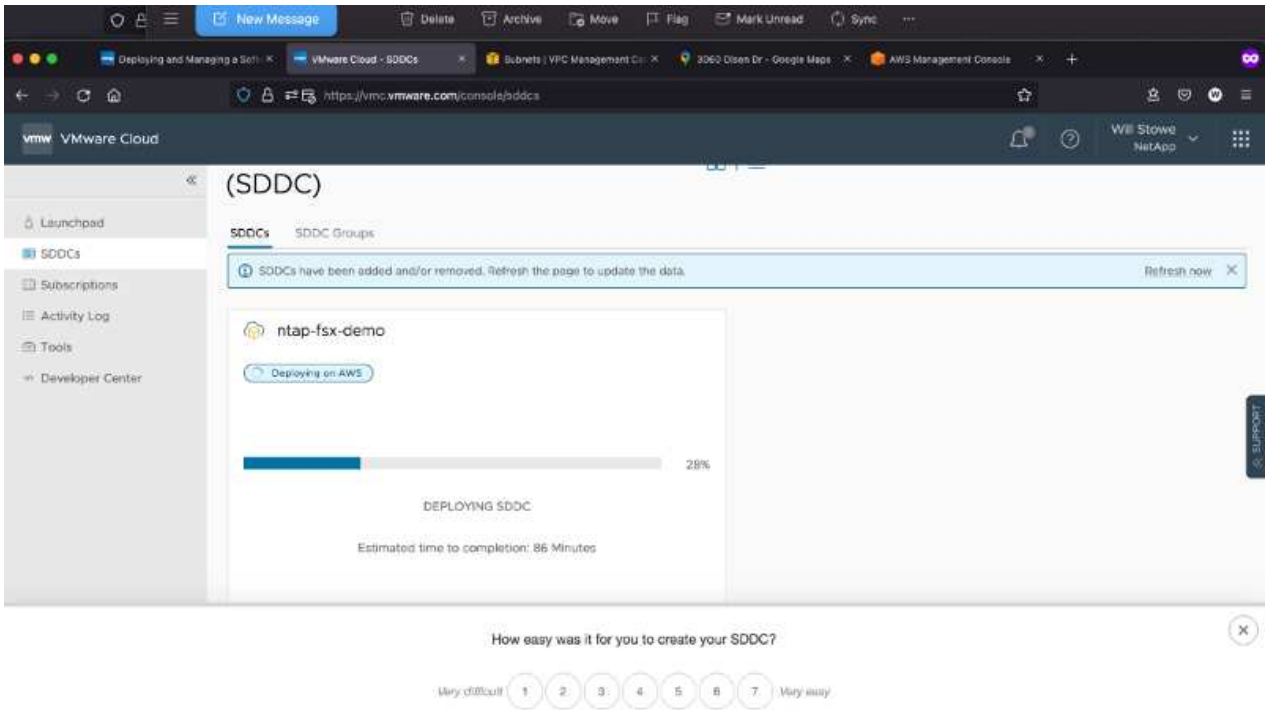
5. Configure la subred de administración de VMC; esta subred contiene servicios administrados por VMC, como vCenter, NSX, etc. No elija un espacio de direcciones superpuesto con otras redes que necesiten conectividad con el entorno SDDC. Por último, siga las recomendaciones para el tamaño de CIDR que se indican a continuación.



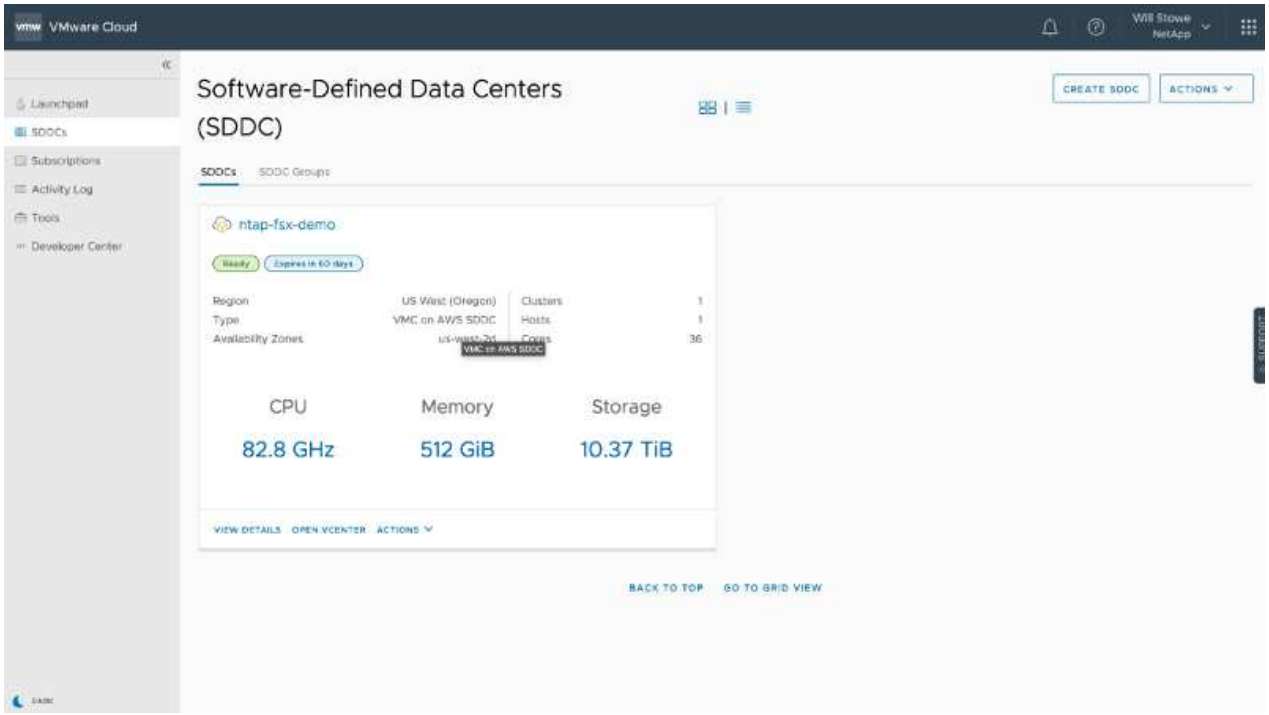
6. Revise y reconozca la configuración del SDDC y luego haga clic en implementar el SDDC.



El proceso de implementación normalmente demora aproximadamente dos horas para completarse.



7. Una vez finalizado, el SDDC estará listo para su uso.

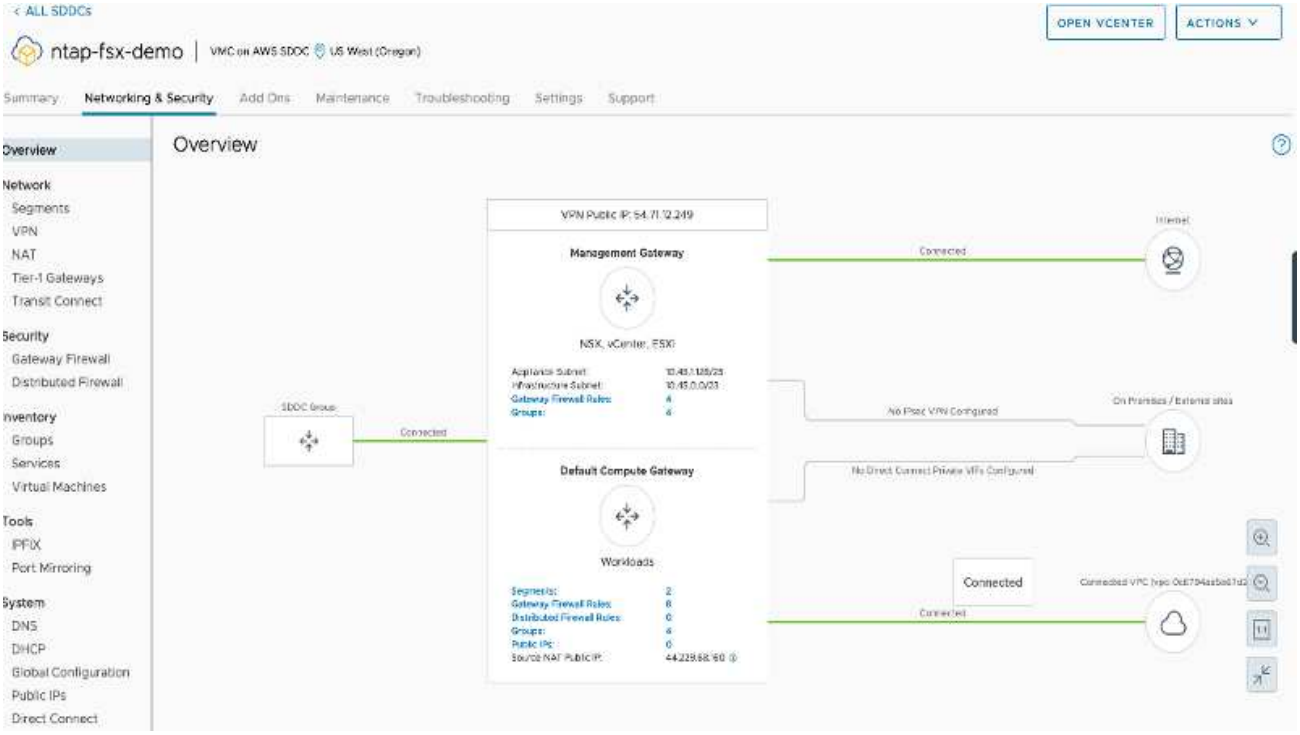


Para obtener una guía paso a paso sobre la implementación de SDDC, consulte"Implementar un SDDC desde la consola VMC" .

▼ **Conecte VMware Cloud a FSx ONTAP**

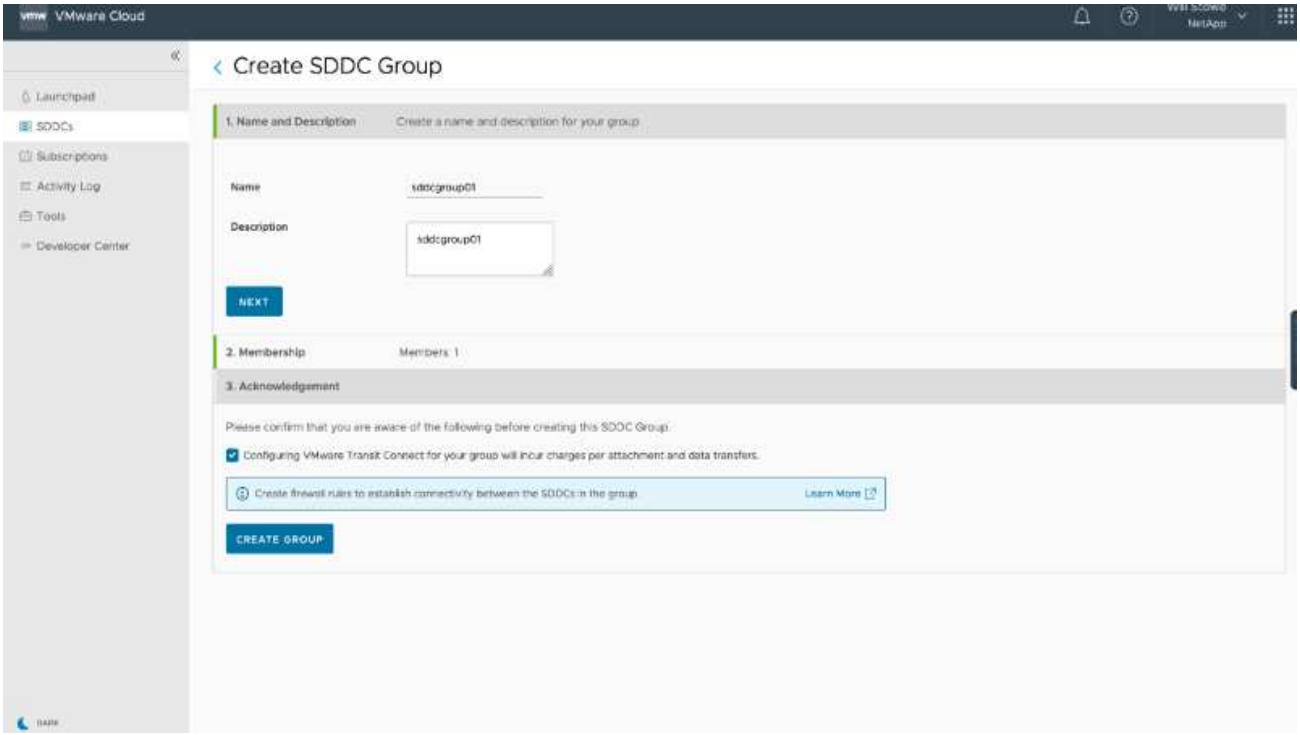
Para conectar VMware Cloud a FSx ONTAP, complete los siguientes pasos:

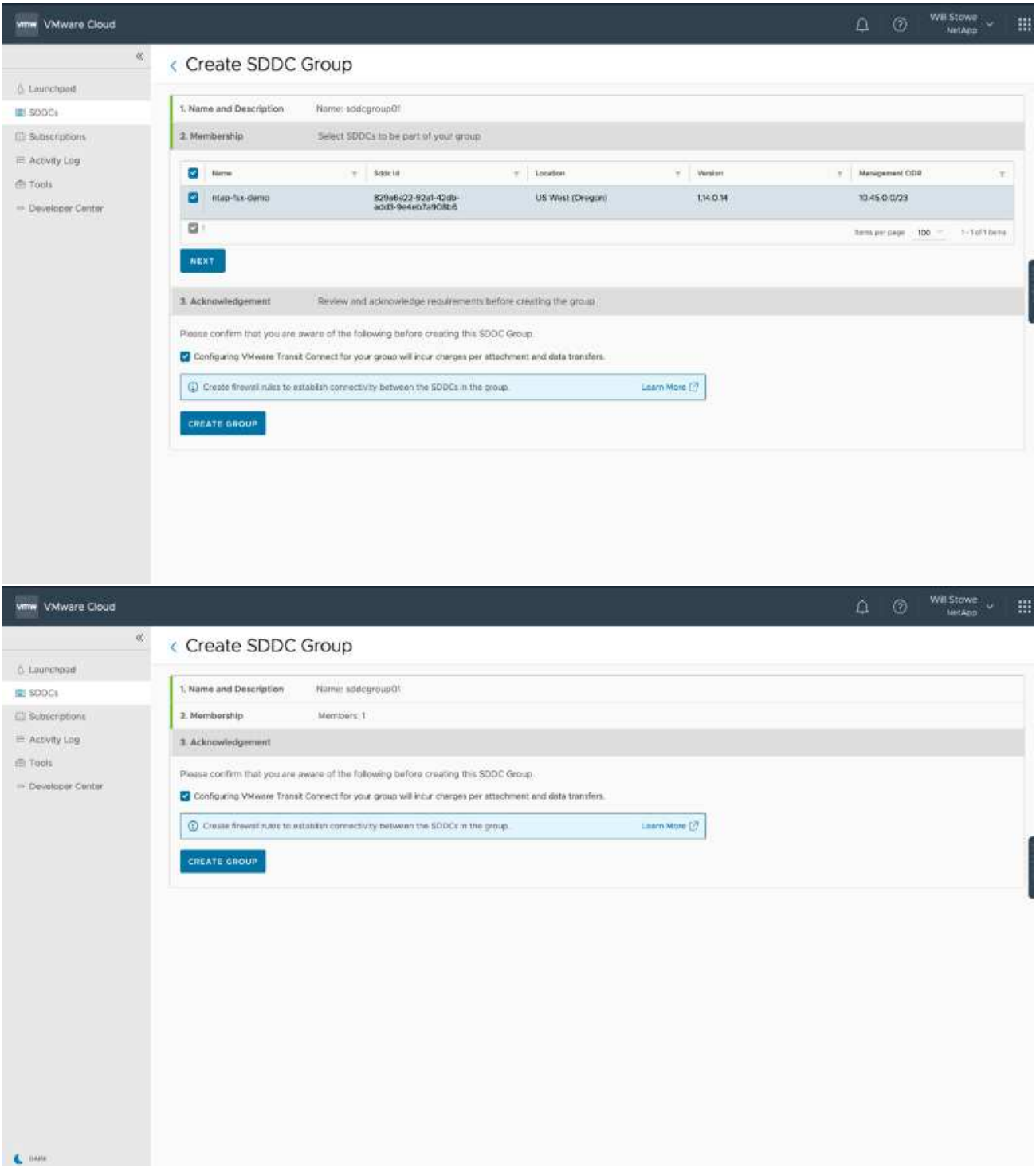
1. Una vez completada la implementación de VMware Cloud y conectada a AWS VPC, debe implementar Amazon FSx ONTAP en una nueva VPC en lugar de la VPC conectada original (consulte la captura de pantalla a continuación). No se puede acceder a FSx (IP flotantes NFS y SMB) si está implementado en la VPC conectada. Tenga en cuenta que los puntos finales ISCSI como Cloud Volumes ONTAP funcionan bien desde la VPC conectada.



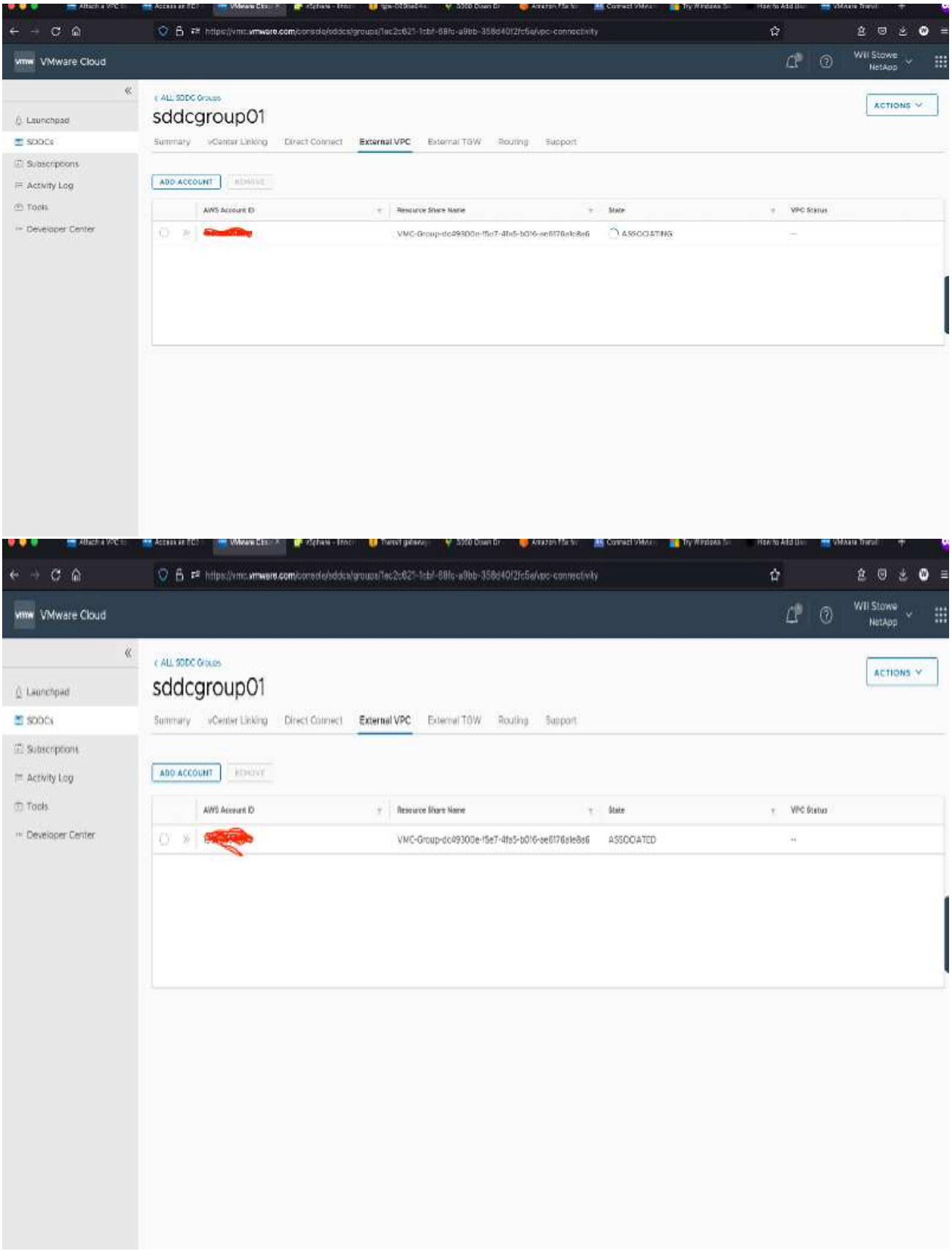
2. Implemente una VPC adicional en la misma región y luego implemente Amazon FSx ONTAP en la nueva VPC.

   La configuración de un grupo SDDC en la consola de VMware Cloud habilita las opciones de configuración de red necesarias para conectarse a la nueva VPC donde se implementa FSx. En el paso 3, verifique que la opción "Configurar VMware Transit Connect para su grupo generará cargos por cada archivo adjunto y transferencia de datos" esté marcada y luego elija Crear grupo. El proceso puede tardar unos minutos en completarse.

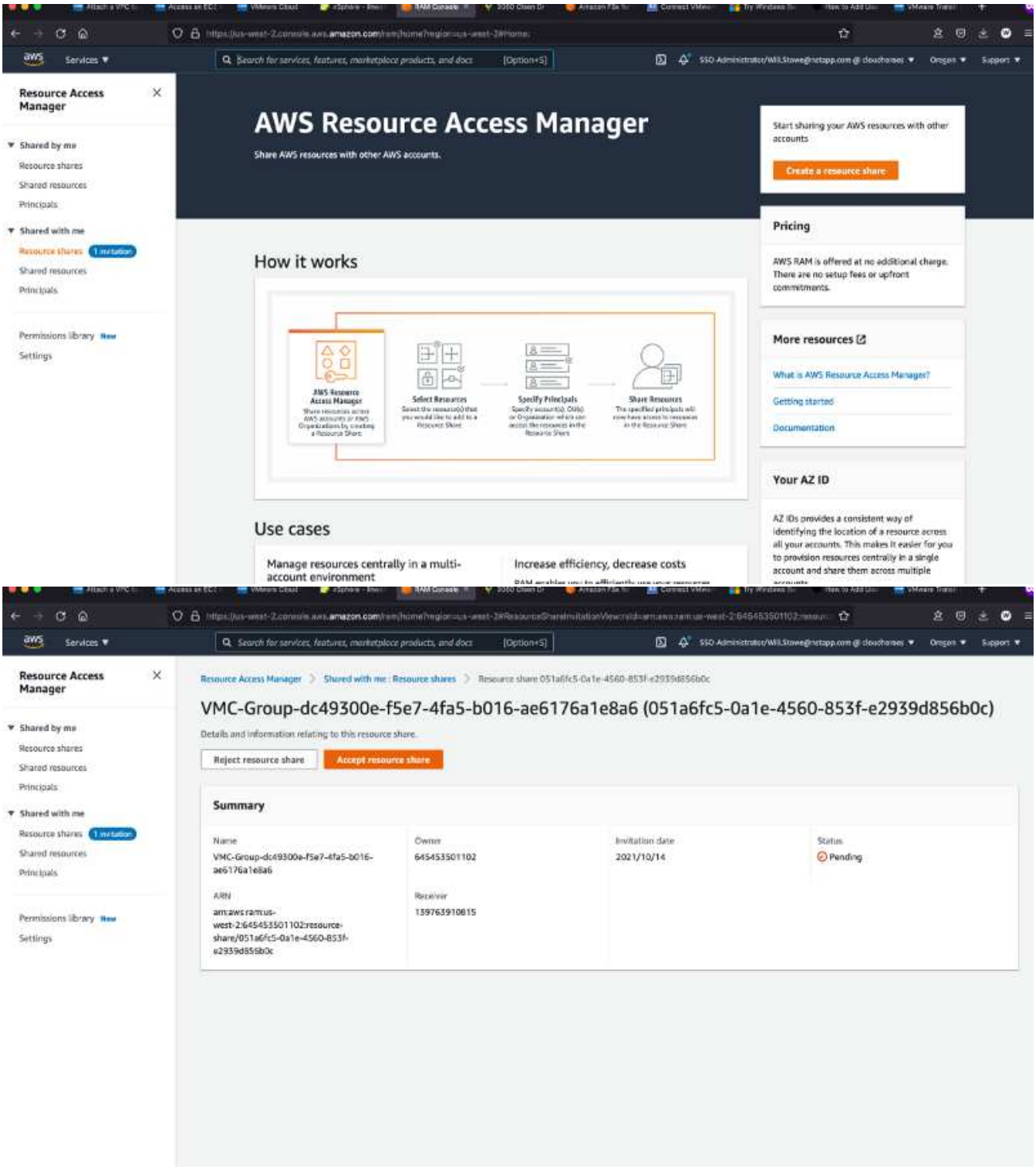




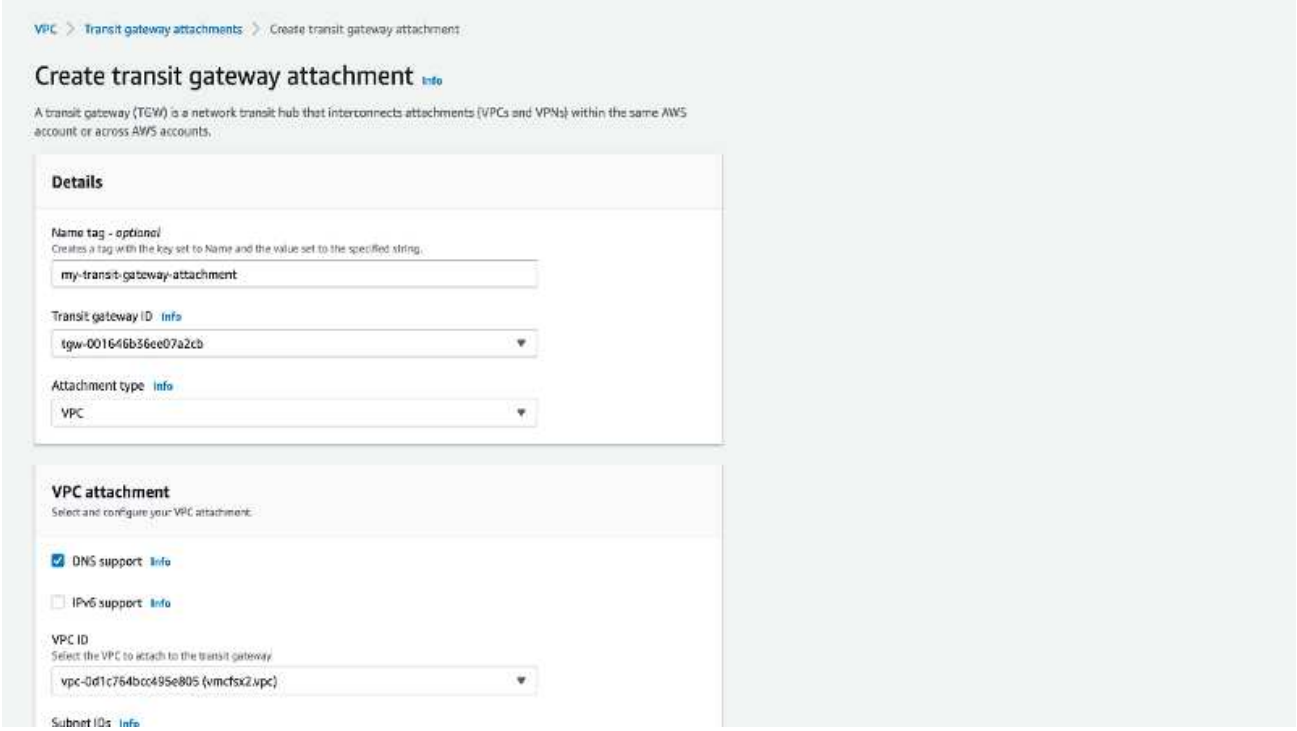
3. Adjunte la VPC recién creada al grupo SDDC recién creado. Seleccione la pestaña VPC externa y siga las instrucciones."Instrucciones para conectar una VPC externa" al grupo. Este proceso puede tardar entre 10 y 15 minutos en completarse.



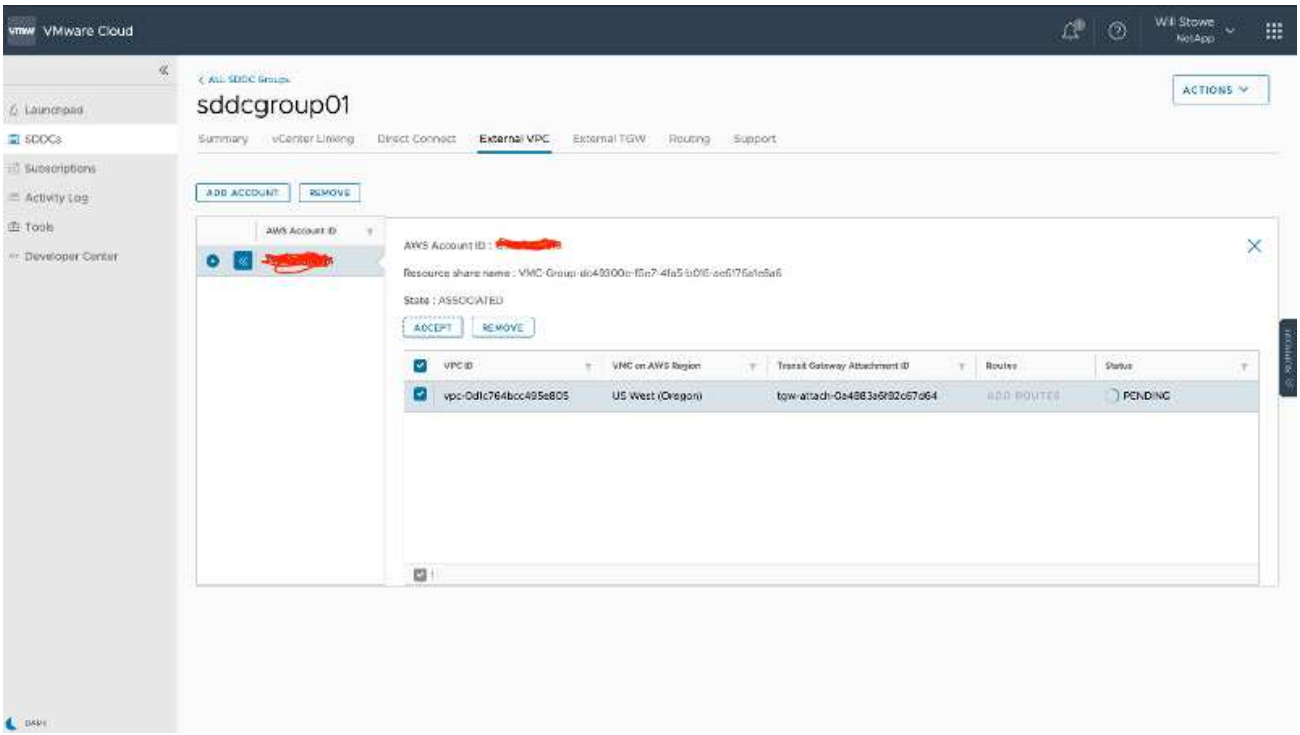
4. Como parte del proceso de VPC externo, se le solicita a través de la consola de AWS un nuevo recurso compartido mediante el Administrador de acceso a recursos. El recurso compartido es el"Puerta de enlace de tránsito de AWS" administrado por VMware Transit Connect.



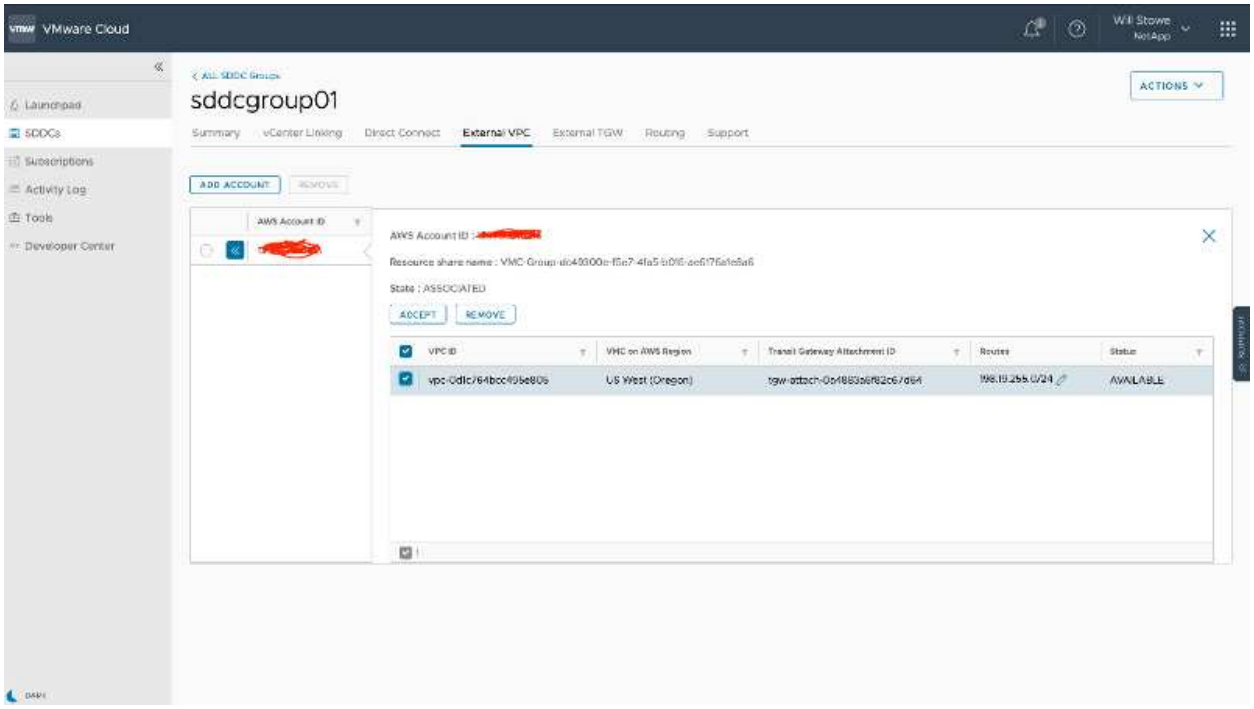
5. Cree el archivo adjunto de la puerta de enlace de tránsito.



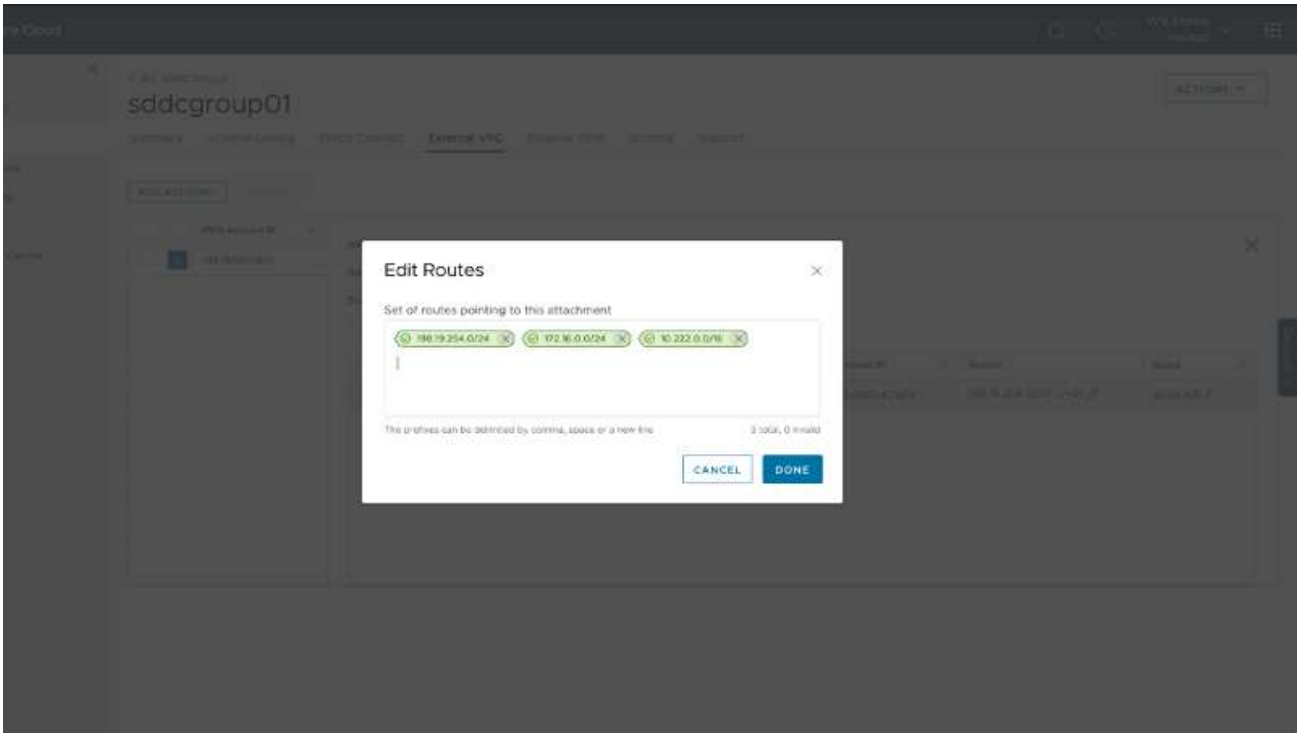
6. De regreso en la consola VMC, acepte la conexión de VPC. Este proceso puede tardar aproximadamente 10 minutos en completarse.



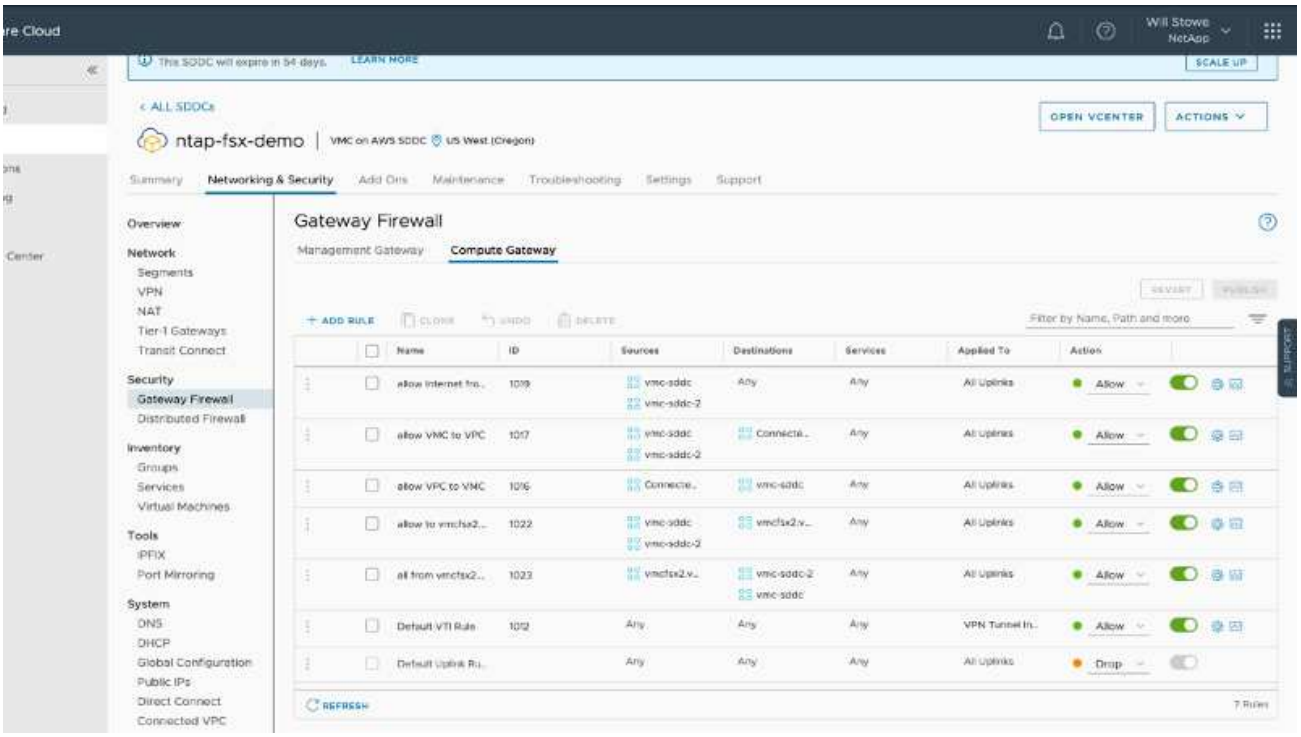
7. Mientras esté en la pestaña VPC externa, haga clic en el ícono de edición en la columna Rutas y agregue las siguientes rutas requeridas:
   - Una ruta para el rango de IP flotante para Amazon FSx ONTAP"IP flotantes" .
   - Una ruta para el rango de IP flotante para Cloud Volumes ONTAP (si corresponde).
   - Una ruta para el espacio de direcciones VPC externo recién creado.



8. Por último, permitir el tráfico bidireccional"reglas de firewall" para acceder a FSx/CVO. Sigue estos"pasos detallados" para reglas de firewall de puerta de enlace de cómputo para la conectividad de carga de trabajo de SDDC.



9. Una vez configurados los grupos de firewall para la puerta de enlace de administración y de cómputo, se puede acceder a vCenter de la siguiente manera:



El siguiente paso es verificar que Amazon FSx ONTAP o Cloud Volumes ONTAP esté configurado según sus requisitos y que los volúmenes estén aprovisionados para descargar componentes de almacenamiento de vSAN para optimizar la implementación.

Implementar y configurar el entorno de virtualización en Azure

Al igual que en las instalaciones locales, la planificación de Azure VMware Solution es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

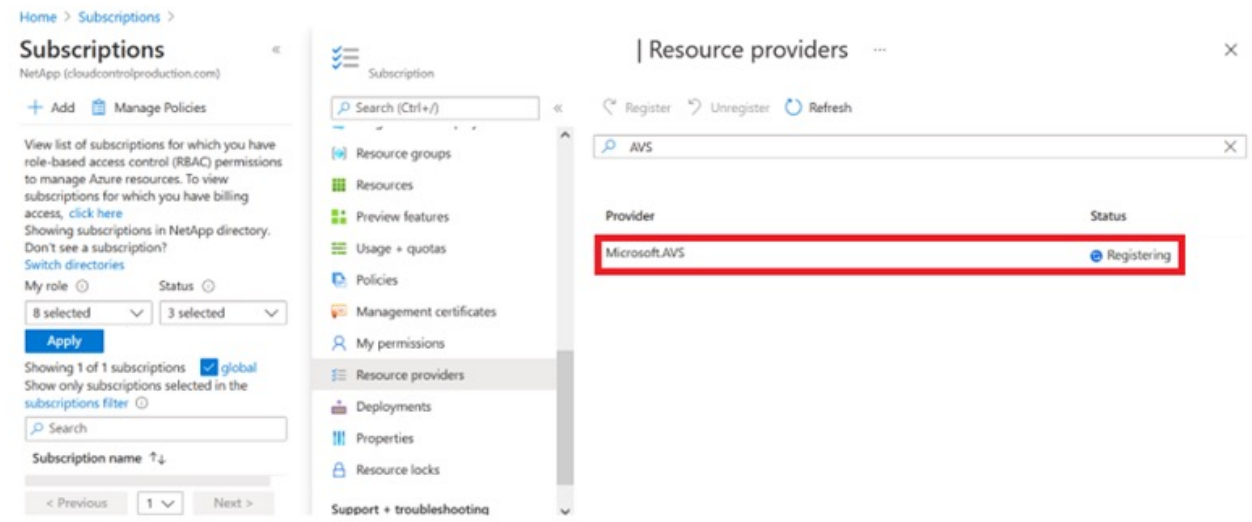
En esta sección se describe cómo configurar y administrar Azure VMware Solution y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

El proceso de configuración se puede dividir en los siguientes pasos:

▼ **Registrar el proveedor de recursos y crear una nube privada**

Para utilizar Azure VMware Solution, primero registre el proveedor de recursos dentro de la suscripción identificada:

1. Sign in en el portal de Azure.
2. En el menú del portal de Azure, seleccione Todos los servicios.
3. En el cuadro de diálogo Todos los servicios, ingrese la suscripción y luego seleccione Suscripciones.
4. Para ver, seleccione la suscripción de la lista de suscripciones.
5. Seleccione Proveedores de recursos e ingrese Microsoft.AVS en la búsqueda.
6. Si el proveedor de recursos no está registrado, seleccione Registrar.



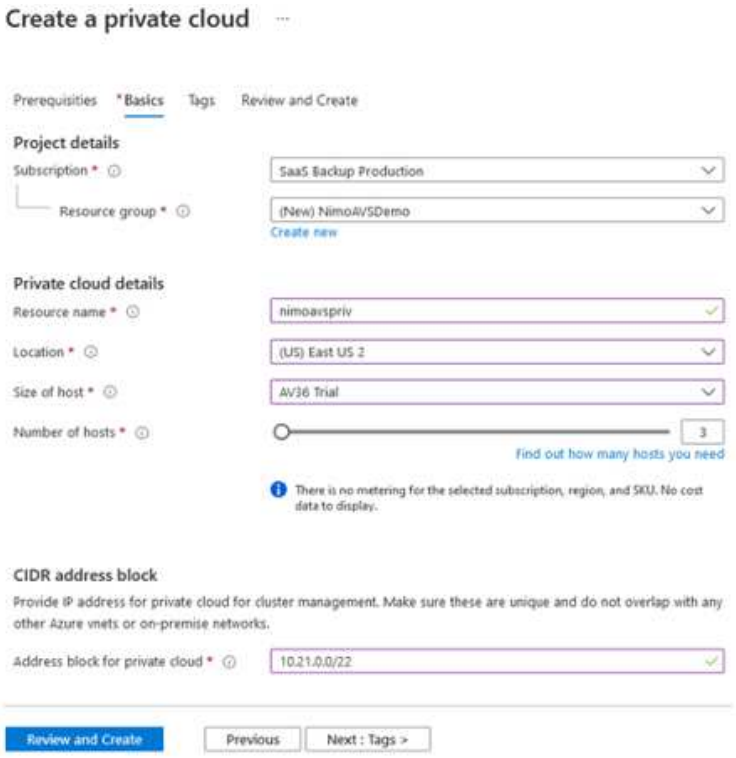


7. Una vez registrado el proveedor de recursos, cree una nube privada de Azure VMware Solution mediante el portal de Azure.
8. Sign in en el portal de Azure.
9. Seleccione Crear un nuevo recurso.
10. En el cuadro de texto Buscar en Marketplace, ingrese Azure VMware Solution y selecciónelo de los resultados.
11. En la página de Azure VMware Solution, seleccione Crear.

12. Desde la pestaña Básico, ingrese los valores en los campos y seleccione Revisar + Crear.

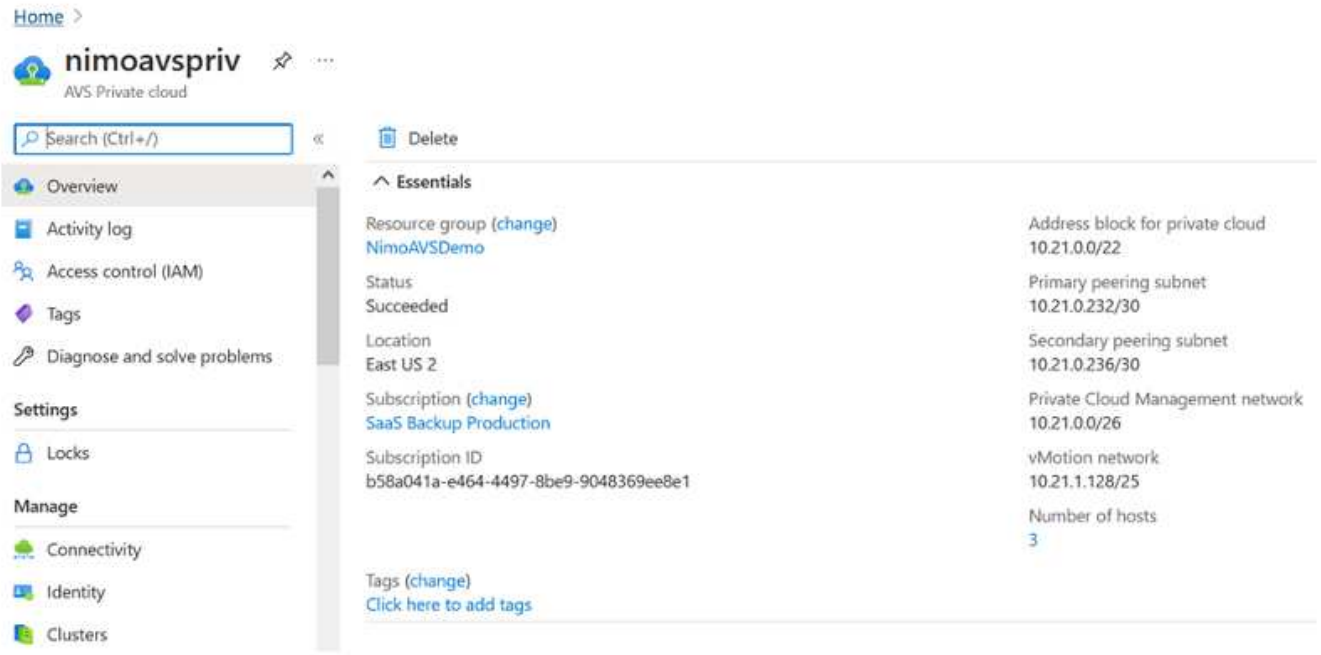
Notas:

- Para comenzar rápidamente, recopile la información necesaria durante la fase de planificación.
- Seleccione un grupo de recursos existente o cree un nuevo grupo de recursos para la nube privada. Un grupo de recursos es un contenedor lógico en el que se implementan y administran los recursos de Azure.
- Asegúrese de que la dirección CIDR sea única y no se superponga con otras redes virtuales de Azure o redes locales. El CIDR representa la red de administración de nube privada y se utiliza para los servicios de administración de clúster, como vCenter Server y NSX-T Manager. NetApp recomienda utilizar un espacio de dirección /22. En este ejemplo, se utiliza 10.21.0.0/22.



El proceso de aprovisionamiento tarda aproximadamente entre 4 y 5 horas. Una vez completado el proceso, verifique que la implementación se haya realizado correctamente accediendo a la nube privada desde el portal de Azure. Se muestra el estado “Exitoso” cuando se completa la implementación.

Una nube privada de Azure VMware Solution requiere una red virtual de Azure. Debido a que Azure VMware Solution no es compatible con vCenter local, se requieren pasos adicionales para integrarlo con un entorno local existente. También es necesario configurar un circuito ExpressRoute y una puerta de enlace de red virtual. Mientras espera que se complete el aprovisionamiento del clúster, cree una nueva red virtual o use una existente para conectarse a Azure VMware Solution.



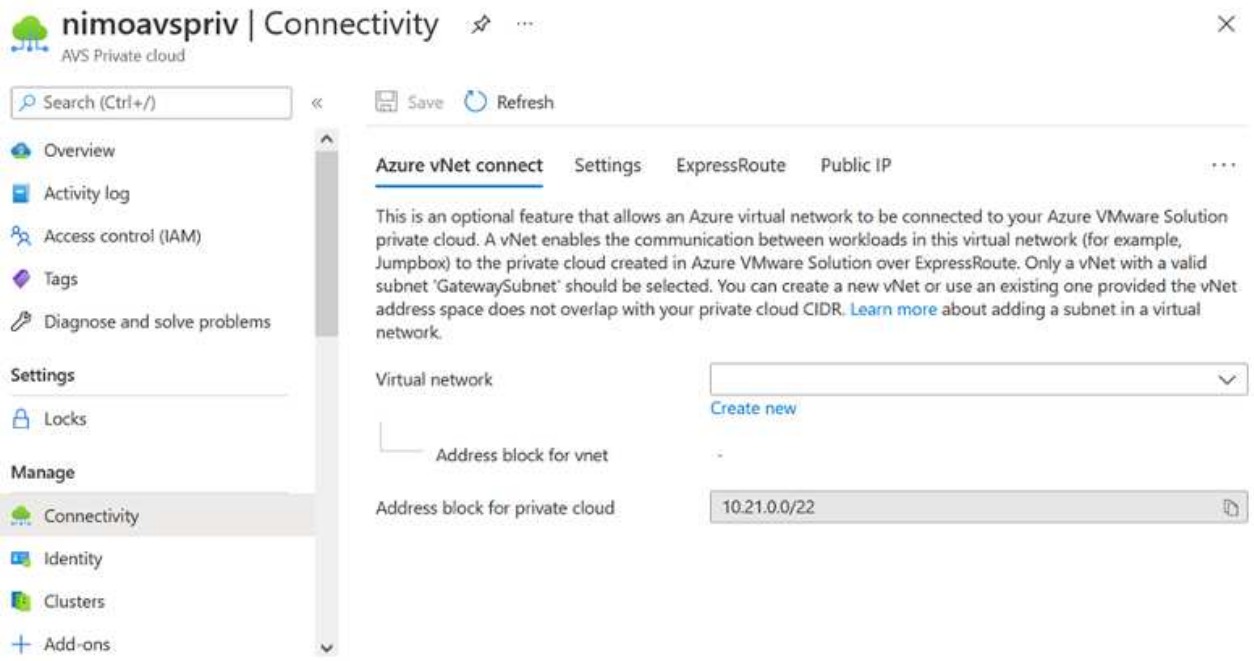
▼ **Conectarse a una puerta de enlace de red virtual ExpressRoute nueva o existente**

Para crear una nueva red virtual de Azure (VNet), seleccione la pestaña Conectar red virtual de Azure. Como alternativa, puede crear uno manualmente desde el portal de Azure utilizando el asistente Crear red virtual:

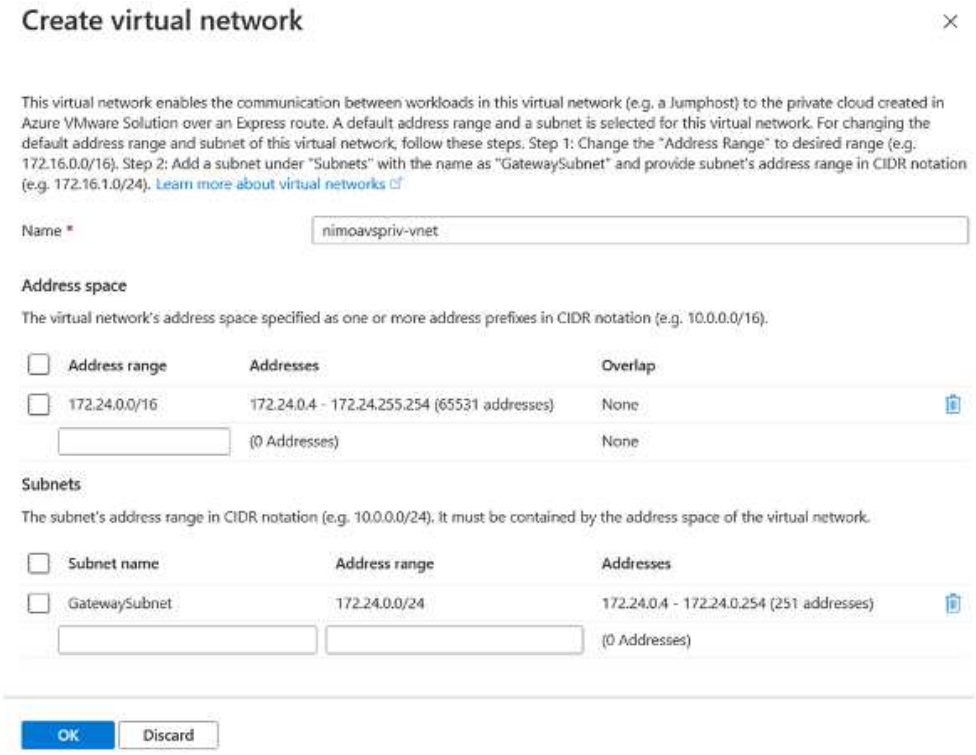
1. Vaya a la nube privada de Azure VMware Solution y acceda a Conectividad en la opción Administrar.
2. Seleccione Azure VNet Connect.
3. Para crear una nueva VNet, seleccione la opción Crear nuevo.

   Esta característica permite conectar una red virtual a la nube privada de Azure VMware Solution. La red virtual permite la comunicación entre cargas de trabajo en esta red virtual al crear automáticamente los componentes necesarios (por ejemplo, Jump Box, servicios compartidos como Azure NetApp Files y Cloud Volume ONTAP) en la nube privada creada en Azure VMware Solution sobre ExpressRoute.

   Nota: El espacio de direcciones de VNet no debe superponerse con el CIDR de la nube privada.



4. Proporcione o actualice la información para la nueva VNet y seleccione Aceptar.



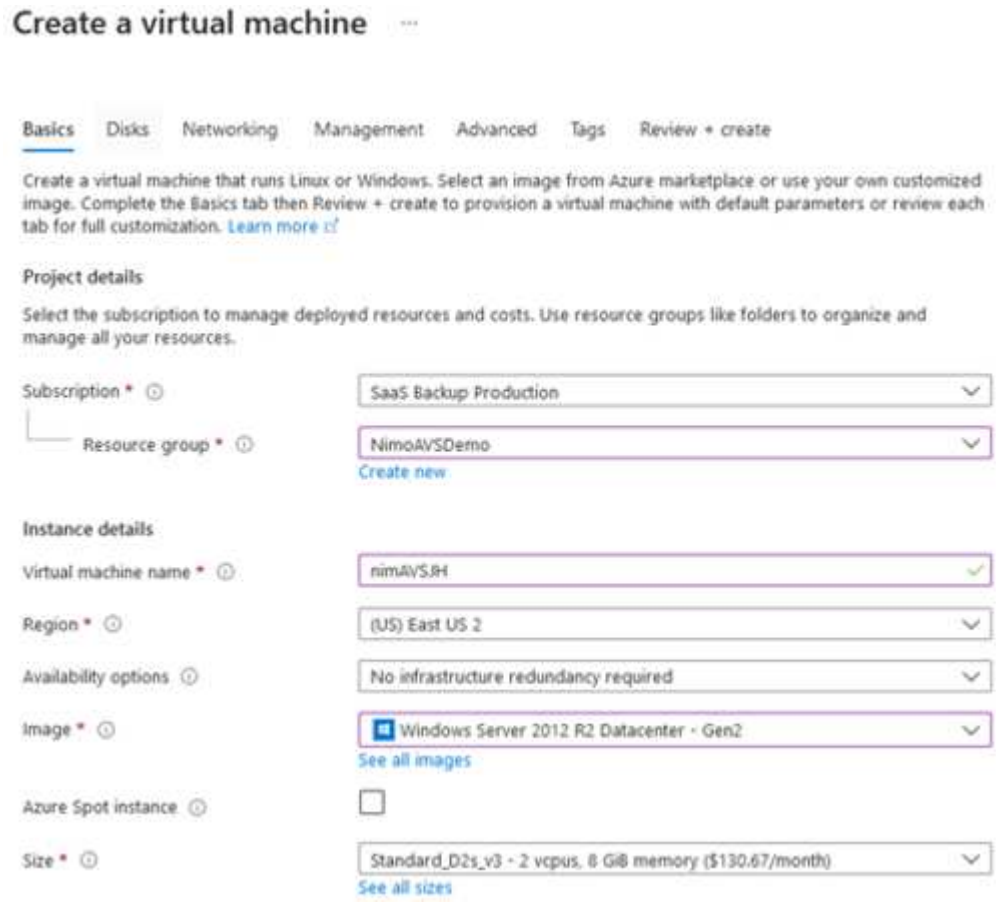
La red virtual con el rango de direcciones proporcionado y la subred de puerta de enlace se crea en la suscripción y el grupo de recursos designados.

Si crea una red virtual manualmente, cree una puerta de enlace de red virtual con el SKU adecuado y ExpressRoute como tipo de puerta de enlace. Una vez completada la implementación, conecte la conexión ExpressRoute a la puerta de enlace de red virtual que contiene la nube privada de Azure VMware Solution usando la clave de autorización. Para

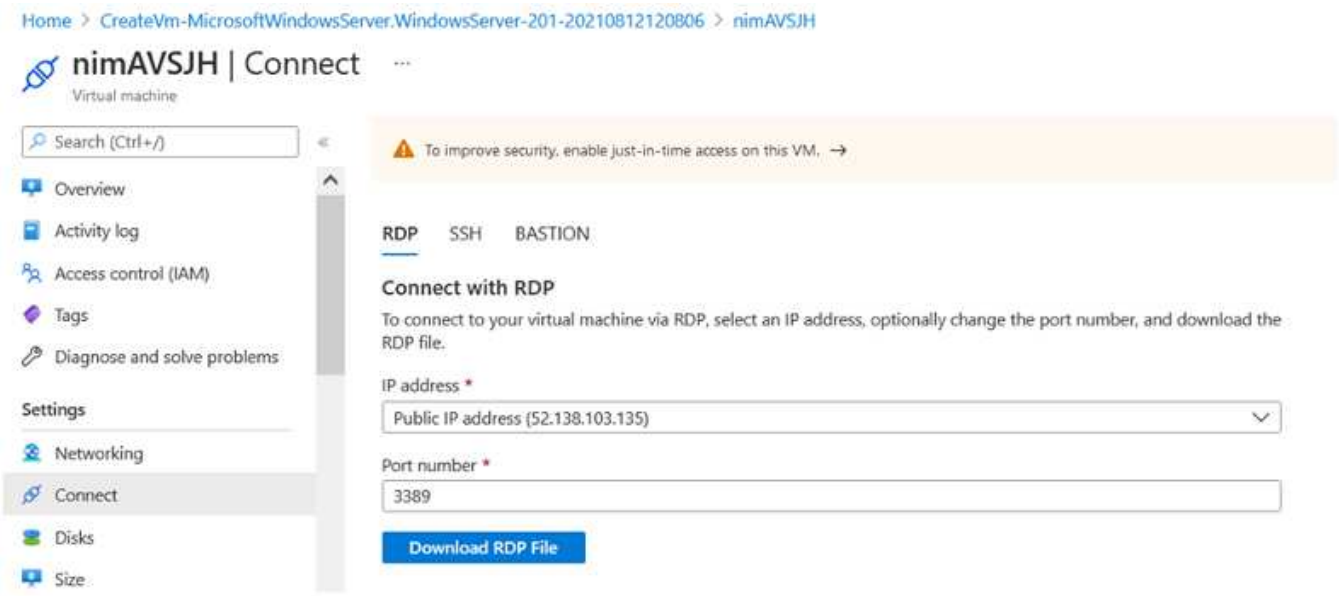
obtener más información, consulte "Configurar la red para su nube privada de VMware en Azure" .

▼ **Validar la conexión de red y el acceso a la nube privada de Azure VMware Solution**

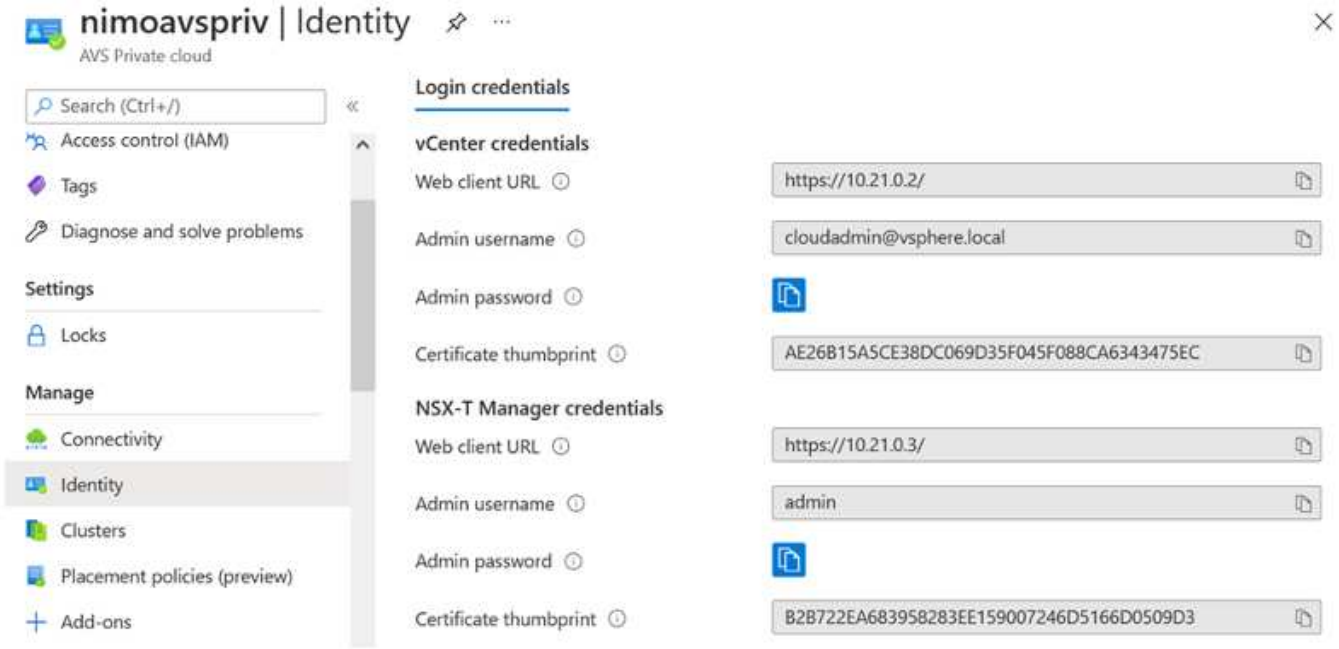
Azure VMware Solution no le permite administrar una nube privada con VMware vCenter local. En su lugar, se requiere un host de salto para conectarse a la instancia de vCenter de Azure VMware Solution. Cree un host de salto en el grupo de recursos designado e inicie sesión en Azure VMware Solution vCenter. Este host de salto debe ser una máquina virtual de Windows en la misma red virtual que se creó para la conectividad y debe proporcionar acceso tanto a vCenter como a NSX Manager.



Una vez aprovisionada la máquina virtual, utilice la opción Conectar para acceder a RDP.



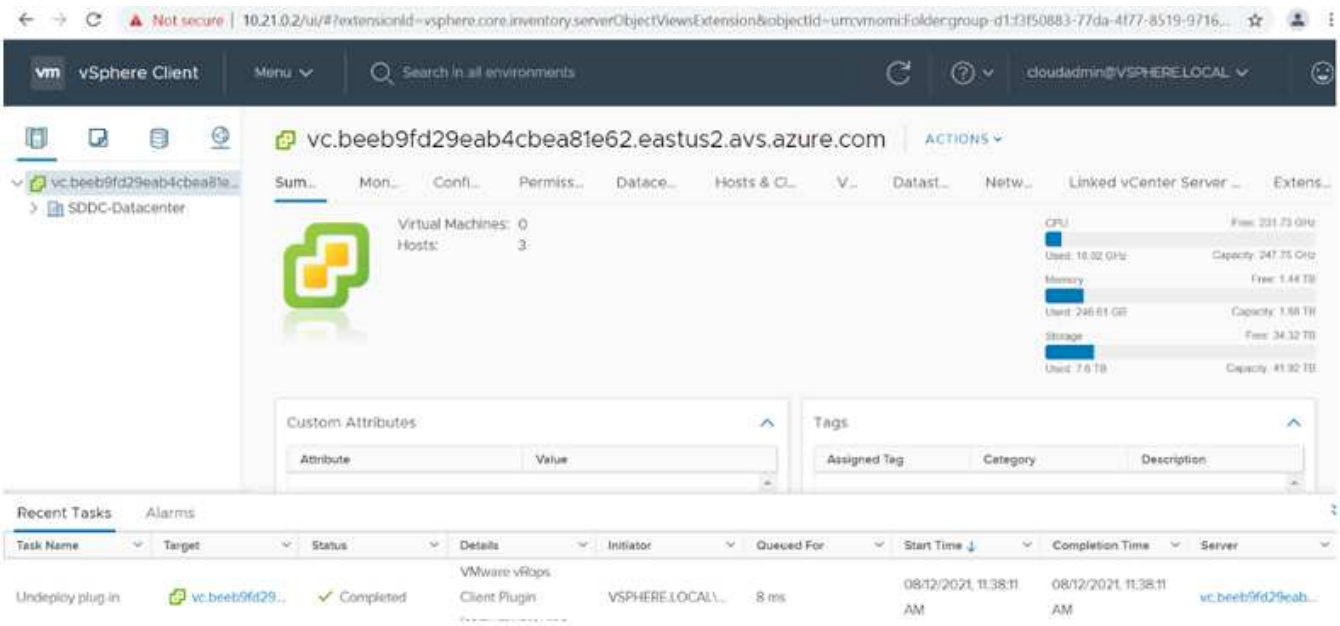
Sign in en vCenter desde esta máquina virtual de host de salto recién creada utilizando el usuario administrador de la nube. Para acceder a las credenciales, vaya al portal de Azure y navegue a Identidad (en la opción Administrar dentro de la nube privada). Las URL y las credenciales de usuario para la nube privada vCenter y NSX-T Manager se pueden copiar desde aquí.



En la máquina virtual de Windows, abra un navegador y navegue hasta la URL del cliente web de vCenter(`"https://10.21.0.2/"`) y use el nombre de usuario administrador como **cloudadmin@vsphere.local** y pegue la contraseña copiada. De manera similar, también se puede acceder al administrador de NSX-T mediante la URL del cliente web(`"https://10.21.0.3/"`) y use el nombre de usuario administrador y pegue la contraseña copiada para crear nuevos segmentos o modificar las puertas de enlace de niveles existentes.

Las URL del cliente web son diferentes para cada SDDC aprovisionado.





El SDDC de Azure VMware Solution ya está implementado y configurado. Aproveche ExpressRoute Global Reach para conectar el entorno local a la nube privada de Azure VMware Solution. Para obtener más información, consulte "Vincular entornos locales a Azure VMware Solution" .

Implementar y configurar el entorno de virtualización en Google Cloud Platform (GCP)

Al igual que en las instalaciones locales, la planificación de Google Cloud VMware Engine (GCVE) es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

Esta sección describe cómo configurar y administrar GCVE y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

El proceso de configuración se puede dividir en los siguientes pasos:

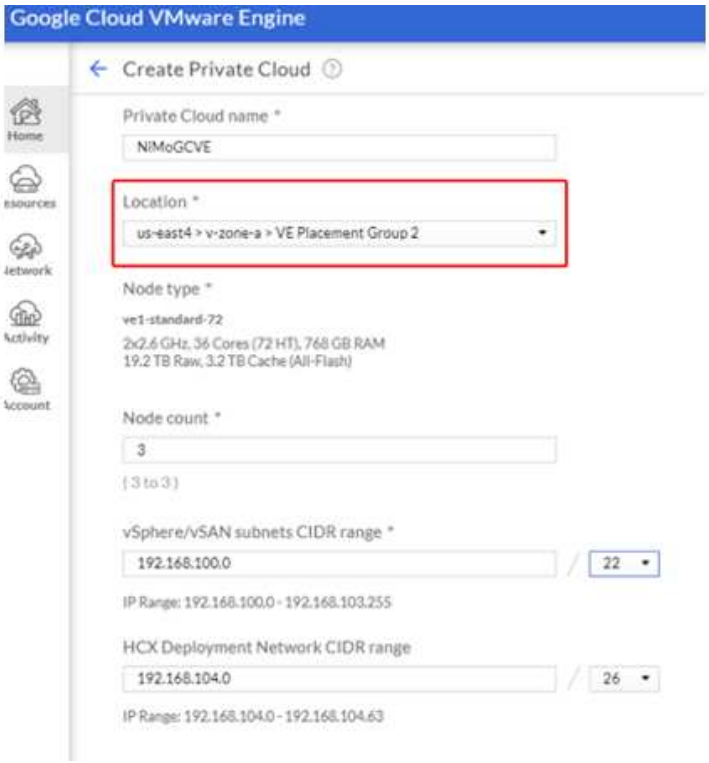
▼ Implementar y configurar GCVE

Para configurar un entorno GCVE en GCP, inicie sesión en la consola de GCP y acceda al portal de VMware Engine.

Haga clic en el botón “Nueva nube privada” e ingrese la configuración deseada para la nube privada GCVE. En "Ubicación", asegúrese de implementar la nube privada en la misma región/zona donde se implementa NetApp Volumes/CVO, para garantizar el mejor rendimiento y la menor latencia.

Prerrequisitos:

- Configurar la función de administrador de IAM del servicio VMware Engine
- "Habilitar el acceso a la API de VMWare Engine y la cuota de nodo"
- Asegúrese de que el rango CIDR no se superponga con ninguna de sus subredes locales o en la nube. El rango CIDR debe ser /27 o superior.



Nota: La creación de una nube privada puede tardar entre 30 minutos y 2 horas.

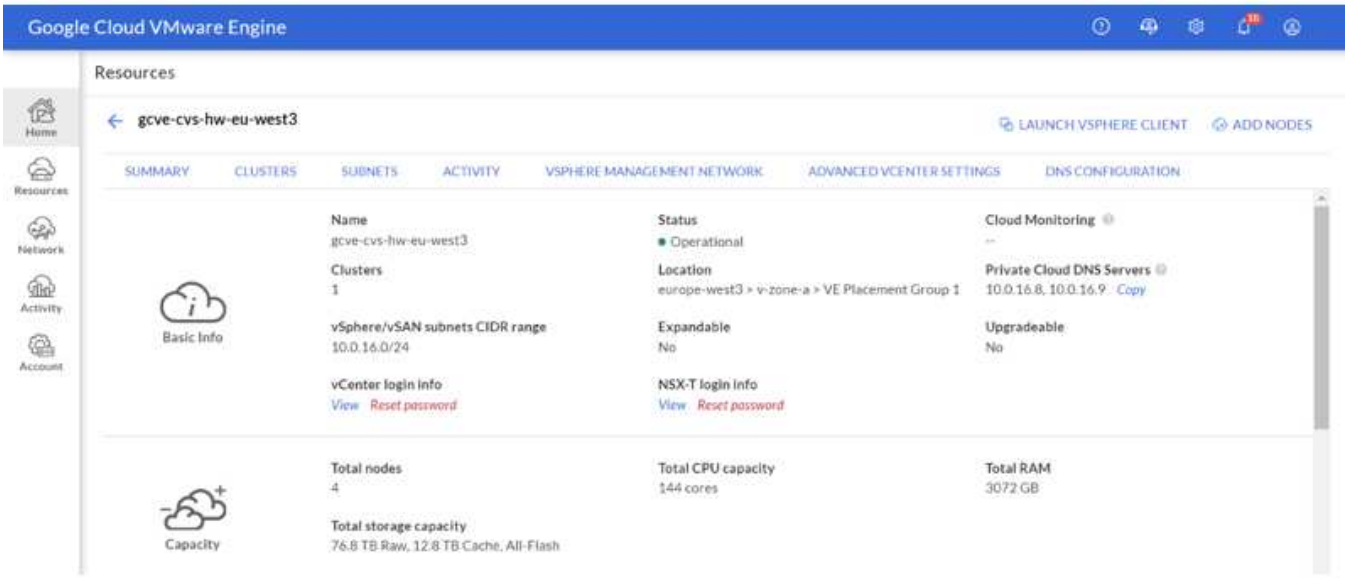
▼ Habilitar el acceso privado a GCVE

Una vez aprovisionada la nube privada, configure el acceso privado a la nube privada para una conexión de ruta de datos de alto rendimiento y baja latencia.

Esto garantizará que la red VPC donde se ejecutan las instancias de Cloud Volumes ONTAP pueda comunicarse con la nube privada de GCVE. Para ello, sigue "Documentación de GCP". Para Cloud Volume Service, establece una conexión entre VMware Engine y Google Cloud NetApp Volumes realizando un emparejamiento único entre los proyectos host del tenant. Para ver los pasos detallados, sigue "enlace".

Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

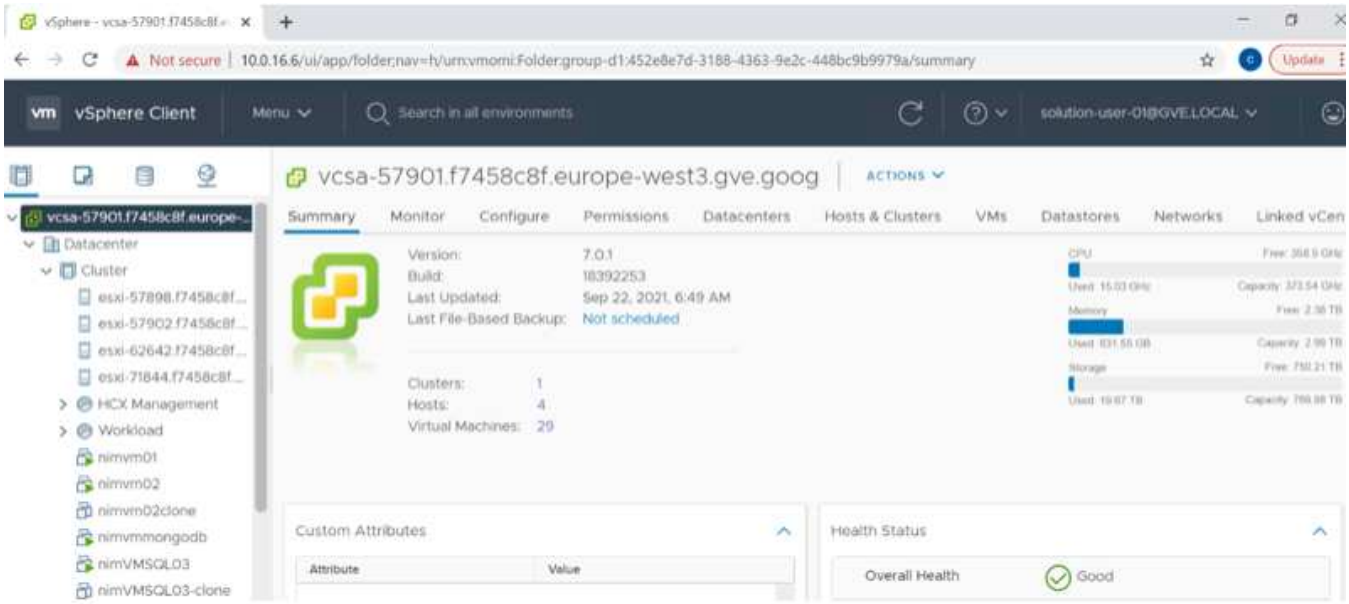
Sign in en vCenter con el usuario CloudOwner@gve.local. Para acceder a las credenciales, vaya al portal de VMware Engine, vaya a Recursos y seleccione la nube privada adecuada. En la sección Información básica, haga clic en el enlace Ver para obtener la información de inicio de sesión de vCenter (vCenter Server, HCX Manager) o la información de inicio de sesión de NSX-T (NSX Manager).



En una máquina virtual de Windows, abra un navegador y navegue hasta la URL del cliente web de vCenter(`"https://10.0.16.6/"`) y use el nombre de usuario administrador como CloudOwner@gve.local y pegue la contraseña copiada. De manera similar, también se puede acceder al administrador de NSX-T mediante la URL del cliente web(`"https://10.0.16.11/"`) y use el nombre de usuario administrador y pegue la contraseña copiada para crear nuevos segmentos o modificar las puertas de enlace de niveles existentes.

Para conectarse desde una red local a la nube privada de VMware Engine, aproveche la VPN en la nube o Cloud Interconnect para obtener una conectividad adecuada y asegúrese de que los puertos necesarios estén abiertos. Para conocer los pasos detallados, siga este"enlace" .





▼ **Implementar el almacén de datos complementario de Google Cloud NetApp Volumes en GCVE**

Referirse"Procedimiento para implementar un almacén de datos NFS complementario con volúmenes NetApp en GCVE"

Almacenamiento de NetApp en nubes públicas

Opciones de almacenamiento de NetApp para proveedores de nube pública

Explore las opciones para NetApp como almacenamiento en los tres hiperescaladores principales.

AWS/VMC

AWS admite el almacenamiento de NetApp en las siguientes configuraciones:

- FSx ONTAP como almacenamiento conectado para invitados
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- FSx ONTAP como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para VMC" . Ver el detalle"Opciones de almacén de datos NFS complementario para VMC" .

Azure/AVS

Azure admite el almacenamiento de NetApp en las siguientes configuraciones:

- Azure NetApp Files (ANF) como almacenamiento conectado invitado
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- Azure NetApp Files (ANF) como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para AVS" . Ver el detalle"Opciones de almacén de datos NFS complementarias para AVS" .

GCP / GCVE

Google Cloud admite el almacenamiento de NetApp en las siguientes configuraciones:

- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- Google Cloud NetApp Volumes (NetApp Volumes) como almacenamiento conectado para invitados
- Google Cloud NetApp Volumes (NetApp Volumes) como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para GCVE" . Ver el detalle"Opciones de almacén de datos NFS suplementarias para GCVE" .

Leer más sobre"Compatibilidad del almacén de datos de Google Cloud NetApp Volumes con Google Cloud VMware Engine (blog de NetApp)" o"Cómo usar Google Cloud NetApp Volumes como almacenes de datos para Google Cloud VMware Engine (blog de Google)"

Amazon Web Services: Opciones para utilizar el almacenamiento de NetApp

El almacenamiento de NetApp se puede conectar a Amazon Web Services como almacenamiento complementario o conectado por invitado.

Amazon FSx for NetApp ONTAP (FSx ONTAP) como almacén de datos NFS complementario

Amazon FSx ONTAP ofrece excelentes opciones para implementar y administrar cargas de trabajo de aplicaciones junto con servicios de archivos, al tiempo que reduce el TCO al hacer que los requisitos de datos se integren perfectamente en la capa de aplicación. Cualquiera que sea el caso de uso, elija VMware Cloud on AWS junto con Amazon FSx ONTAP para obtener rápidamente los beneficios de la nube, una infraestructura consistente y operaciones desde las instalaciones locales hasta AWS, portabilidad bidireccional de cargas de trabajo y capacidad y rendimiento de nivel empresarial. Es el mismo proceso y procedimientos familiares utilizados para conectar el almacenamiento.

Para obtener más información, visite:

- "FSx ONTAP como almacén de datos NFS complementario: descripción general"
- "Amazon FSx para ONTAP como almacén de datos complementario"

Amazon FSx for NetApp ONTAP como almacenamiento conectado para invitados

Amazon FSx ONTAP es un servicio completamente administrado que proporciona almacenamiento de archivos altamente confiable, escalable, de alto rendimiento y rico en funciones, creado sobre el popular sistema de archivos ONTAP de NetApp. FSx ONTAP combina las características, el rendimiento, las capacidades y las operaciones API familiares de los sistemas de archivos NetApp con la agilidad, la escalabilidad y la simplicidad de un servicio de AWS completamente administrado.

FSx ONTAP ofrece almacenamiento de archivos compartido rápido, flexible y repleto de funciones, al que se puede acceder ampliamente desde instancias de cómputo de Linux, Windows y macOS que se ejecutan en AWS o en las instalaciones. FSx ONTAP ofrece almacenamiento en unidad de estado sólido (SSD) de alto rendimiento con latencias de submilisegundos. Con FSx ONTAP, puede lograr niveles de rendimiento SSD para su carga de trabajo mientras paga por almacenamiento SSD solo para una pequeña fracción de sus datos.

Administrar sus datos con FSx ONTAP es más fácil porque puede tomar instantáneas, clonar y replicar sus archivos con solo hacer clic en un botón. Además, FSx ONTAP organiza automáticamente sus datos en un almacenamiento elástico de menor costo, lo que reduce la necesidad de aprovisionar o administrar capacidad.

FSx ONTAP también proporciona almacenamiento duradero y de alta disponibilidad con copias de seguridad totalmente administradas y soporte para recuperación ante desastres entre regiones. Para facilitar la protección y seguridad de sus datos, FSx ONTAP admite aplicaciones antivirus y de seguridad de datos populares.

Para obtener más información, visite"FSx ONTAP como almacenamiento conectado para invitados"

Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados

Cloud Volumes ONTAP, o CVO, es la solución de gestión de datos en la nube líder en la industria basada en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Es una versión definida por software de ONTAP que consume almacenamiento nativo de la nube, lo que le permite tener el mismo software de almacenamiento en la nube y en las instalaciones, lo que reduce la necesidad de volver a capacitar a su personal de TI en métodos completamente nuevos para administrar sus datos.

CVO brinda a los clientes la capacidad de mover datos sin problemas desde el borde al centro de datos, a la nube y viceversa, unificando su nube híbrida, todo administrado con una consola de administración de panel único, NetApp Cloud Manager.

Por diseño, CVO ofrece un rendimiento extremo y capacidades avanzadas de gestión de datos para satisfacer incluso sus aplicaciones más exigentes en la nube.

Para obtener más información, visite"CVO como almacenamiento conectado para invitados" .

TR-4938: Montar Amazon FSx ONTAP como un almacén de datos NFS con VMware Cloud on AWS

Este documento describe cómo montar Amazon FSx ONTAP como un almacén de datos NFS con VMware Cloud en AWS.

Introducción

Toda organización exitosa está en un camino de transformación y modernización. Como parte de este proceso, las empresas generalmente utilizan sus inversiones existentes en VMware para aprovechar los beneficios de la nube y explorar cómo migrar, ampliar, extender y brindar recuperación ante desastres para los procesos de la manera más fluida posible. Los clientes que migran a la nube deben evaluar los casos de uso en términos de elasticidad y explosión, salida del centro de datos, consolidación del centro de datos, escenarios de fin de vida útil, fusiones, adquisiciones, etc.

Si bien VMware Cloud on AWS es la opción preferida por la mayoría de los clientes debido a que ofrece capacidades híbridas únicas, las opciones de almacenamiento nativo limitadas han restringido su utilidad para las organizaciones con cargas de trabajo con gran capacidad de almacenamiento. Debido a que el almacenamiento está directamente vinculado a los hosts, la única forma de escalar el almacenamiento es agregar más hosts, lo que puede aumentar los costos en un 35-40% o más para cargas de trabajo intensivas en almacenamiento. Estas cargas de trabajo necesitan almacenamiento adicional y rendimiento segregado, no potencia adicional, pero eso significa pagar por hosts adicionales. Aquí es donde el "integración reciente" FSx ONTAP resulta útil para cargas de trabajo intensivas en almacenamiento y rendimiento con VMware Cloud en AWS.

Consideremos el siguiente escenario: un cliente requiere ocho hosts en términos de potencia (vCPU/vMem), pero también tiene un requisito sustancial de almacenamiento. Según su evaluación, necesitan 16 hosts para cumplir con los requisitos de almacenamiento. Esto aumenta el TCO general porque deben comprar toda esa potencia adicional cuando lo que realmente necesitan es más almacenamiento. Esto es aplicable a cualquier

caso de uso, incluida migración, recuperación ante desastres, ráfagas, desarrollo/prueba, etc.

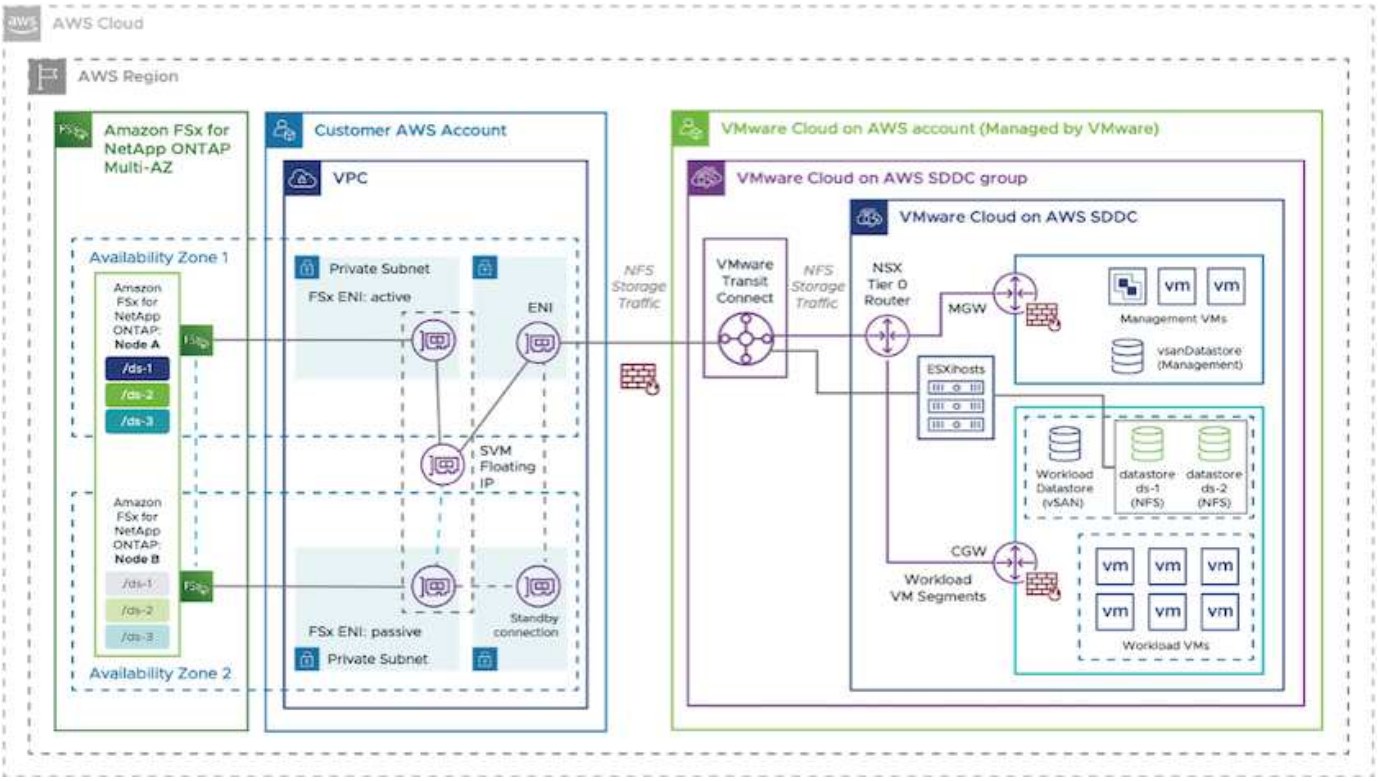
Este documento lo guía a través de los pasos necesarios para aprovisionar y adjuntar FSx ONTAP como un almacén de datos NFS para VMware Cloud on AWS.

Esta solución también está disponible en VMware. Por favor visite el"Documentación de VMware Cloud en AWS" Para más información.

Opciones de conectividad

VMware Cloud on AWS admite implementaciones de FSx ONTAP tanto en una sola zona de disponibilidad como en varias zonas de disponibilidad.

Esta sección describe la arquitectura de conectividad de alto nivel junto con los pasos necesarios para implementar la solución para expandir el almacenamiento en un clúster SDDC sin la necesidad de agregar hosts adicionales.



Los pasos de implementación de alto nivel son los siguientes:

1. Cree Amazon FSx ONTAP en una nueva VPC designada.
2. Crear un grupo SDDC.
3. Cree VMware Transit Connect y un archivo adjunto TGW.
4. Configurar el enrutamiento (AWS VPC y SDDC) y los grupos de seguridad.
5. Adjunte un volumen NFS como almacén de datos al clúster SDDC.

Antes de aprovisionar y conectar FSx ONTAP como un almacén de datos NFS, primero debe configurar un entorno SDDC de VMware on Cloud o actualizar un SDDC existente a v1.20 o superior. Para obtener más información, consulte "Introducción a VMware Cloud en AWS" .

Actualmente, FSx ONTAP no es compatible con clústeres extendidos.

Conclusión

Este documento cubre los pasos necesarios para configurar Amazon FSx ONTAP con VMware Cloud en AWS. Amazon FSx ONTAP ofrece excelentes opciones para implementar y administrar cargas de trabajo de aplicaciones junto con servicios de archivos, al tiempo que reduce el TCO al hacer que los requisitos de datos se integren perfectamente en la capa de aplicación. Cualquiera que sea el caso de uso, elija VMware Cloud on AWS junto con Amazon FSx ONTAP para obtener rápidamente los beneficios de la nube, una infraestructura consistente y operaciones desde las instalaciones locales hasta AWS, portabilidad bidireccional de cargas de trabajo y capacidad y rendimiento de nivel empresarial. Es el mismo proceso y procedimientos familiares utilizados para conectar el almacenamiento. Recuerde que lo único que cambió fue la posición de los datos junto con los nuevos nombres; las herramientas y los procesos siguen siendo los mismos, y Amazon FSx ONTAP ayuda a optimizar la implementación general.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado.

Amazon FSx ONTAP VMware Cloud

Creación de un almacén de datos NFS complementario en AWS

Una vez que VMware Cloud esté listo y conectado a AWS VPC, debe implementar Amazon FSx ONTAP en una VPC recientemente designada en lugar de la VPC original conectada o predeterminada existente.

Para comenzar, implemente una VPC adicional en la misma región y zona de disponibilidad donde reside SDDC y luego implemente Amazon FSx ONTAP en la nueva VPC. "Configuración de un grupo SDDC en VMware Cloud" La consola habilita las opciones de configuración de red necesarias para conectarse a la VPC recién designada donde se implementará FSx ONTAP .

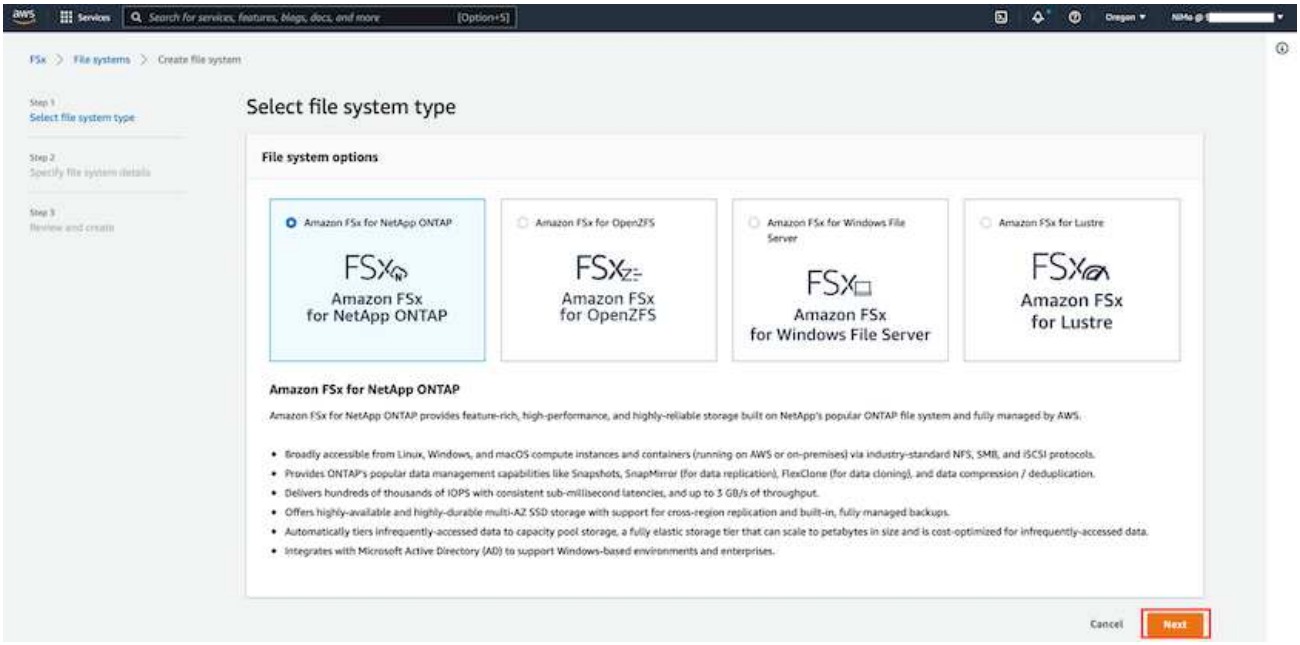
Implemente FSx ONTAP en la misma zona de disponibilidad que VMware Cloud on AWS SDDC.

No se puede implementar FSx ONTAP en la VPC conectada. En su lugar, debe implementarlo en una nueva VPC designada y luego conectar la VPC a un VMware Managed Transit Gateway (vTGW) a través de grupos SDDC.

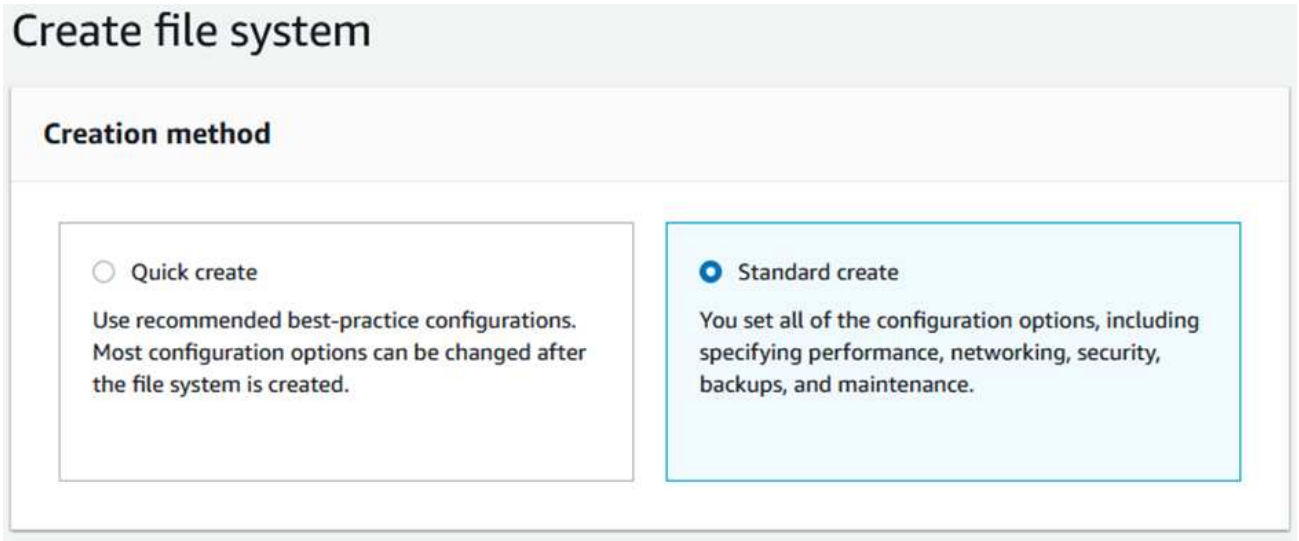
▼ **Paso 1: Cree Amazon FSx ONTAP en una nueva VPC designada**

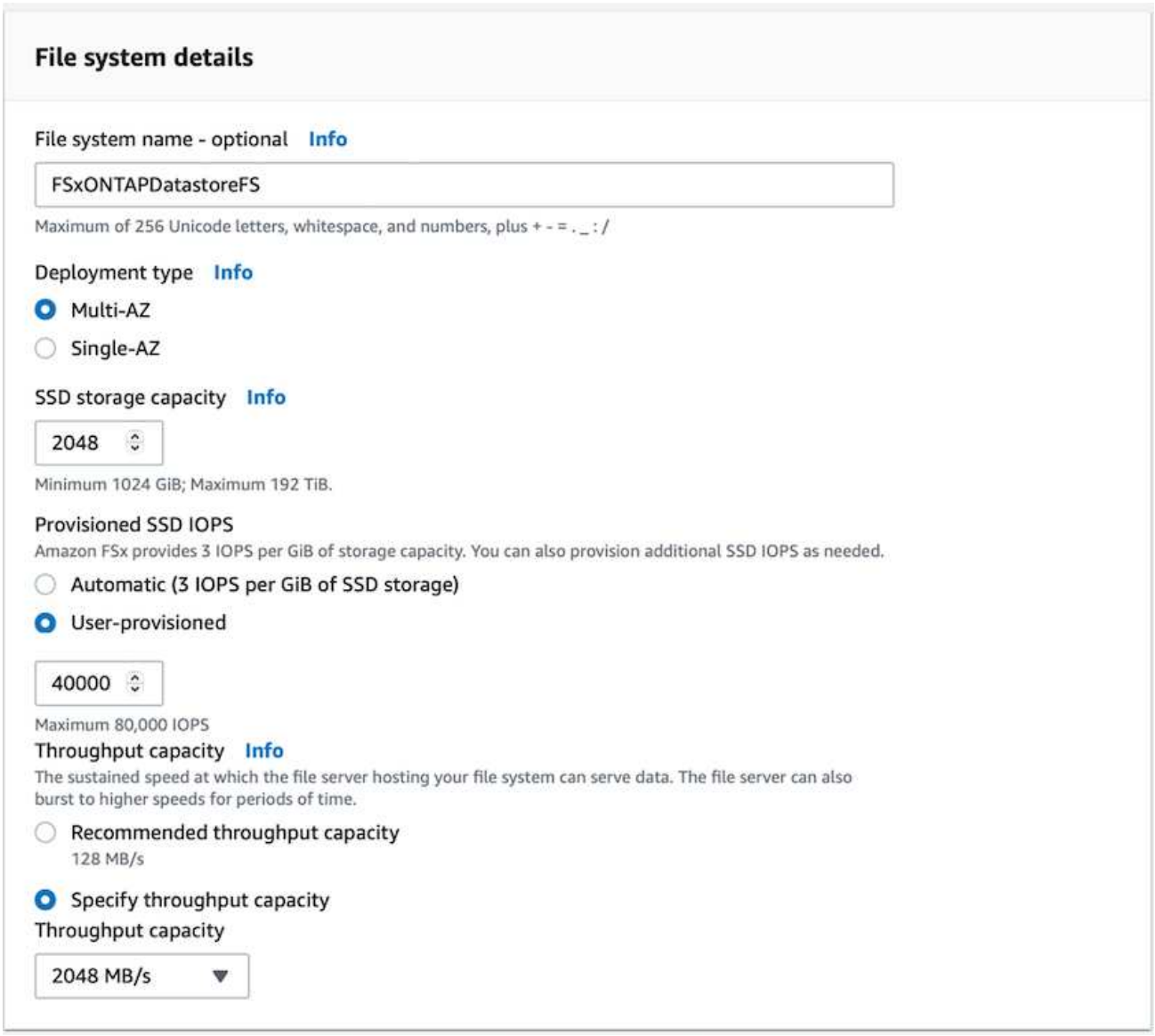
Para crear y montar el sistema de archivos de Amazon FSx ONTAP , complete los siguientes pasos:

1. Abra la consola de Amazon FSx en `https://console.aws.amazon.com/fsx/` y seleccione **Crear sistema de archivos** para iniciar el asistente de **Creación del sistema de archivos**.
2. En la página Seleccionar tipo de sistema de archivos, seleccione * Amazon FSx ONTAP* y luego haga clic en * Siguiente **. Aparece la página *Crear sistema de archivos**.



3. Para el método de creación, elija **Creación estándar**.





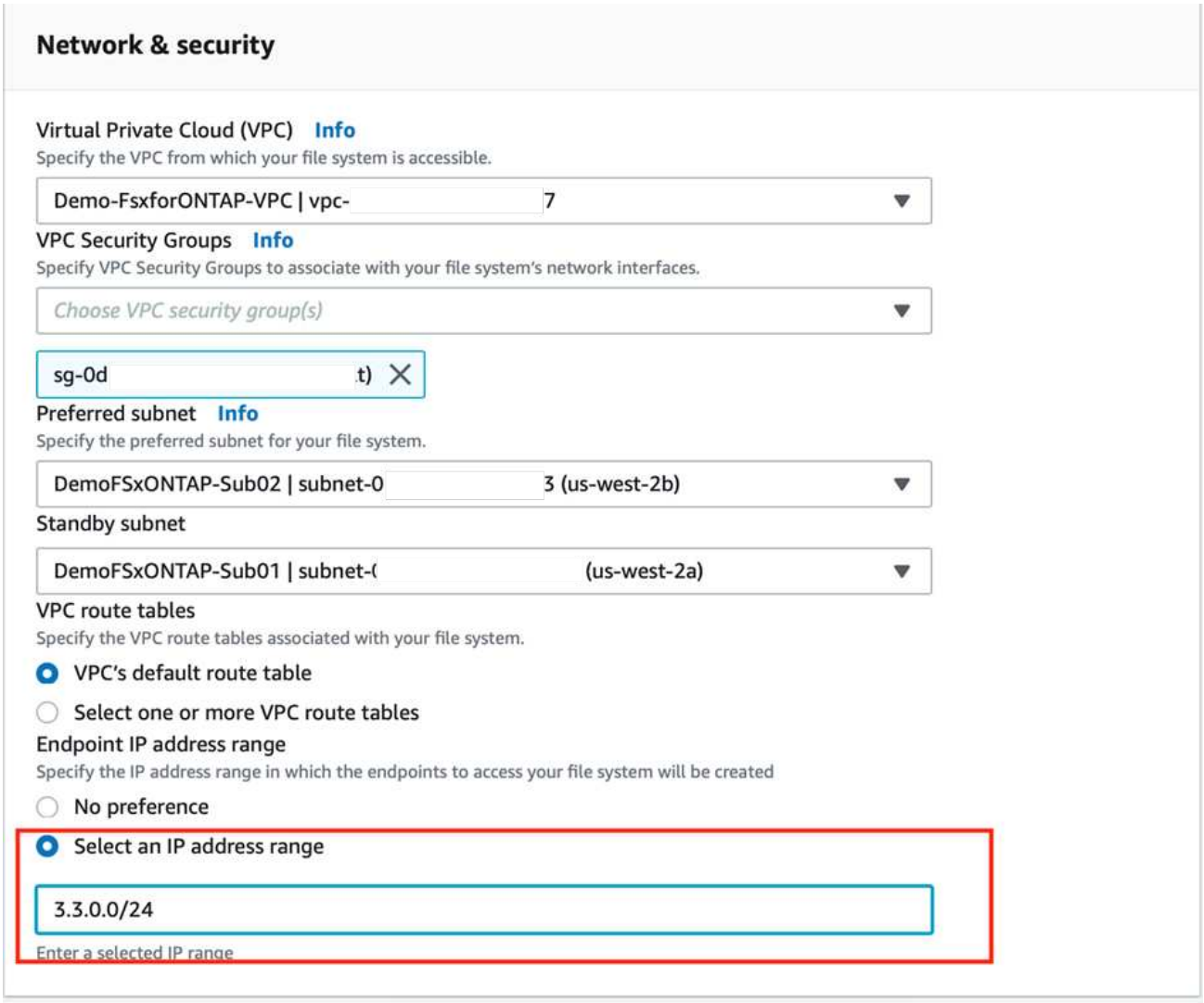
Los tamaños de los almacenes de datos varían bastante de un cliente a otro. Si bien la cantidad recomendada de máquinas virtuales por almacén de datos NFS es subjetiva, muchos factores determinan la cantidad óptima de máquinas virtuales que se pueden colocar en cada almacén de datos. Aunque la mayoría de los administradores solo consideran la capacidad, la cantidad de E/S simultánea que se envía a los VMDK es uno de los factores más importantes para el rendimiento general. Utilice las estadísticas de rendimiento locales para dimensionar los volúmenes del almacén de datos según corresponda.

4. En la sección **Redes** de Nube privada virtual (VPC), elija la VPC adecuada y las subredes preferidas junto con la tabla de rutas. En este caso, se selecciona Demo-FSxforONTAP-VPC en el menú desplegable.

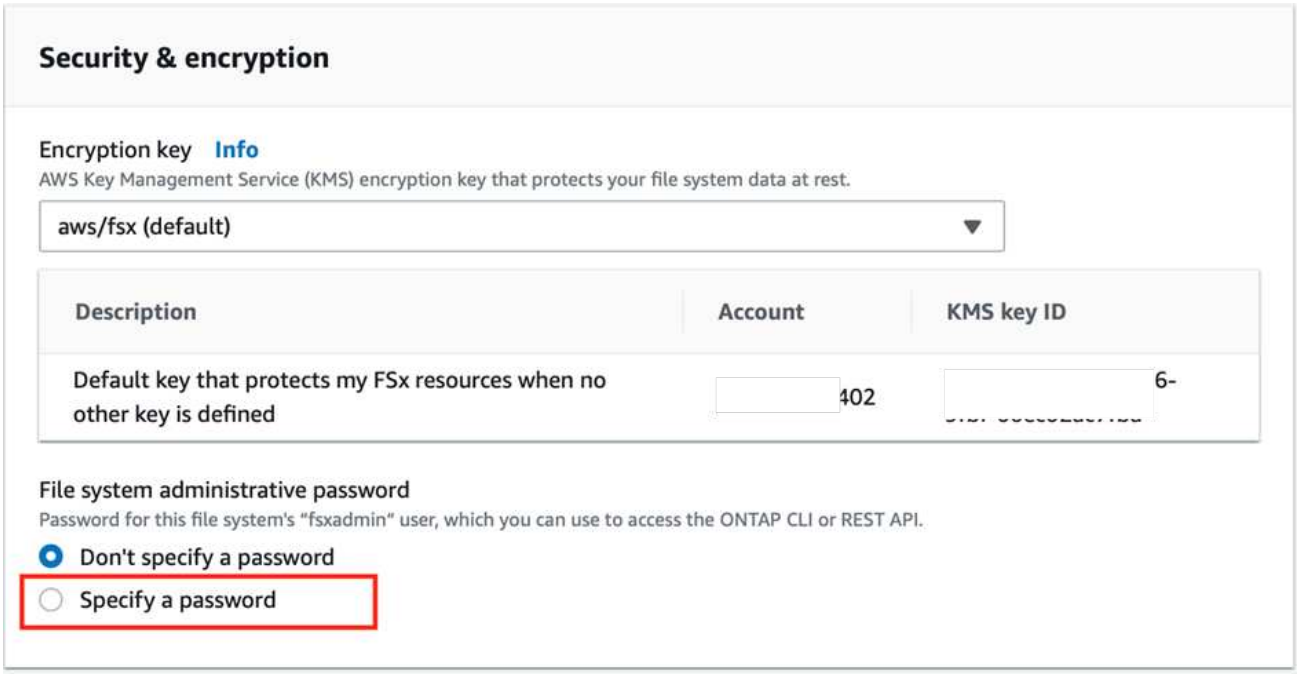
Asegúrese de que sea una VPC nueva y designada y no la VPC conectada.

De forma predeterminada, FSx ONTAP utiliza 198.19.0.0/16 como el rango de direcciones IP del punto final predeterminado para el sistema de archivos. Asegúrese de que el rango de direcciones IP del punto final no entre en conflicto con la VMC en AWS

SDDC, las subredes de VPC asociadas y la infraestructura local. Si no está seguro, utilice un rango que no se superponga y que no presente conflictos.

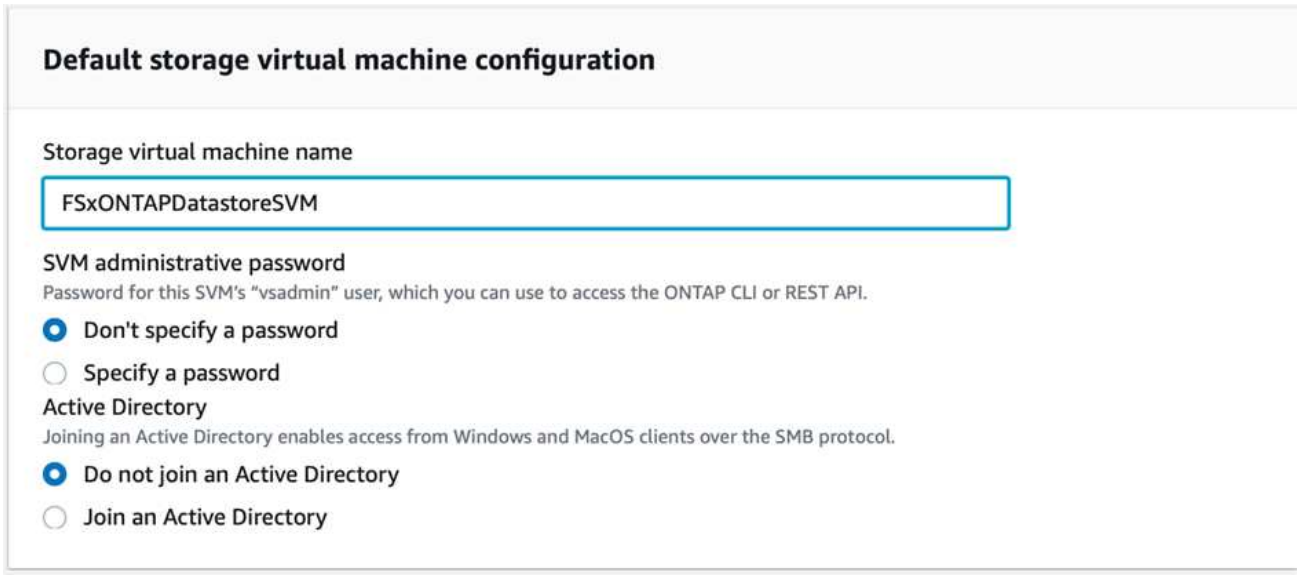


5. En la sección **Seguridad y cifrado** de la clave de cifrado, elija la clave de cifrado de AWS Key Management Service (AWS KMS) que protege los datos del sistema de archivos en reposo. Para la **Contraseña administrativa del sistema de archivos**, ingrese una contraseña segura para el usuario fsxadmin.



6. En la sección **Configuración de máquina virtual de almacenamiento predeterminada**, especifique el nombre de la SVM.

   A partir de GA, se admiten cuatro almacenes de datos NFS.



7. En la sección **Configuración de volumen predeterminada**, especifique el nombre y el tamaño del volumen necesarios para el almacén de datos y haga clic en **Siguiente**. Este debe ser un volumen NFSv3. Para **Eficiencia de almacenamiento**, elija **Habilitado** para activar las funciones de eficiencia de almacenamiento de ONTAP (compresión, deduplicación y compactación). Después de la creación, use el shell para modificar los parámetros del volumen usando ***volume modification*** de la siguiente manera:

Valor	Configuración
Garantía de volumen (Estilo de garantía de espacio)	Ninguno (aprovisionamiento fino): configurado de forma predeterminada
reserva_fraccional (reserva-fraccional)	0% – establecido por defecto
snap_reserve (porcentaje de espacio para instantáneas)	0%
Tamaño automático (modo de tamaño automático)	crecer_encoger
Eficiencia de almacenamiento	Habilitado – establecido por defecto
Borrado automático	volumen / más antiguo_primero
Política de niveles de volumen	Solo instantánea: configurado de forma predeterminada
prueba_primero	Crecimiento automático
Política de instantáneas	Ninguno

Utilice el siguiente comando SSH para crear y modificar volúmenes:

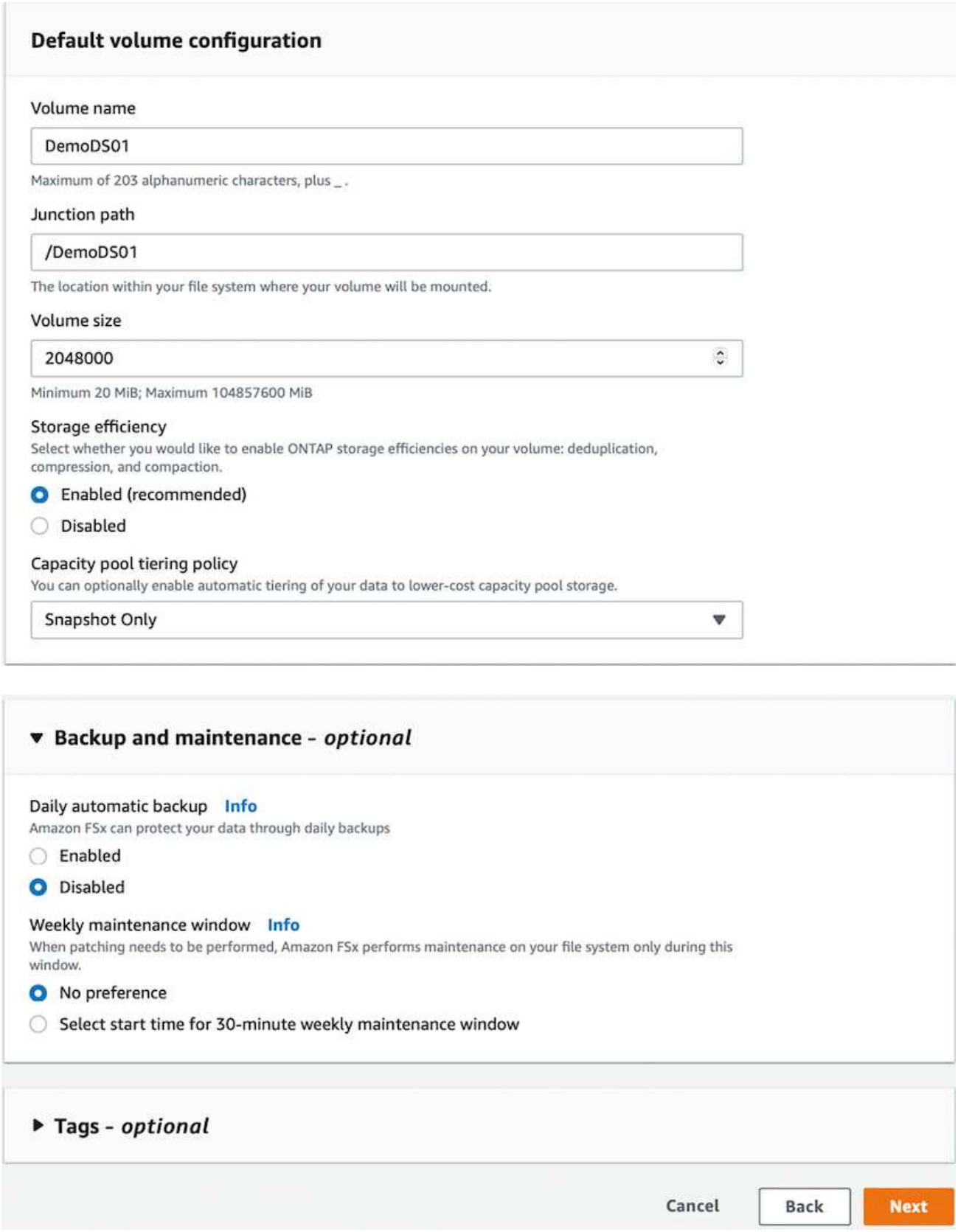
Comando para crear un nuevo volumen de almacén de datos desde el shell:

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy snapshot-
only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy
none -junction-path /DemoDS002
```

Nota: Los volúmenes creados a través del shell tardarán unos minutos en aparecer en la consola de AWS.

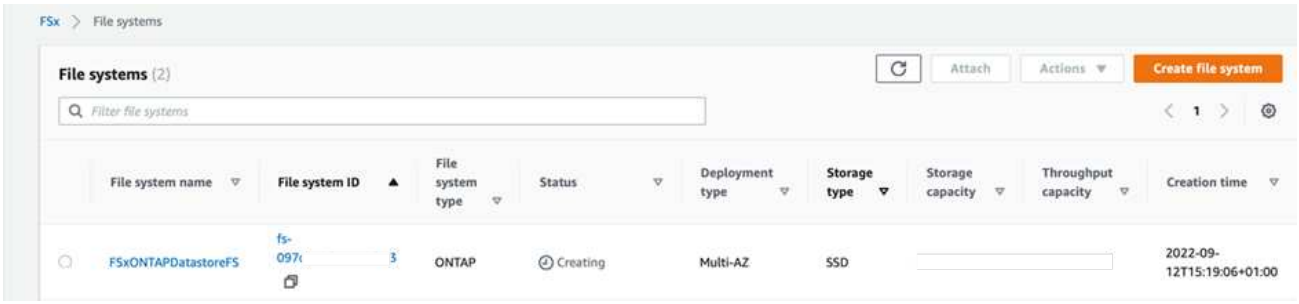
Comando para modificar parámetros de volumen que no están configurados por defecto:

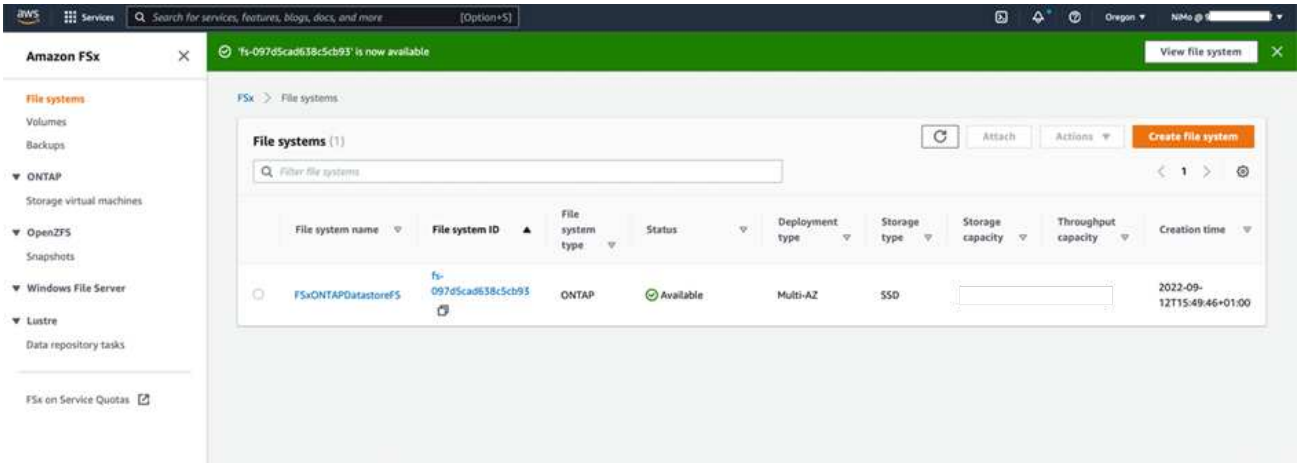
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```



Durante el escenario de migración inicial, la política de instantáneas predeterminada puede provocar problemas de capacidad máxima en el almacén de datos. Para solucionarlo, modifique la política de instantáneas para adaptarla a las necesidades.

8. Revise la configuración del sistema de archivos que se muestra en la página **Crear sistema de archivos**.
9. Haga clic en **Crear sistema de archivos**.





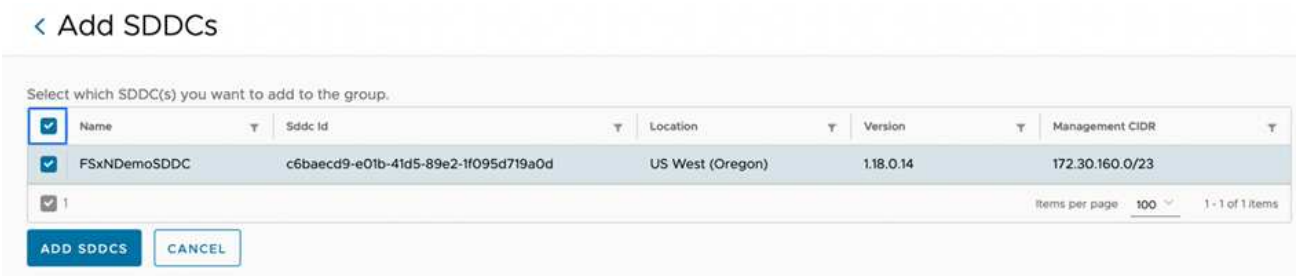
Repita los pasos anteriores para crear más máquinas virtuales de almacenamiento o sistemas de archivos y volúmenes de almacén de datos según los requisitos de capacidad y rendimiento.

Para obtener más información sobre el rendimiento de Amazon FSx ONTAP , consulte "Rendimiento de Amazon FSx ONTAP" .

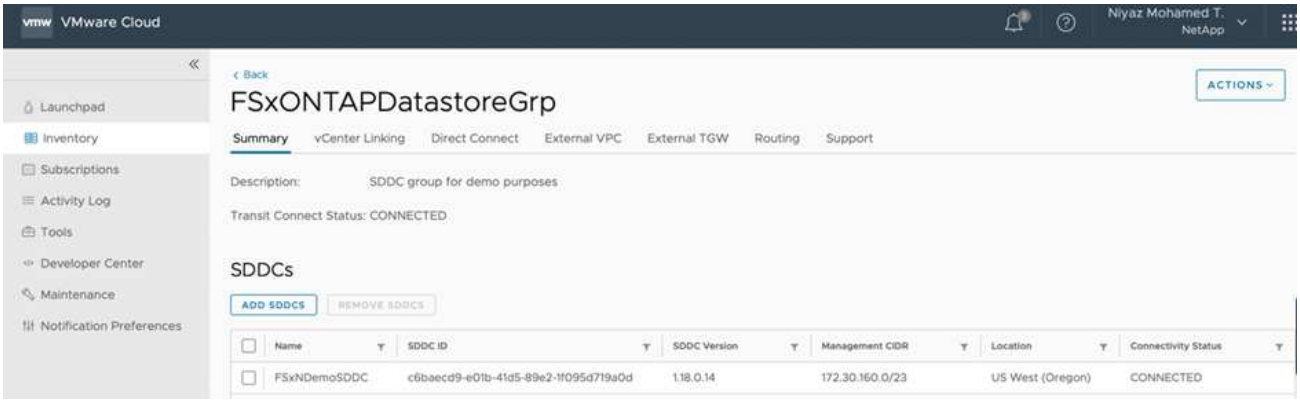
▼ Paso 2: Crear un grupo SDDC

Una vez creados los sistemas de archivos y las SVM, utilice VMware Console para crear un grupo SDDC y configurar VMware Transit Connect. Para ello, complete los siguientes pasos y recuerde que debe navegar entre VMware Cloud Console y AWS Console.

1. Inicie sesión en la consola VMC en `https://vmc.vmware.com` .
2. En la página **Inventario**, haga clic en **Grupos SDDC**.
3. En la pestaña **Grupos SDDC**, haga clic en **ACCIONES** y seleccione **Crear grupo SDDC**. Para fines de demostración, el grupo SDDC se denomina `FSxONTAPDatastoreGrp` .
4. En la cuadrícula de Membresía, seleccione los SDDC que desea incluir como miembros del grupo.

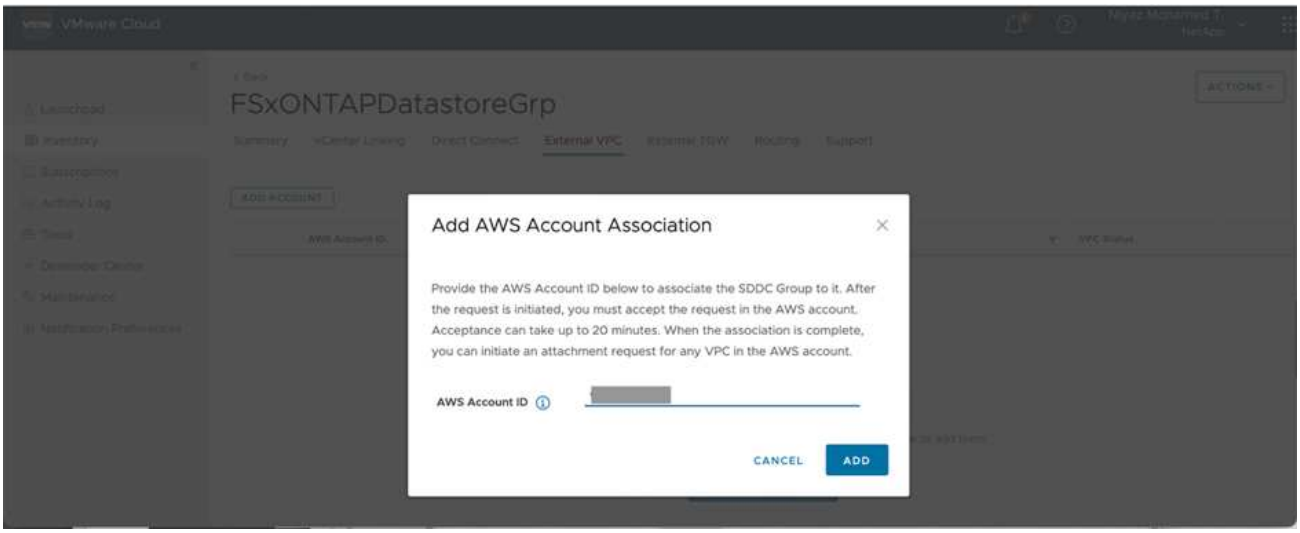


5. Verifique que la opción "Configurar VMware Transit Connect para su grupo generará cargos por cada archivo adjunto y transferencia de datos" esté marcada y luego seleccione **Crear grupo**. El proceso puede tardar unos minutos en completarse.

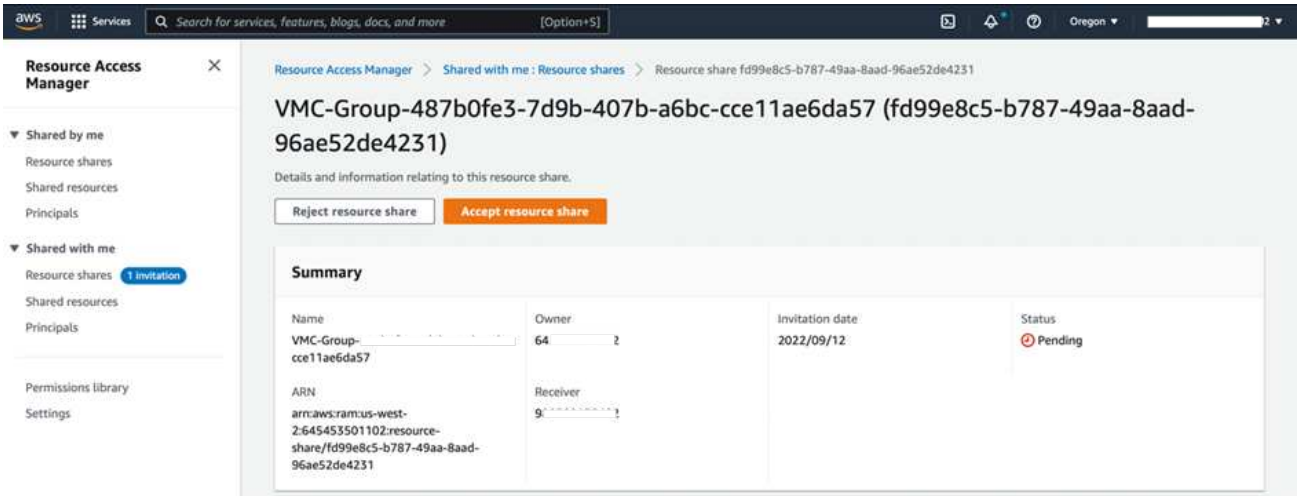


▼ **Paso 3: Configurar VMware Transit Connect**

1. Adjunte la VPC designada recién creada al grupo SDDC. Seleccione la pestaña **VPC externa** y siga las instrucciones. "Instrucciones para adjuntar una VPC externa al grupo" . Este proceso puede tardar entre 10 y 15 minutos en completarse.

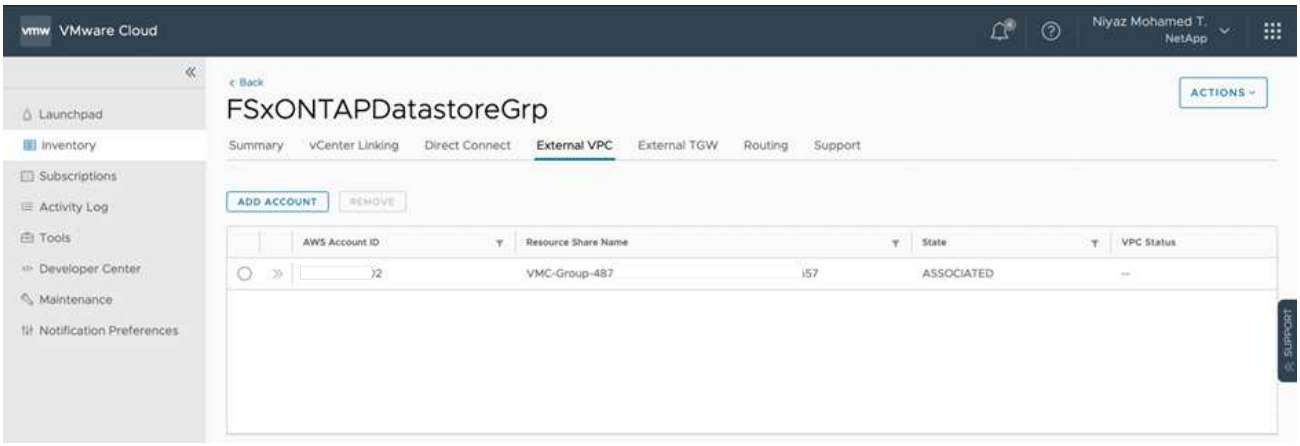


2. Haga clic en **Agregar cuenta**.
   a. Proporcione la cuenta de AWS que se utilizó para aprovisionar el sistema de archivos FSx ONTAP .
   b. Haga clic en **Agregar**.
3. De regreso en la consola de AWS, inicie sesión en la misma cuenta de AWS y navegue a la página del servicio **Resource Access Manager**. Hay un botón para que usted acepte compartir el recurso.



Como parte del proceso de VPC externo, se le solicitará a través de la consola de AWS un nuevo recurso compartido mediante el Administrador de acceso a recursos. El recurso compartido es AWS Transit Gateway administrado por VMware Transit Connect.

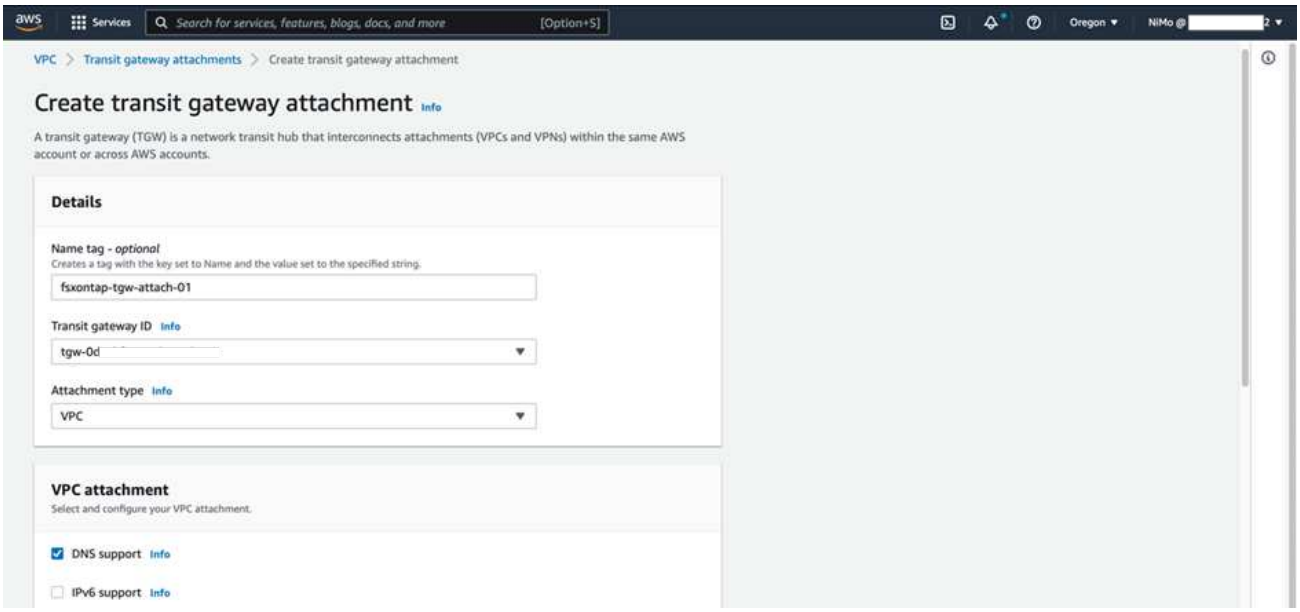
4. Haga clic en **Aceptar compartir recursos**.



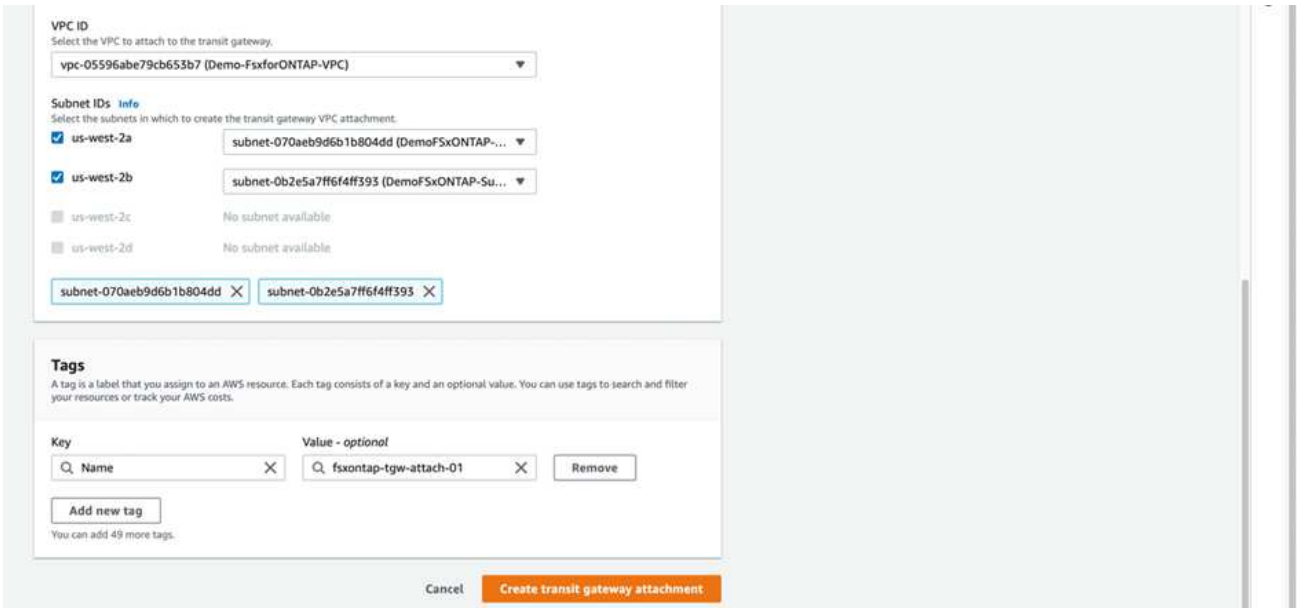
5. De regreso en la consola VMC, ahora verá que la VPC externa está en un estado asociado. Esto puede tardar varios minutos en aparecer.

▼ **Paso 4: Crear un archivo adjunto de puerta de enlace de tránsito**

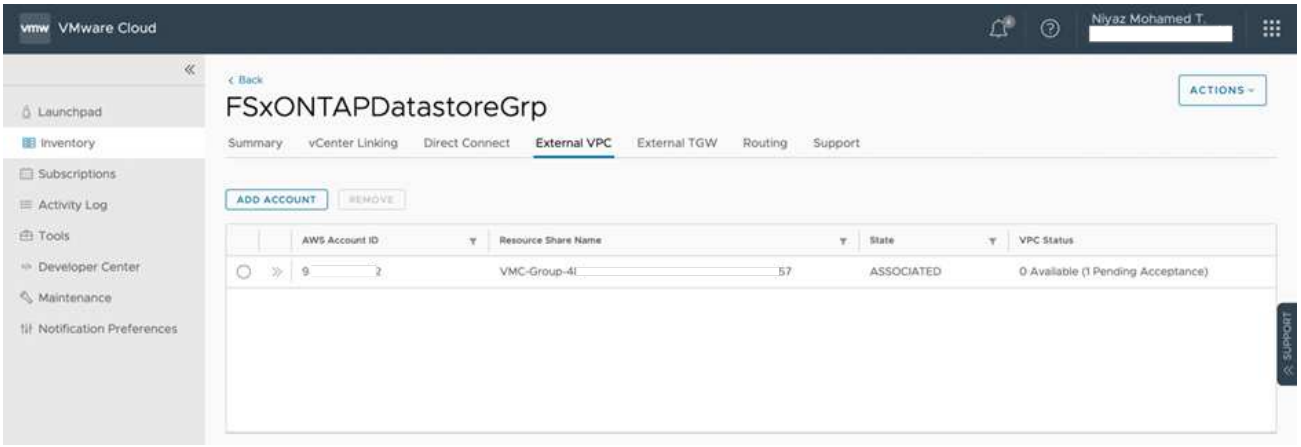
1. En la consola de AWS, vaya a la página del servicio VPC y navegue hasta la VPC que se utilizó para aprovisionar el sistema de archivos FSx. Aquí puede crear un archivo adjunto de puerta de enlace de tránsito haciendo clic en **Archivo adjunto de puerta de enlace de tránsito** en el panel de navegación de la derecha.
2. En **Adjunto VPC**, asegúrese de que la opción Compatibilidad con DNS esté marcada y seleccione la VPC en la que se implementó FSx ONTAP .

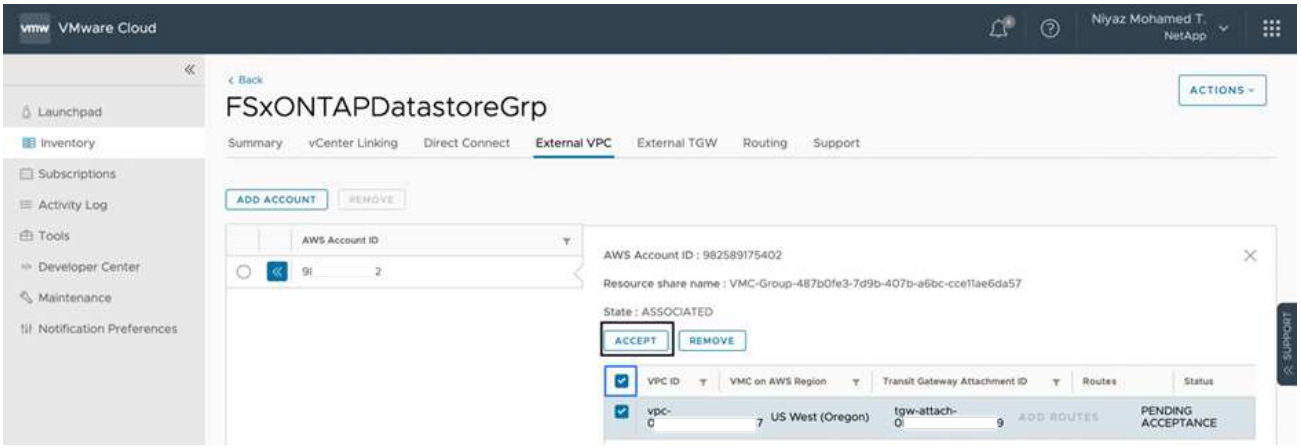


3. Haga clic en **Crear archivo adjunto de puerta de enlace de tránsito**.



4. De regreso en VMware Cloud Console, navegue nuevamente a Grupo SDDC > pestaña VPC externa. Seleccione el ID de la cuenta de AWS utilizada para FSx, haga clic en VPC y haga clic en **Aceptar**.

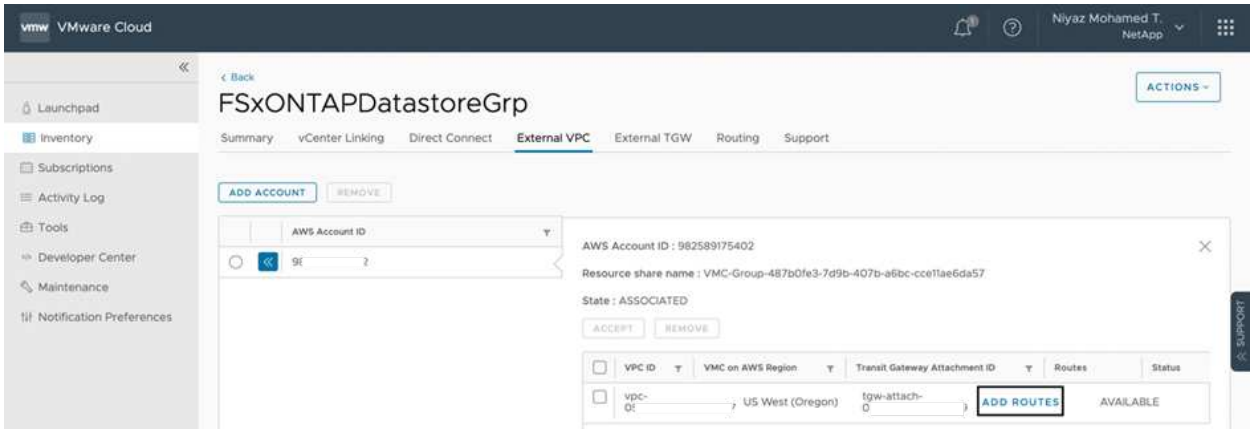


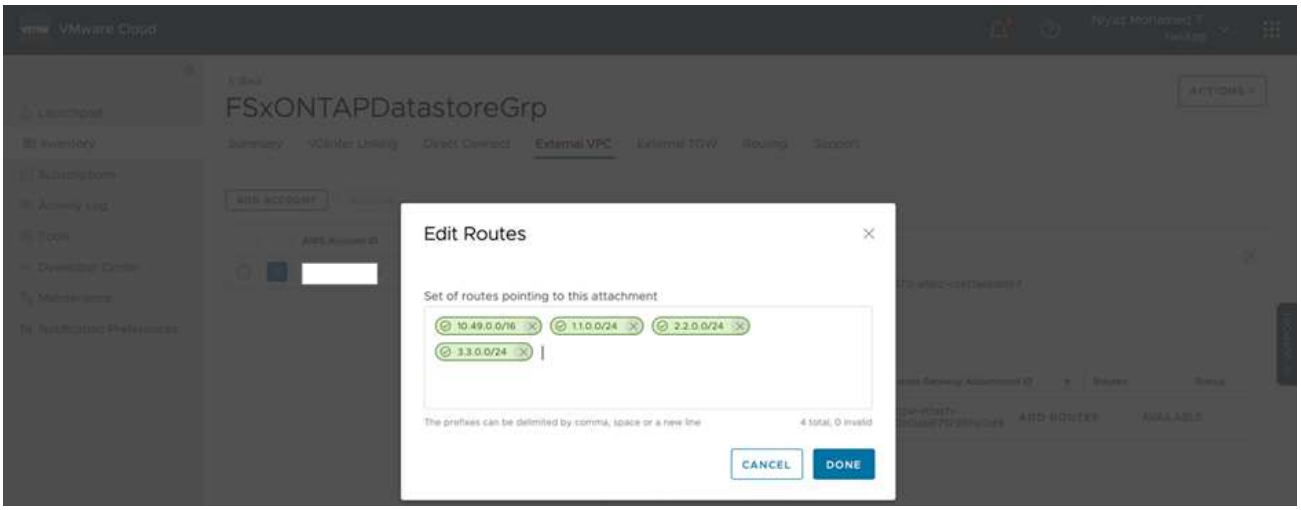


Esta opción puede tardar varios minutos en aparecer.

5. Luego, en la pestaña **VPC externa**, en la columna **Rutas**, haga clic en la opción **Agregar rutas** y agregue las rutas requeridas:

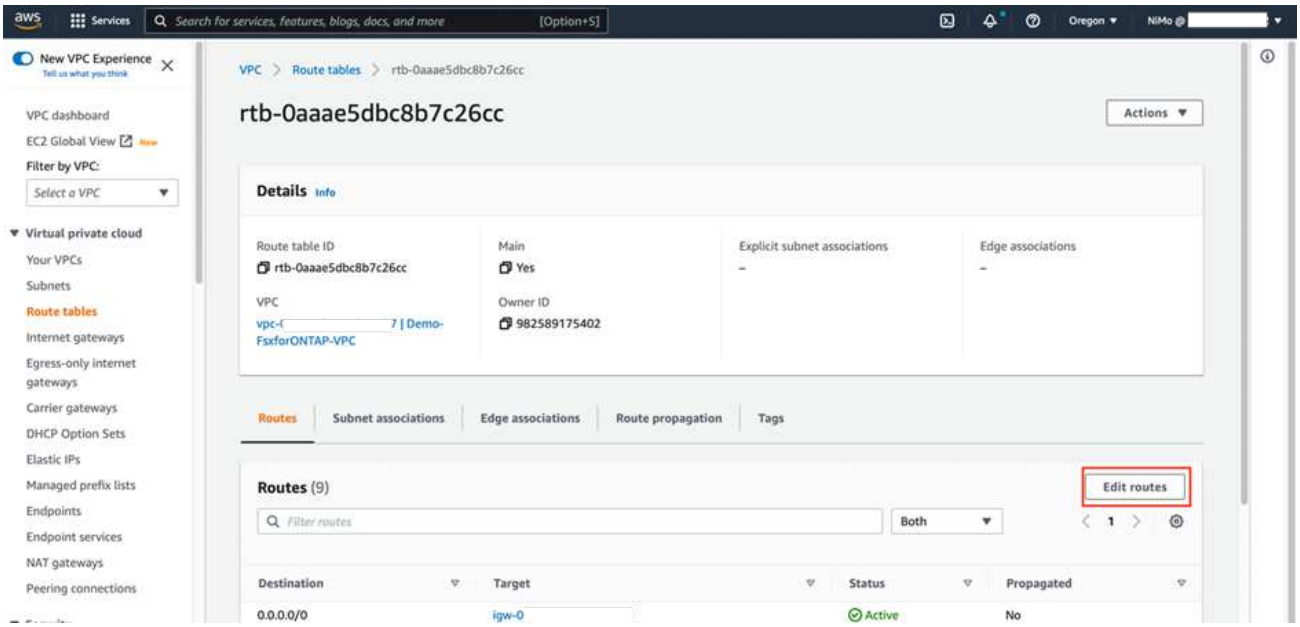
   - Una ruta para el rango de IP flotante para las IP flotantes de Amazon FSx ONTAP .
   - Una ruta para el espacio de direcciones VPC externo recién creado.



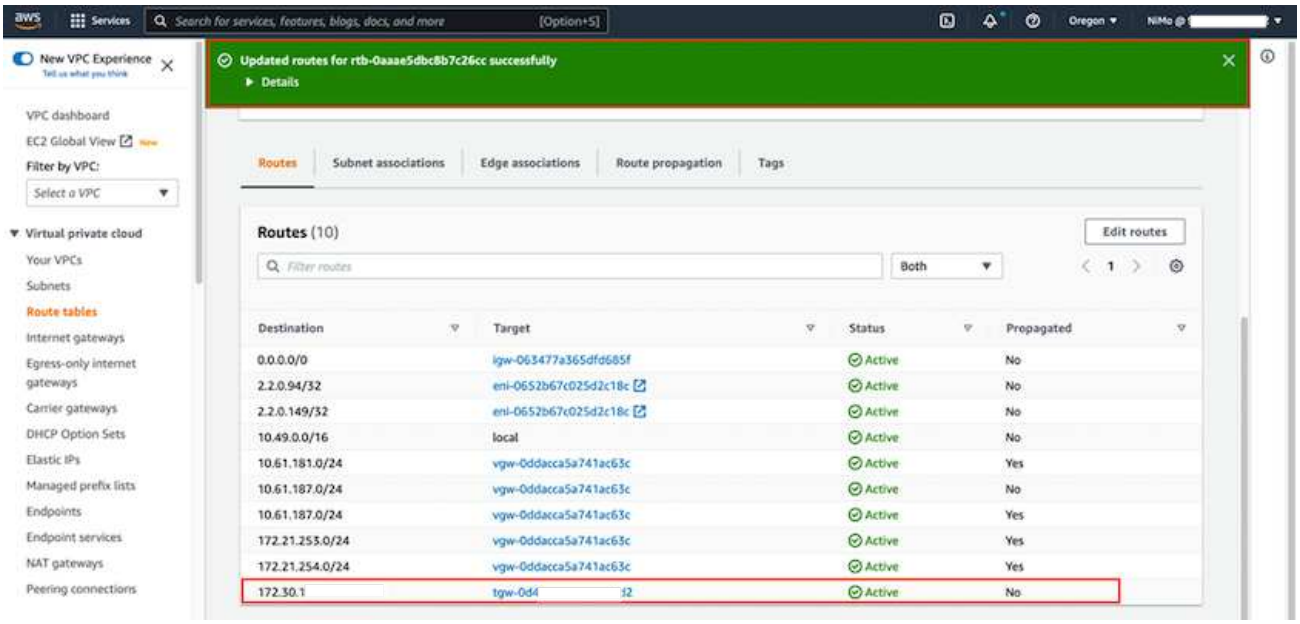


▼ **Paso 5: Configurar el enrutamiento (AWS VPC y SDDC) y los grupos de seguridad**

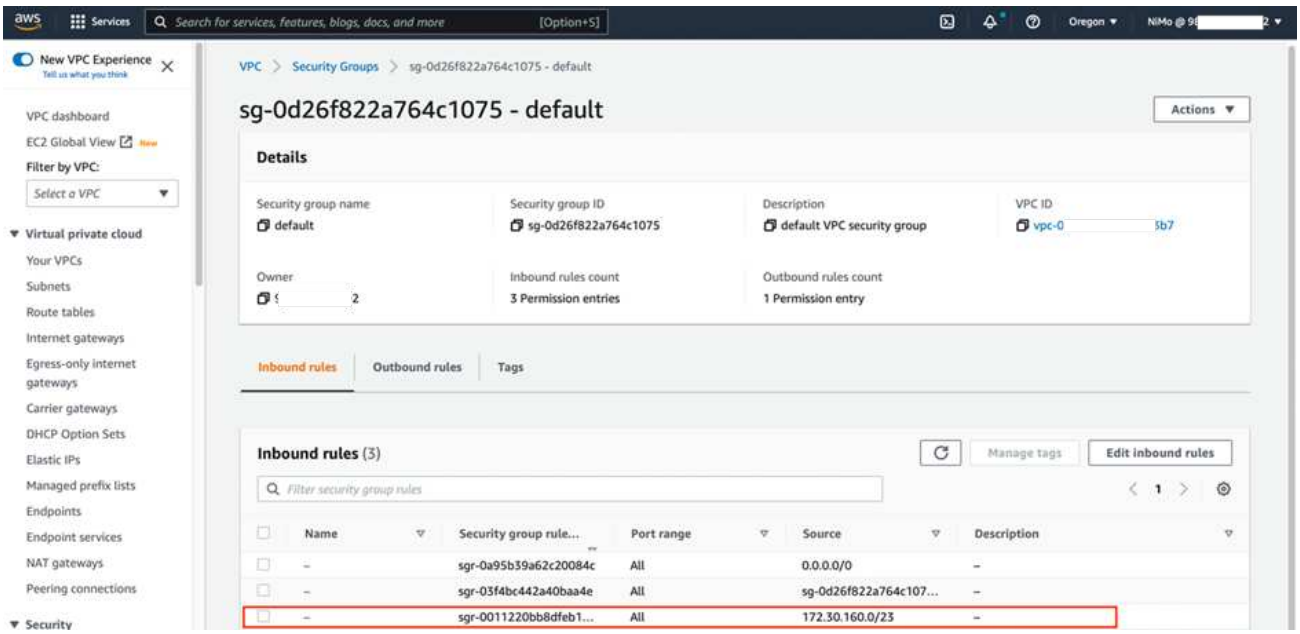
1. En la consola de AWS, cree la ruta de regreso al SDDC ubicando la VPC en la página de servicio de VPC y seleccione la tabla de ruta **principal** para la VPC.
2. Busque la tabla de rutas en el panel inferior y haga clic en **Editar rutas**.



3. En el panel **Editar rutas**, haga clic en **Agregar ruta** e ingrese el CIDR para la infraestructura SDDC seleccionando **Puerta de tránsito** y el ID de TGW asociado. Haga clic en **Guardar cambios**.



4. El siguiente paso es verificar que el grupo de seguridad en la VPC asociada esté actualizado con las reglas de entrada correctas para el CIDR del grupo SDDC.
5. Actualice la regla de entrada con el bloque CIDR de la infraestructura SDDC.



Verifique que la tabla de rutas de VPC (donde reside FSx ONTAP) esté actualizada para evitar problemas de conectividad.

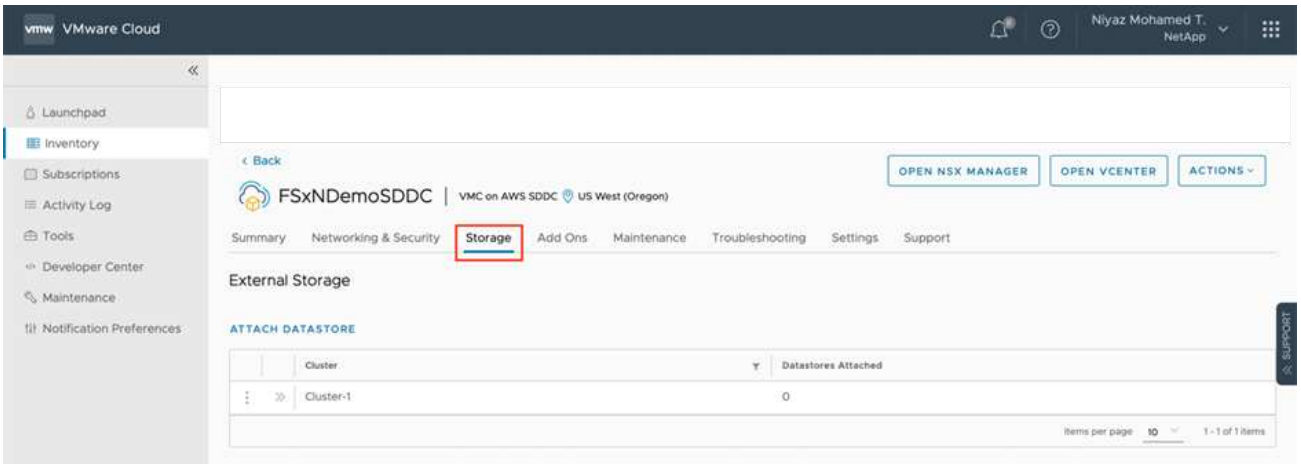
Actualice el grupo de seguridad para aceptar tráfico NFS.

Este es el paso final en la preparación de la conectividad al SDDC apropiado. Con el sistema de archivos configurado, las rutas agregadas y los grupos de seguridad actualizados, es momento de montar los almacenes de datos.

▼ Paso 6: Adjuntar un volumen NFS como almacén de datos al clúster SDDC

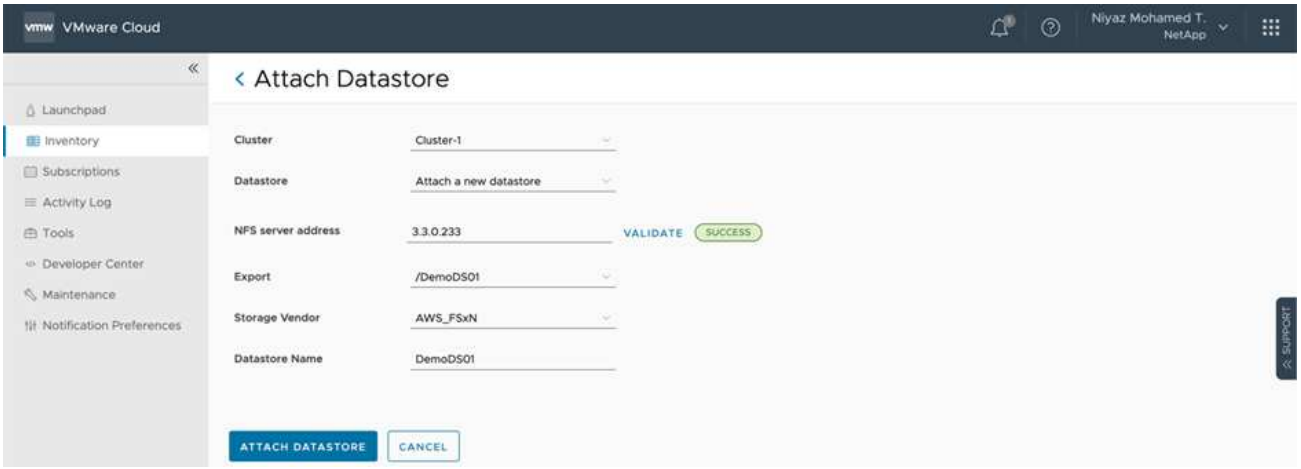
Una vez aprovisionado el sistema de archivos y establecida la conectividad, acceda a VMware Cloud Console para montar el almacén de datos NFS.

1. En la consola VMC, abra la pestaña **Almacenamiento** del SDDC.

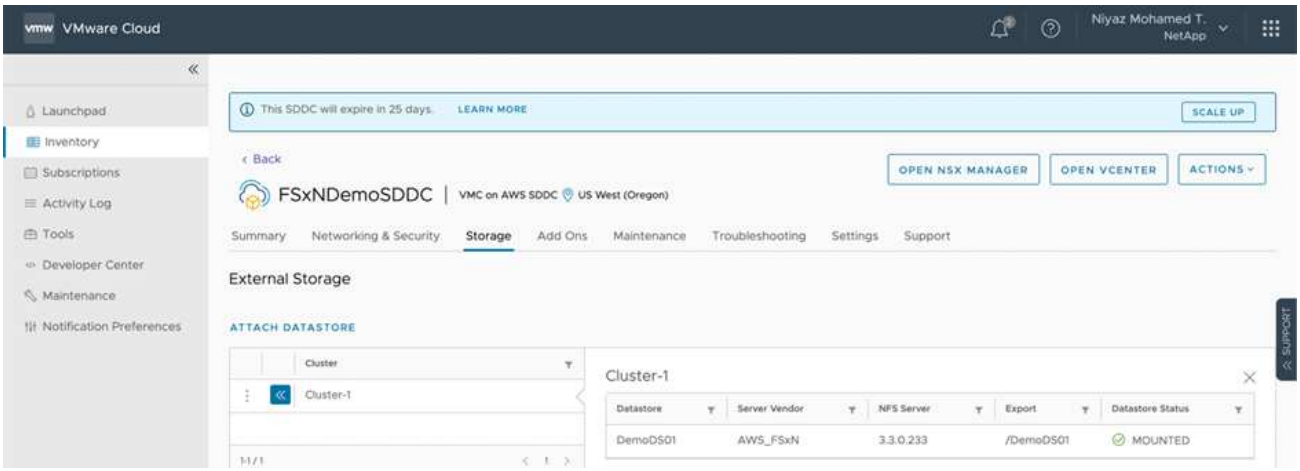


2. Haga clic en **ADJUNTAR ALMACÉN DE DATOS** y complete los valores requeridos.

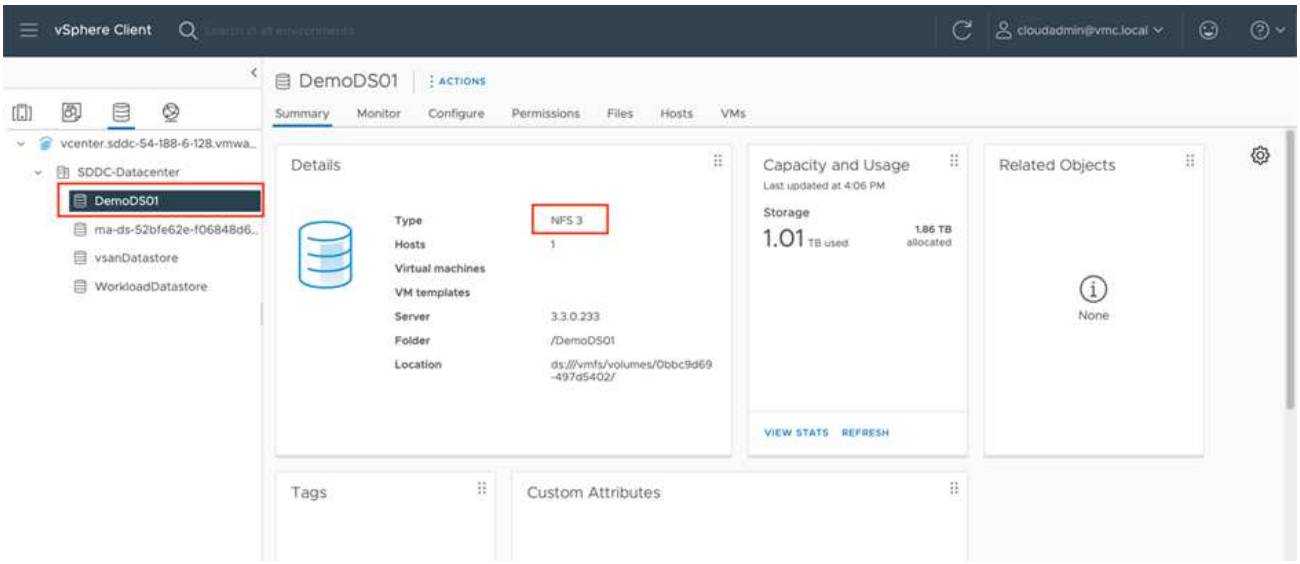
> La dirección del servidor NFS es la dirección IP de NFS que se puede encontrar en la pestaña FSx > Máquinas virtuales de almacenamiento > Puntos finales dentro de la consola de AWS.



3. Haga clic en **ADJUNTAR ALMACÉN DE DATOS** para adjuntar el almacén de datos al clúster.



4. Valide el almacén de datos NFS accediendo a vCenter como se muestra a continuación:



Opciones de almacenamiento conectado para invitados de NetApp para AWS

AWS admite el almacenamiento NetApp conectado a invitados con el servicio FSx nativo (FSx ONTAP) o con Cloud Volumes ONTAP (CVO).

FSx ONTAP

Amazon FSx ONTAP es un servicio completamente administrado que proporciona almacenamiento de archivos altamente confiable, escalable, de alto rendimiento y rico en funciones, creado sobre el popular sistema de archivos ONTAP de NetApp. FSx ONTAP combina las características, el rendimiento, las capacidades y las operaciones API familiares de los sistemas de archivos NetApp con la agilidad, la escalabilidad y la simplicidad de un servicio de AWS completamente administrado.

FSx ONTAP ofrece almacenamiento de archivos compartido rápido, flexible y repleto de funciones, al que se puede acceder ampliamente desde instancias de cómputo de Linux, Windows y macOS que se ejecutan en AWS o en las instalaciones. FSx ONTAP ofrece almacenamiento en unidad de estado sólido (SSD) de alto rendimiento con latencias de submilisegundos. Con FSx ONTAP, puede lograr niveles de rendimiento SSD para su carga de trabajo mientras paga por almacenamiento SSD solo para una pequeña fracción de sus datos.

Administrar sus datos con FSx ONTAP es más fácil porque puede tomar instantáneas, clonar y replicar sus archivos con solo hacer clic en un botón. Además, FSx ONTAP organiza automáticamente sus datos en un almacenamiento elástico de menor costo, lo que reduce la necesidad de aprovisionar o administrar capacidad.

FSx ONTAP también proporciona almacenamiento duradero y de alta disponibilidad con copias de seguridad totalmente administradas y soporte para recuperación ante desastres entre regiones. Para facilitar la protección y seguridad de sus datos, FSx ONTAP admite aplicaciones antivirus y de seguridad de datos populares.

FSx ONTAP como almacenamiento conectado para invitados

▼ **Configurar Amazon FSx ONTAP con VMware Cloud en AWS**

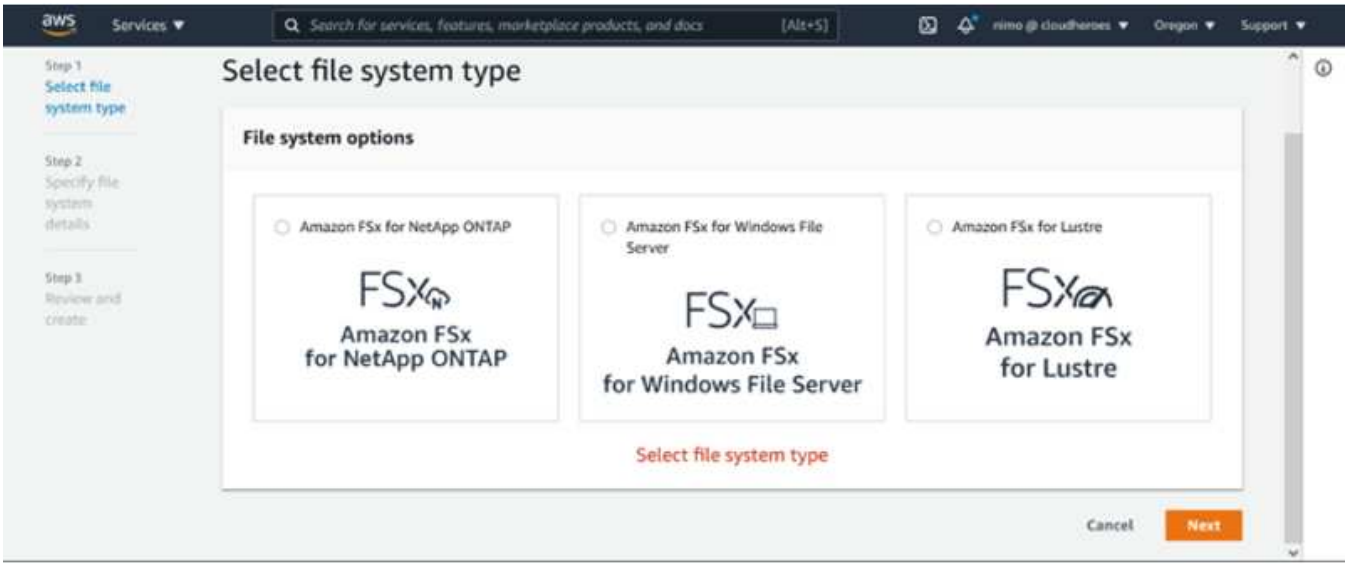
Los recursos compartidos de archivos y LUN de Amazon FSx ONTAP se pueden montar desde máquinas virtuales creadas dentro del entorno VMware SDDC en VMware Cloud en AWS. Los volúmenes también se pueden montar en el cliente Linux y mapear en el cliente Windows usando el protocolo NFS o SMB, y se puede acceder a los LUN en clientes Linux o Windows como dispositivos de bloque cuando se montan sobre iSCSI. Amazon FSx para el sistema de archivos NetApp ONTAP se puede configurar rápidamente con los siguientes pasos.

> ⓘ Amazon FSx ONTAP y VMware Cloud on AWS deben estar en la misma zona de disponibilidad para lograr un mejor rendimiento y evitar cargos por transferencia de datos entre zonas de disponibilidad.

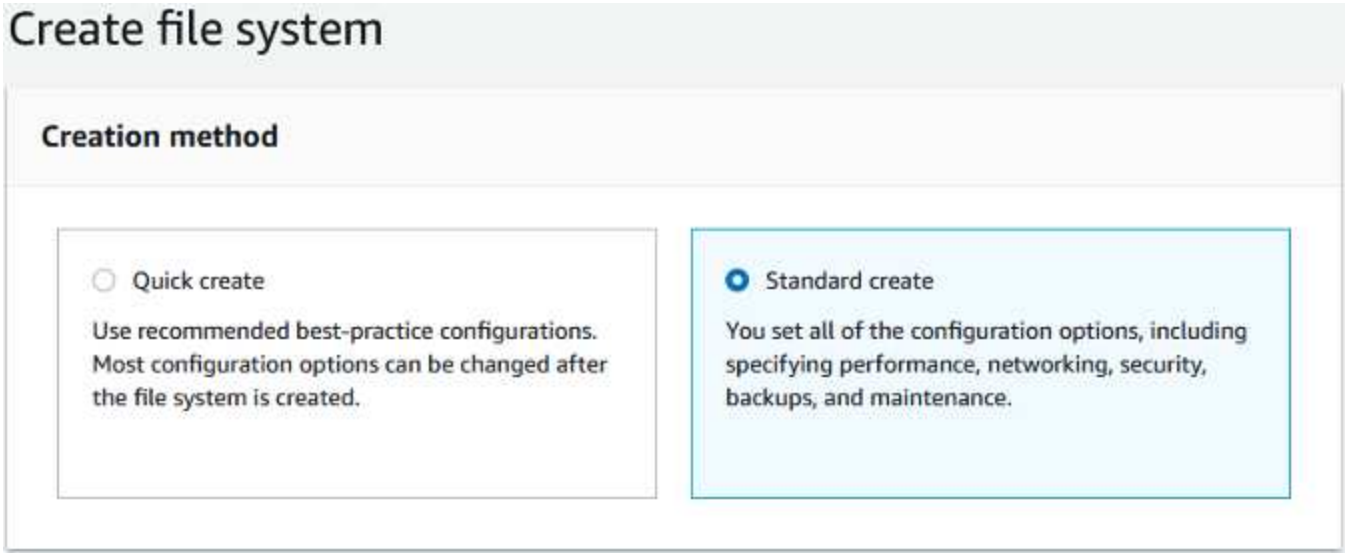
▼ **Crear y montar volúmenes de Amazon FSx ONTAP**

Para crear y montar el sistema de archivos de Amazon FSx ONTAP , complete los siguientes pasos:

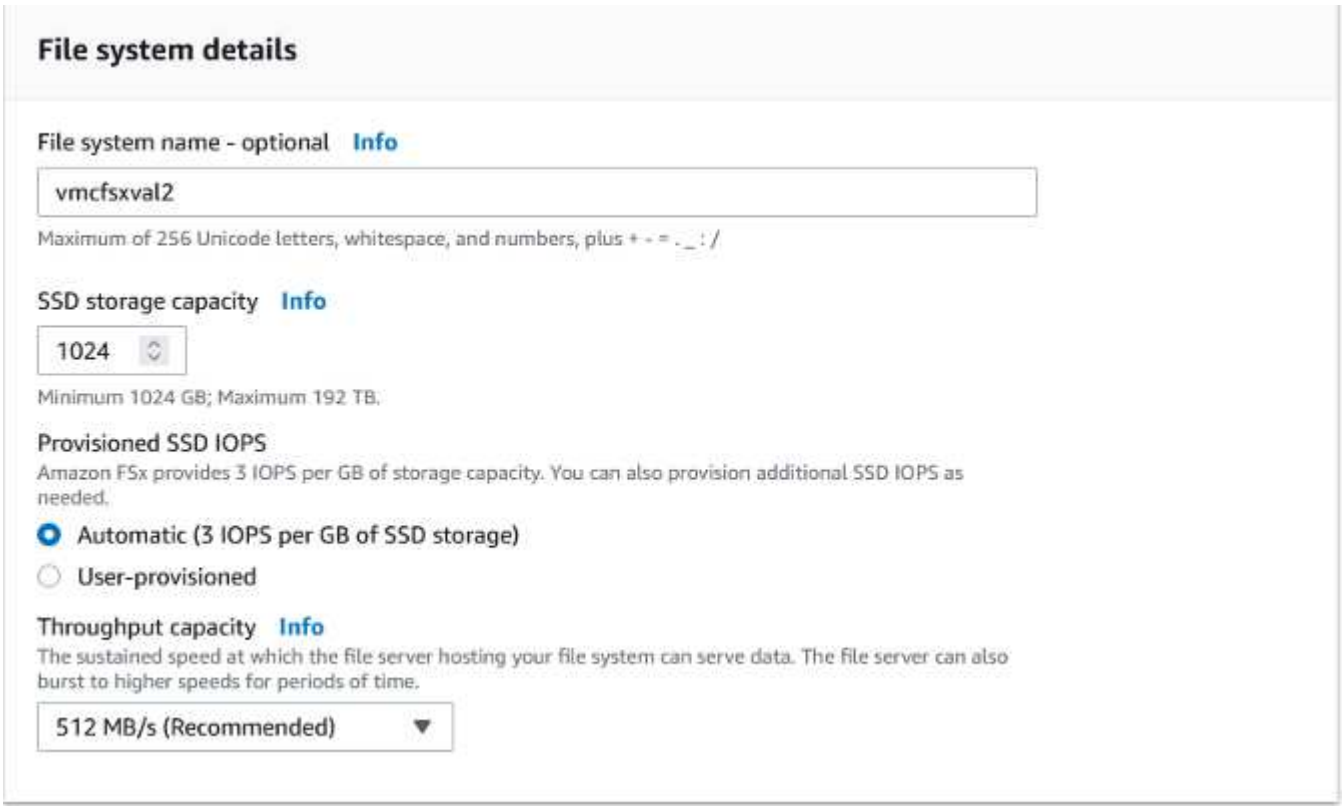
1. Abrir el"Consola de Amazon FSx" y elija Crear sistema de archivos para iniciar el asistente de creación del sistema de archivos.
2. En la página Seleccionar tipo de sistema de archivos, elija Amazon FSx ONTAP y luego elija Siguiente. Aparece la página Crear sistema de archivos.



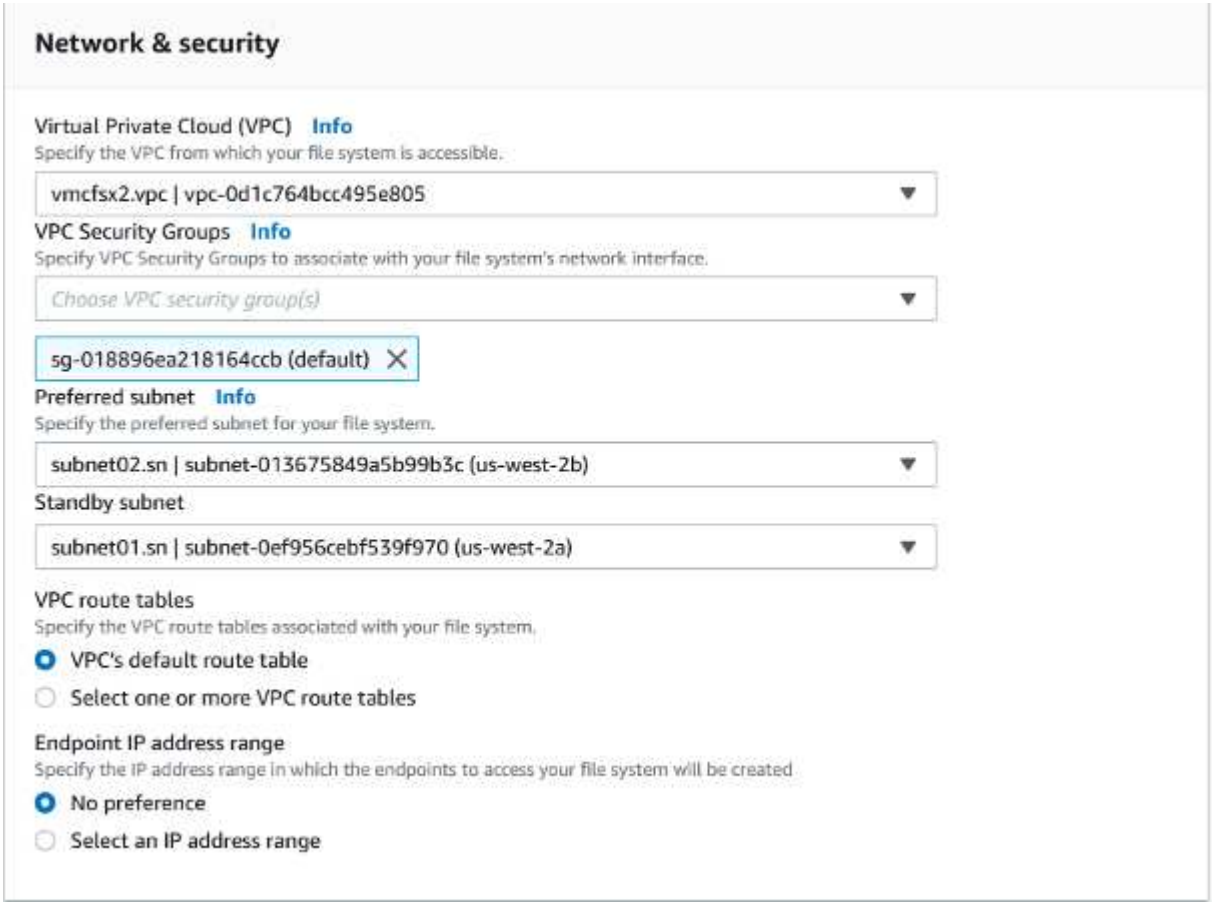
1. En la sección Redes, para Nube privada virtual (VPC), elija la VPC adecuada y las subredes preferidas junto con la tabla de rutas. En este caso, se selecciona vmcfsx2.vpc del menú desplegable.



1. Para el método de creación, elija Creación estándar. También puede elegir Creación rápida, pero este documento utiliza la opción de creación estándar.

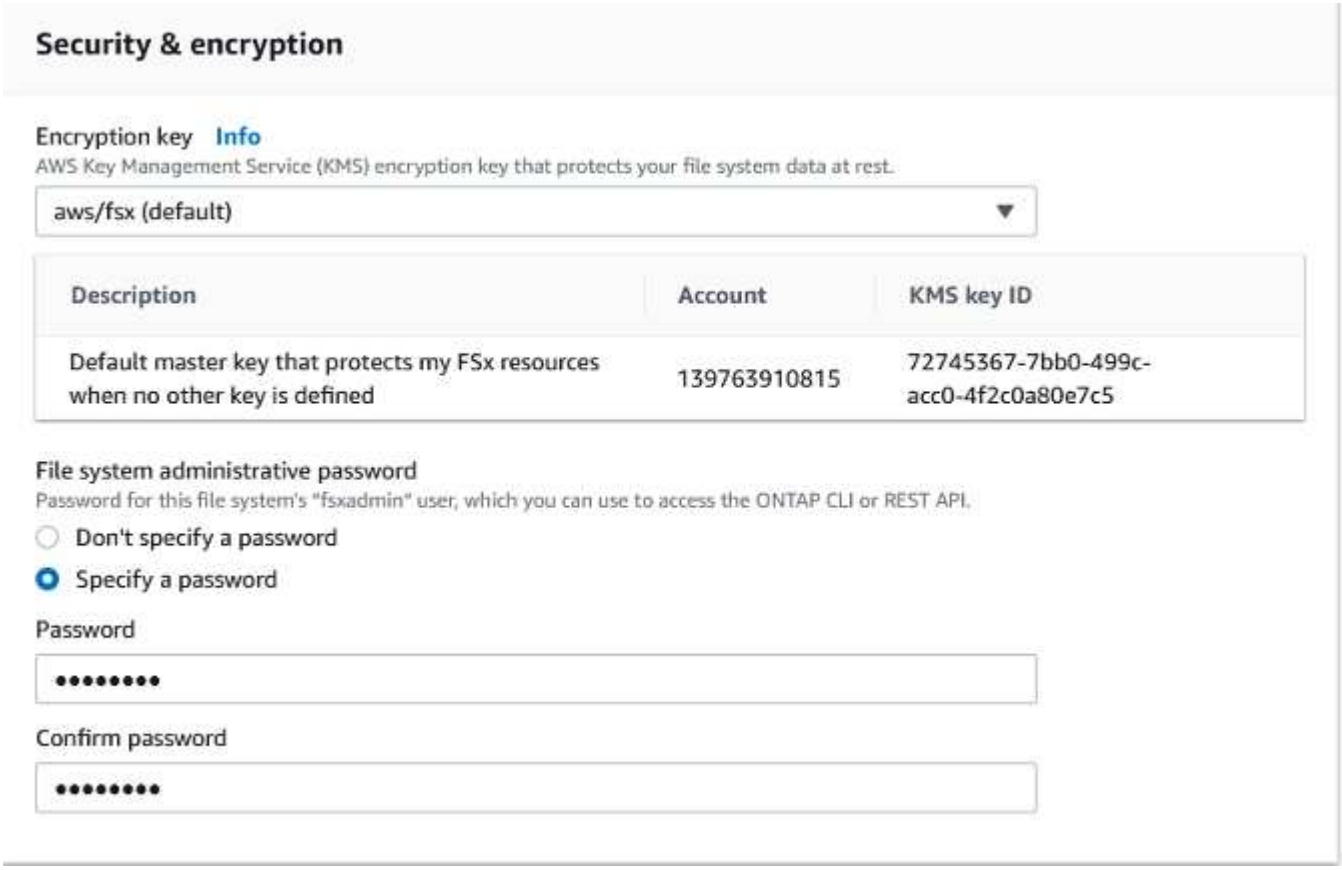


1. En la sección Redes, para Nube privada virtual (VPC), elija la VPC adecuada y las subredes preferidas junto con la tabla de rutas. En este caso, se selecciona vmcfsx2.vpc del menú desplegable.

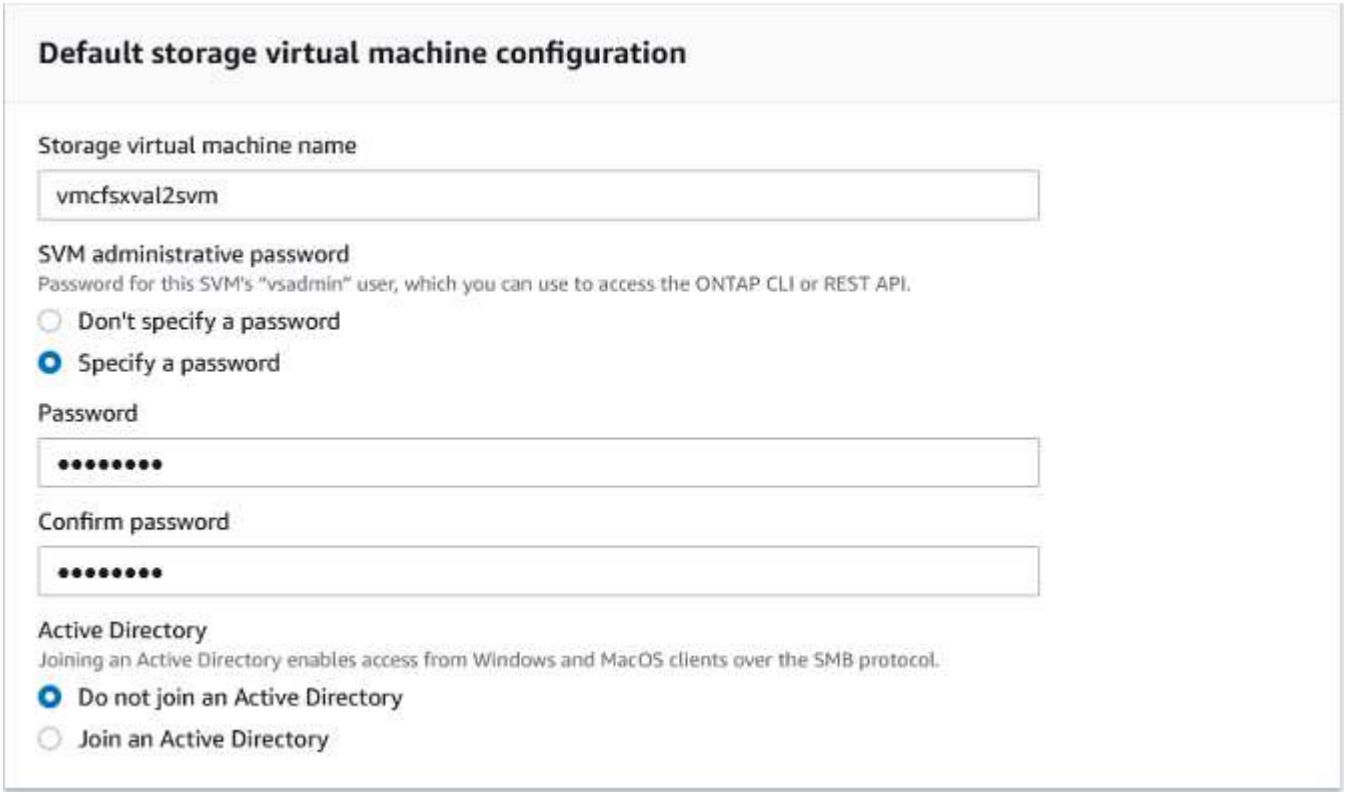


En la sección Redes, para Nube privada virtual (VPC), elija la VPC adecuada y las subredes preferidas junto con la tabla de rutas. En este caso, se selecciona vmcfsx2.vpc del menú desplegable.

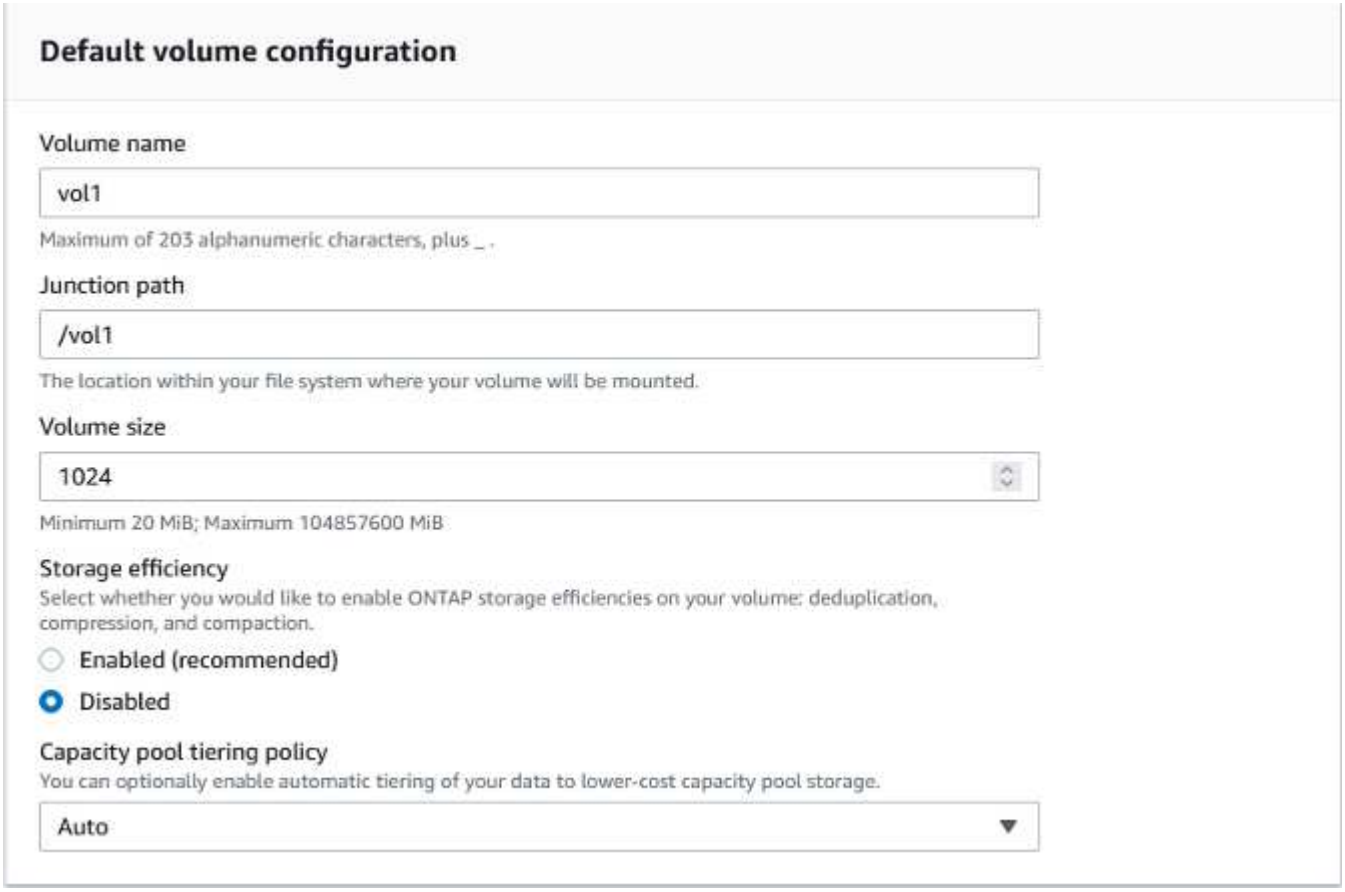
1. En la sección Seguridad y cifrado, para la Clave de cifrado, elija la clave de cifrado de AWS Key Management Service (AWS KMS) que protege los datos del sistema de archivos en reposo. Para la contraseña administrativa del sistema de archivos, ingrese una contraseña segura para el usuario fsxadmin.



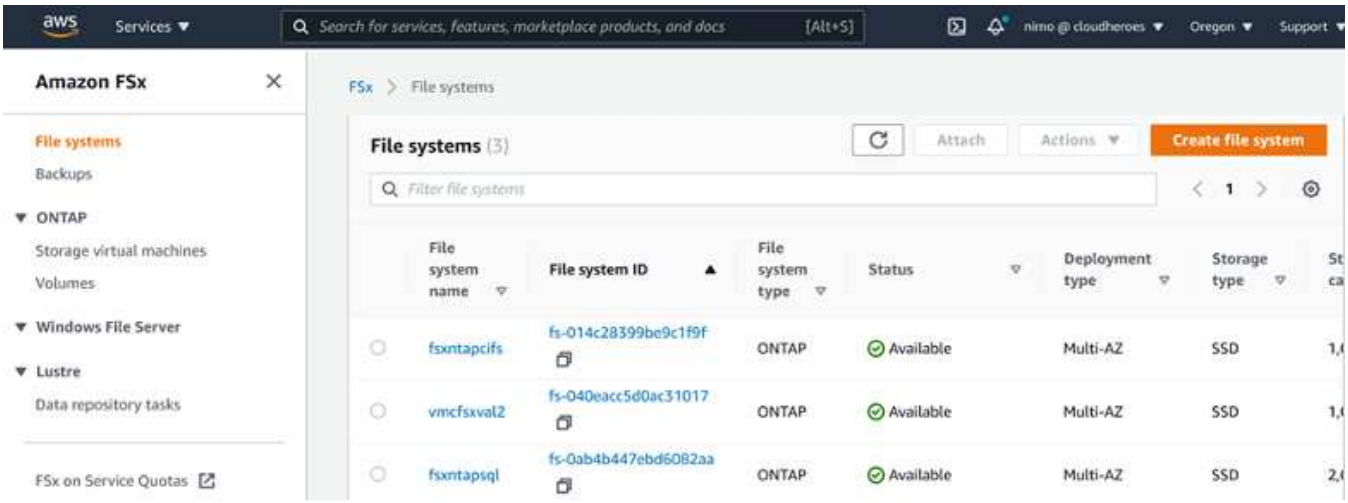
1. En la máquina virtual, especifique la contraseña que se utilizará con vsadmin para administrar ONTAP mediante las API REST o la CLI. Si no se especifica ninguna contraseña, se puede utilizar un usuario fsxadmin para administrar el SVM. En la sección Active Directory, asegúrese de unir Active Directory a la SVM para aprovisionar recursos compartidos SMB. En la sección Configuración de máquina virtual de almacenamiento predeterminada, proporcione un nombre para el almacenamiento. En esta validación, los recursos compartidos de SMB se aprovisionan mediante un dominio de Active Directory autoadministrado.

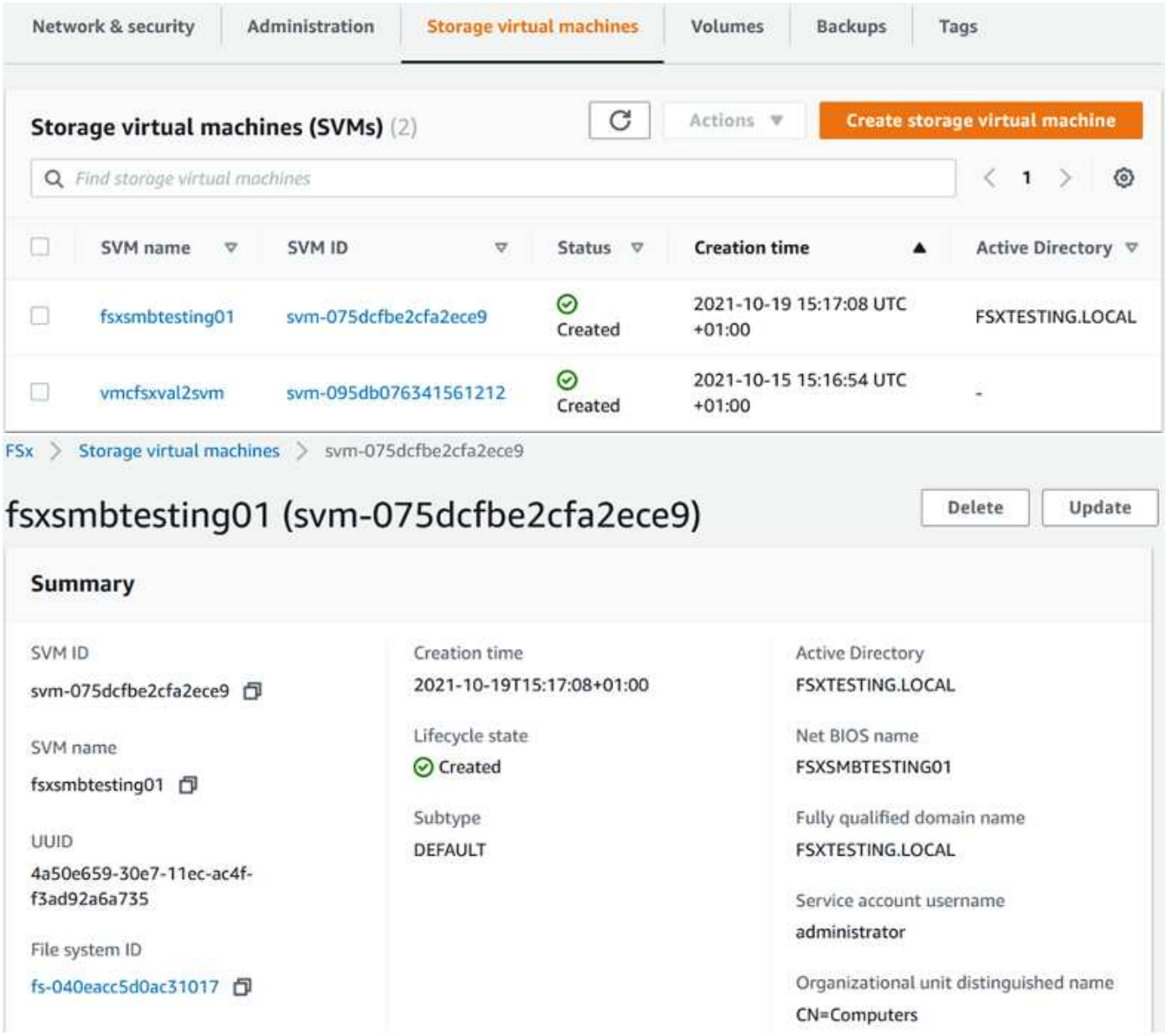


1. En la sección Configuración de volumen predeterminada, especifique el nombre y el tamaño del volumen. Este es un volumen NFS. Para Eficiencia de almacenamiento, elija Habilitado para activar las funciones de eficiencia de almacenamiento de ONTAP (compresión, deduplicación y compactación) o Deshabilitado para desactivarlas.



1. Revise la configuración del sistema de archivos que se muestra en la página Crear sistema de archivos.
2. Haga clic en Crear sistema de archivos.





Para obtener información más detallada, consulte"Introducción a Amazon FSx ONTAP" .

Después de crear el sistema de archivos como se indica arriba, cree el volumen con el tamaño y protocolo requeridos.

1. Abrir el"Consola de Amazon FSx" .
2. En el panel de navegación izquierdo, seleccione Sistemas de archivos y, a continuación, elija el sistema de archivos ONTAP para el que desea crear un volumen.
3. Seleccione la pestaña Volúmenes.
4. Seleccione la pestaña Crear volumen.
5. Aparece el cuadro de diálogo Crear volumen.

Para fines de demostración, en esta sección se crea un volumen NFS que se puede montar fácilmente en máquinas virtuales que se ejecutan en VMware Cloud en AWS. nfsdemovol01 se crea como se muestra a continuación:



▼ **Montar el volumen FSx ONTAP en el cliente Linux**

Para montar el volumen FSx ONTAP creado en el paso anterior desde las máquinas virtuales Linux dentro de VMC en AWS SDDC, complete los siguientes pasos:

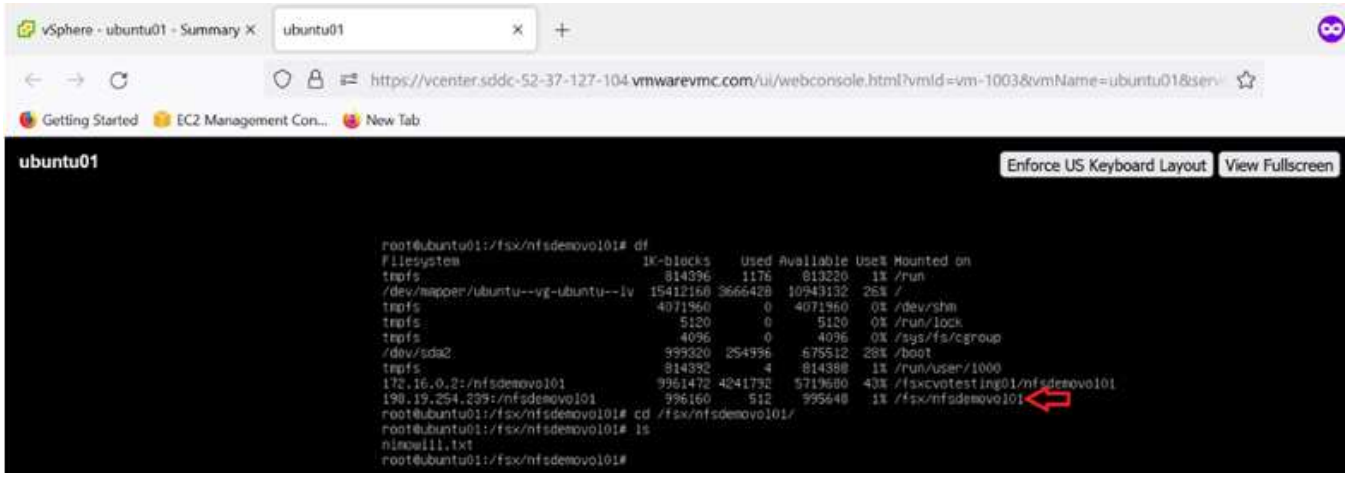
1. Conectarse a la instancia de Linux designada.
2. Abra una terminal en la instancia usando Secure Shell (SSH) e inicie sesión con las credenciales adecuadas.
3. Cree un directorio para el punto de montaje del volumen con el siguiente comando:

```
 $ sudo mkdir /fsx/nfsdemovol01
. Monte el volumen NFS de Amazon FSx ONTAP en el directorio que se
creó en el paso anterior.
```

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. Una vez ejecutado, ejecute el comando df para validar el montaje.



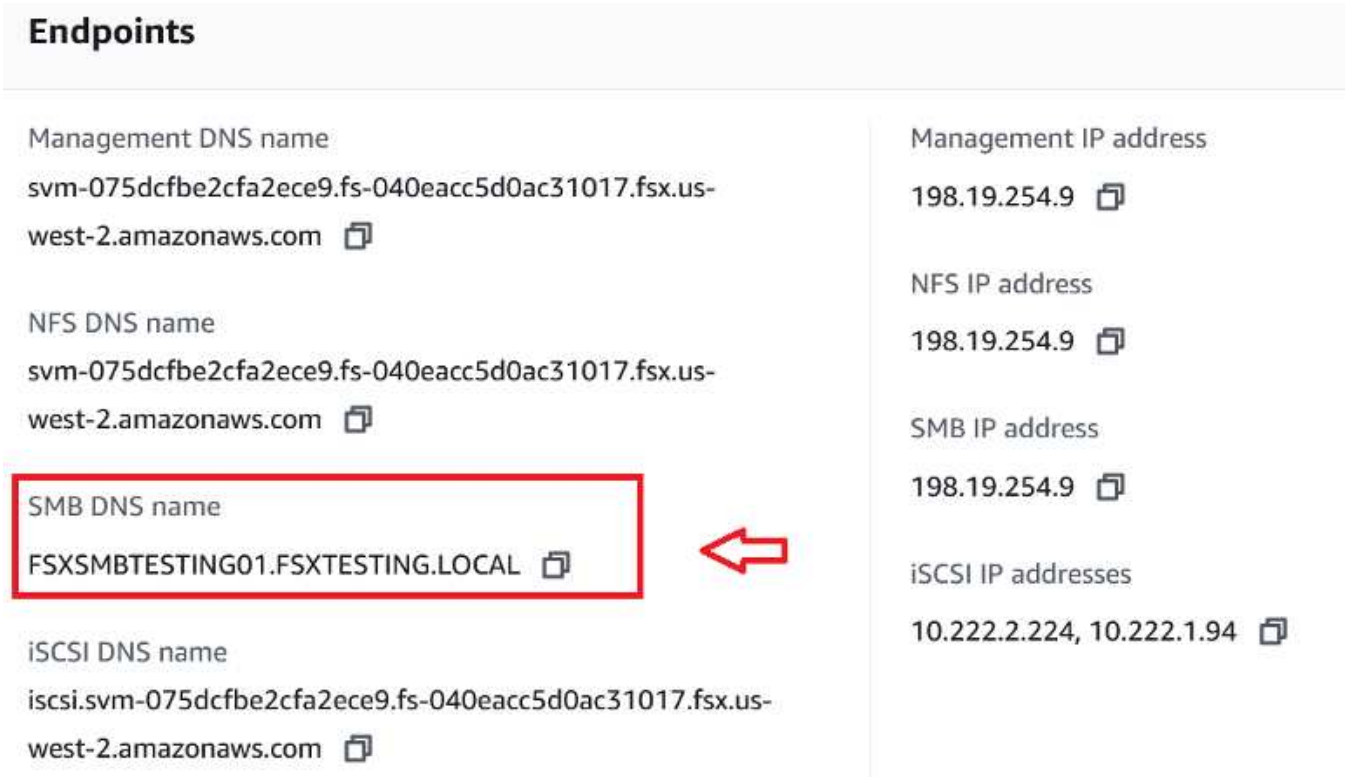
Montar el volumen FSx ONTAP en el cliente Linux

▼ **Adjuntar volúmenes de FSx ONTAP a clientes de Microsoft Windows**

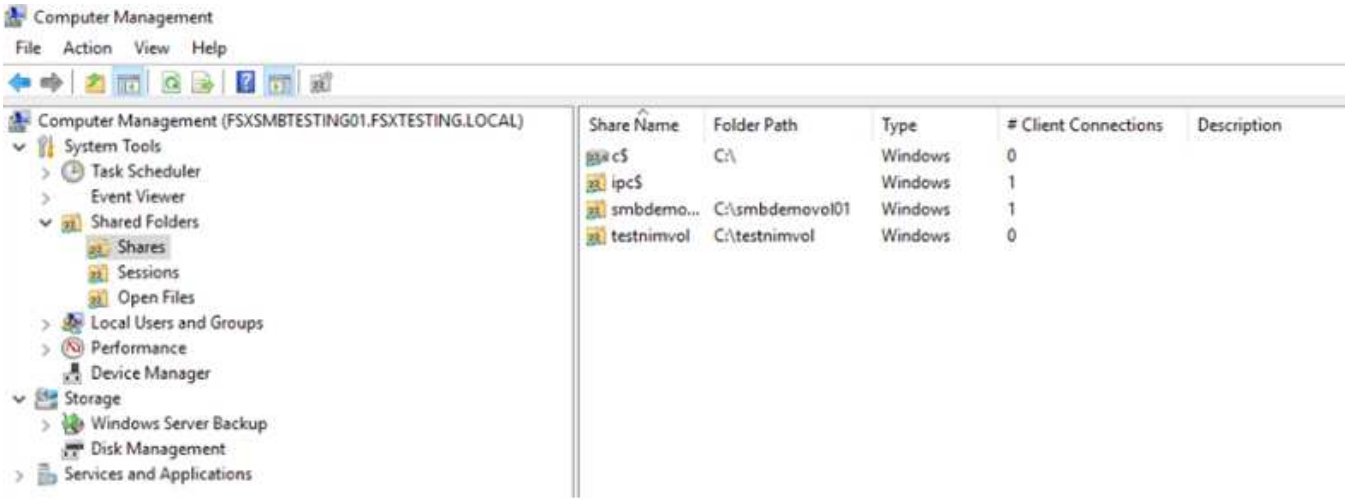
Para administrar y mapear recursos compartidos de archivos en un sistema de archivos de Amazon FSx , se debe utilizar la GUI de Carpetas compartidas.

1. Abra el menú Inicio y ejecute fsmgmt.msc usando Ejecutar como administrador. Al hacer esto se abre la herramienta GUI de Carpetas compartidas.
2. Haga clic en Acción > Todas las tareas y elija Conectar a otra computadora.
3. Para otra computadora, ingrese el nombre DNS de la máquina virtual de almacenamiento (SVM). Por ejemplo, en este ejemplo se utiliza FSXSMBTESTING01.FSXTESTING.LOCAL.

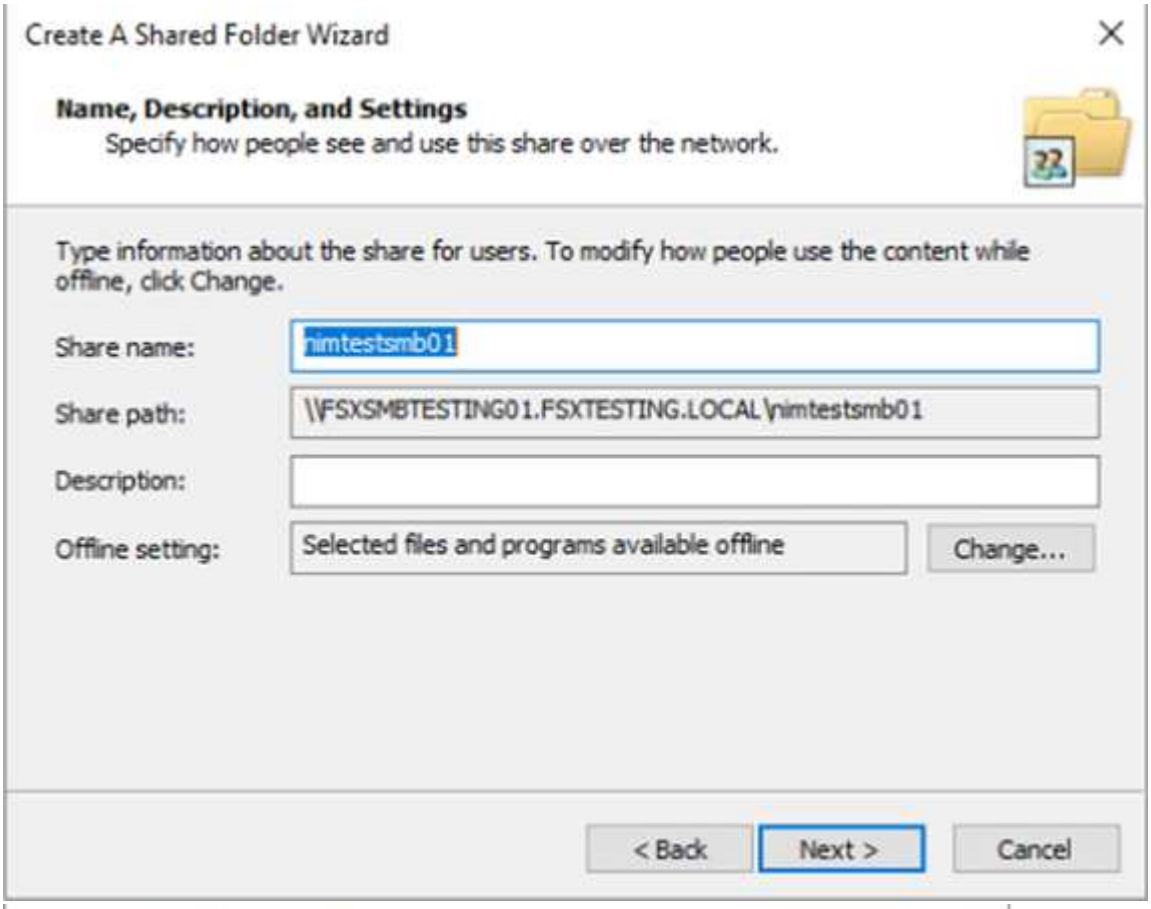
> ⓘ Para encontrar el nombre DNS de SVM en la consola de Amazon FSx , seleccione Máquinas virtuales de almacenamiento, seleccione SVM y luego desplácese hacia abajo hasta Puntos finales para encontrar el nombre DNS de SMB. Haga clic en Aceptar. El sistema de archivos de Amazon FSx aparece en la lista de carpetas compartidas.



1. En la herramienta Carpetas compartidas, seleccione Recursos compartidos en el panel izquierdo para ver los recursos compartidos activos para el sistema de archivos de Amazon FSx .



1. Ahora elija un nuevo recurso compartido y complete el asistente Crear una carpeta compartida.

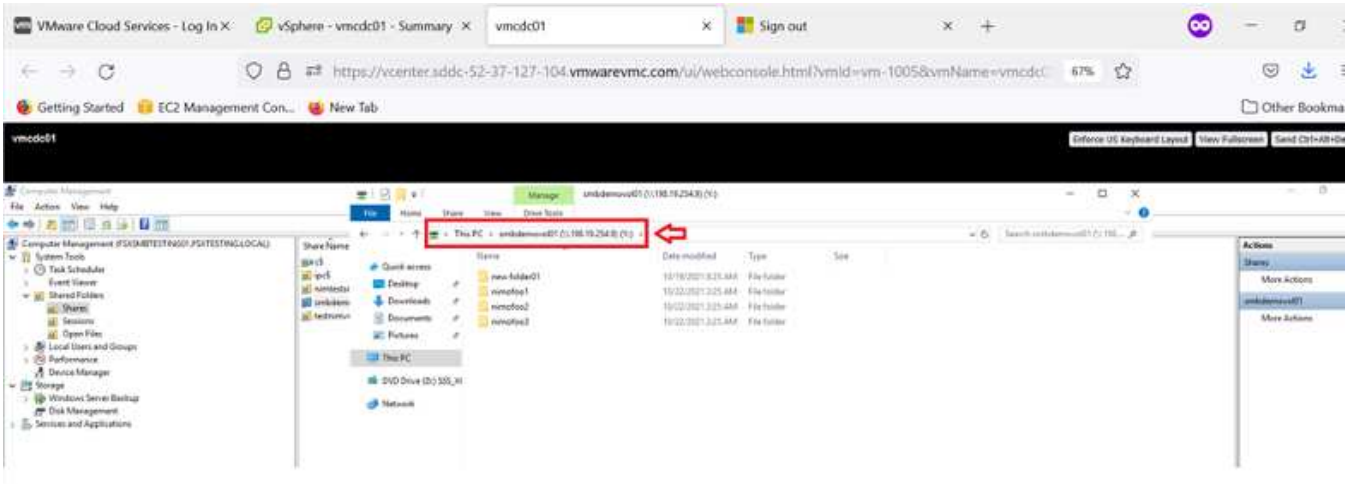




Para obtener más información sobre cómo crear y administrar recursos compartidos SMB en un sistema de archivos de Amazon FSx , consulte"Creación de recursos compartidos SMB" .

1. Una vez establecida la conectividad, se puede conectar el recurso compartido SMB y usarlo para datos

de la aplicación. Para lograr esto, copie la ruta compartida y use la opción Asignar unidad de red para montar el volumen en la VM que se ejecuta en VMware Cloud en AWS SDDC.



▼ **Conecte un LUN de FSx ONTAP a un host mediante iSCSI**

Conecte un LUN de FSx ONTAP a un host mediante iSCSI

El tráfico iSCSI para FSx atraviesa VMware Transit Connect/AWS Transit Gateway a través de las rutas proporcionadas en la sección anterior. Para configurar un LUN en Amazon FSx ONTAP, siga la documentación que se encuentra"aquí" .

En los clientes Linux, asegúrese de que el demonio iSCSI se esté ejecutando. Una vez aprovisionados los LUN, consulte la guía detallada sobre la configuración de iSCSI con Ubuntu (como ejemplo)"aquí" .

En este artículo se describe la conexión del LUN iSCSI a un host Windows:

▼ **Aprovisionar un LUN en FSx ONTAP:**

1. Acceda a la CLI de NetApp ONTAP mediante el puerto de administración de FSx para el sistema de archivos ONTAP .
2. Cree los LUN con el tamaño requerido como lo indica la salida de tamaño.

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

En este ejemplo, creamos un LUN de tamaño 5g (5368709120).

1. Cree los igroups necesarios para controlar qué hosts tienen acceso a LUN específicos.

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators
```

```
--------- ------------ -------- --------
-----------------------------------

vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

Se mostraron dos entradas.

1. Asigne los LUN a igroups mediante el siguiente comando:

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------- ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

Se mostraron dos entradas.

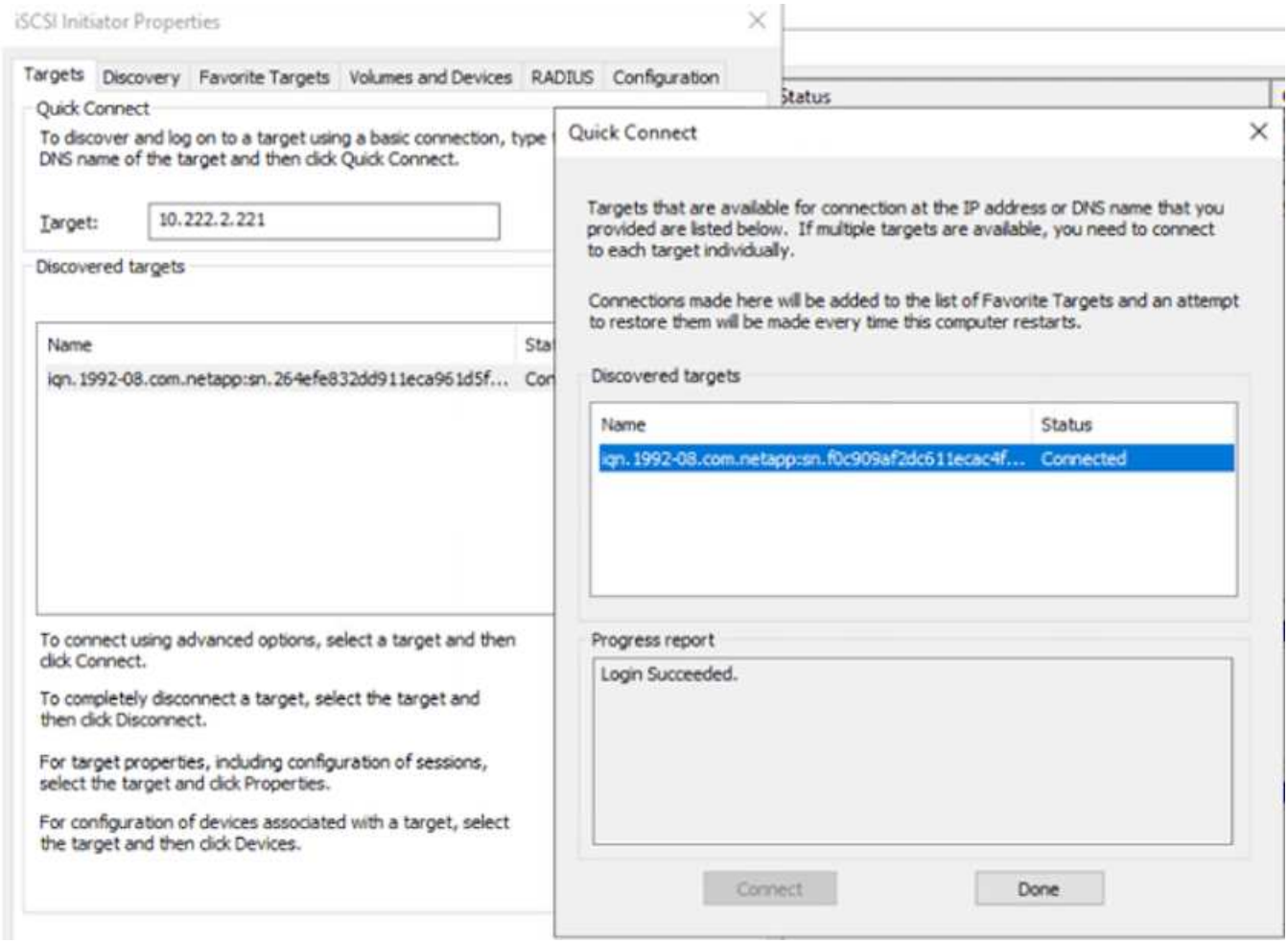
1. Conecte el LUN recién aprovisionado a una máquina virtual de Windows:

Para conectar el nuevo LUN a un host de Windows que reside en VMware Cloud en AWS SDDC, complete los siguientes pasos:

1. RDP a la máquina virtual de Windows alojada en VMware Cloud en AWS SDDC.

2. Vaya a Administrador del servidor > Panel de control > Herramientas > Iniciador iSCSI para abrir el cuadro de diálogo Propiedades del iniciador iSCSI.
3. Desde la pestaña Descubrimiento, haga clic en Descubrir portal o Agregar portal y luego ingrese la dirección IP del puerto de destino iSCSI.
4. Desde la pestaña Objetivos, seleccione el objetivo descubierto y luego haga clic en Iniciar sesión o Conectar.
5. Seleccione Habilitar múltiples rutas y luego seleccione "Restaurar esta conexión automáticamente cuando se inicia la computadora" o "Agregar esta conexión a la lista de destinos favoritos". Haga clic en Avanzado.

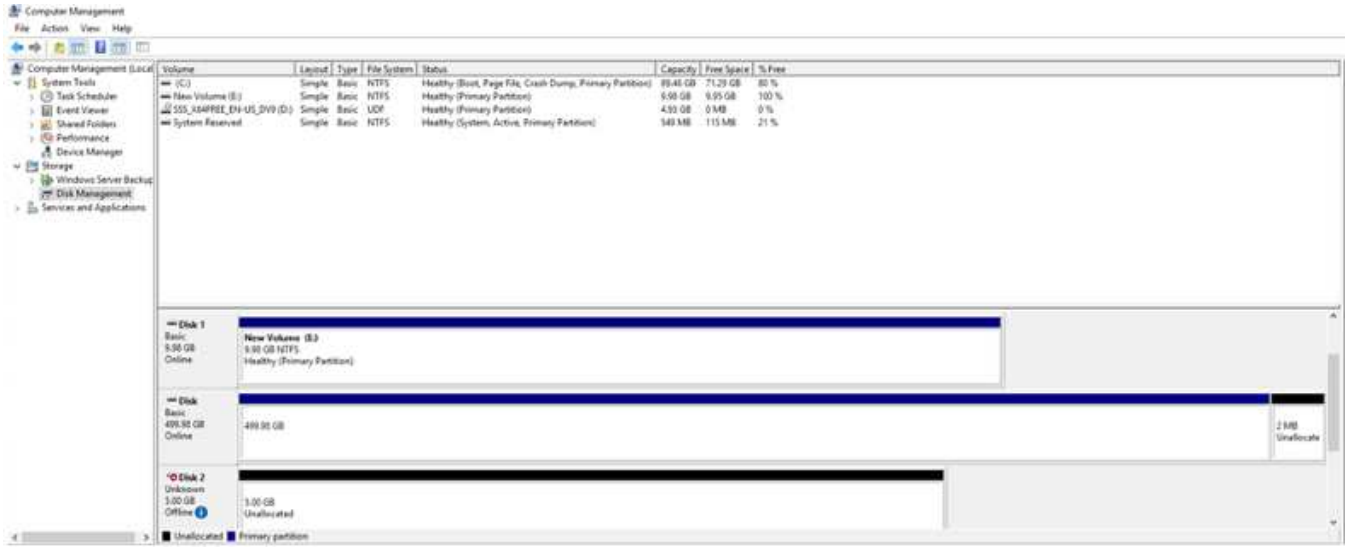
El host de Windows debe tener una conexión iSCSI a cada nodo del clúster. El DSM nativo selecciona las mejores rutas a utilizar.



Los LUN en la máquina virtual de almacenamiento (SVM) aparecen como discos para el host de Windows. El host no detecta automáticamente ningún disco nuevo que se agregue. Active un nuevo escaneo manual para descubrir los discos completando los siguientes pasos:

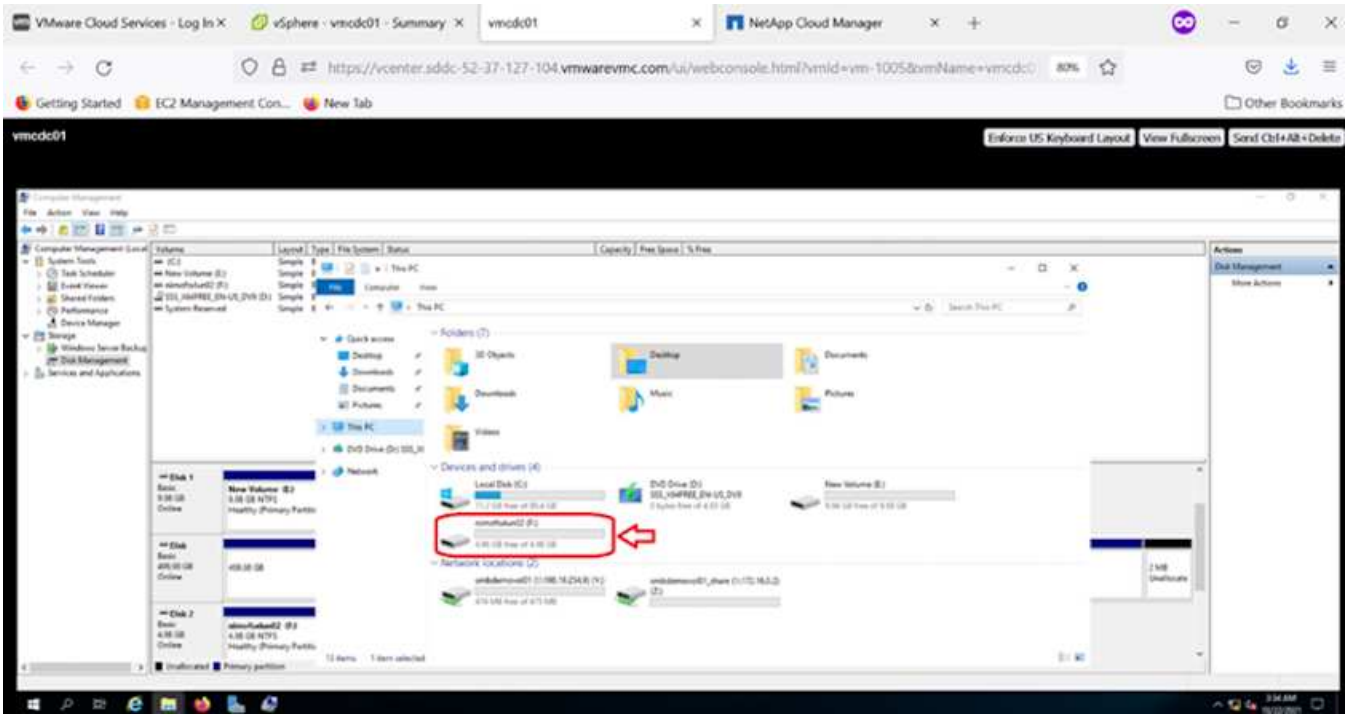
1. Abra la utilidad de Administración de equipos de Windows: Inicio > Herramientas administrativas > Administración de equipos.
2. Expanda el nodo Almacenamiento en el árbol de navegación.
3. Haga clic en Administración de discos.

4. Haga clic en Acción > Volver a escanear discos.



Cuando el host de Windows accede por primera vez a un nuevo LUN, éste no tiene partición ni sistema de archivos. Inicialice el LUN y, opcionalmente, formatee el LUN con un sistema de archivos completando los siguientes pasos:

1. Inicie la Administración de discos de Windows.
2. Haga clic con el botón derecho en el LUN y luego seleccione el tipo de disco o partición requerido.
3. Siga las instrucciones del asistente. En este ejemplo, la unidad F: está montada.



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, o CVO, es la solución de gestión de datos en la nube líder en la industria basada en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Es una versión definida por software de ONTAP que consume almacenamiento nativo de la nube, lo que le permite tener el mismo software de almacenamiento en la nube y en las instalaciones, lo que reduce la necesidad de volver a capacitar a su personal de TI en métodos completamente nuevos para administrar sus datos.

CVO brinda a los clientes la capacidad de mover datos sin problemas desde el borde al centro de datos, a la nube y viceversa, unificando su nube híbrida, todo administrado con una consola de administración de panel único, NetApp Cloud Manager.

Por diseño, CVO ofrece un rendimiento extremo y capacidades avanzadas de gestión de datos para satisfacer incluso sus aplicaciones más exigentes en la nube.

Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados

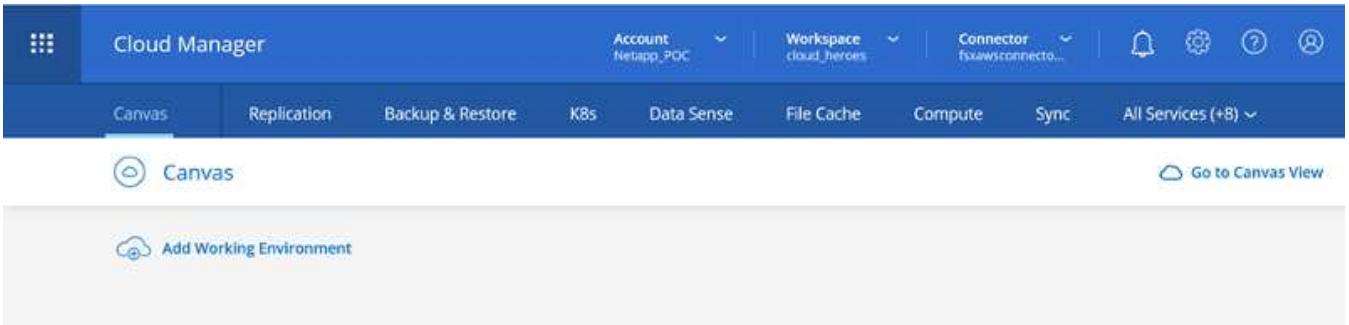
▼ **Implemente una nueva instancia de Cloud Volumes ONTAP en AWS (hágalo usted mismo)**

Los recursos compartidos y LUN de Cloud Volumes ONTAP se pueden montar desde máquinas virtuales creadas en el entorno SDDC de VMware Cloud on AWS. Los volúmenes también se pueden montar en clientes Windows de AWS VM Linux nativos, y se puede acceder a los LUN en clientes Linux o Windows como dispositivos de bloque cuando se montan sobre iSCSI porque Cloud Volumes ONTAP admite los protocolos iSCSI, SMB y NFS. Los volúmenes de Cloud Volumes ONTAP se pueden configurar en unos pocos y sencillos pasos.

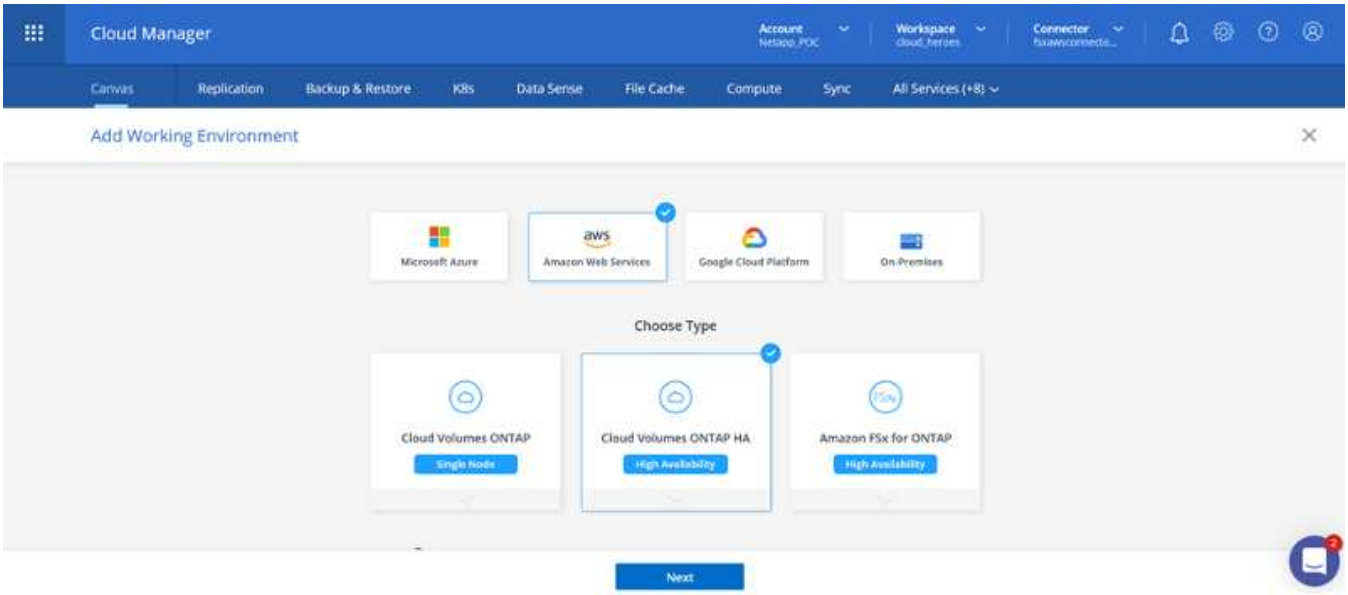
Para replicar volúmenes de un entorno local a la nube con fines de recuperación ante desastres o migración, establezca conectividad de red a AWS, ya sea mediante una VPN de sitio a sitio o DirectConnect. La replicación de datos desde las instalaciones locales a Cloud Volumes ONTAP está fuera del alcance de este documento. Para replicar datos entre sistemas locales y Cloud Volumes ONTAP , consulte"Configuración de la replicación de datos entre sistemas" .

Utiliza "Dimensionador de Cloud Volumes ONTAP" para dimensionar con precisión las instancias de Cloud Volumes ONTAP. Además, supervisa el rendimiento local para utilizar esos datos como información de entrada en la herramienta de dimensionamiento de Cloud Volumes ONTAP.

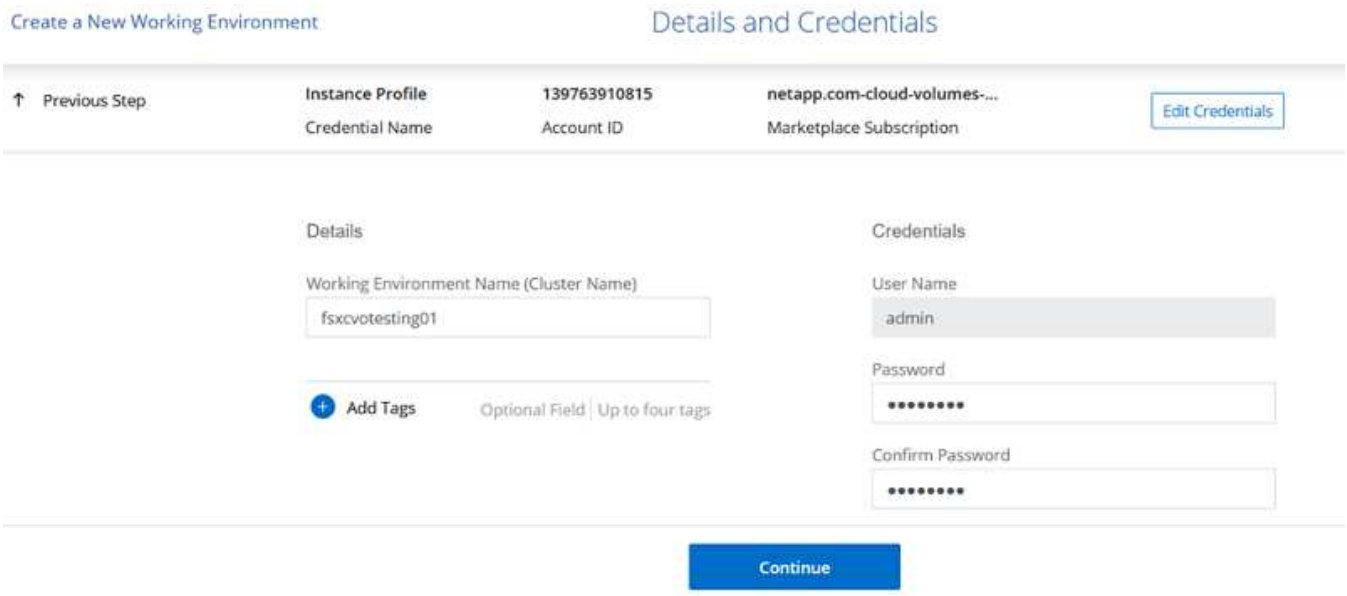
1. Inicie sesión en NetApp Cloud Central; se muestra la pantalla Vista de Fabric. Localice la pestaña Cloud Volumes ONTAP y seleccione Ir a Cloud Manager. Después de iniciar sesión, se mostrará la pantalla Canvas.



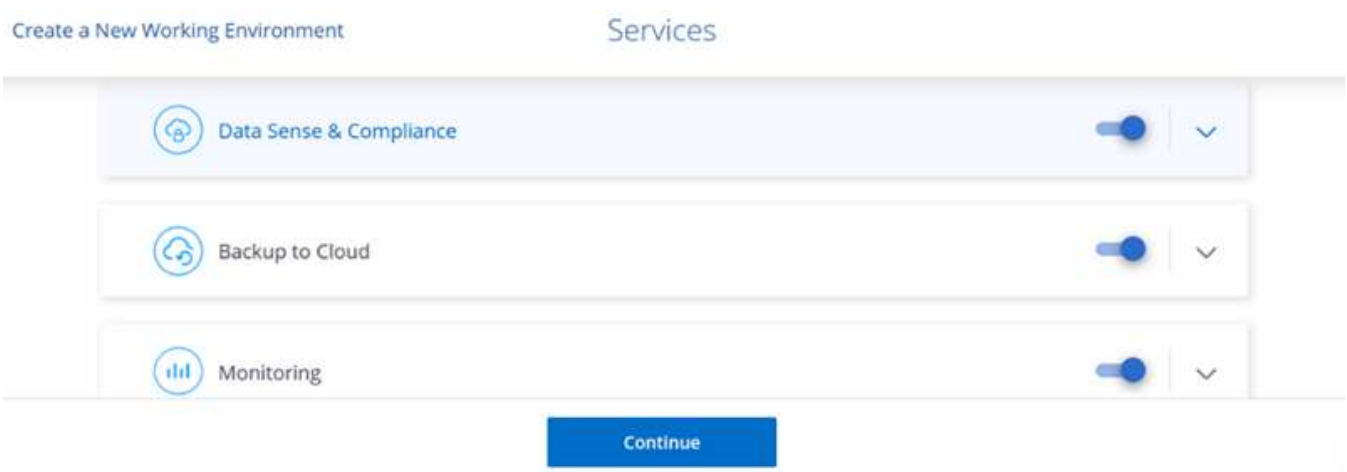
1. En la página de inicio de Cloud Manager, haga clic en Agregar un entorno de trabajo y luego seleccione AWS como la nube y el tipo de configuración del sistema.



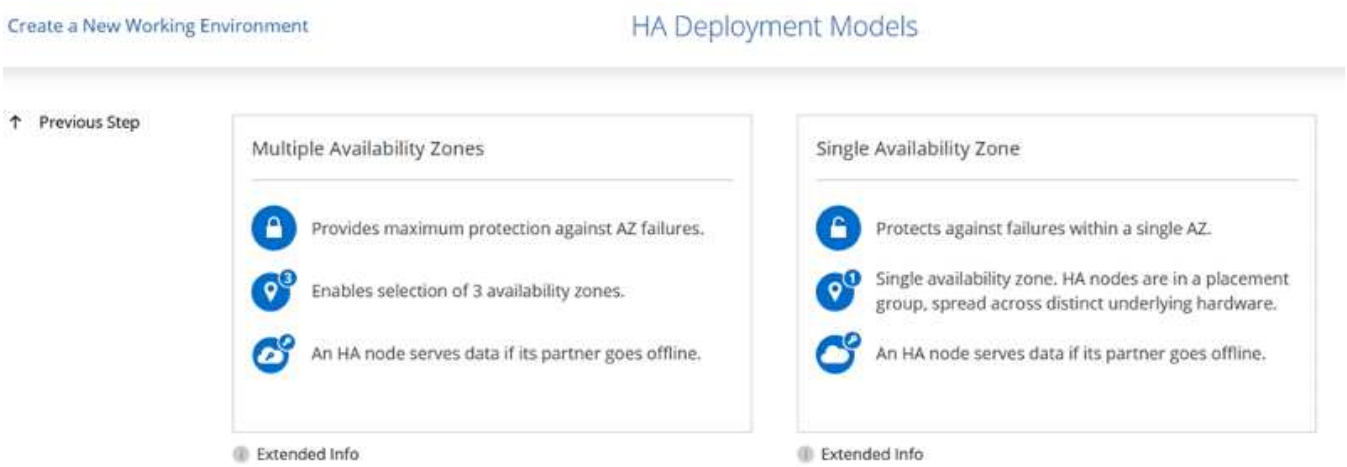
1. Proporcione los detalles del entorno que se creará, incluido el nombre del entorno y las credenciales de administrador. Haga clic en Continuar.



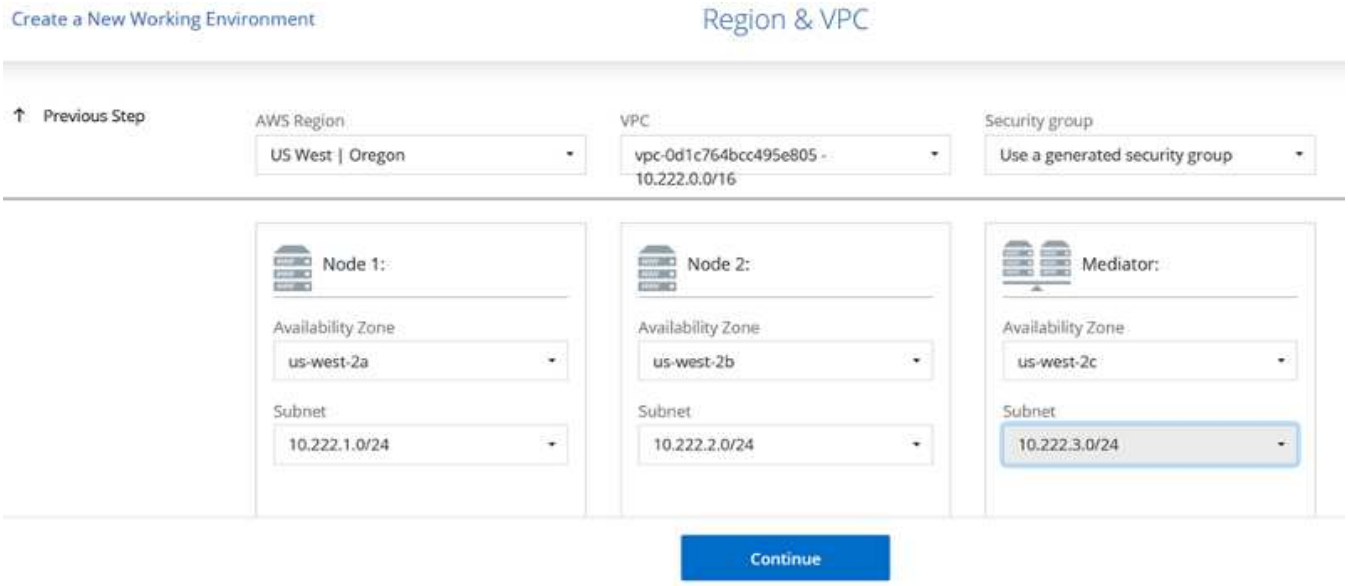
1. Selecciona los servicios complementarios para la implementación de Cloud Volumes ONTAP, incluidos NetApp Data Classification, NetApp Backup and Recovery y Data Infrastructure Insights. Haz clic en Continue.



1. En la página Modelos de implementación de HA, elija la configuración Zonas de disponibilidad múltiples.

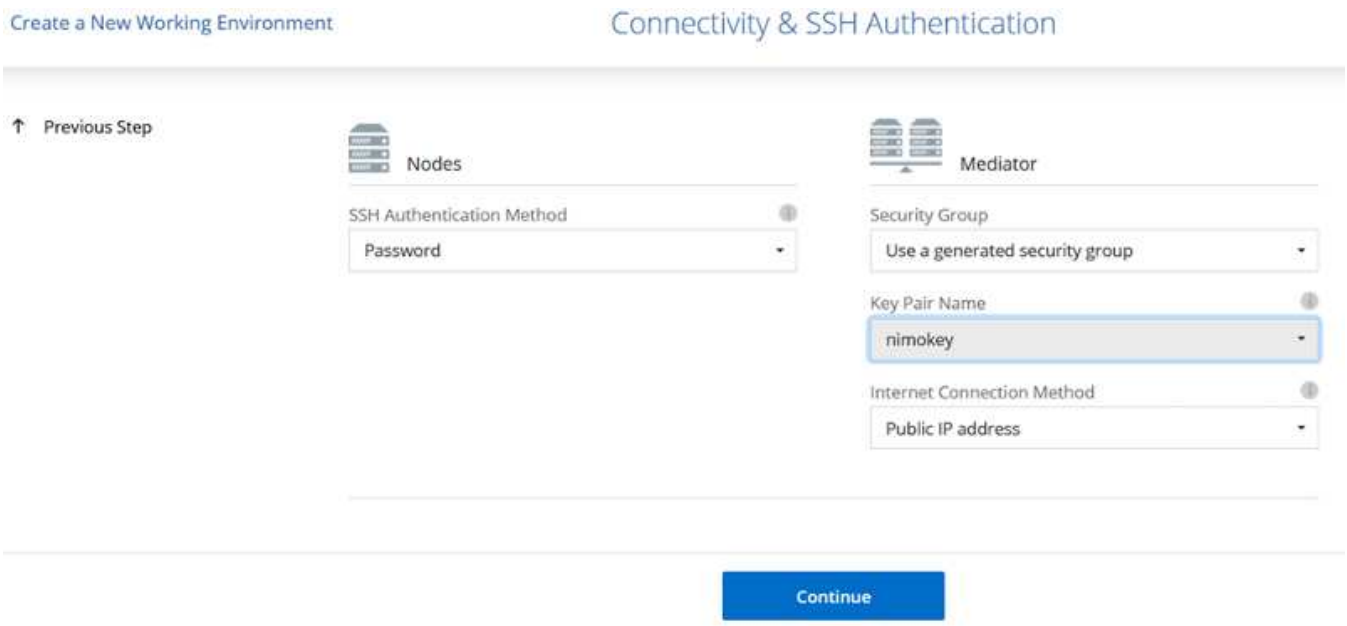


1. En la página Región y VPC, ingrese la información de la red y luego haga clic en Continuar.

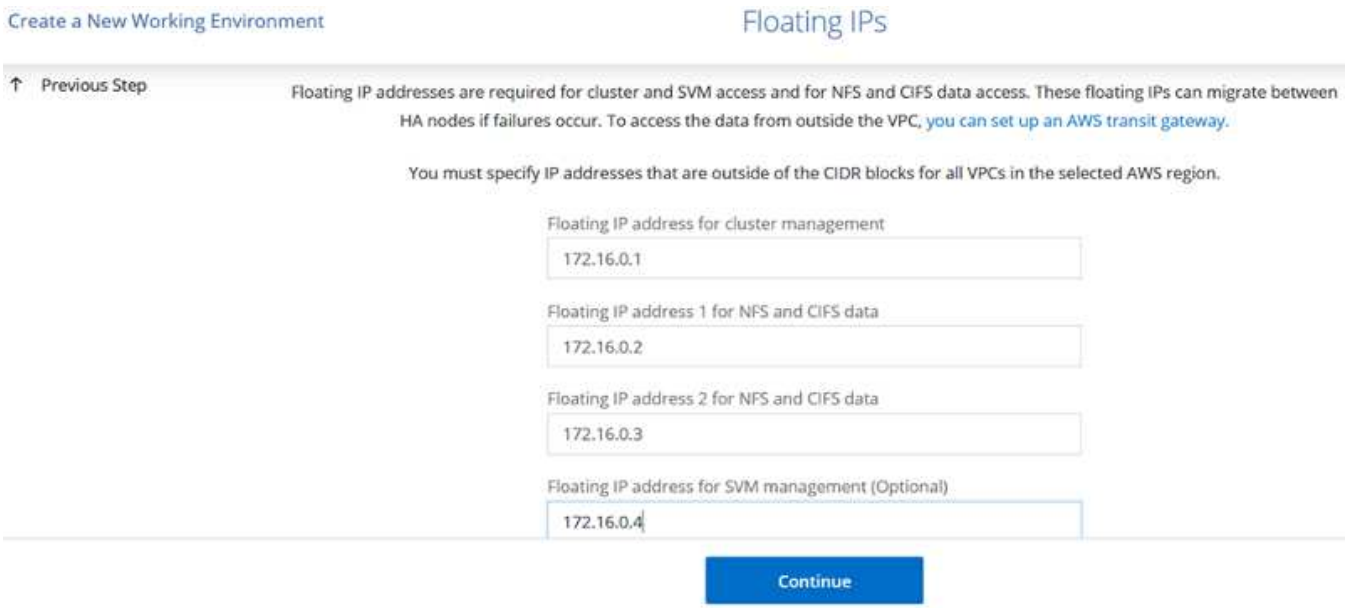


1. En la página Conectividad y autenticación SSH, elija los métodos de conexión para el par HA y el

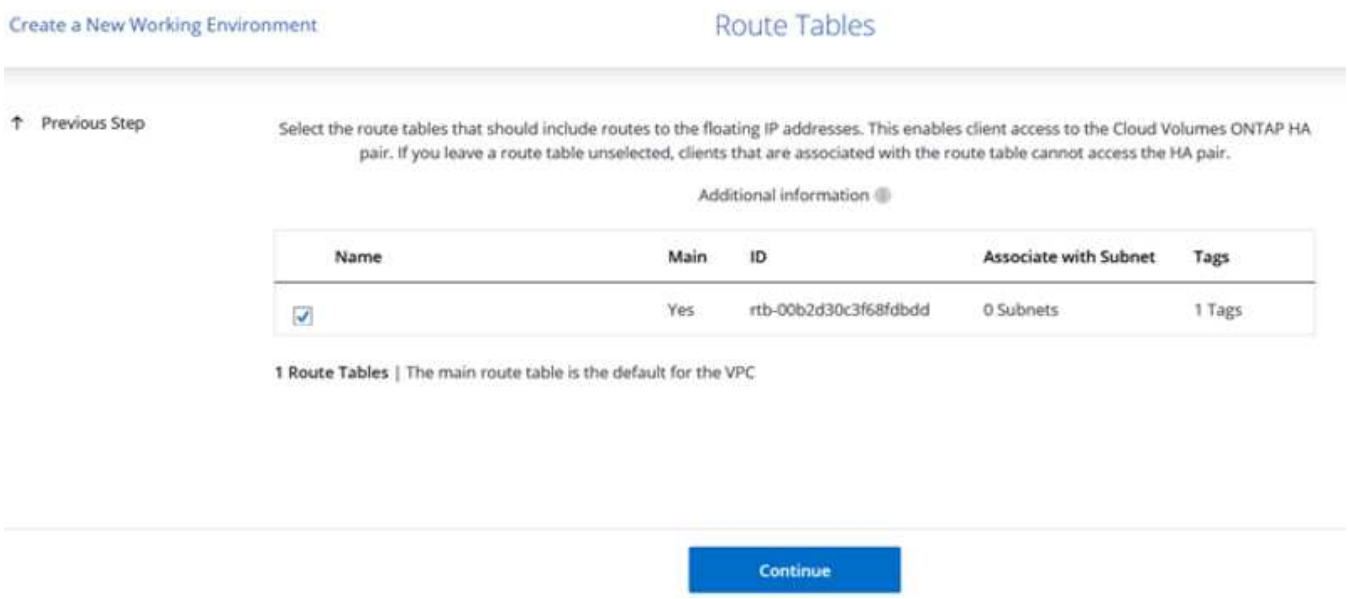
mediador.



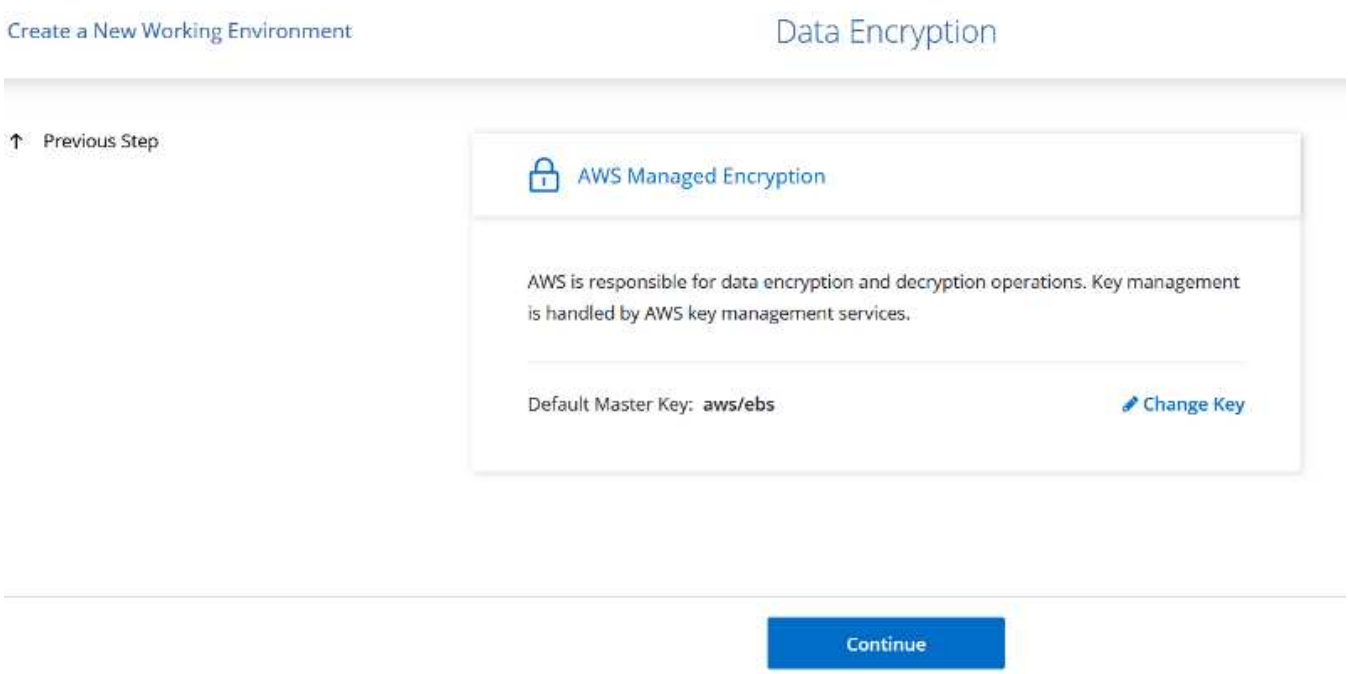
1. Especifique las direcciones IP flotantes y luego haga clic en Continuar.



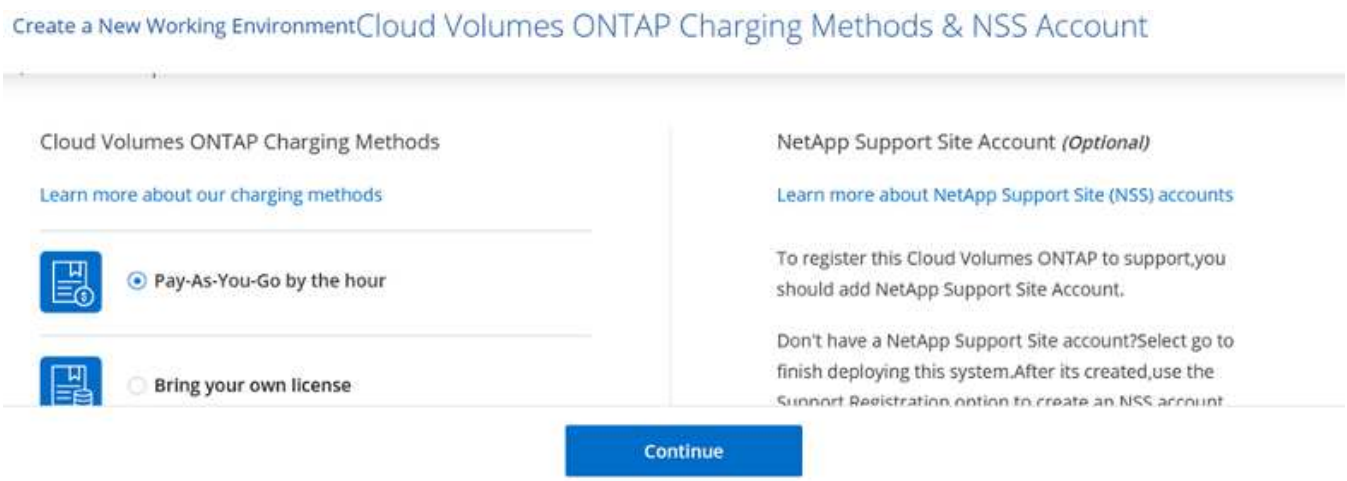
1. Seleccione las tablas de rutas adecuadas para incluir rutas a las direcciones IP flotantes y luego haga clic en Continuar.



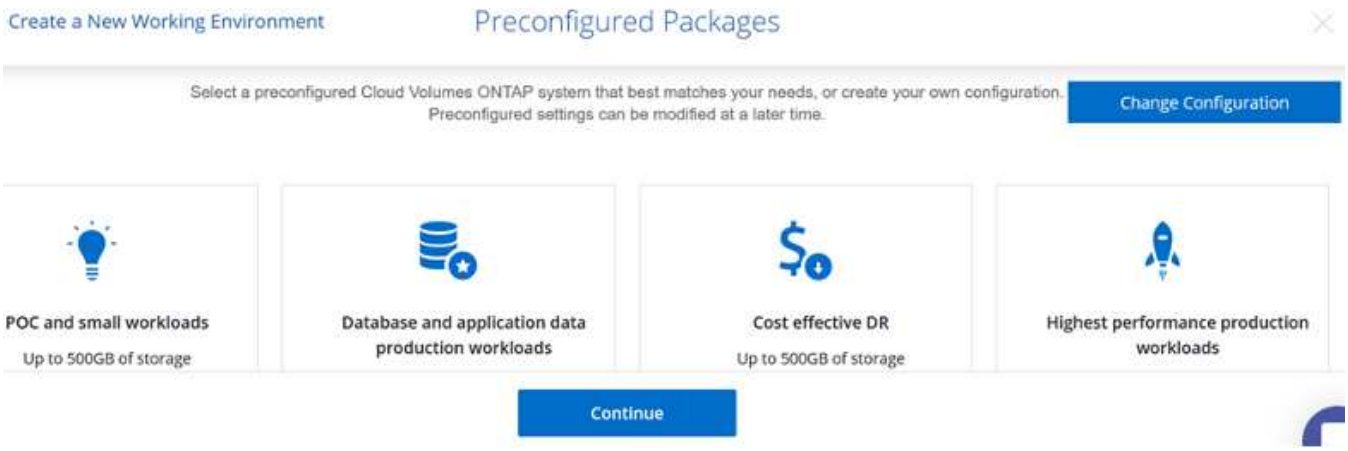
1. En la página Cifrado de datos, elija cifrado administrado por AWS.



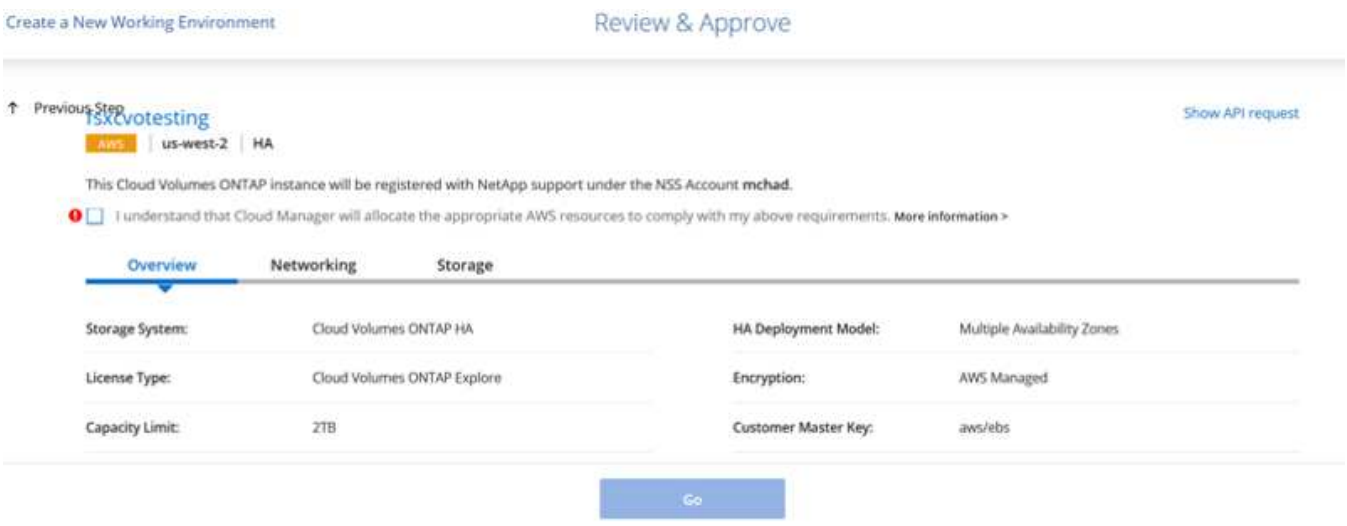
1. Seleccione la opción de licencia: Pago por uso o BYOL para utilizar una licencia existente. En este ejemplo se utiliza la opción de pago por uso.



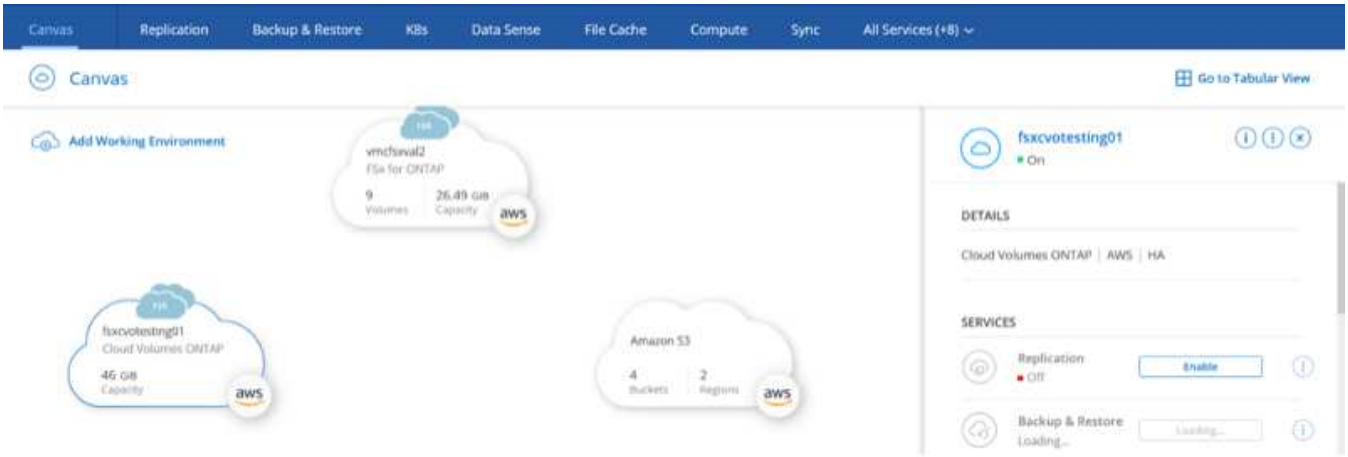
1. Seleccione entre varios paquetes preconfigurados disponibles según el tipo de carga de trabajo que se implementará en las máquinas virtuales que se ejecutan en VMware Cloud en AWS SDDC.



1. En la página Revisar y aprobar, revise y confirme las selecciones. Para crear la instancia de Cloud Volumes ONTAP , haga clic en Ir.

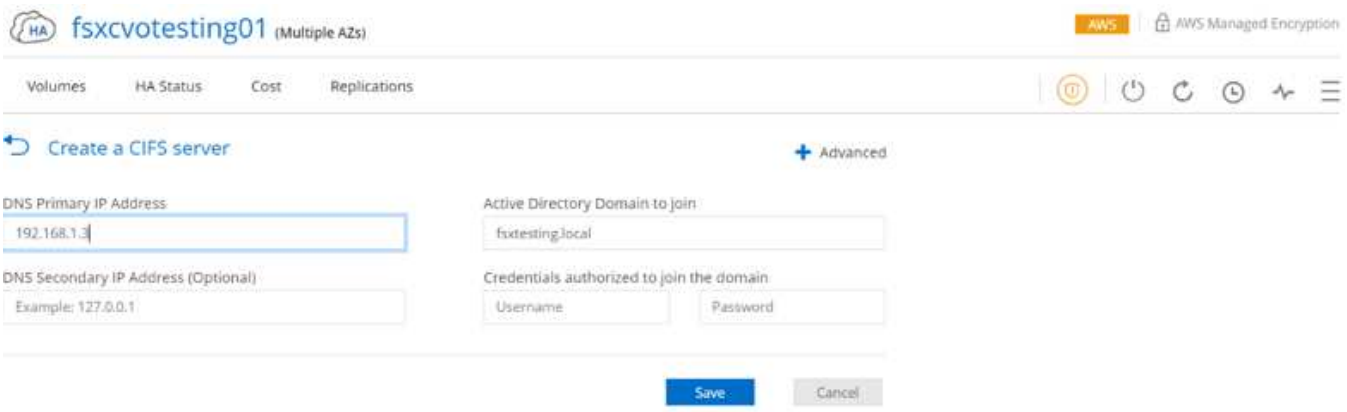


1. Una vez aprovisionado Cloud Volumes ONTAP , aparece en los entornos de trabajo en la página Canvas.

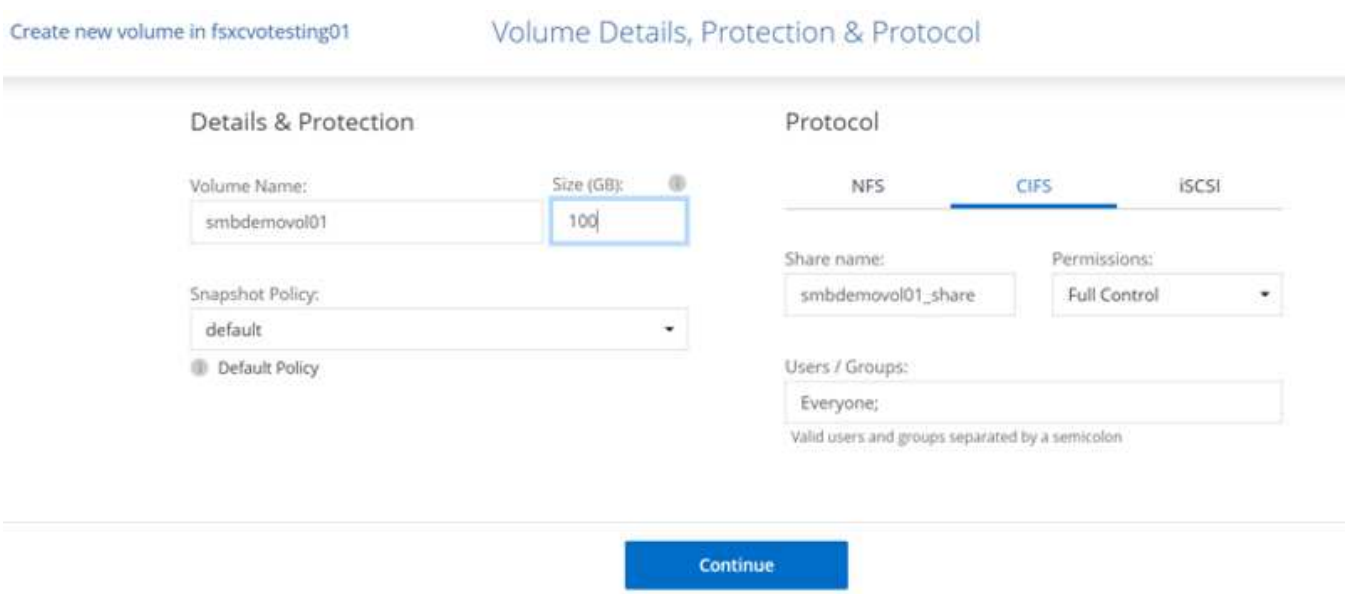


▼ **Configuraciones adicionales para volúmenes SMB**

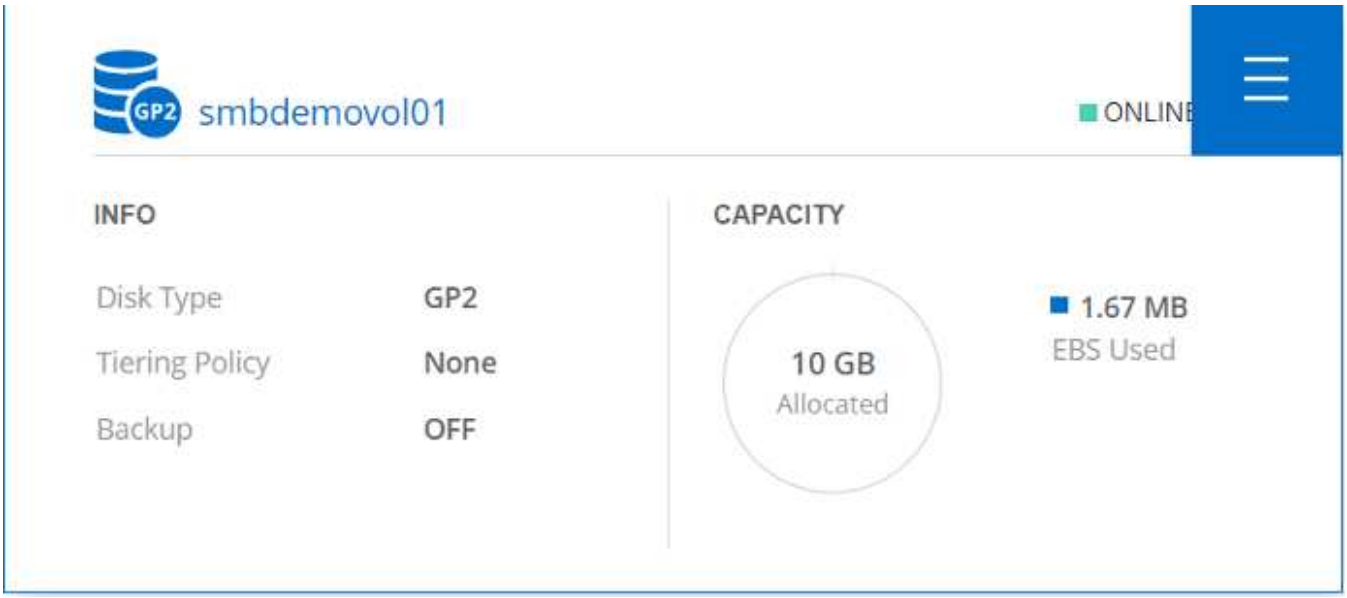
1. Una vez que el entorno de trabajo esté listo, asegúrese de que el servidor CIFS esté configurado con los parámetros de configuración de DNS y Active Directory adecuados. Este paso es necesario antes de poder crear el volumen SMB.



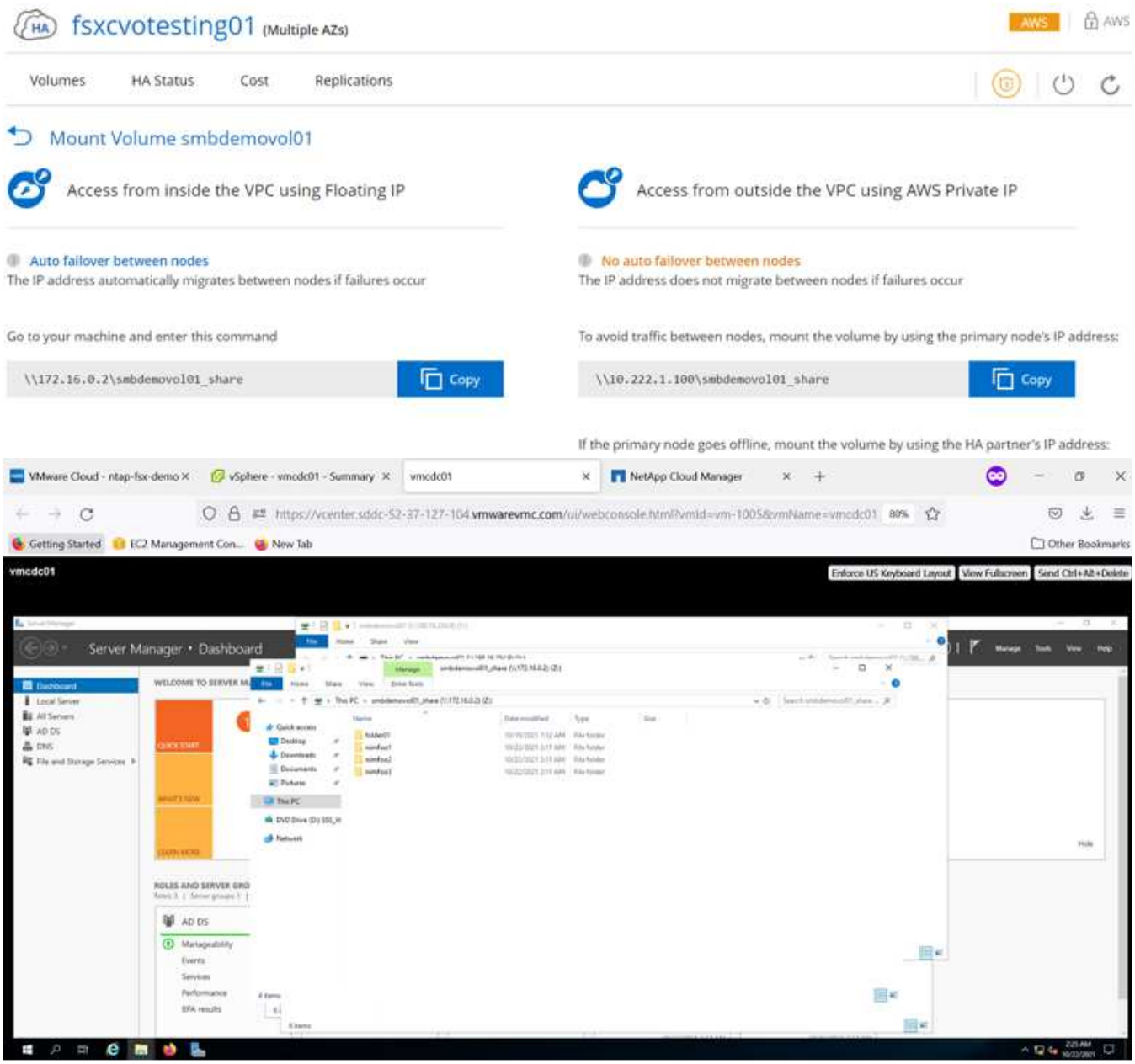
1. Seleccione la instancia CVO para crear el volumen y haga clic en la opción Crear volumen. Elija el tamaño apropiado y el administrador de la nube elige el agregado contenedor o utiliza un mecanismo de asignación avanzado para colocarlo en un agregado específico. Para esta demostración, se selecciona SMB como protocolo.



1. Una vez aprovisionado el volumen, estará disponible en el panel Volúmenes. Dado que se aprovisiona un recurso compartido CIFS, debe otorgar a sus usuarios o grupos permiso para acceder a los archivos y carpetas, y verificar que esos usuarios puedan acceder al recurso compartido y crear un archivo.



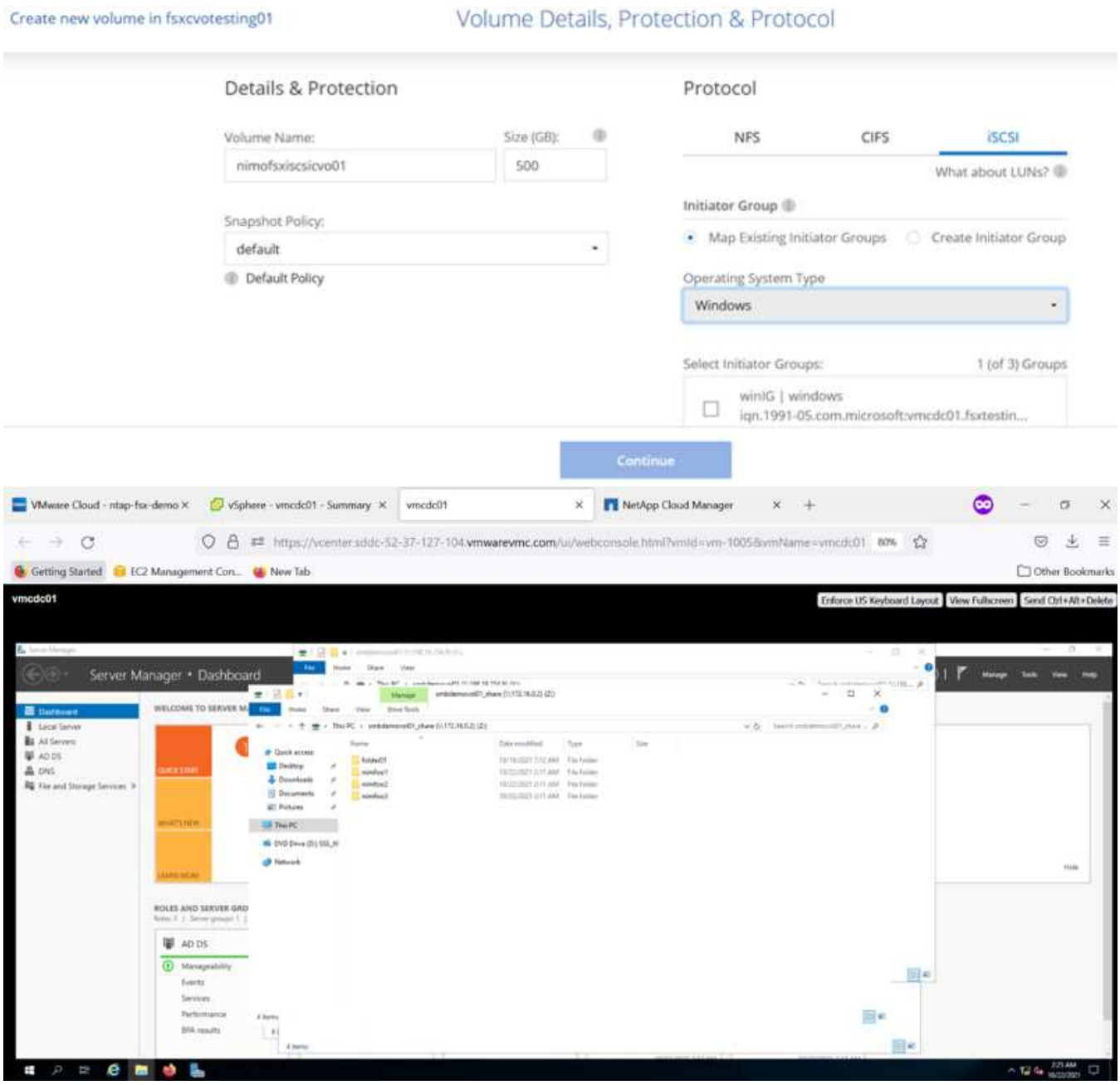
1. Una vez creado el volumen, use el comando mount para conectarse al recurso compartido desde la máquina virtual que se ejecuta en los hosts VMware Cloud en AWS SDDC.
2. Copie la siguiente ruta y use la opción Asignar unidad de red para montar el volumen en la máquina virtual que se ejecuta en VMware Cloud en AWS SDDC.



▼ **Conectar el LUN a un host**

Para conectar el LUN de Cloud Volumes ONTAP a un host, complete los siguientes pasos:

1. En la página Canvas de Cloud Manager, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP para crear y administrar volúmenes.
2. Haga clic en Agregar volumen > Nuevo volumen, seleccione iSCSI y haga clic en Crear grupo de iniciadores. Haga clic en Continuar.



1. Una vez aprovisionado el volumen, seleccione el volumen y haga clic en IQN de destino. Para copiar el nombre calificado iSCSI (IQN), haga clic en Copiar. Configure una conexión iSCSI desde el host al LUN.

Para lograr lo mismo para el host que reside en VMware Cloud on AWS SDDC, complete los siguientes pasos:

1. RDP a la máquina virtual alojada en VMware Cloud en AWS.
2. Abra el cuadro de diálogo Propiedades del iniciador iSCSI: Administrador del servidor > Panel de control > Herramientas > Iniciador iSCSI.
3. Desde la pestaña Descubrimiento, haga clic en Descubrir portal o Agregar portal y luego ingrese la dirección IP del puerto de destino iSCSI.
4. Desde la pestaña Objetivos, seleccione el objetivo descubierto y luego haga clic en Iniciar sesión o Conectar.

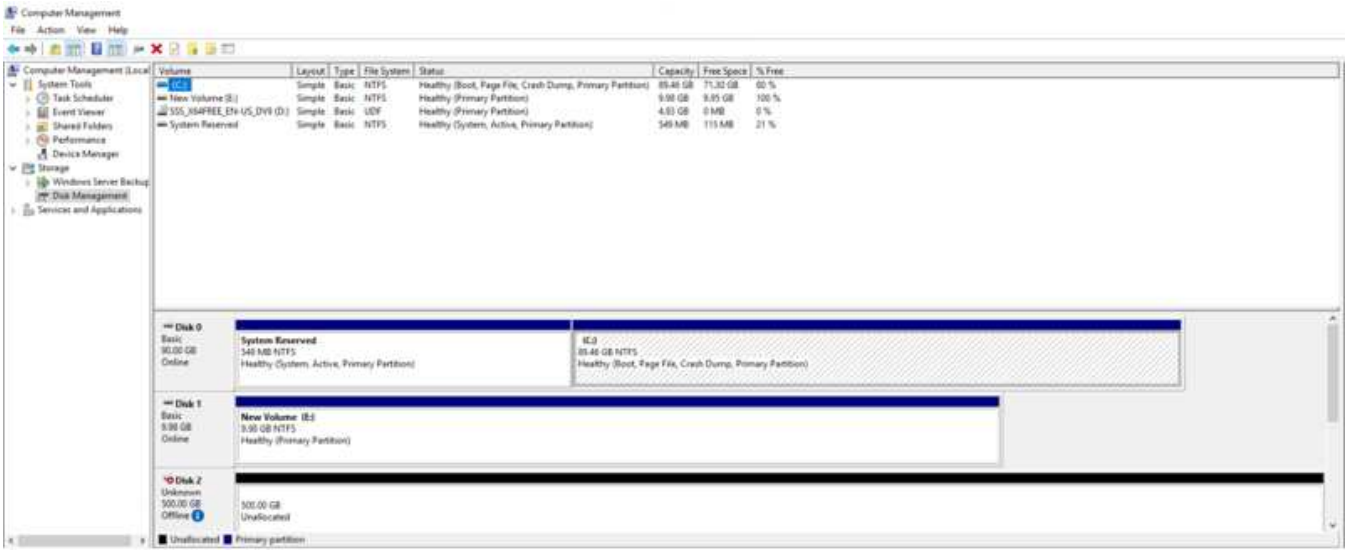
5. Seleccione Habilitar múltiples rutas y, a continuación, seleccione Restaurar automáticamente esta conexión cuando se inicie la computadora o Agregar esta conexión a la lista de destinos favoritos. Haga clic en Avanzado.

El host de Windows debe tener una conexión iSCSI a cada nodo del clúster. El DSM nativo selecciona las mejores rutas a utilizar.



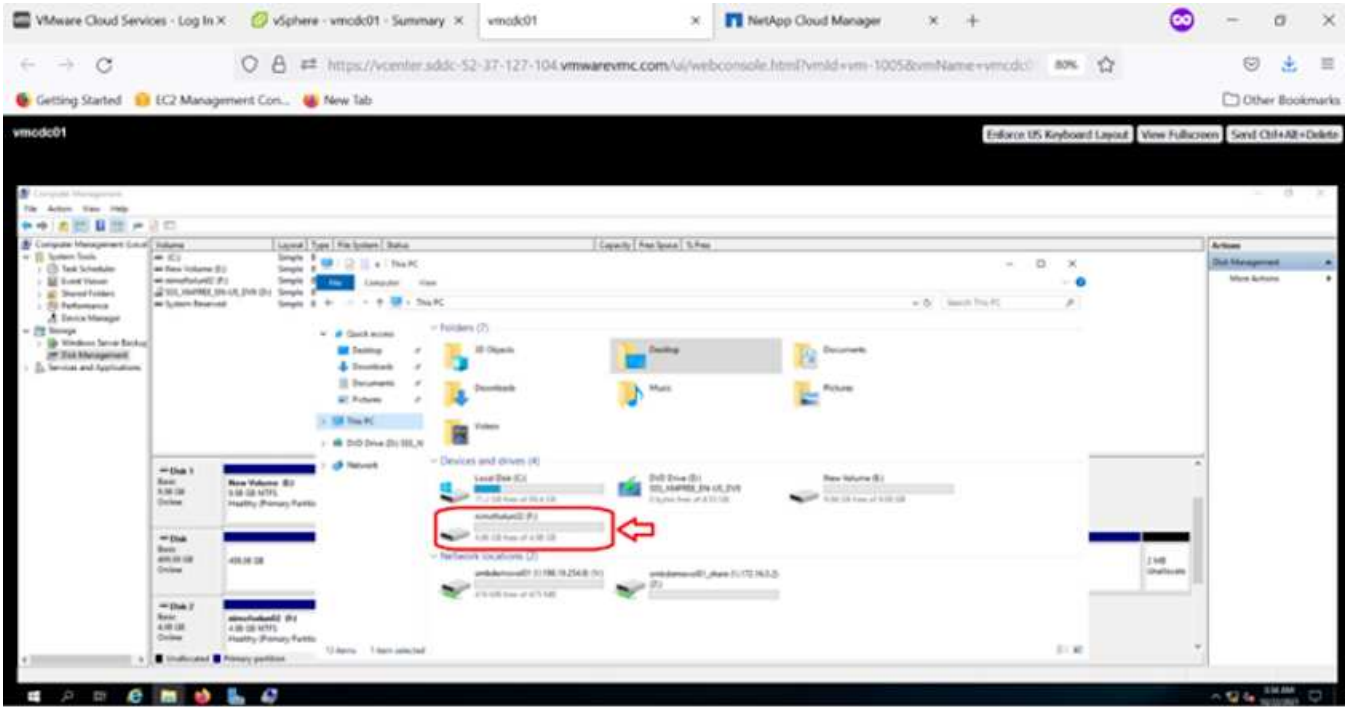
Los LUN de la SVM aparecen como discos para el host de Windows. El host no detecta automáticamente ningún disco nuevo que se agregue. Active un nuevo escaneo manual para descubrir los discos completando los siguientes pasos:

1. Abra la utilidad de Administración de equipos de Windows: Inicio > Herramientas administrativas > Administración de equipos.
2. Expanda el nodo Almacenamiento en el árbol de navegación.
3. Haga clic en Administración de discos.
4. Haga clic en Acción > Volver a escanear discos.



Cuando el host de Windows accede por primera vez a un nuevo LUN, éste no tiene partición ni sistema de archivos. Inicialice el LUN y, opcionalmente, formatee el LUN con un sistema de archivos completando los siguientes pasos:

1. Inicie la Administración de discos de Windows.
2. Haga clic con el botón derecho en el LUN y luego seleccione el tipo de disco o partición requerido.
3. Siga las instrucciones del asistente. En este ejemplo, la unidad F: está montada.



En los clientes Linux, asegúrese de que el demonio iSCSI esté ejecutándose. Una vez aprovisionados los LUN, consulte la guía detallada sobre la configuración de iSCSI para su distribución de Linux. Por ejemplo, la configuración iSCSI de Ubuntu se puede encontrar"aquí" . Para verificar, ejecute lsblk cmd desde el shell.

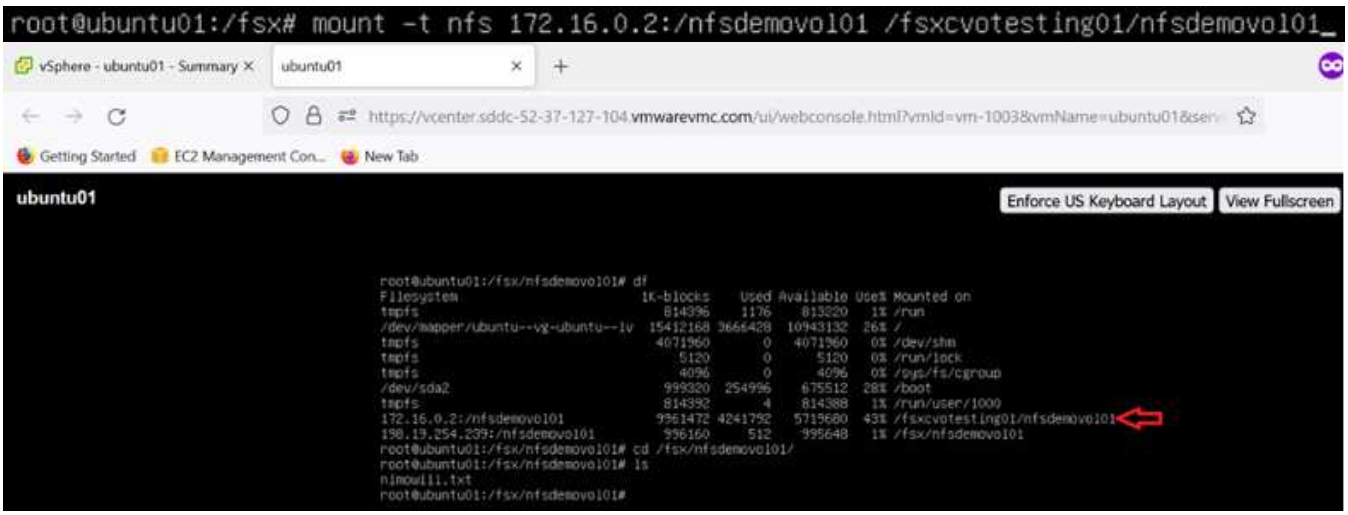
▼ Montar un volumen NFS de Cloud Volumes ONTAP en un cliente Linux

Para montar el sistema de archivos Cloud Volumes ONTAP (DIY) desde las máquinas virtuales dentro de VMC en AWS SDDC, complete los siguientes pasos:

1. Conectarse a la instancia de Linux designada.
2. Abra una terminal en la instancia usando shell seguro (SSH) e inicie sesión con las credenciales adecuadas.
3. Cree un directorio para el punto de montaje del volumen con el siguiente comando.

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. Monte el volumen NFS de Amazon FSx ONTAP en el directorio que se
creó en el paso anterior.
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```



Servicio de virtualización de Azure: opciones para usar el almacenamiento de NetApp

El almacenamiento de NetApp se puede conectar al servicio VMware de Azure como almacenamiento complementario o conectado como invitado.

Azure NetApp Files (ANF) como almacén de datos NFS complementario

La compatibilidad con almacenes de datos NFS se introdujo con la versión 3 de ESXi en implementaciones locales, lo que amplió enormemente las capacidades de almacenamiento de vSphere.

Ejecutar vSphere en NFS es una opción ampliamente adoptada para implementaciones de virtualización locales porque ofrece un gran rendimiento y estabilidad. Si tiene una cantidad significativa de almacenamiento conectado a red (NAS) en un centro de datos local, debería considerar implementar un SDDC de solución VMware de Azure en Azure con almacenes de datos de Azure NetApp File para superar los desafíos de capacidad y rendimiento.

Azure NetApp Files está basado en el software de gestión de datos NetApp ONTAP de alta disponibilidad y líder en la industria. Los servicios de Microsoft Azure se agrupan en tres categorías: básicos, generales y especializados. Azure NetApp Files pertenece a la categoría especializada y está respaldado por hardware ya implementado en muchas regiones. Con alta disponibilidad (HA) incorporada, Azure NetApp Files protege sus datos de la mayoría de las interrupciones y le ofrece un SLA líder en la industria del 99,99 %^ de tiempo de

actividad.

Para obtener más información sobre ANF como almacén de datos NFS complementario, visite:

- "ANF como almacén de datos NFS complementario: descripción general"
- "Opción de almacén de datos NFS complementario en Azure"

Azure NetApp Files (ANF) como almacenamiento conectado invitado

Azure NetApp Files lleva la administración y el almacenamiento de datos de nivel empresarial a Azure para que pueda administrar sus cargas de trabajo y aplicaciones con facilidad. Migre sus cargas de trabajo a la nube y ejecútelas sin sacrificar el rendimiento.

Azure NetApp Files elimina los obstáculos para que puedas trasladar todas tus aplicaciones basadas en archivos a la nube. Por primera vez, no tiene que rediseñar sus aplicaciones y obtiene almacenamiento persistente para sus aplicaciones sin complejidad.

Debido a que el servicio se brinda a través del Portal de Microsoft Azure, los usuarios experimentan un servicio completamente administrado como parte de su Acuerdo empresarial de Microsoft. El soporte de primer nivel, administrado por Microsoft, le brinda total tranquilidad. Esta única solución le permite agregar cargas de trabajo multiprotocolo de manera rápida y sencilla. Puede crear e implementar aplicaciones basadas en archivos de Windows y Linux, incluso para entornos heredados.

Para obtener más información, visite"ANF como almacenamiento conectado para invitados" .

Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados

Cloud Volumes ONTAP (CVO) es la solución de gestión de datos en la nube líder en la industria basada en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Es una versión definida por software de ONTAP que consume almacenamiento nativo de la nube, lo que le permite tener el mismo software de almacenamiento en la nube y en las instalaciones, lo que reduce la necesidad de volver a capacitar a su personal de TI en métodos completamente nuevos para administrar sus datos.

CVO brinda a los clientes la capacidad de mover datos sin problemas desde el borde al centro de datos, a la nube y viceversa, unificando su nube híbrida, todo administrado con una consola de administración de panel único, NetApp Cloud Manager.

Por diseño, CVO ofrece un rendimiento extremo y capacidades avanzadas de gestión de datos para satisfacer incluso sus aplicaciones más exigentes en la nube.

Para obtener más información, visite"CVO como almacenamiento conectado para invitados" .

Descripción general de las soluciones de almacenamiento de datos de ANF

Toda organización exitosa está en un camino de transformación y modernización. Como parte de este proceso, las empresas generalmente utilizan sus inversiones existentes en VMware mientras aprovechan los beneficios de la nube y exploran cómo hacer que los procesos de migración, expansión, extensión y recuperación ante desastres sean lo más fluidos posible. Los clientes que migran a la nube deben evaluar las cuestiones de elasticidad y explosión, salida del centro de datos, consolidación del centro de datos,

escenarios de fin de vida útil, fusiones, adquisiciones, etc. El enfoque adoptado por cada organización puede variar en función de sus respectivas prioridades comerciales. A la hora de elegir operaciones basadas en la nube, un objetivo fundamental es seleccionar un modelo de bajo coste con un rendimiento adecuado y unos obstáculos mínimos. Además de elegir la plataforma adecuada, la orquestación del almacenamiento y el flujo de trabajo es particularmente importante para liberar el poder de la implementación y la elasticidad de la nube.

Casos de uso

Si bien la solución Azure VMware ofrece capacidades híbridas únicas para el cliente, las opciones de almacenamiento nativo limitadas han restringido su utilidad para las organizaciones con cargas de trabajo con gran capacidad de almacenamiento. Debido a que el almacenamiento está directamente vinculado a los hosts, la única forma de escalar el almacenamiento es agregar más hosts, lo que puede aumentar los costos entre un 35 % y un 40 % o más para cargas de trabajo con uso intensivo de almacenamiento. Estas cargas de trabajo necesitan almacenamiento adicional, no potencia adicional, pero eso significa pagar por hosts adicionales.

Consideremos el siguiente escenario: un cliente requiere seis hosts en términos de potencia (vCPU/vMem), pero también tiene un requisito sustancial de almacenamiento. Según su evaluación, necesitan 12 hosts para cumplir con los requisitos de almacenamiento. Esto aumenta el TCO general porque deben comprar toda esa potencia adicional cuando lo que realmente necesitan es más almacenamiento. Esto es aplicable a cualquier caso de uso, incluida migración, recuperación ante desastres, ráfagas, desarrollo/prueba, etc.

Otro caso de uso común de Azure VMware Solution es la recuperación ante desastres (DR). La mayoría de las organizaciones no cuentan con una estrategia de recuperación ante desastres infalible, o pueden tener dificultades para justificar la operación de un centro de datos fantasma solo para recuperación ante desastres. Los administradores pueden explorar opciones de recuperación ante desastres sin huella con un clúster piloto o un clúster a pedido. Luego podrían escalar el almacenamiento sin agregar hosts adicionales, una opción potencialmente atractiva.

Así pues, para resumir, los casos de uso se pueden clasificar de dos maneras:

- Escalar la capacidad de almacenamiento mediante almacenes de datos ANF
- Uso de almacenes de datos ANF como destino de recuperación ante desastres para un flujo de trabajo de recuperación rentable desde las instalaciones locales o dentro de regiones de Azure entre los centros de datos definidos por software (SDDC). Esta guía proporciona información sobre el uso de Azure NetApp Files para proporcionar almacenamiento optimizado para almacenes de datos (actualmente en versión preliminar pública) junto con las mejores capacidades de protección de datos y recuperación ante desastres en una solución de Azure VMware, que le permite descargar la capacidad de almacenamiento del almacenamiento de vSAN.



Comuníquese con los arquitectos de soluciones de NetApp o Microsoft en su región para obtener información adicional sobre el uso de almacenes de datos ANF.

Opciones de VMware Cloud en Azure

Solución VMware de Azure

Azure VMware Solution (AVS) es un servicio de nube híbrida que proporciona SDDC de VMware totalmente funcionales dentro de una nube pública de Microsoft Azure. AVS es una solución propia totalmente administrada y respaldada por Microsoft y verificada por VMware que utiliza la infraestructura de Azure. Por lo

tanto, los clientes obtienen VMware ESXi para la virtualización informática, vSAN para el almacenamiento hiperconvergente y NSX para redes y seguridad, todo ello mientras aprovechan la presencia global de Microsoft Azure, las instalaciones de centros de datos líderes en su clase y la proximidad al rico ecosistema de servicios y soluciones nativos de Azure. Una combinación de Azure VMware Solution SDDC y Azure NetApp Files proporciona el mejor rendimiento con una latencia de red mínima.

Independientemente de la nube utilizada, cuando se implementa un VMware SDDC, el clúster inicial incluye los siguientes componentes:

- Hosts VMware ESXi para virtualización informática con un dispositivo de servidor vCenter para administración.
- Almacenamiento hiperconvergente VMware vSAN que incorpora los activos de almacenamiento físico de cada host ESXi.
- VMware NSX para redes virtuales y seguridad con un clúster NSX Manager para administración.

Conclusión

Ya sea que su objetivo sea una nube completa o una nube híbrida, los archivos de Azure NetApp brindan excelentes opciones para implementar y administrar las cargas de trabajo de las aplicaciones junto con los servicios de archivos, al tiempo que reducen el TCO al hacer que los requisitos de datos se integren perfectamente con la capa de aplicación. Cualquiera que sea el caso de uso, elija Azure VMware Solution junto con Azure NetApp Files para obtener rápidamente beneficios de la nube, infraestructura y operaciones consistentes en las instalaciones y en múltiples nubes, portabilidad bidireccional de cargas de trabajo y capacidad y rendimiento de nivel empresarial. Es el mismo proceso y procedimientos familiares utilizados para conectar el almacenamiento. Recuerde que lo único que cambió fue la posición de los datos junto con los nuevos nombres; las herramientas y los procesos siguen siendo los mismos, y Azure NetApp Files ayuda a optimizar la implementación general.

Comida para llevar

Los puntos clave de este documento incluyen:

- Ahora puede usar Azure NetApp Files como almacén de datos en AVS SDDC.
- Aumente los tiempos de respuesta de las aplicaciones y ofrezca una mayor disponibilidad para proporcionar acceso a los datos de la carga de trabajo cuándo y dónde se necesiten.
- Simplifique la complejidad general del almacenamiento vSAN con capacidades de cambio de tamaño simples e instantáneas.
- Rendimiento garantizado para cargas de trabajo de misión crítica mediante capacidades de remodelación dinámica.
- Si Azure VMware Solution Cloud es el destino, Azure NetApp Files es la solución de almacenamiento adecuada para una implementación optimizada.

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes enlaces de sitios web:

- Documentación de Azure VMware Solution

  "https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Documentación de Azure NetApp Files

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- Adjuntar almacenes de datos de Azure NetApp Files a hosts de Azure VMware Solution (versión preliminar)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

Creación de un almacén de datos NFS complementario en Azure

La compatibilidad con almacenes de datos NFS se introdujo con la versión 3 de ESXi en implementaciones locales, lo que amplió enormemente las capacidades de almacenamiento de vSphere.

Ejecutar vSphere en NFS es una opción ampliamente adoptada para implementaciones de virtualización locales porque ofrece un gran rendimiento y estabilidad. Si tiene una cantidad significativa de almacenamiento conectado a red (NAS) en un centro de datos local, debería considerar implementar un SDDC de solución VMware de Azure en Azure con almacenes de datos de Azure NetApp File para superar los desafíos de capacidad y rendimiento.

Azure NetApp Files está basado en el software de administración de datos NetApp ONTAP de alta disponibilidad y líder en la industria. Los servicios de Microsoft Azure se agrupan en tres categorías: básicos, generales y especializados. Azure NetApp Files pertenece a la categoría especializada y está respaldado por hardware ya implementado en muchas regiones. Con alta disponibilidad (HA) incorporada, Azure NetApp Files protege sus datos de la mayoría de las interrupciones y le ofrece un SLA líder en la industria de "99.99%" tiempo de actividad.

Antes de la introducción de la capacidad de almacenamiento de datos de Azure NetApp Files , la operación de escalamiento horizontal para los clientes que planeaban alojar cargas de trabajo intensivas en rendimiento y almacenamiento requería la expansión tanto del cómputo como del almacenamiento.

Tenga en cuenta las siguientes cuestiones:

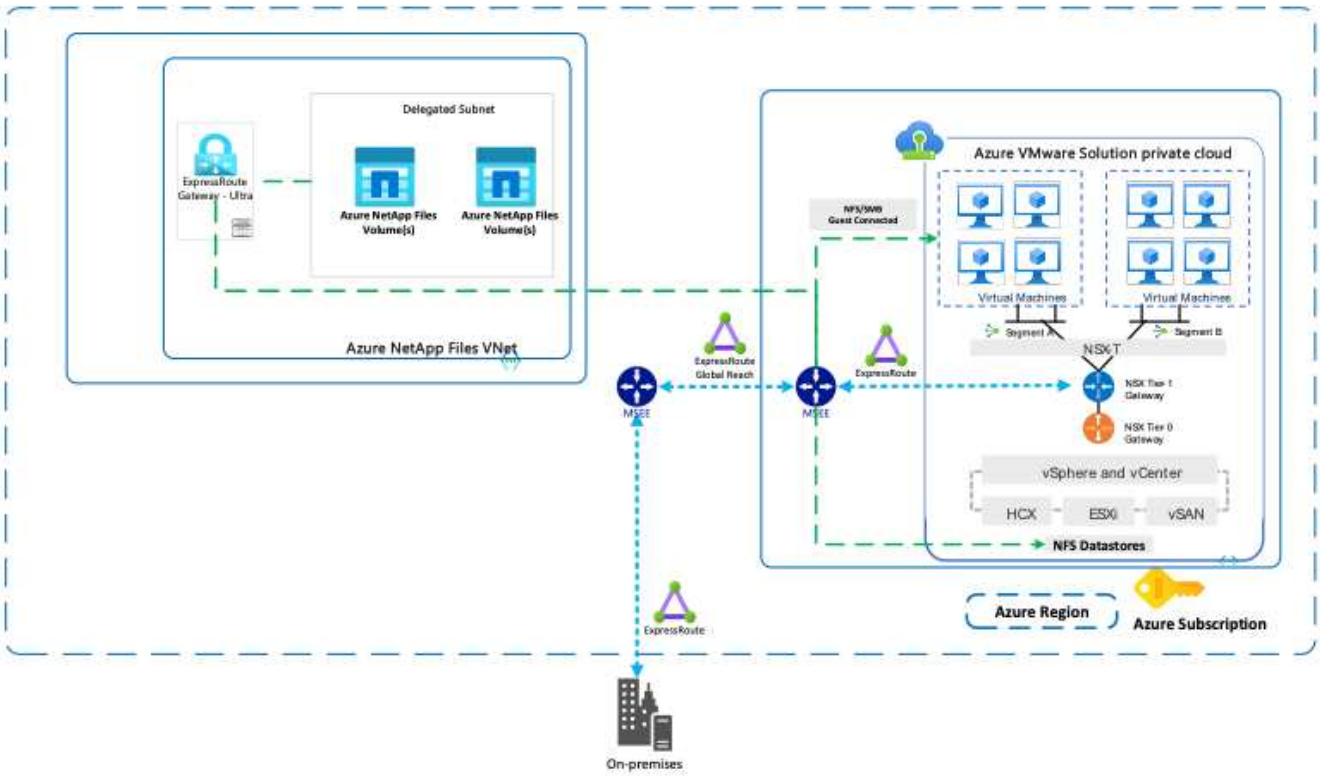
- No se recomiendan configuraciones de clúster desequilibradas en un clúster SDDC. Por lo tanto, ampliar el almacenamiento significa agregar más hosts, lo que implica mayor TCO.
- Solo es posible un entorno vSAN. Por lo tanto, todo el tráfico de almacenamiento compite directamente con las cargas de trabajo de producción.
- No existe la opción de proporcionar múltiples niveles de rendimiento para alinear los requisitos de la aplicación, el rendimiento y el costo.
- Es fácil alcanzar los límites de la capacidad de almacenamiento de vSAN construida sobre hosts de clúster. Al integrar ofertas de plataforma como servicio (PaaS) nativas de Azure, como Azure NetApp Files , como almacén de datos, los clientes tienen la opción de escalar independientemente su almacenamiento por separado y solo agregar nodos de cómputo al clúster SDDC según sea necesario. Esta capacidad supera los desafíos mencionados anteriormente.

Azure NetApp Files también le permite implementar múltiples almacenes de datos, lo que ayuda a imitar un modelo de implementación local al colocar máquinas virtuales en el almacén de datos adecuado y asignar el nivel de servicio requerido para cumplir con los requisitos de rendimiento de la carga de trabajo. Con la capacidad única de soporte de múltiples protocolos, el almacenamiento invitado es una opción adicional para cargas de trabajo de bases de datos como SQL y Oracle mientras que también utiliza la capacidad de almacenamiento de datos NFS complementaria para alojar los VMDK restantes. Aparte de esto, la capacidad de instantáneas nativas le permite realizar copias de seguridad rápidas y restauraciones granulares.

Comuníquese con los arquitectos de soluciones de Azure y NetApp para planificar y dimensionar el almacenamiento y determinar la cantidad de hosts necesarios. NetApp recomienda identificar los requisitos de rendimiento del almacenamiento antes de finalizar el diseño del almacén de datos para las implementaciones de prueba, POC y producción.

Arquitectura detallada

Desde una perspectiva de alto nivel, esta arquitectura describe cómo lograr la conectividad de la nube híbrida y la portabilidad de aplicaciones en entornos locales y Azure. También describe el uso de Azure NetApp Files como un almacén de datos NFS complementario y como una opción de almacenamiento interno para máquinas virtuales invitadas alojadas en la solución Azure VMware.



Apresto

El aspecto más importante en la migración o recuperación ante desastres es determinar el tamaño correcto para el entorno de destino. Es muy importante comprender cuántos nodos se requieren para realizar un ejercicio de elevación y traslado desde las instalaciones locales a la solución VMware de Azure.

Para dimensionar, utilice datos históricos del entorno local mediante RVTools (preferido) u otras herramientas como Live Optics o Azure Migrate. RVTools es una herramienta ideal para capturar vCPU, vMem, vDisk y toda la información necesaria, incluidas las máquinas virtuales encendidas o apagadas, para caracterizar el entorno de destino.

Para ejecutar RVtools, complete los siguientes pasos:

1. Descargue e instale RVTools.
2. Ejecute RVTools, ingrese la información requerida para conectarse a su servidor vCenter local y presione Iniciar sesión.
3. Exportar el inventario a una hoja de cálculo de Excel.

4. Edite la hoja de cálculo y elimine cualquier máquina virtual que no sea candidata ideal de la pestaña vInfo. Este enfoque proporciona un resultado claro acerca de los requisitos de almacenamiento que se pueden usar para dimensionar correctamente el clúster de Azure VMware SDDC con la cantidad de hosts requerida.

> Las máquinas virtuales invitadas utilizadas con almacenamiento interno se deben calcular por separado; sin embargo, Azure NetApp Files puede cubrir fácilmente la capacidad de almacenamiento adicional, lo que mantiene bajo el costo total de propiedad general.

Implementación y configuración de Azure VMware Solution

Al igual que en las instalaciones locales, la planificación de una solución VMware de Azure es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

En esta sección se describe cómo configurar y administrar AVS para su uso en combinación con Azure NetApp Files como un almacén de datos con almacenamiento invitado también.

El proceso de configuración se puede dividir en tres partes:

- Registre el proveedor de recursos y cree una nube privada.
- Conéctese a una puerta de enlace de red virtual ExpressRoute nueva o existente.
- Validar la conectividad de la red y acceder a la nube privada. Consulte esto"enlace" para una guía paso a paso del proceso de aprovisionamiento de SDDC de la solución VMware de Azure.

Configurar Azure NetApp Files con Azure VMware Solution

La nueva integración entre Azure NetApp Files le permite crear almacenes de datos NFS a través de las API/CLI del proveedor de recursos de Azure VMware Solution con volúmenes de Azure NetApp Files y montar los almacenes de datos en los clústeres de su elección en una nube privada. Además de alojar los VMDK de máquinas virtuales y aplicaciones, los volúmenes de archivos de Azure NetApp también se pueden montar desde máquinas virtuales creadas en el entorno SDDC de Azure VMware Solution. Los volúmenes se pueden montar en el cliente Linux y asignarse en un cliente Windows, porque Azure NetApp Files admite los protocolos Bloque de mensajes de servidor (SMB) y Sistema de archivos de red (NFS).

> Para obtener un rendimiento óptimo, implemente Azure NetApp Files en la misma zona de disponibilidad que la nube privada. La coubicación con la ruta rápida Express Route proporciona el mejor rendimiento, con una latencia de red mínima.

Para adjuntar un volumen de archivos de Azure NetApp como almacén de datos de VMware de una nube privada de Azure VMware Solution, asegúrese de que se cumplan los siguientes requisitos previos.

▼ Prerrequisitos

1. Utilice az login y valide que la suscripción esté registrada en la función CloudSanExperience en el espacio de nombres Microsoft.AVS.

```
az login –tenant xcvxcvxc- vxcv- xcvx- cvxc- vxcvxcvxcv
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

1. Si no está registrado, regístrelo.

```
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

El registro puede tardar aproximadamente 15 minutos en completarse.

1. Para comprobar el estado del registro, ejecute el siguiente comando.

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
--query properties.state
```

1. Si el registro queda estancado en un estado intermedio durante más de 15 minutos, cancele el registro y vuelva a registrar la bandera.

```
az feature unregister --name "CloudSanExperience" --namespace
"Microsoft.AVS"
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

1. Verifique que la suscripción esté registrada en la función AnfDatastoreExperience en el espacio de nombres Microsoft.AVS.

```
az feature show --name "AnfDatastoreExperience" --namespace
"Microsoft.AVS" --query properties.state
```

1. Verifique que la extensión VMware esté instalada.

```
az extension show --name vmware
```

1. Si la extensión ya está instalada, verifique que la versión sea 3.0.0. Si está instalada una versión anterior, actualice la extensión.

```
az extension update --name vmware
```

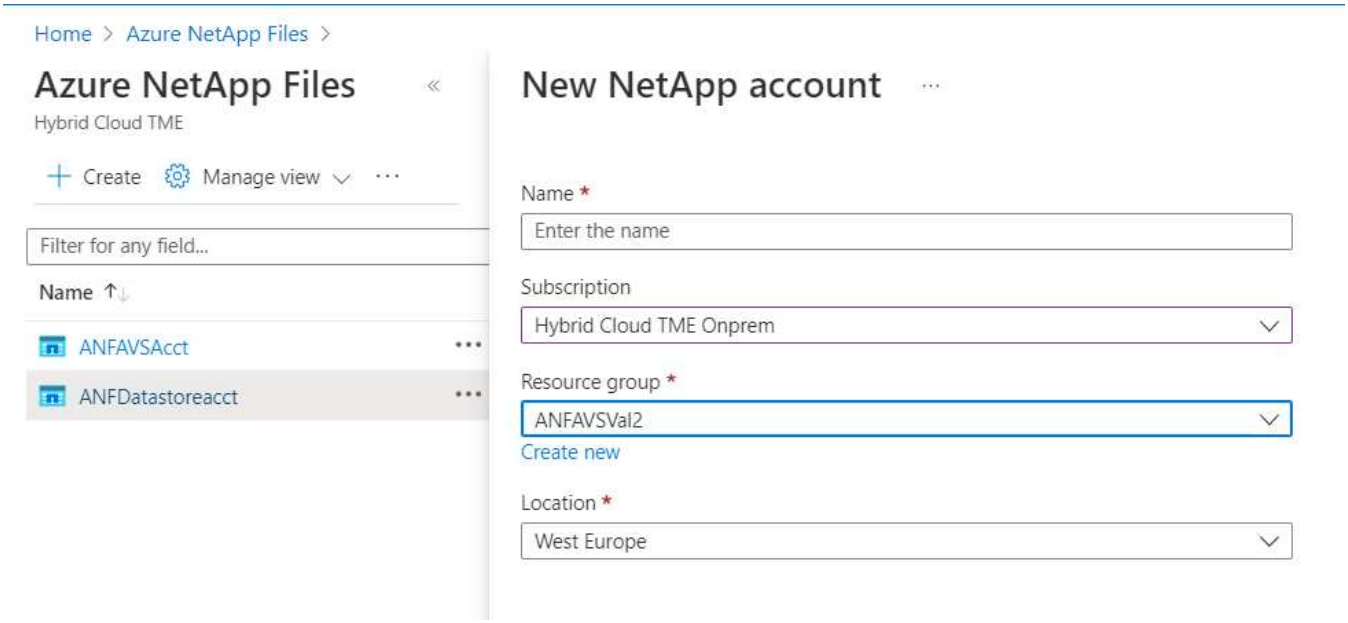
1. Si la extensión aún no está instalada, instálela.

```
az extension add --name vmware
```

▼ **Crear y montar volúmenes de Azure NetApp Files**

1. Inicie sesión en el Portal de Azure y acceda a Azure NetApp Files. Verifique el acceso al servicio Azure NetApp Files y registre el proveedor de recursos de Azure NetApp Files mediante el `az provider`

`register --namespace Microsoft.NetApp –wait` dominio. Después de registrarse, cree una cuenta de NetApp . Consulte esto "enlace" para conocer los pasos detallados.



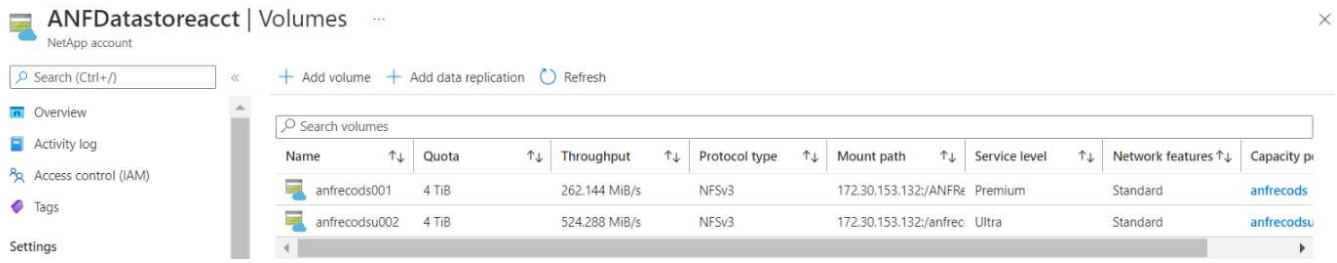
1. Después de crear una cuenta de NetApp , configure grupos de capacidad con el tamaño y el nivel de servicio requeridos. Para obtener información detallada, consulte este "enlace" .



Puntos para recordar

- NFSv3 es compatible con almacenes de datos en Azure NetApp Files.
- Utilice el nivel Premium o estándar para cargas de trabajo con límite de capacidad y el nivel Ultra para cargas de trabajo con límite de rendimiento cuando sea necesario y al mismo tiempo complemente el almacenamiento vSAN predeterminado.

1. Configure una subred delegada para Azure NetApp Files y especifique esta subred al crear volúmenes. Para conocer los pasos detallados para crear una subred delegada, consulte este "enlace" .
2. Agregue un volumen NFS para el almacén de datos mediante la hoja Volúmenes debajo de la hoja Grupos de capacidad.



Para obtener más información sobre el rendimiento del volumen de Azure NetApp Files por tamaño o cuota, consulte"Consideraciones de rendimiento para Azure NetApp Files" .

▼ Agregar un almacén de datos de archivos de Azure NetApp a la nube privada

> El volumen de Azure NetApp Files se puede conectar a su nube privada mediante el Portal de Azure. Sigue esto"enlace de Microsoft" para un enfoque paso a paso sobre el uso del portal de Azure para montar un almacén de datos de archivos de Azure NetApp .

Para agregar un almacén de datos de archivos de Azure NetApp a una nube privada, complete los siguientes pasos:

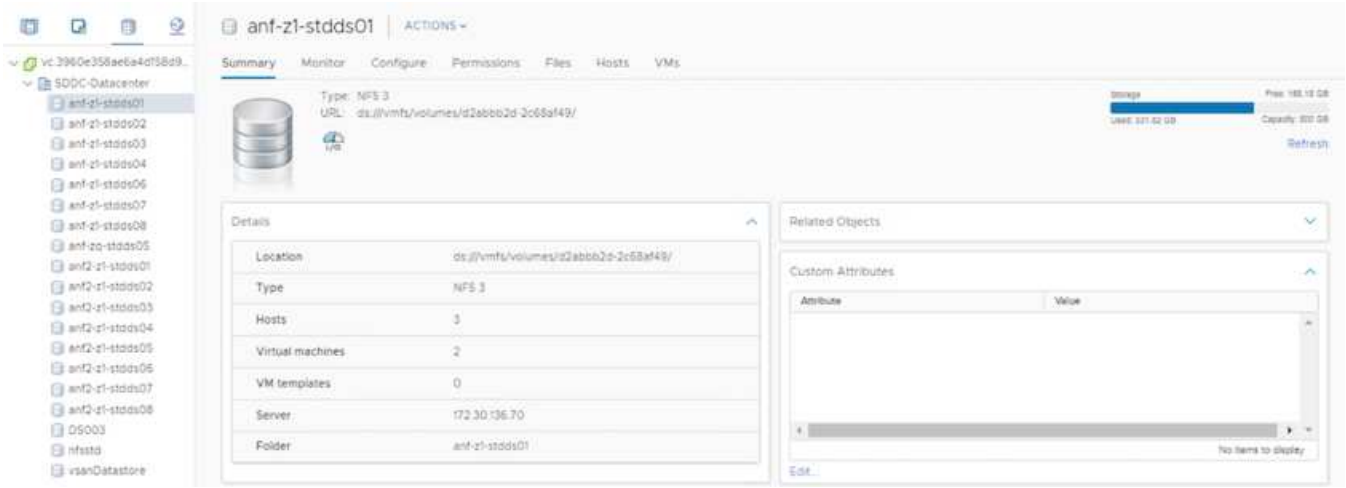
1. Una vez registradas las características necesarias, adjunte un almacén de datos NFS al clúster de nube privada de Azure VMware Solution ejecutando el comando apropiado.
2. Cree un almacén de datos utilizando un volumen ANF existente en el clúster de nube privada de Azure VMware Solution.

```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}
```

```
. List all the datastores in a private cloud cluster.
```

C:\Usuarios\niyaz>az vmware datastore list --resource-group anfavsval2 --cluster Cluster-1 --private-cloud ANFDataClus [{ "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDS001", "name": " ANFRecoDS001", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp /netAppAccounts/anfdatastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001", "resourceGroup": "anfavsval2" }, "provisioningState": "Correcto", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }, { "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002", "resourceGroup": "anfavsval2" }, "provisioningState": " Correcto", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }]

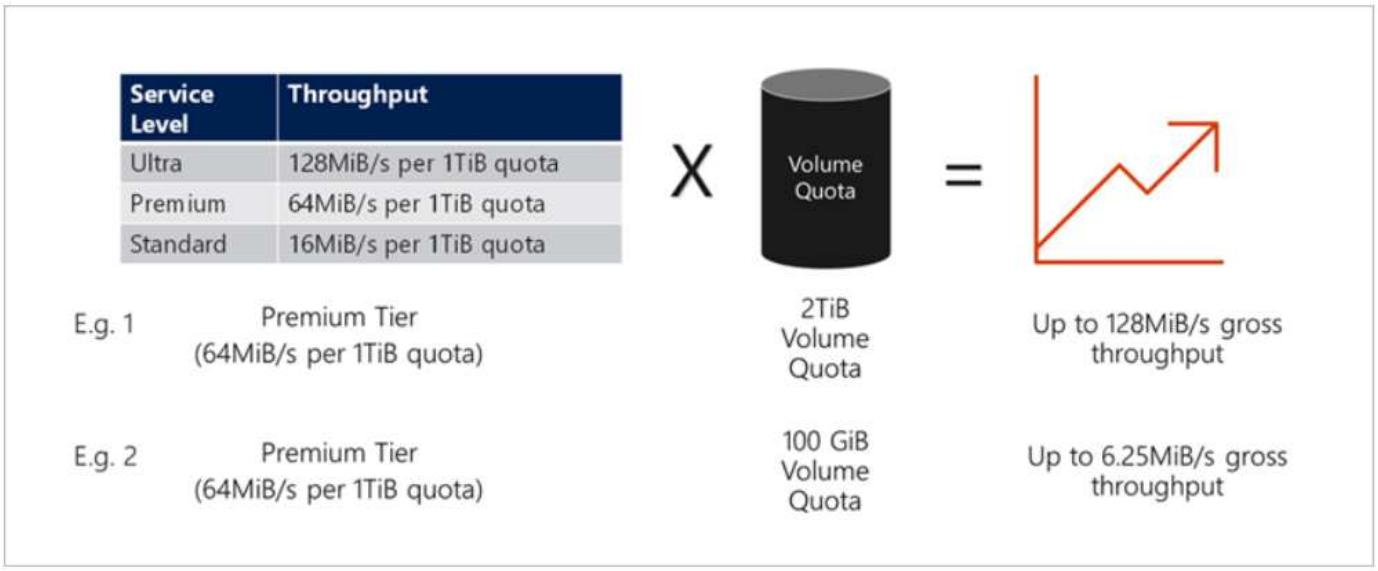
1. Una vez establecida la conectividad necesaria, los volúmenes se montan como un almacén de datos.



Optimización del tamaño y el rendimiento

Azure NetApp Files admite tres niveles de servicio: Estándar (16 MBps por terabyte), Premium (64 MBps por terabyte) y Ultra (128 MBps por terabyte). Aprovisionar el tamaño de volumen correcto es importante para un rendimiento óptimo de la carga de trabajo de la base de datos. Con Azure NetApp Files, el rendimiento del volumen y el límite de rendimiento se determinan en función de los siguientes factores:

- El nivel de servicio del grupo de capacidad al que pertenece el volumen
- La cuota asignada al volumen
- El tipo de calidad de servicio (QoS) (automático o manual) del grupo de capacidad



Para obtener más información, consulte "Niveles de servicio para Azure NetApp Files" .

Consulte esto"enlace de Microsoft" para obtener puntos de referencia de rendimiento detallados que se pueden utilizar durante un ejercicio de dimensionamiento.

Puntos para recordar
• Utilice el nivel Premium o Estándar para los volúmenes de almacén de datos para lograr una capacidad y un rendimiento óptimos. Si se requiere rendimiento, se puede utilizar el nivel Ultra. • Para los requisitos de montaje de invitados, utilice el nivel Premium o Ultra y, para los requisitos de uso compartido de archivos para las máquinas virtuales invitadas, utilice volúmenes de nivel Estándar o Premium.

Consideraciones de rendimiento

Es importante comprender que con la versión 3 de NFS solo hay una tubería activa para la conexión entre el host ESXi y un único destino de almacenamiento. Esto significa que, si bien puede haber conexiones alternativas disponibles para la conmutación por error, el ancho de banda para un solo almacén de datos y el almacenamiento subyacente están limitados a lo que una sola conexión puede proporcionar.

Para aprovechar más ancho de banda disponible con los volúmenes de Azure NetApp Files , un host ESXi debe tener múltiples conexiones a los destinos de almacenamiento. Para solucionar este problema, puede configurar varios almacenes de datos, y cada uno de ellos utilizará conexiones independientes entre el host ESXi y el almacenamiento.

Para lograr un mayor ancho de banda, como práctica recomendada se recomienda crear múltiples almacenes de datos utilizando múltiples volúmenes ANF, crear VMDK y distribuir los volúmenes lógicos entre los VMDK.

Consulte esto"enlace de Microsoft" para obtener puntos de referencia de rendimiento detallados que se pueden utilizar durante un ejercicio de dimensionamiento.

Puntos para recordar

- La solución VMware de Azure permite ocho almacenes de datos NFS de forma predeterminada. Esto se puede aumentar mediante una solicitud de soporte.
- Aproveche ER Fastpath junto con Ultra SKU para obtener mayor ancho de banda y menor latencia. Más información
- Con las características de red "Básicas" en los archivos de Azure NetApp , la conectividad de Azure VMware Solution está limitada por el ancho de banda del circuito ExpressRoute y la puerta de enlace ExpressRoute.
- Para los volúmenes de Azure NetApp Files con características de red "Estándar", se admite ExpressRoute FastPath. Cuando está habilitado, FastPath envía tráfico de red directamente a los volúmenes de Azure NetApp Files , sin pasar por la puerta de enlace, lo que proporciona mayor ancho de banda y menor latencia.

Aumentar el tamaño del almacén de datos

La remodelación del volumen y los cambios dinámicos del nivel de servicio son completamente transparentes para el SDDC. En Azure NetApp Files, estas capacidades proporcionan optimizaciones continuas de rendimiento, capacidad y costos. Aumente el tamaño de los almacenes de datos NFS modificando el tamaño del volumen desde el Portal de Azure o mediante la CLI. Una vez que haya terminado, acceda a vCenter, vaya a la pestaña del almacén de datos, haga clic con el botón derecho en el almacén de datos apropiado y seleccione Actualizar información de capacidad. Este enfoque se puede utilizar para aumentar la capacidad del almacén de datos y aumentar el rendimiento del mismo de manera dinámica y sin tiempo de inactividad. Este proceso también es completamente transparente para las aplicaciones.

Puntos para recordar

- La reestructuración del volumen y la capacidad de nivel de servicio dinámico le permiten optimizar los costos mediante el dimensionamiento para cargas de trabajo en estado estable y así evitar el sobreaprovisionamiento.
- VAAI no está habilitado.

Cargas de trabajo

▼ **Migración**

Uno de los casos de uso más comunes es la migración. Utilice VMware HCX o vMotion para mover máquinas virtuales locales. Como alternativa, puede usar Rivermeadow para migrar máquinas virtuales a almacenes de datos de Azure NetApp Files .

▼ **Protección de datos**

La realización de copias de seguridad de máquinas virtuales y su rápida recuperación son dos de las grandes fortalezas de los almacenes de datos ANF. Utilice copias instantáneas para realizar copias rápidas de su máquina virtual o almacén de datos sin afectar el rendimiento y luego envíelas al almacenamiento de Azure para una protección de datos a largo plazo o a una región secundaria mediante la replicación entre regiones para fines de recuperación ante desastres. Este enfoque minimiza el espacio de almacenamiento y el ancho de banda de la red almacenando únicamente la información modificada.

Utilice copias instantáneas de Azure NetApp Files para protección general y use herramientas de aplicación para proteger datos transaccionales como SQL Server u Oracle que residen en las máquinas virtuales invitadas. Estas copias instantáneas son diferentes de las instantáneas de VMware (consistencia) y son adecuadas para una protección a largo plazo.

Con los almacenes de datos ANF, la opción Restaurar a nuevo volumen se puede usar para clonar un volumen de almacén de datos completo, y el volumen restaurado se puede montar como otro almacén de datos en los hosts dentro de AVS SDDC. Una vez montado un almacén de datos, las máquinas virtuales dentro de él se pueden registrar, reconfigurar y personalizar como si fueran máquinas virtuales clonadas individualmente.

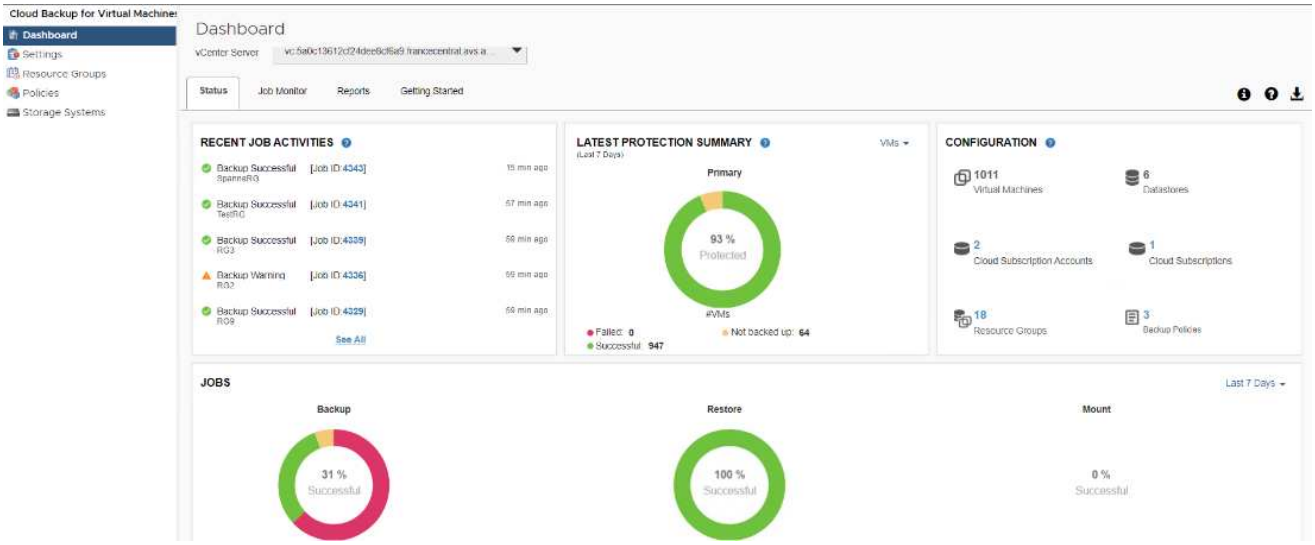
▼ NetApp Backup and Recovery para máquinas virtuales

NetApp Backup and Recovery for Virtual Machines proporciona una GUI de cliente web de vSphere en vCenter para proteger las máquinas virtuales de Azure VMware Solution y los almacenes de datos de archivos de Azure NetApp mediante políticas de backup. Estas políticas pueden definir la programación, la retención y otras capacidades. La funcionalidad de NetApp Backup and Recovery for Virtual Machines se puede implementar mediante el comando Run.

Las políticas de configuración y protección se pueden instalar completando los siguientes pasos:

1. Instala NetApp Backup and Recovery for Virtual Machine en la nube privada de Azure VMware Solution mediante el comando Run.
2. Agregue las credenciales de suscripción a la nube (valor de cliente y secreto) y luego agregue una cuenta de suscripción a la nube (cuenta de NetApp y grupo de recursos asociado) que contenga los recursos que desea proteger.
3. Cree una o más políticas de respaldo que administren la retención, la frecuencia y otras configuraciones para las copias de seguridad del grupo de recursos.
4. Cree un contenedor para agregar uno o más recursos que necesiten protegerse con políticas de respaldo.
5. En caso de falla, restaure toda la VM o VMDK individuales específicos en la misma ubicación.

Con la tecnología Snapshot de Azure NetApp Files , las copias de seguridad y las restauraciones son muy rápidas.



▼ Recuperación ante desastres con Azure NetApp Files, JetStream DR y Azure VMware Solution

La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos (por ejemplo, ransomware). Con el marco VMware VAIO, las cargas de trabajo locales de VMware se pueden replicar en el almacenamiento de Azure Blob y recuperar, lo que permite una pérdida de datos mínima o casi nula y un

RTO cercano a cero. JetStream DR se puede utilizar para recuperar sin problemas las cargas de trabajo replicadas desde las instalaciones locales a AVS y, específicamente, a Azure NetApp Files. Permite una recuperación ante desastres rentable mediante el uso de recursos mínimos en el sitio de recuperación ante desastres y un almacenamiento en la nube rentable. JetStream DR automatiza la recuperación a almacenes de datos ANF a través de Azure Blob Storage. JetStream DR recupera máquinas virtuales independientes o grupos de máquinas virtuales relacionadas en la infraestructura del sitio de recuperación de acuerdo con el mapeo de la red y proporciona recuperación en un punto en el tiempo para la protección contra ransomware.

"Solución DR con ANF, JetStream y AVS" .

Opciones de almacenamiento conectado para invitados de NetApp para Azure

Azure admite el almacenamiento NetApp conectado a invitados con el servicio nativo Azure NetApp Files (ANF) o con Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure netApp Files lleva la administración y el almacenamiento de datos de nivel empresarial a Azure para que pueda administrar sus cargas de trabajo y aplicaciones con facilidad. Migre sus cargas de trabajo a la nube y ejecútelas sin sacrificar el rendimiento.

Azure netApp Files elimina los obstáculos para que puedas trasladar todas tus aplicaciones basadas en archivos a la nube. Por primera vez, no tiene que rediseñar sus aplicaciones y obtiene almacenamiento persistente para sus aplicaciones sin complejidad.

Debido a que el servicio se brinda a través del Portal de Microsoft Azure, los usuarios experimentan un servicio completamente administrado como parte de su Acuerdo empresarial de Microsoft. El soporte de primer nivel, administrado por Microsoft, le brinda total tranquilidad. Esta única solución le permite agregar cargas de trabajo multiprotocolo de manera rápida y sencilla. Puede crear e implementar aplicaciones basadas en archivos de Windows y Linux, incluso para entornos heredados.

Azure NetApp Files (ANF) como almacenamiento conectado invitado

▼ **Configurar Azure NetApp Files con Azure VMware Solution (AVS)**

Los recursos compartidos de Azure NetApp Files se pueden montar desde máquinas virtuales creadas en el entorno SDDC de Azure VMware Solution. Los volúmenes también se pueden montar en el cliente Linux y asignar en el cliente Windows porque Azure NetApp Files admite los protocolos SMB y NFS. Los volúmenes de Azure NetApp Files se pueden configurar en cinco sencillos pasos.

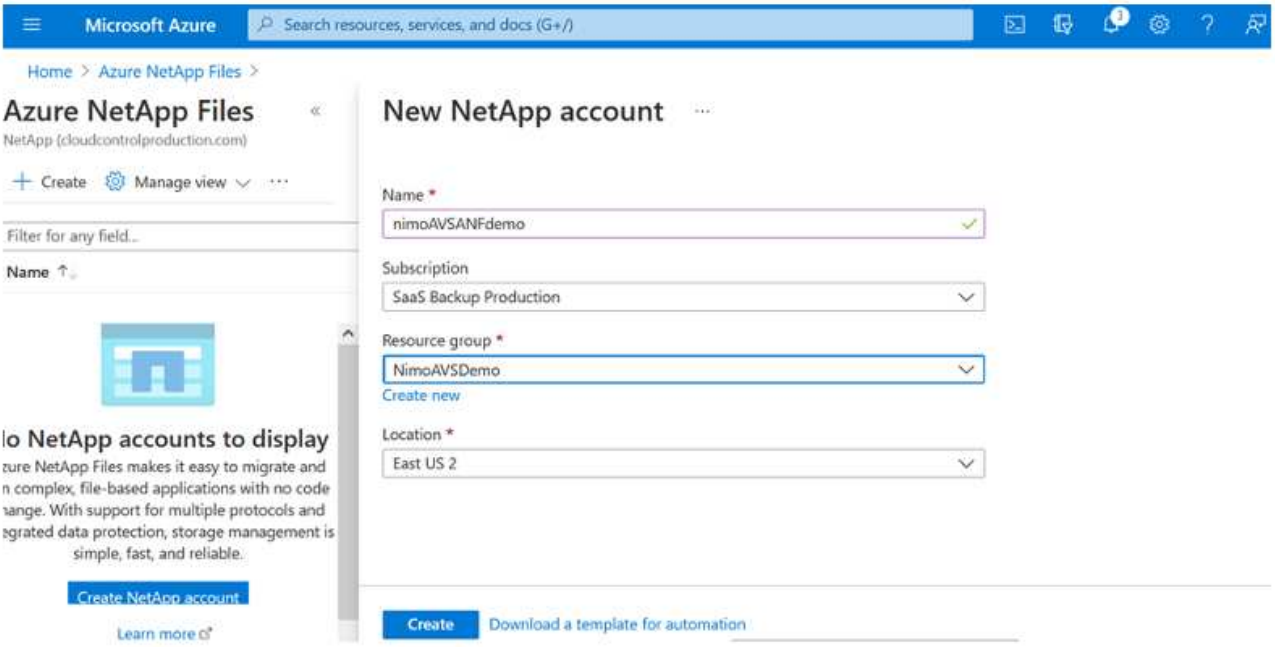
Azure NetApp Files y Azure VMware Solution deben estar en la misma región de Azure.

▼ **Crear y montar volúmenes de Azure NetApp Files**

Para crear y montar volúmenes de Azure NetApp Files , complete los siguientes pasos:

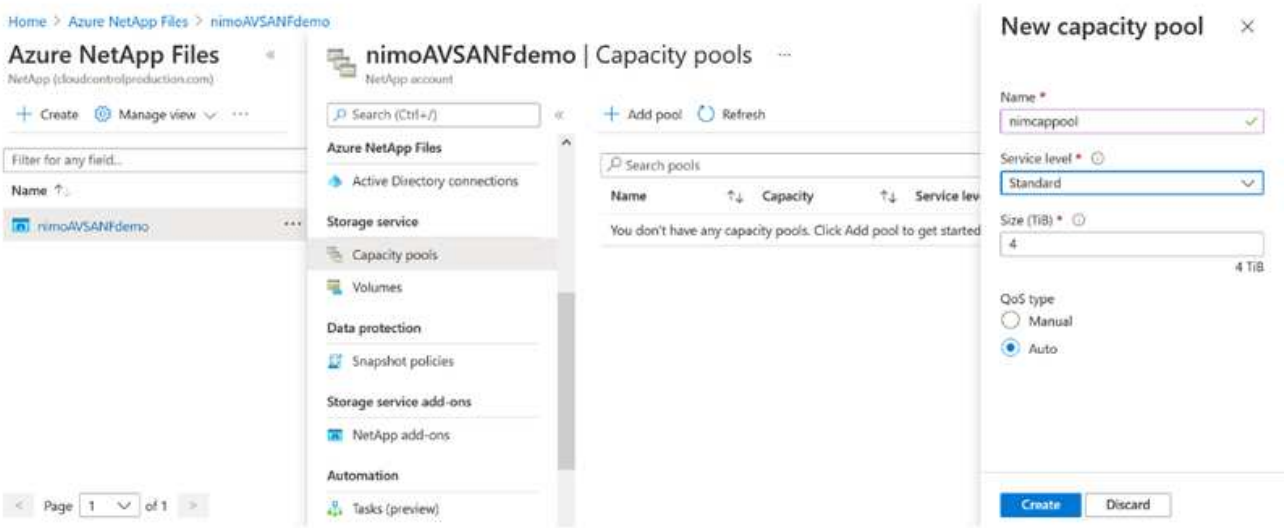
1. Inicie sesión en el Portal de Azure y acceda a Azure NetApp Files. Verifique el acceso al servicio Azure NetApp Files y registre el proveedor de recursos de Azure NetApp Files mediante el comando *az provider register --namespace Microsoft. NetApp –wait*. Una vez completado el registro, cree una cuenta de NetApp .

   Para conocer los pasos detallados, consulte"Recursos compartidos de Azure NetApp Files" . Esta página le guiará a través del proceso paso a paso.

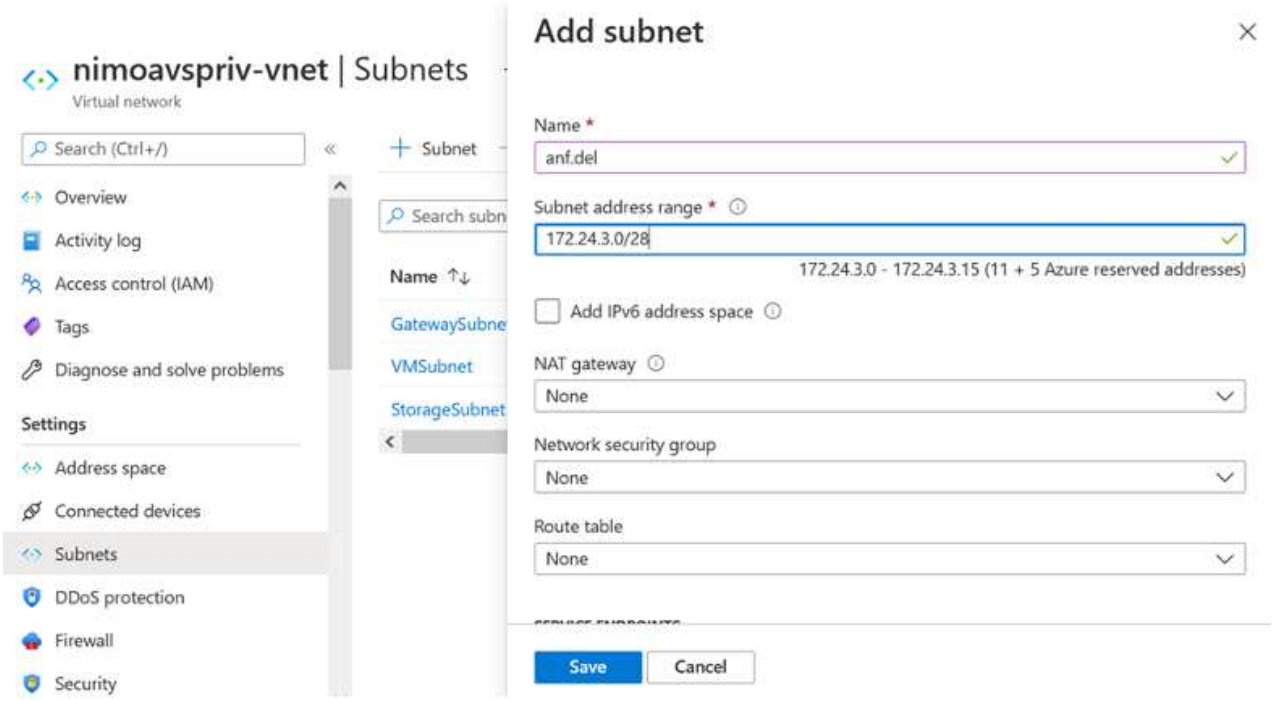


2. Una vez creada la cuenta de NetApp , configure los grupos de capacidad con el tamaño y el nivel de servicio necesarios.

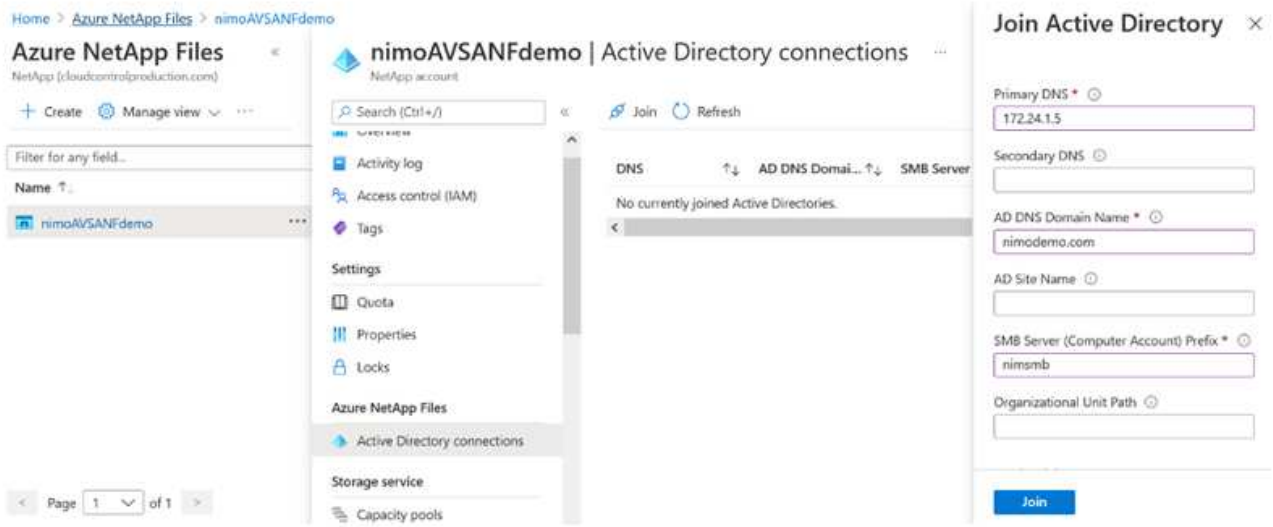
   Para obtener más información, consulte "Crear un fondo de capacidad" .



3. Configure la subred delegada para Azure NetApp Files y especifique esta subred al crear los volúmenes. Para conocer los pasos detallados para crear una subred delegada, consulte"Delegar una subred a Azure NetApp Files" .

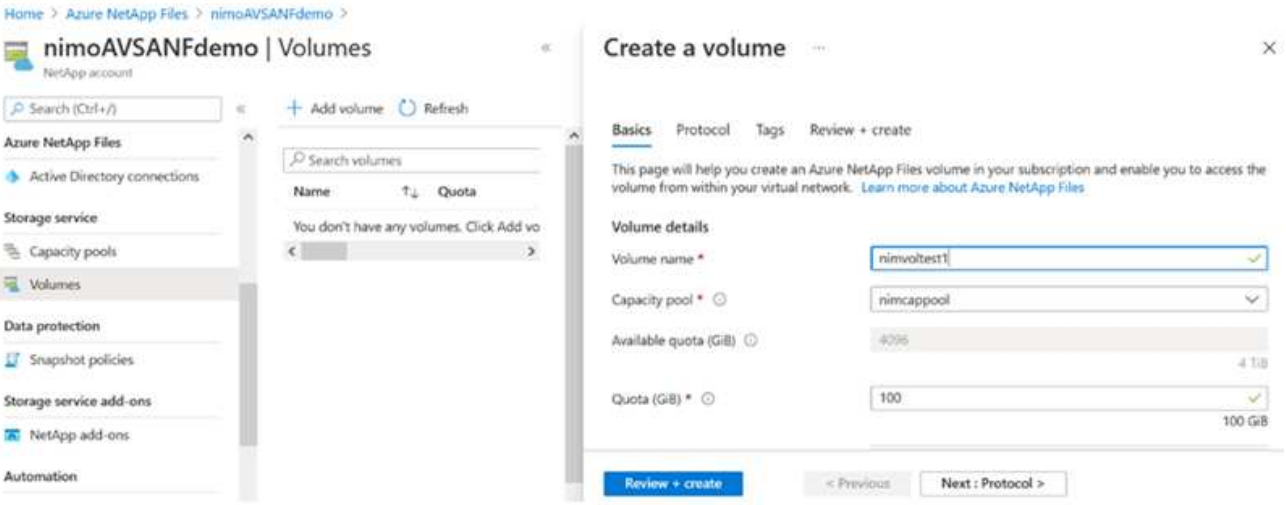


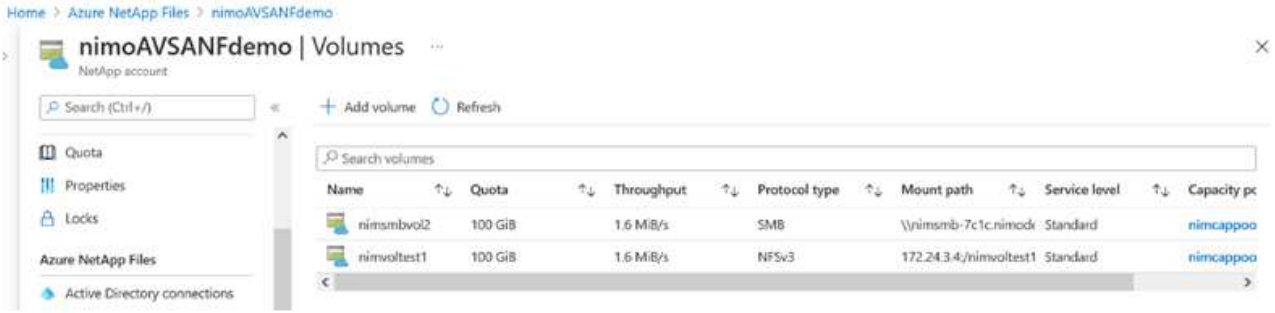
4. Agregue un volumen SMB utilizando la hoja Volúmenes debajo de la hoja Grupos de capacidad. Asegúrese de que el conector de Active Directory esté configurado antes de crear el volumen SMB.



5. Haga clic en Revisar + Crear para crear el volumen SMB.

   Si la aplicación es SQL Server, habilite la disponibilidad continua de SMB.

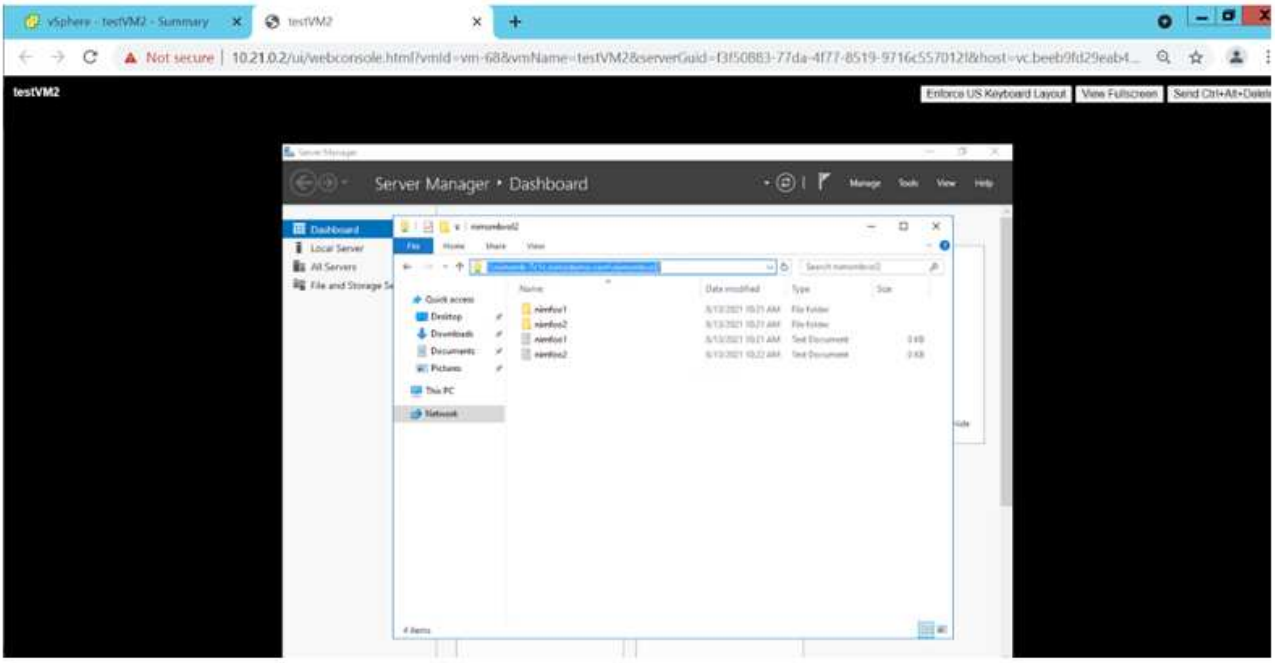


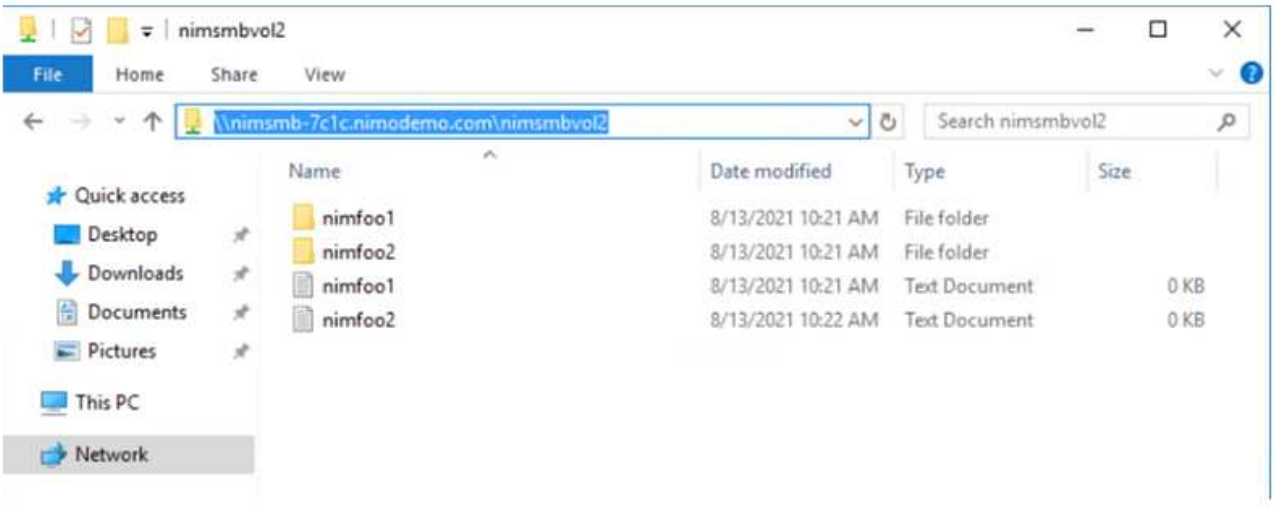


Para obtener más información sobre el rendimiento del volumen de Azure NetApp Files por tamaño o cuota, consulte"Consideraciones de rendimiento para Azure NetApp Files" .

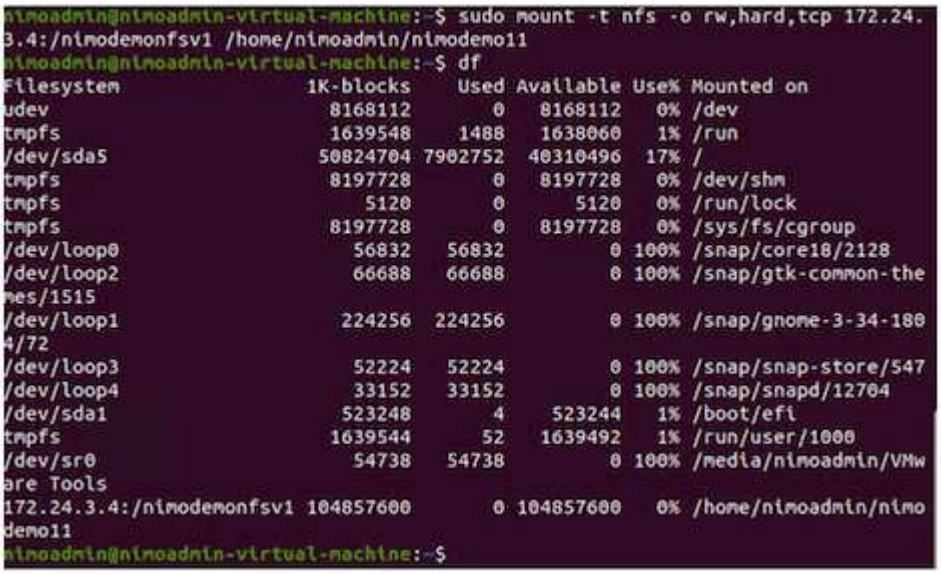
6. Una vez establecida la conectividad, se puede montar el volumen y usarlo para datos de la aplicación.

   Para lograr esto, desde el portal de Azure, haga clic en la hoja Volúmenes y luego seleccione el volumen que desea montar y acceda a las instrucciones de montaje. Copie la ruta y use la opción Asignar unidad de red para montar el volumen en la máquina virtual que se ejecuta en Azure VMware Solution SDDC.





7. Para montar volúmenes NFS en máquinas virtuales Linux que se ejecutan en Azure VMware Solution SDDC, utilice este mismo proceso. Utilice la remodelación de volumen o la capacidad de nivel de servicio dinámico para satisfacer las demandas de carga de trabajo.



Para obtener más información, consulte "Cambiar dinámicamente el nivel de servicio de un volumen" .

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, o CVO, es la solución de gestión de datos en la nube líder en la industria basada en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Es una versión definida por software de ONTAP que consume almacenamiento nativo de la nube, lo que le permite tener el mismo software de almacenamiento en la nube y en las instalaciones, lo que reduce la necesidad de volver a capacitar a su personal de TI en métodos completamente nuevos para administrar sus datos.

CVO brinda a los clientes la capacidad de mover datos sin problemas desde el borde al centro de datos, a la nube y viceversa, unificando su nube híbrida, todo administrado con una consola de administración de panel único, NetApp Cloud Manager.

Por diseño, CVO ofrece un rendimiento extremo y capacidades avanzadas de gestión de datos para satisfacer incluso sus aplicaciones más exigentes en la nube.

Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados

▼ Implementar nuevos Cloud Volumes ONTAP en Azure

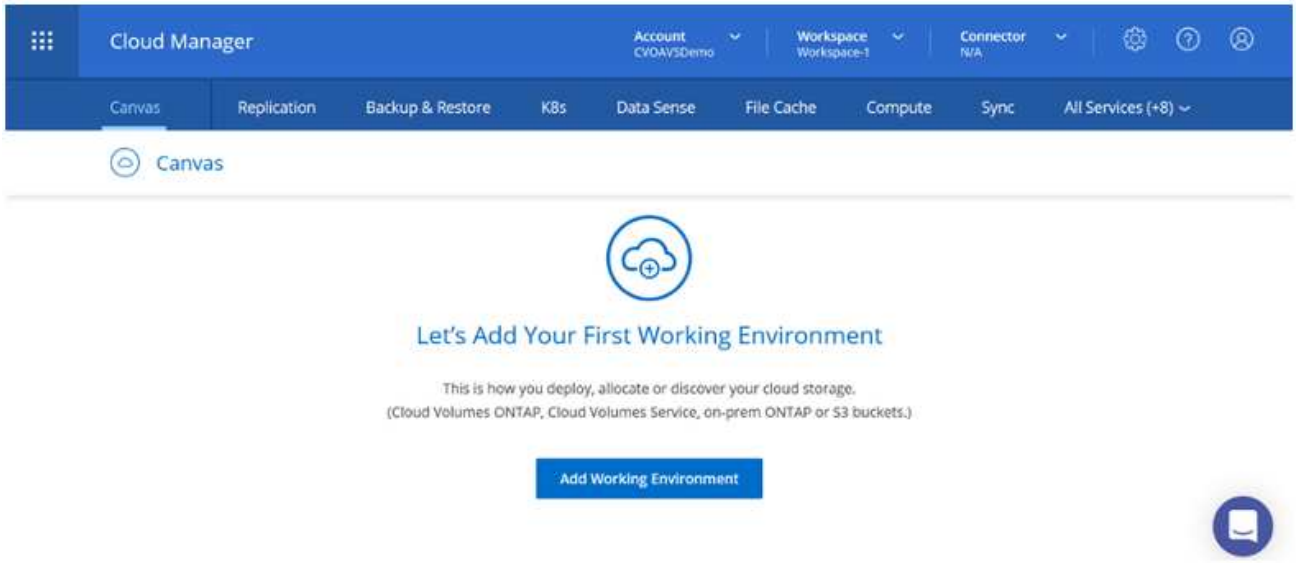
Los recursos compartidos y LUN de Cloud Volumes ONTAP se pueden montar desde máquinas virtuales creadas en el entorno SDDC de Azure VMware Solution. Los volúmenes también se pueden montar en el cliente Linux y en el cliente Windows porque Cloud Volumes ONTAP admite los protocolos iSCSI, SMB y NFS. Los volúmenes Cloud Volumes ONTAP se pueden configurar en unos pocos y sencillos pasos.

Para replicar volúmenes de un entorno local a la nube con fines de recuperación ante desastres o migración, establezca conectividad de red a Azure, ya sea mediante una VPN de sitio a sitio o ExpressRoute. La replicación de datos desde las instalaciones locales a Cloud Volumes ONTAP está fuera del alcance de este documento. Para replicar datos entre sistemas locales y Cloud Volumes ONTAP , consulte"Configuración de la replicación de datos entre sistemas" .

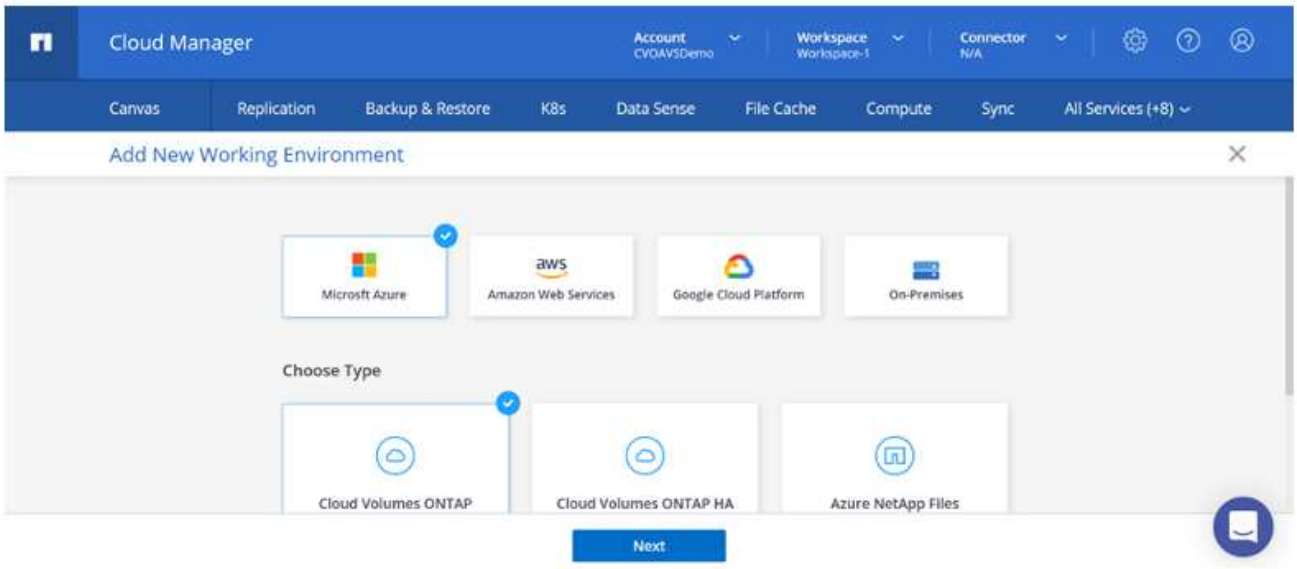
Utiliza "Dimensionador de Cloud Volumes ONTAP" para dimensionar con precisión las instancias de Cloud Volumes ONTAP. Además, supervisa el rendimiento en las instalaciones para usar esos datos como entrada en la herramienta de dimensionamiento de Cloud

Volumes ONTAP.

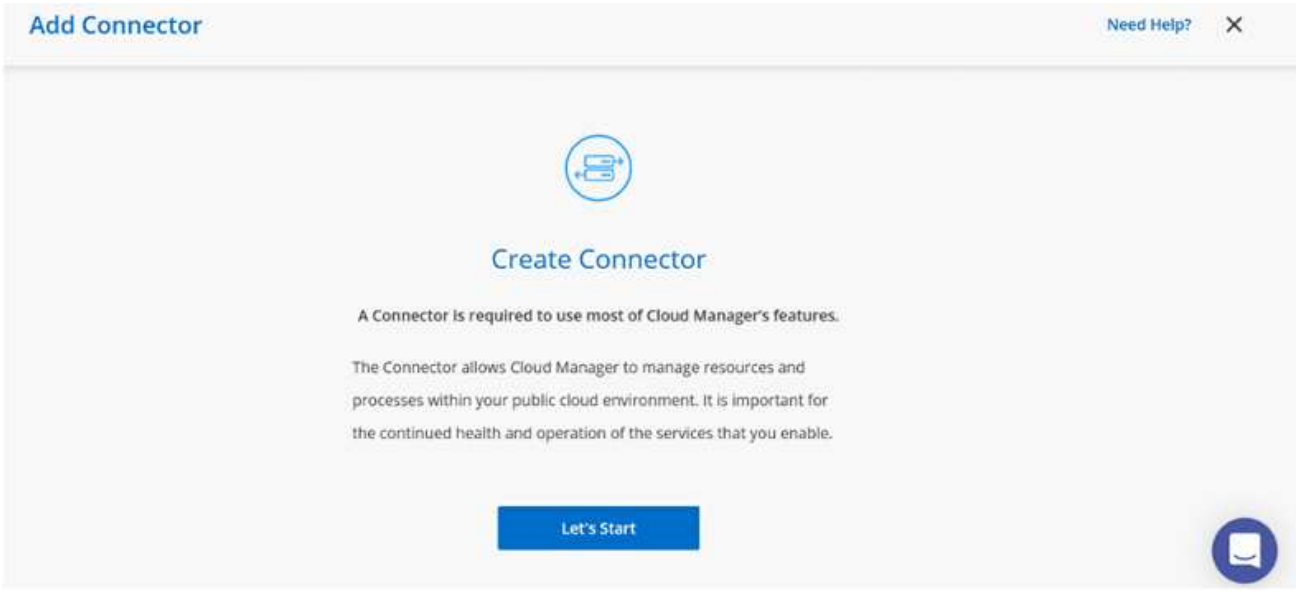
1. Inicie sesión en NetApp Cloud Central: se mostrará la pantalla Vista de Fabric. Localice la pestaña Cloud Volumes ONTAP y seleccione Ir a Cloud Manager. Después de iniciar sesión, se mostrará la pantalla Canvas.



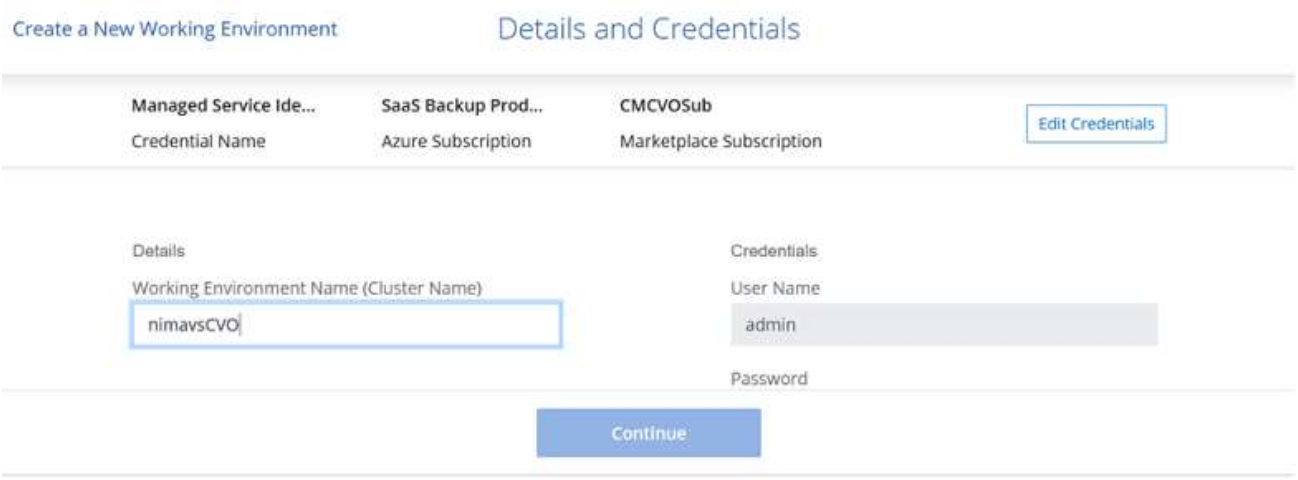
2. En la página de inicio de Cloud Manager, haga clic en Agregar un entorno de trabajo y luego seleccione Microsoft Azure como la nube y el tipo de configuración del sistema.



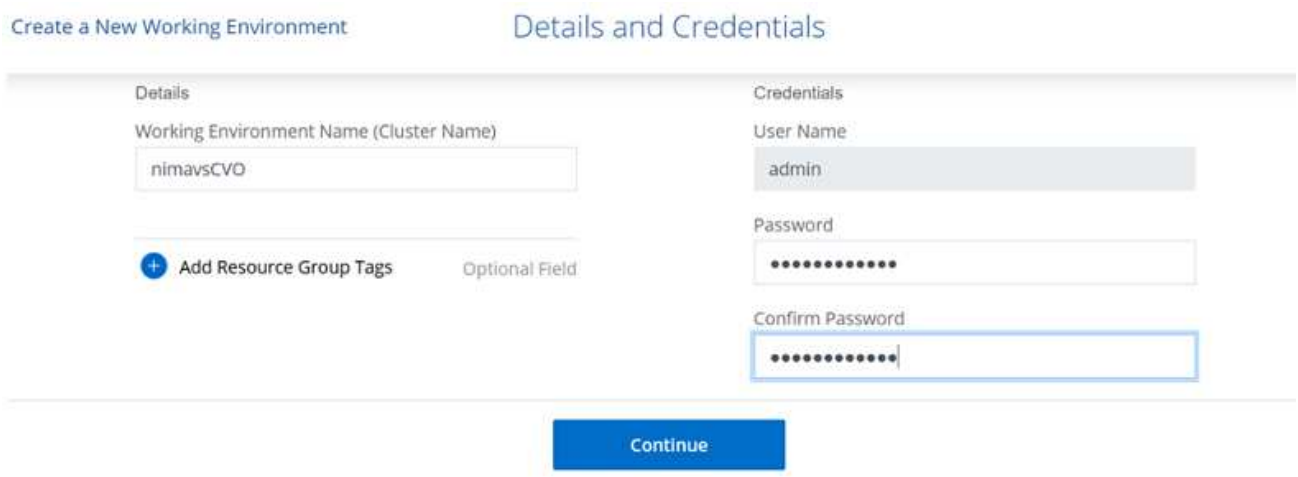
3. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP , Cloud Manager le solicita que implemente un conector.



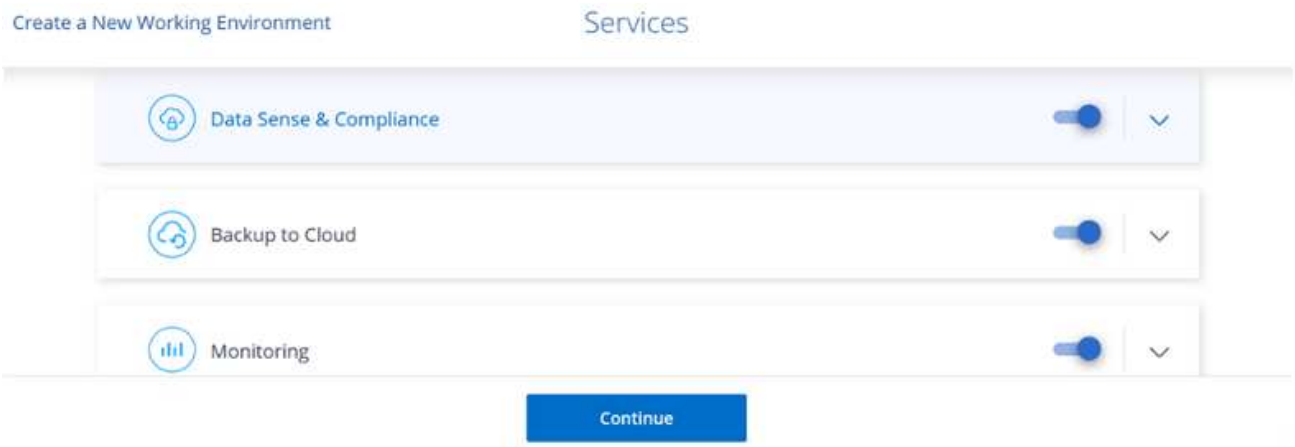
4. Después de crear el conector, actualice los campos Detalles y Credenciales.



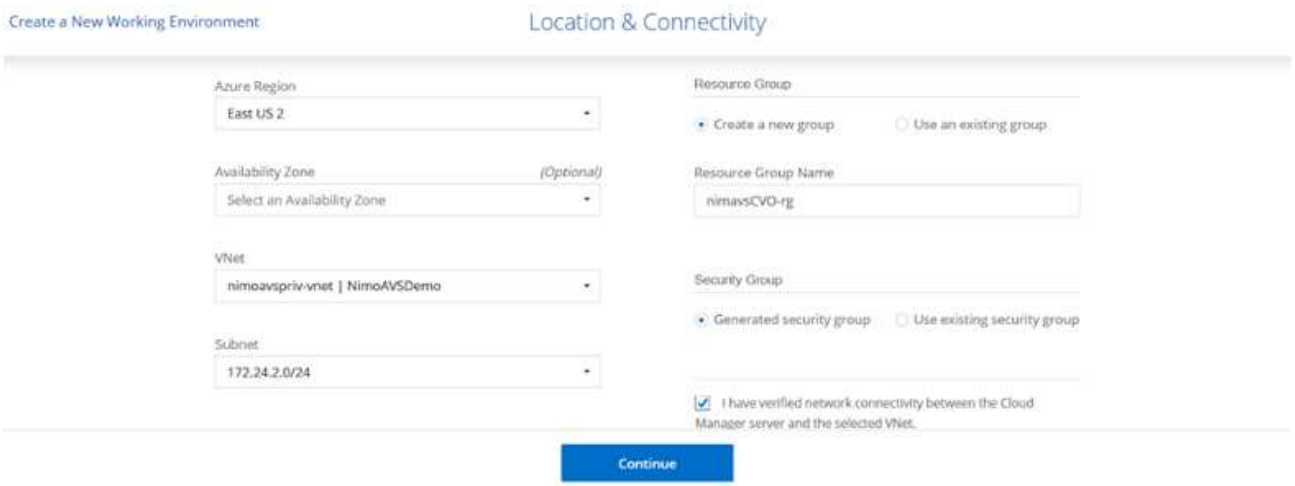
5. Proporcione los detalles del entorno que se creará, incluido el nombre del entorno y las credenciales de administrador. Agregue etiquetas de grupo de recursos para el entorno de Azure como un parámetro opcional. Cuando haya terminado, haga clic en Continuar.



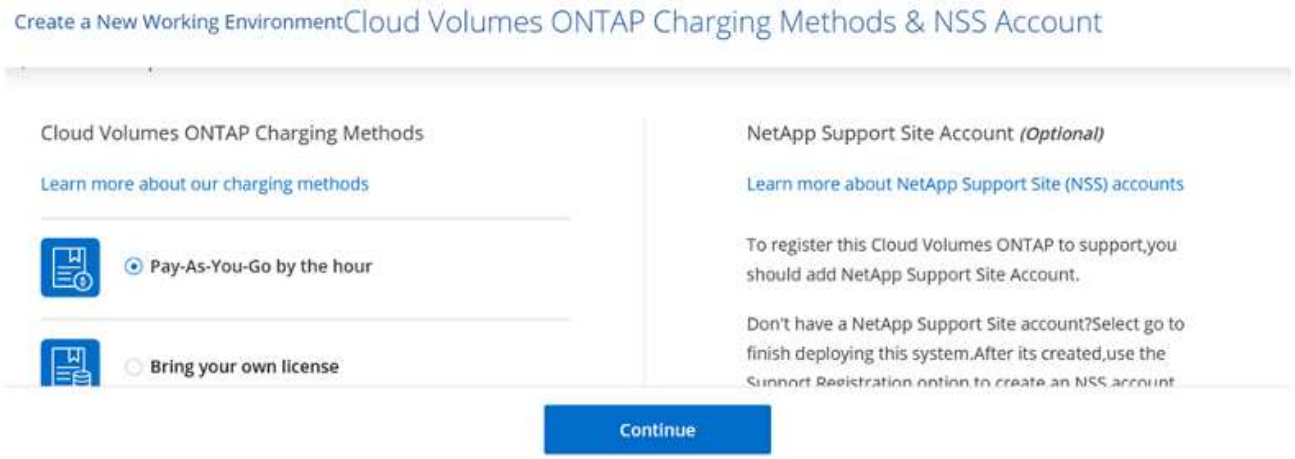
6. Selecciona los servicios complementarios para la implementación de Cloud Volumes ONTAP, incluidos NetApp Data Classification, NetApp Backup and Recovery y Data Infrastructure Insights. Selecciona los servicios y luego haz clic en Continue.



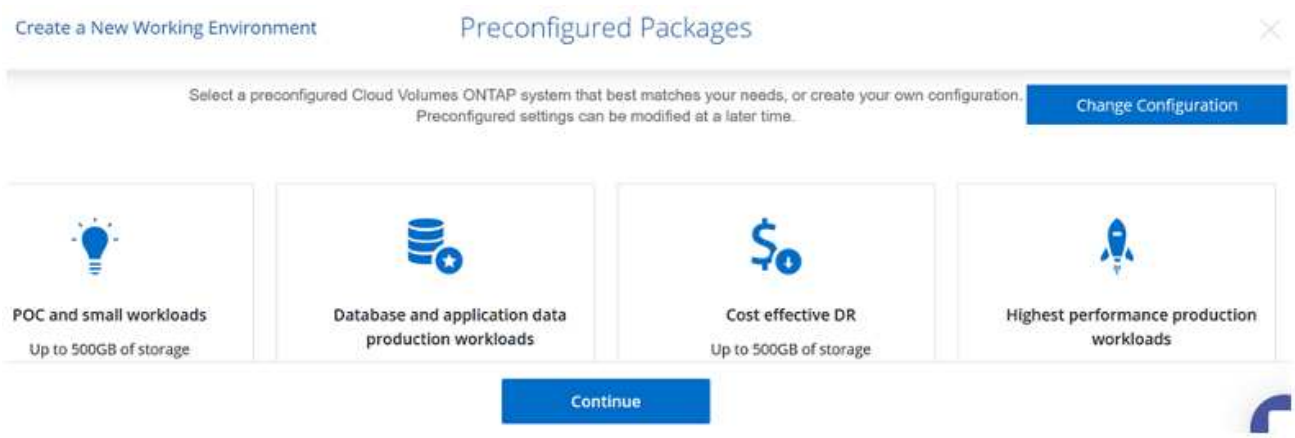
7. Configurar la ubicación y la conectividad de Azure. Seleccione la región de Azure, el grupo de recursos, la red virtual y la subred que se utilizarán.



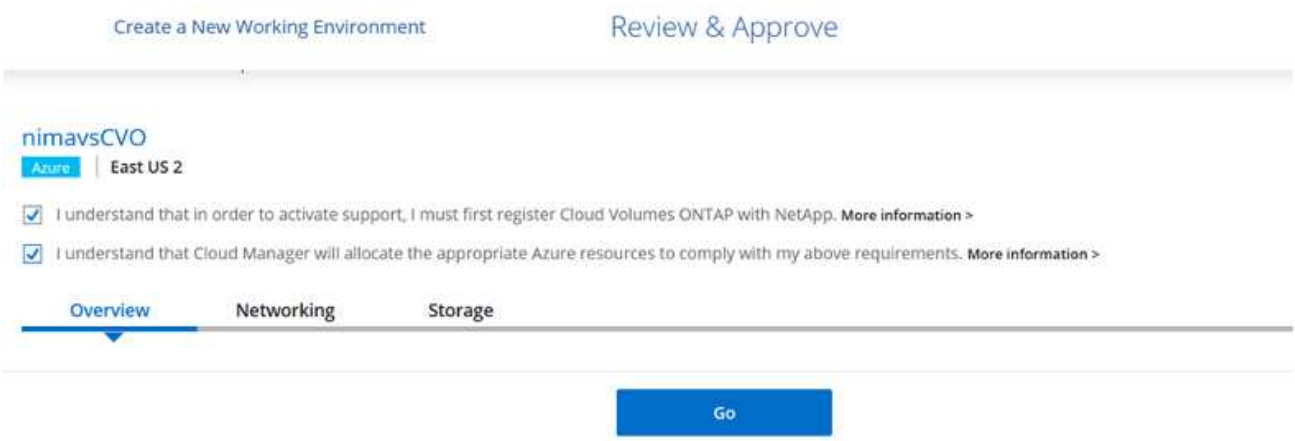
8. Seleccione la opción de licencia: Pago por uso o BYOL para utilizar una licencia existente. En este ejemplo se utiliza la opción de pago por uso.



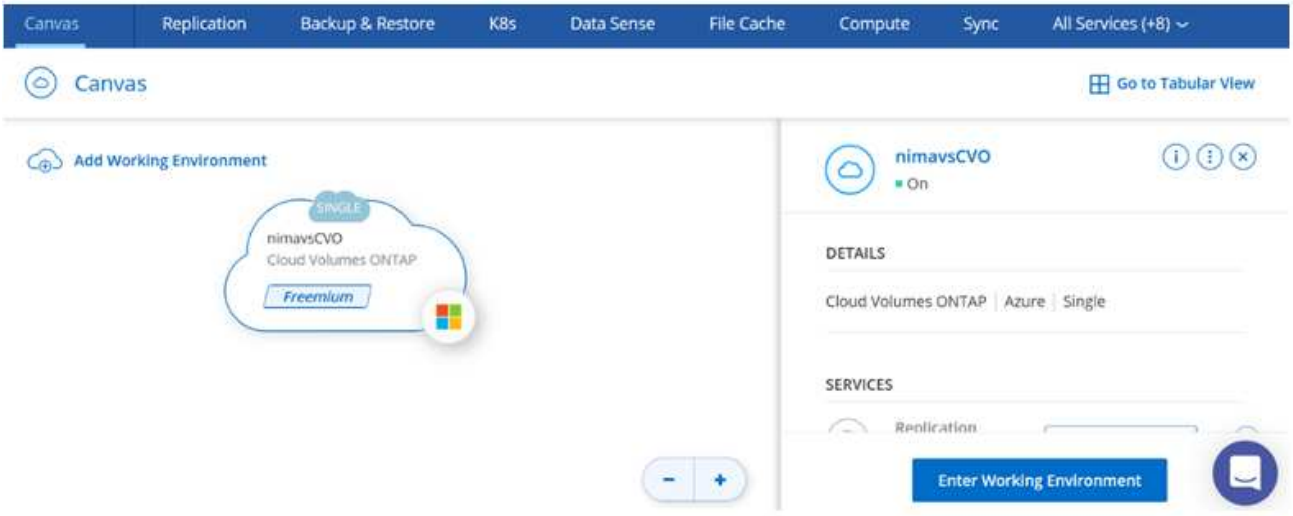
9. Seleccione entre varios paquetes preconfigurados disponibles para los distintos tipos de cargas de trabajo.



10. Acepte los dos acuerdos relacionados con la activación del soporte y la asignación de recursos de Azure. Para crear la instancia de Cloud Volumes ONTAP , haga clic en Ir.

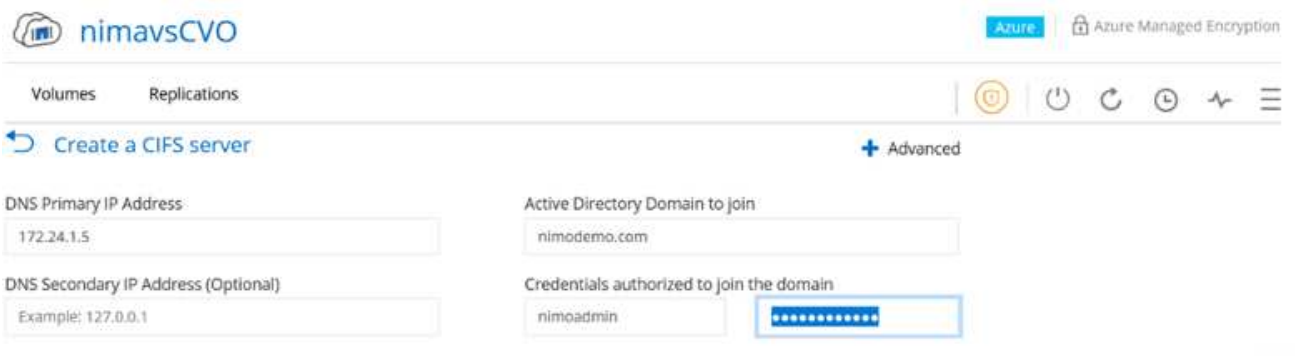


11. Una vez aprovisionado Cloud Volumes ONTAP , aparece en los entornos de trabajo en la página Canvas.

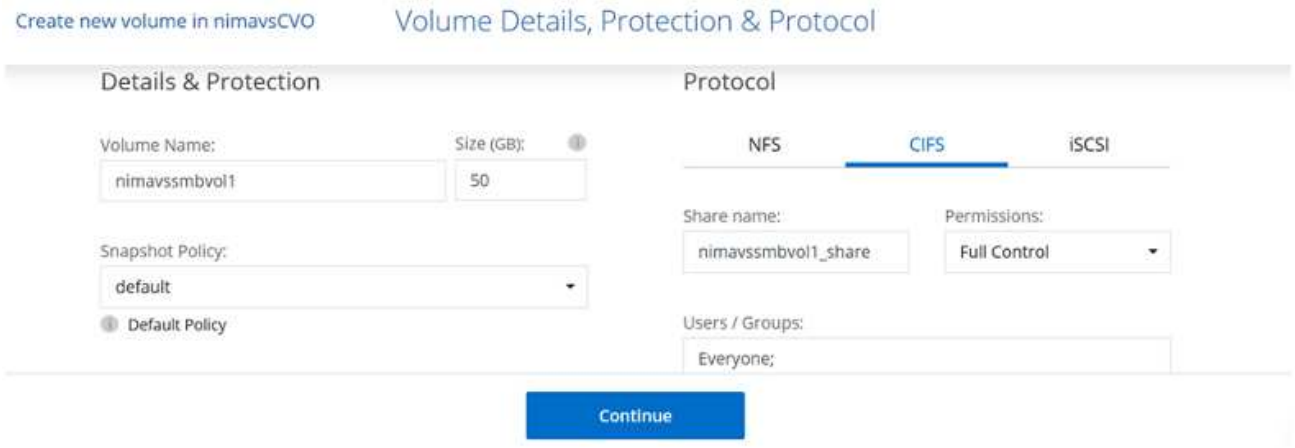


▼ Configuraciones adicionales para volúmenes SMB

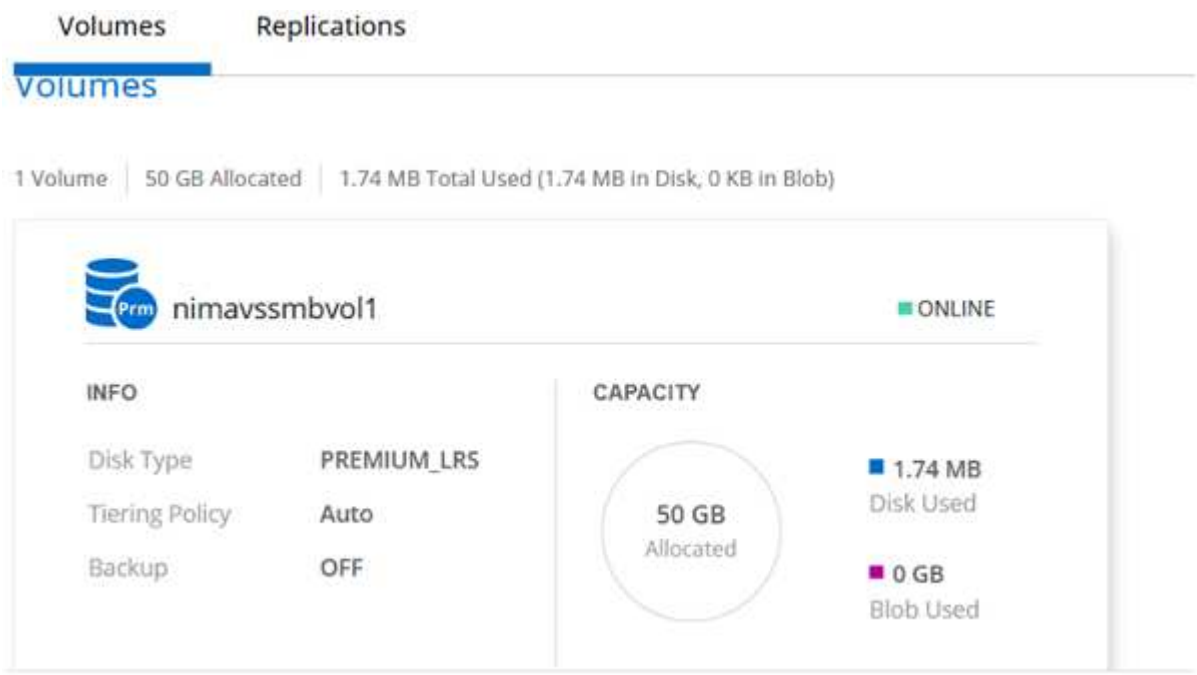
1. Una vez que el entorno de trabajo esté listo, asegúrese de que el servidor CIFS esté configurado con los parámetros de configuración de DNS y Active Directory adecuados. Este paso es necesario antes de poder crear el volumen SMB.



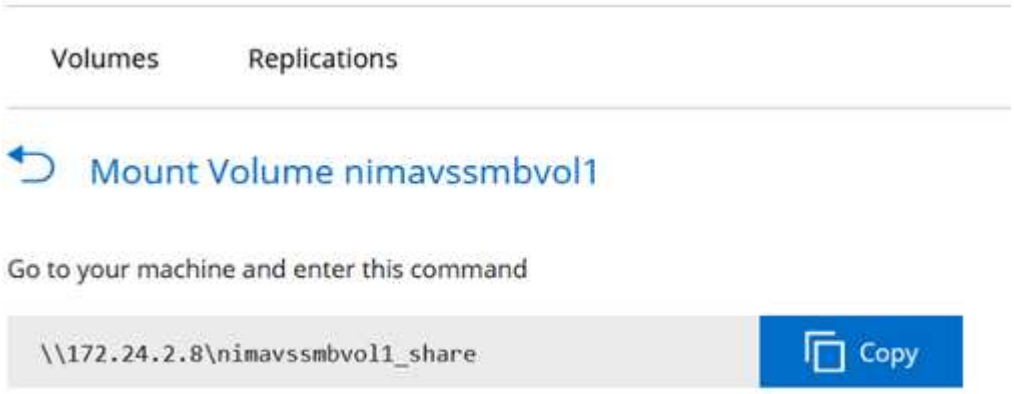
2. Crear el volumen SMB es un proceso sencillo. Seleccione la instancia CVO para crear el volumen y haga clic en la opción Crear volumen. Elija el tamaño apropiado y el administrador de la nube elige el agregado que lo contiene o utiliza un mecanismo de asignación avanzado para colocarlo en un agregado específico. Para esta demostración, se selecciona SMB como protocolo.

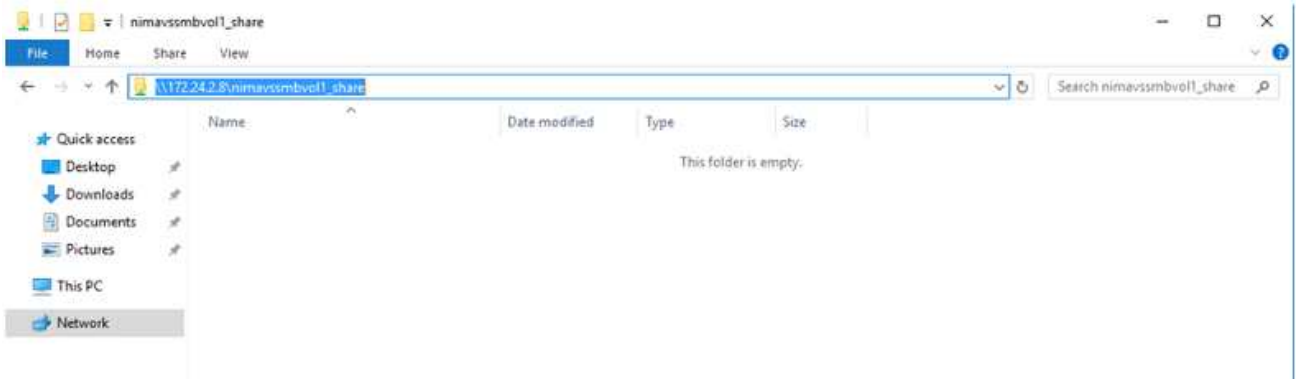


3. Una vez aprovisionado el volumen, estará disponible en el panel Volúmenes. Debido a que se aprovisiona un recurso compartido CIFS, otorgue a sus usuarios o grupos permiso para acceder a los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo. Este paso no es necesario si el volumen se replica desde un entorno local porque los permisos de archivos y carpetas se conservan como parte de la replicación de SnapMirror .



4. Una vez creado el volumen, use el comando mount para conectarse al recurso compartido desde la máquina virtual que se ejecuta en los hosts SDDC de Azure VMware Solution.
5. Copie la siguiente ruta y use la opción Asignar unidad de red para montar el volumen en la máquina virtual que se ejecuta en Azure VMware Solution SDDC.

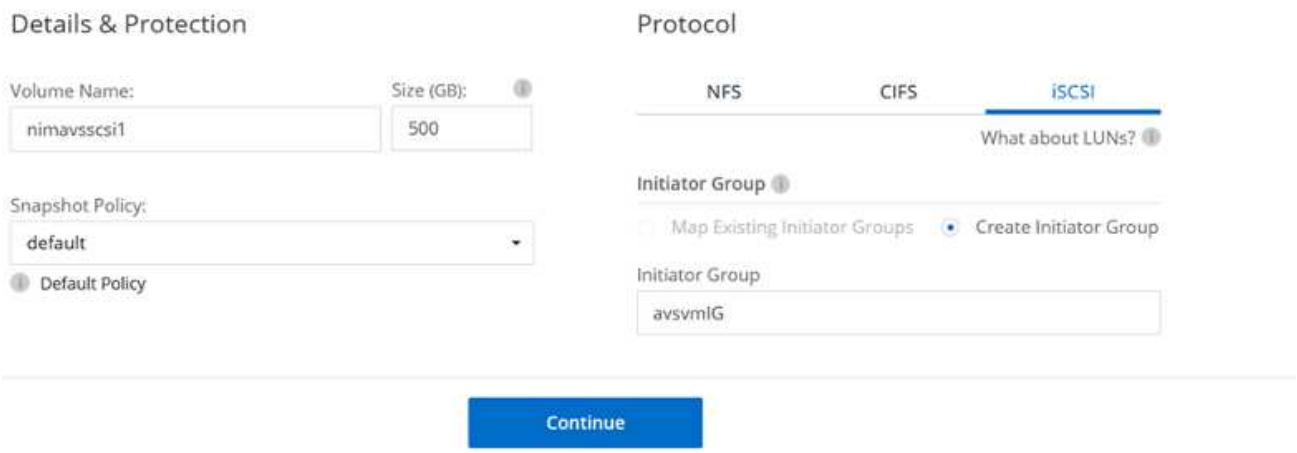




▼ **Conectar el LUN a un host**

Para conectar el LUN a un host, complete los siguientes pasos:

1. En la página Lienzo, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP para crear y administrar volúmenes.
2. Haga clic en Agregar volumen > Nuevo volumen y seleccione iSCSI y haga clic en Crear grupo de iniciadores. Haga clic en Continuar.



3. Una vez aprovisionado el volumen, seleccione el volumen y haga clic en IQN de destino. Para copiar el nombre calificado iSCSI (IQN), haga clic en Copiar. Configure una conexión iSCSI desde el host al LUN.

   Para lograr lo mismo para el host que reside en Azure VMware Solution SDDC:

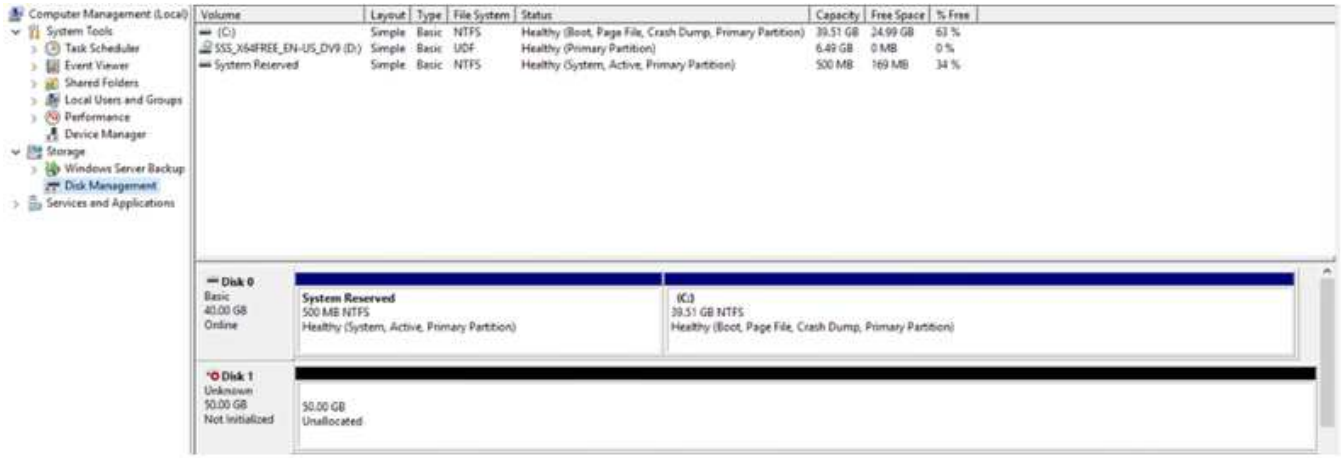
   a. RDP a la máquina virtual alojada en Azure VMware Solution SDDC.
   b. Abra el cuadro de diálogo Propiedades del iniciador iSCSI: Administrador del servidor > Panel de control > Herramientas > Iniciador iSCSI.
   c. Desde la pestaña Descubrimiento, haga clic en Descubrir portal o Agregar portal y luego ingrese la dirección IP del puerto de destino iSCSI.
   d. Desde la pestaña Objetivos, seleccione el objetivo descubierto y luego haga clic en Iniciar sesión o Conectar.
   e. Seleccione Habilitar múltiples rutas y, a continuación, seleccione Restaurar esta conexión automáticamente cuando se inicie el equipo o Agregar esta conexión a la lista de destinos favoritos. Haga clic en Avanzado.

      Nota: El host de Windows debe tener una conexión iSCSI a cada nodo del clúster. El DSM nativo selecciona las mejores rutas a utilizar.



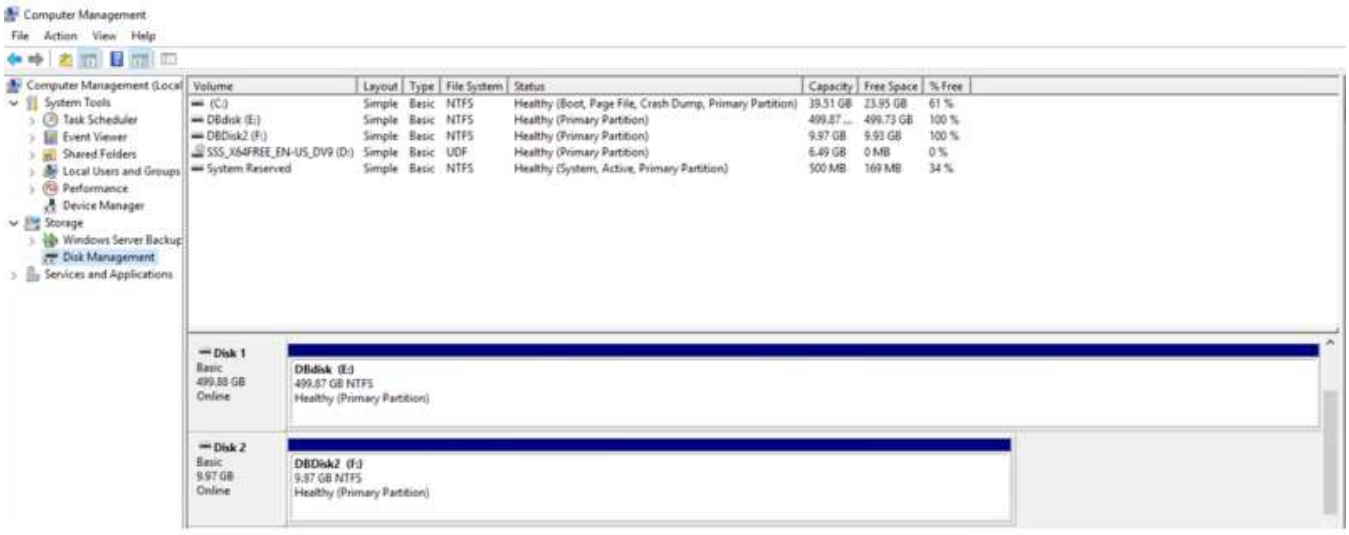
Los LUN en una máquina virtual de almacenamiento (SVM) aparecen como discos para el host de Windows. El host no detecta automáticamente ningún disco nuevo que se agregue. Active un nuevo escaneo manual para descubrir los discos completando los siguientes pasos:

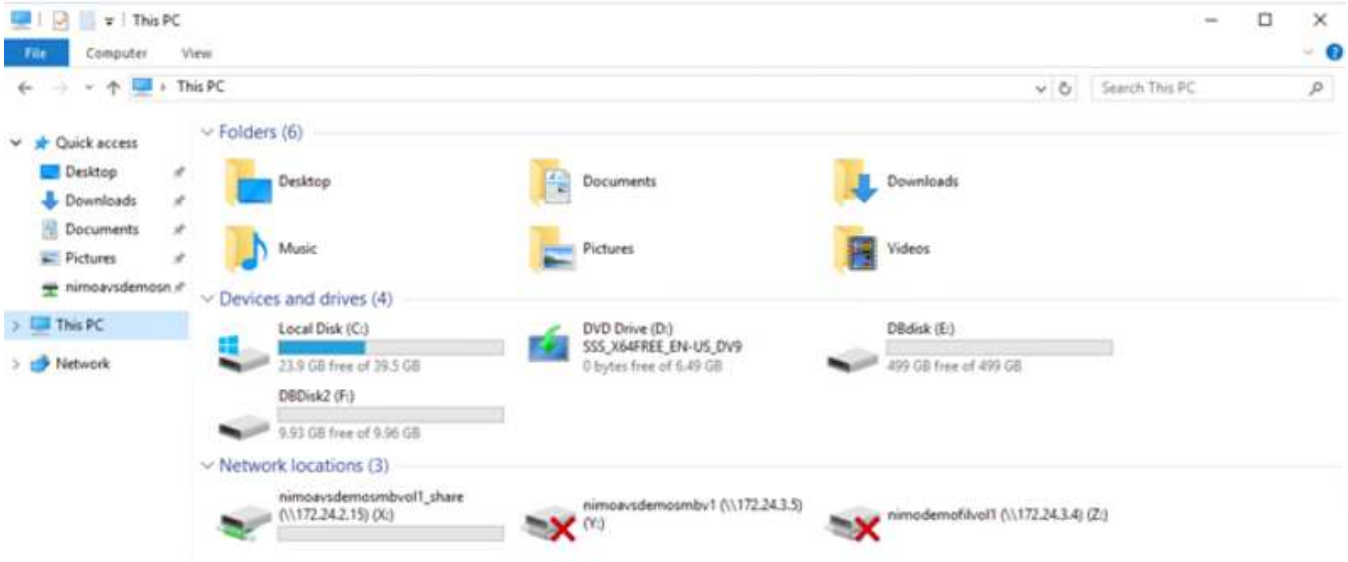
1. Abra la utilidad de Administración de equipos de Windows: Inicio > Herramientas administrativas > Administración de equipos.
2. Expanda el nodo Almacenamiento en el árbol de navegación.
3. Haga clic en Administración de discos.
4. Haga clic en Acción > Volver a escanear discos.



Cuando el host de Windows accede por primera vez a un nuevo LUN, éste no tiene partición ni sistema de archivos. Inicialice el LUN y, opcionalmente, formatee el LUN con un sistema de archivos completando los siguientes pasos:

1. Inicie la Administración de discos de Windows.
2. Haga clic con el botón derecho en el LUN y luego seleccione el tipo de disco o partición requerido.
3. Siga las instrucciones del asistente. En este ejemplo, la unidad E: está montada





Google Cloud VMware Engine: opciones para usar el almacenamiento de NetApp

El almacenamiento de NetApp se puede conectar a Google Cloud Virtualization Engine como almacenamiento complementario o conectado a invitado.

Google Cloud NetApp Volumes (NetApp Volumes) como almacén de datos NFS complementario

Los clientes que requieren capacidad de almacenamiento adicional en su entorno de Google Cloud VMware Engine (GCVE) pueden utilizar Google Cloud NetApp Volumes para montarlo como almacén de datos NFS complementario. El almacenamiento de datos en Google Cloud NetApp Volumes permite a los clientes replicar entre regiones para protegerse contra desastres.

Para obtener más información, visite"Google Cloud NetApp Volumes (NetApp Volumes) como almacén de datos NFS complementario"

NetApp CVO como almacenamiento conectado para invitados

Cloud Volumes ONTAP, o CVO, es la solución de gestión de datos en la nube líder en la industria basada en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Es una versión definida por software de ONTAP que consume almacenamiento nativo de la nube, lo que le permite tener el mismo software de almacenamiento en la nube y en las instalaciones, lo que reduce la necesidad de volver a capacitar a su personal de TI en métodos completamente nuevos para administrar sus datos.

CVO brinda a los clientes la capacidad de mover datos sin problemas desde el borde al centro de datos, a la nube y viceversa, unificando su nube híbrida, todo administrado con una consola de administración de panel único, NetApp Cloud Manager.

Por diseño, CVO ofrece un rendimiento extremo y capacidades avanzadas de gestión de datos para satisfacer incluso sus aplicaciones más exigentes en la nube.

Para obtener más información, visite"NetApp CVO como almacenamiento conectado para invitados"

Google Cloud NetApp Volumes (NetApp Volumes) como almacenamiento conectado para invitados

Los recursos compartidos de Google Cloud NetApp Volumes se pueden montar desde máquinas virtuales creadas en el entorno de VMware Engine. Los volúmenes también se pueden montar en el cliente Linux y mapear en el cliente Windows porque Google Cloud NetApp Volumes admite los protocolos SMB y NFS. Los volúmenes de Google Cloud NetApp Volumes se pueden configurar en pasos sencillos.

Los Google Cloud NetApp Volumes y la nube privada de Google Cloud VMware Engine deben estar en la misma región.

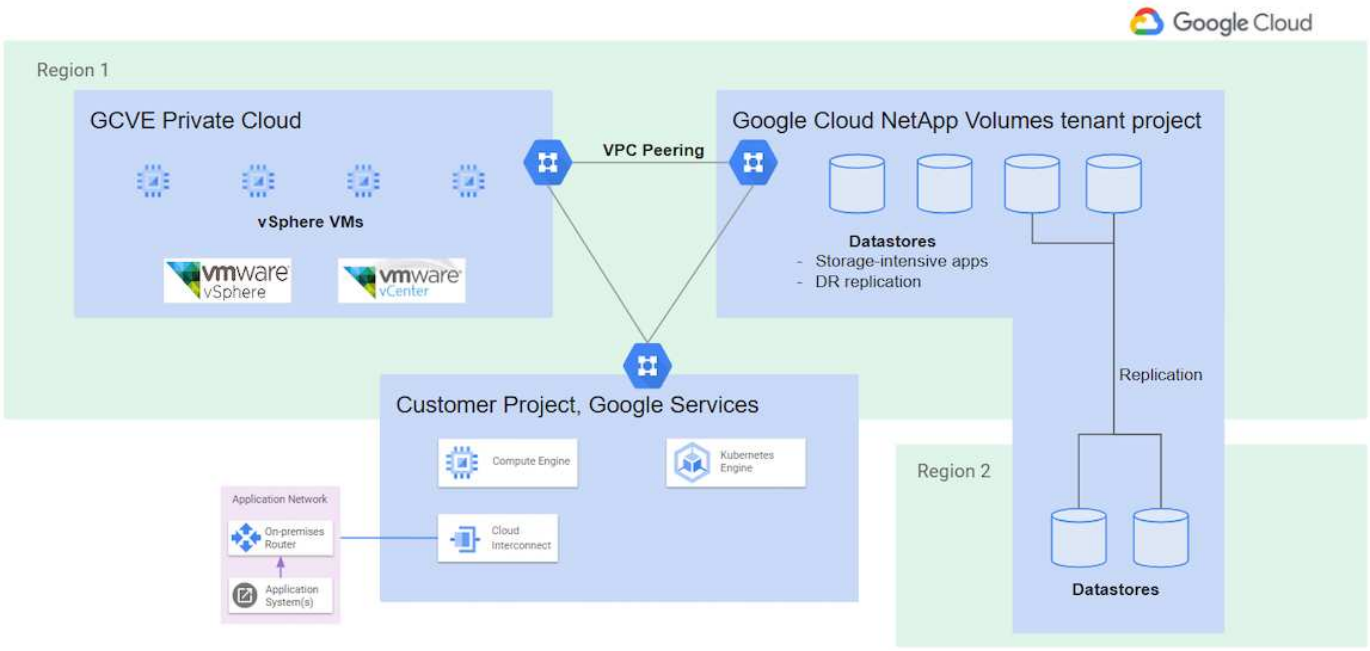
Para obtener más información, visite"Google Cloud NetApp Volumes (NetApp Volumes) como almacenamiento conectado para invitados"

Almacén de datos NFS complementario de VMware Engine de Google Cloud con Google Cloud NetApp Volumes

Los clientes pueden ampliar la capacidad de almacenamiento en Google Cloud VMware Engine mediante el almacén de datos complementario NFS con Google Cloud NetApp Volumes.

Descripción general

Los clientes que requieren capacidad de almacenamiento adicional en su entorno de Google Cloud VMware Engine (GCVE) pueden utilizar Netapp Cloud Volume Service para montarlo como almacén de datos NFS complementario. El almacenamiento de datos en Google Cloud NetApp Volumes permite a los clientes replicar entre regiones para protegerse contra desastres.



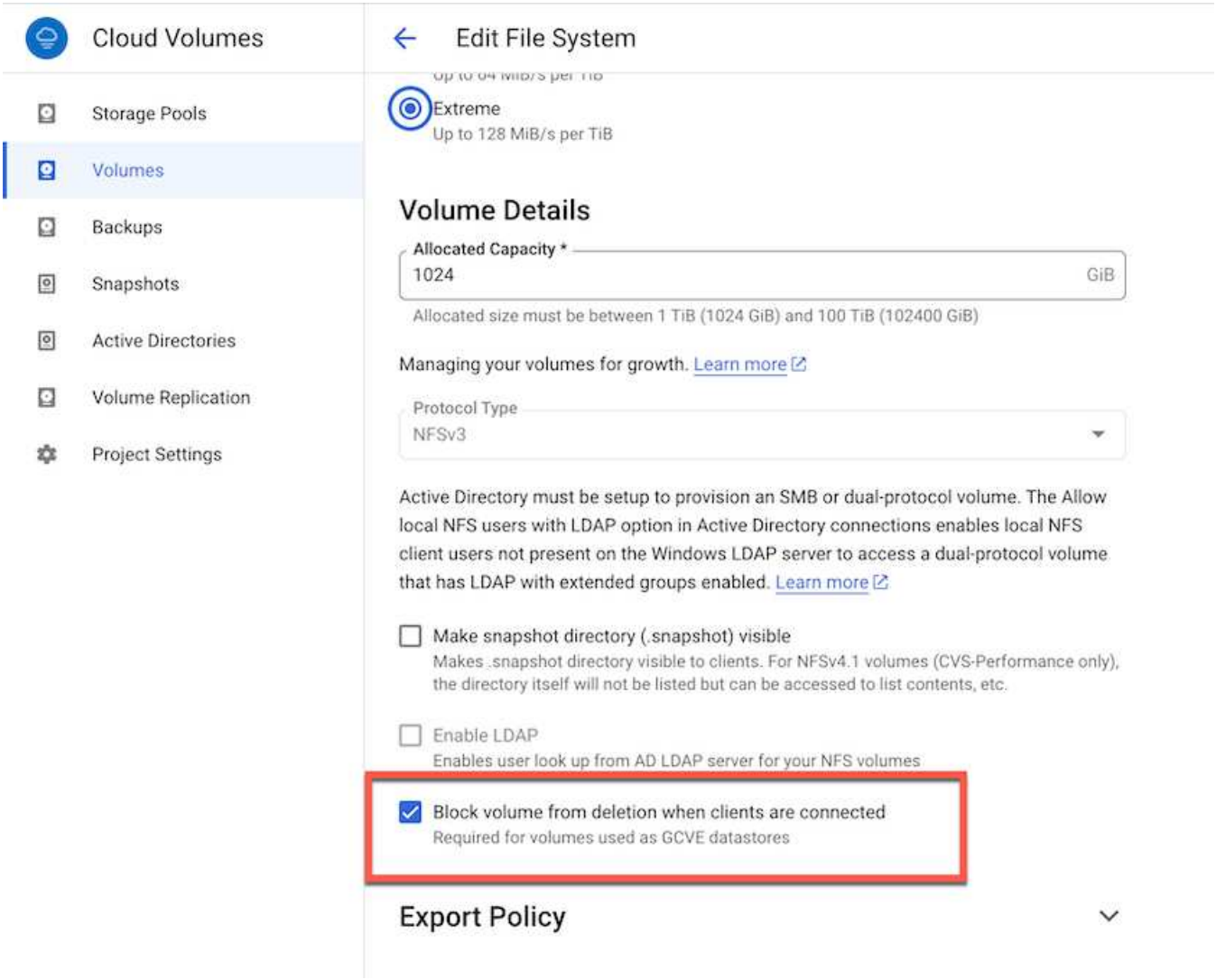
Pasos de implementación para montar un almacén de datos NFS desde Google Cloud NetApp Volumes (NetApp Volumes) en GCVE

▼ Aprovisionamiento de volúmenes NetApp : volumen de rendimiento

El volumen de Google Cloud NetApp Volumes se puede aprovisionar mediante "Uso de Google Cloud Console" "Uso de la CLI o la API de Google Cloud"

▼ Marcar ese volumen de NetApp Volumes como no eliminable

Para evitar la eliminación accidental del volumen mientras la VM está en ejecución, asegúrate de que el volumen esté marcado como no eliminable, como se muestra en la captura de pantalla de abajo.



Para obtener más información, consulta la documentación de "Creación de un volumen NFS".

▼ **Asegúrese de que exista una conexión privada en GCVE para la VPC de inquilino de NetApp Volumes.**

Para montar un almacén de datos NFS, debe existir una conexión privada entre GCVE y el proyecto NetApp Volumes. Para obtener más información, consulte"Cómo configurar el acceso al servicio privado"

▼ **Montar almacén de datos NFS**

Para obtener instrucciones sobre cómo montar el almacén de datos NFS en GCVE, consulte"Cómo crear un almacén de datos NFS con NetApp Volumes"

Como los hosts de vSphere están administrados por Google, no tienes acceso para instalar NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB). Si necesita ayuda con volúmenes virtuales (vVol), infórmenos. Si desea utilizar Jumbo Frames, consulte"Tamaños máximos de MTU admitidos en GCP"

Ahorros con Google Cloud NetApp Volumes

Para obtener más información sobre el ahorro potencial con Google Cloud NetApp Volumes para tus necesidades de almacenamiento en GCVE, consulta "Calculadora de ROI de NetApp"

Enlaces de referencia

- "Blog de Google: Cómo usar NetApp Volumes como almacenes de datos para Google Cloud VMware Engine"
- "Blog de NetApp : Una mejor manera de migrar sus aplicaciones con gran capacidad de almacenamiento a Google Cloud"

Opciones de almacenamiento de NetApp para GCP

GCP admite el almacenamiento NetApp conectado a invitados con Cloud Volumes ONTAP (CVO) o Google Cloud NetApp Volumes (NetApp Volumes).

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, o CVO, es la solución de gestión de datos en la nube líder en la industria basada en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Es una versión definida por software de ONTAP que consume almacenamiento nativo de la nube, lo que le permite tener el mismo software de almacenamiento en la nube y en las instalaciones, lo que reduce la necesidad de volver a capacitar a su personal de TI en métodos completamente nuevos para administrar sus datos.

CVO brinda a los clientes la capacidad de mover datos sin problemas desde el borde al centro de datos, a la nube y viceversa, unificando su nube híbrida, todo administrado con una consola de administración de panel único, NetApp Cloud Manager.

Por diseño, CVO ofrece un rendimiento extremo y capacidades avanzadas de gestión de datos para satisfacer incluso sus aplicaciones más exigentes en la nube.

Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados

▼ **Implementar Cloud Volumes ONTAP en Google Cloud (hazlo tú mismo)**

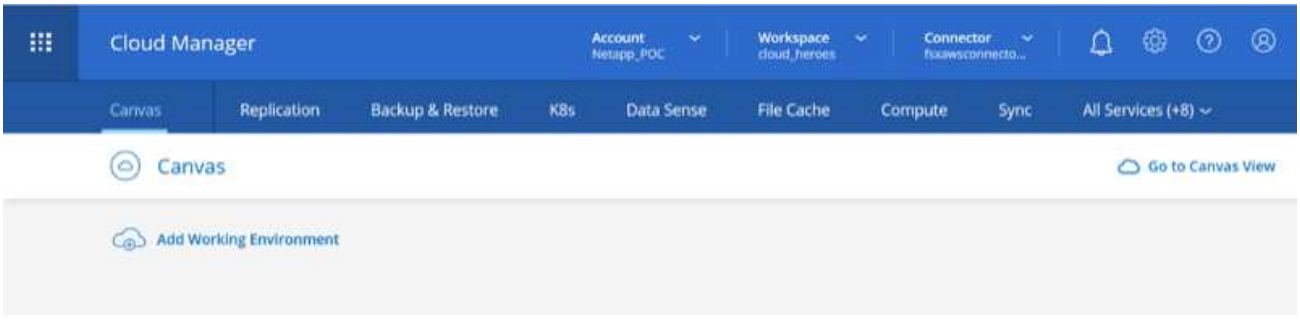
Los recursos compartidos y LUN de Cloud Volumes ONTAP se pueden montar desde máquinas virtuales creadas en el entorno de nube privada de GCVE. Los volúmenes también se pueden montar en el cliente Linux y en el cliente Windows, y se puede acceder a los LUN en clientes Linux o Windows como dispositivos de bloque cuando se montan sobre iSCSI porque Cloud Volumes ONTAP admite los protocolos iSCSI, SMB y NFS. Los volúmenes de Cloud Volumes ONTAP se pueden configurar en unos pocos y sencillos pasos.

Para replicar volúmenes de un entorno local a la nube con fines de recuperación ante desastres o migración, establezca conectividad de red con Google Cloud, ya sea mediante una VPN de sitio a sitio o Cloud Interconnect. La replicación de datos desde las instalaciones locales a Cloud Volumes ONTAP está fuera del alcance de este documento. Para replicar datos entre sistemas locales y Cloud Volumes ONTAP , consulte"Configuración de la replicación de datos entre sistemas" .

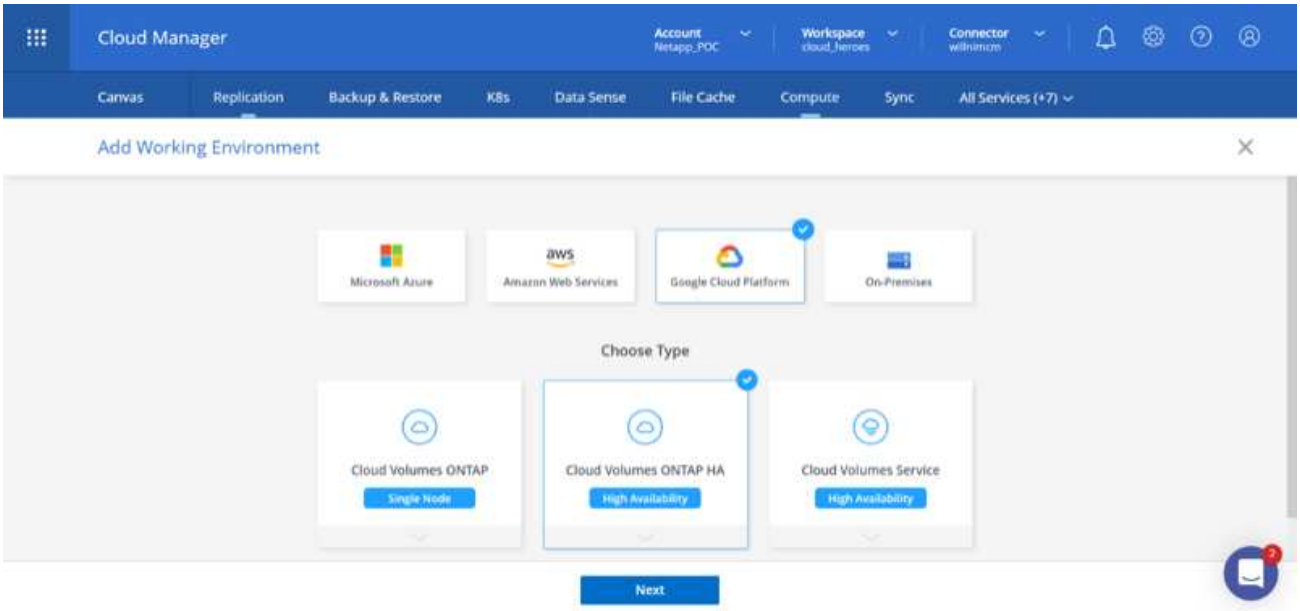
> Utiliza "Dimensionador de Cloud Volumes ONTAP" para dimensionar con precisión las instancias de Cloud Volumes ONTAP. Además, supervisa el rendimiento en las instalaciones para usar esos datos como entrada en la herramienta de dimensionamiento de Cloud Volumes ONTAP.

1. Inicie sesión en NetApp Cloud Central: se mostrará la pantalla Vista de Fabric. Localice la pestaña Cloud Volumes ONTAP y seleccione Ir a Cloud Manager. Después de iniciar sesión, se mostrará la

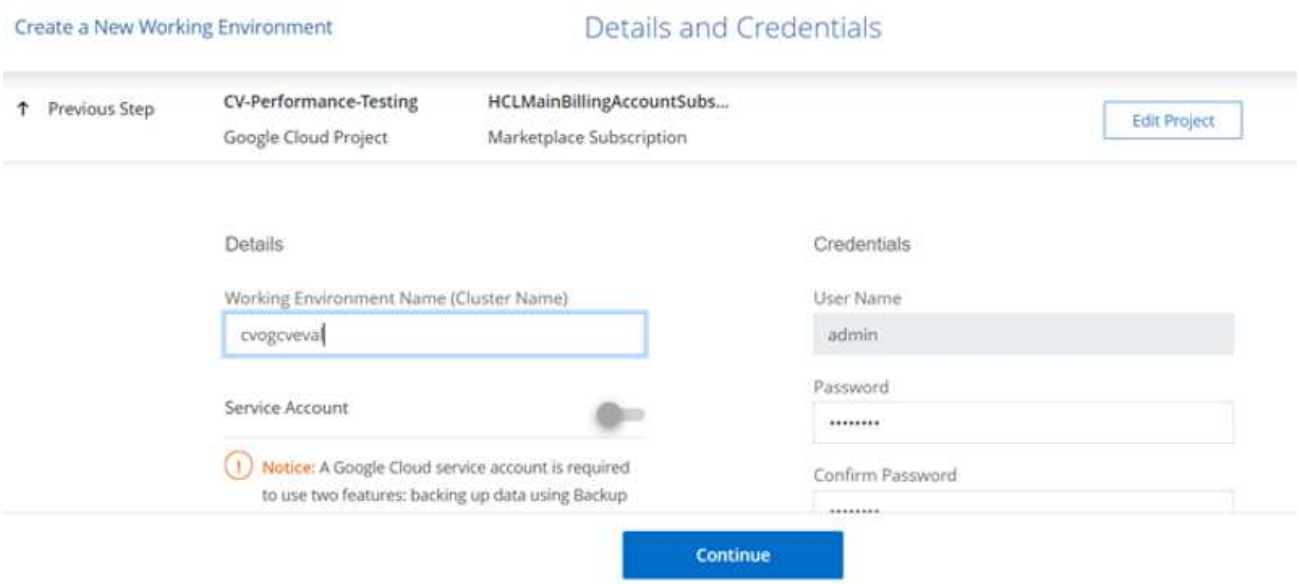
pantalla Canvas.



2. En la pestaña Canvas de Cloud Manager, haga clic en Agregar un entorno de trabajo y luego seleccione Google Cloud Platform como la nube y el tipo de configuración del sistema. Luego, haga clic en Siguiente.

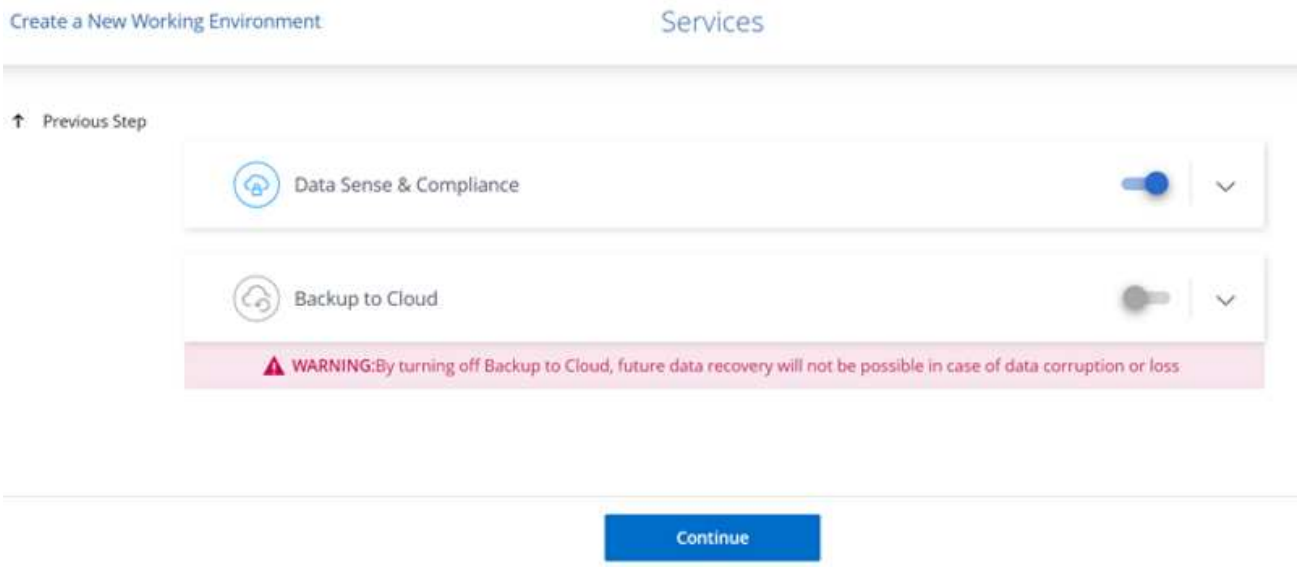


3. Proporcione los detalles del entorno que se creará, incluido el nombre del entorno y las credenciales de administrador. Cuando haya terminado, haga clic en Continuar.

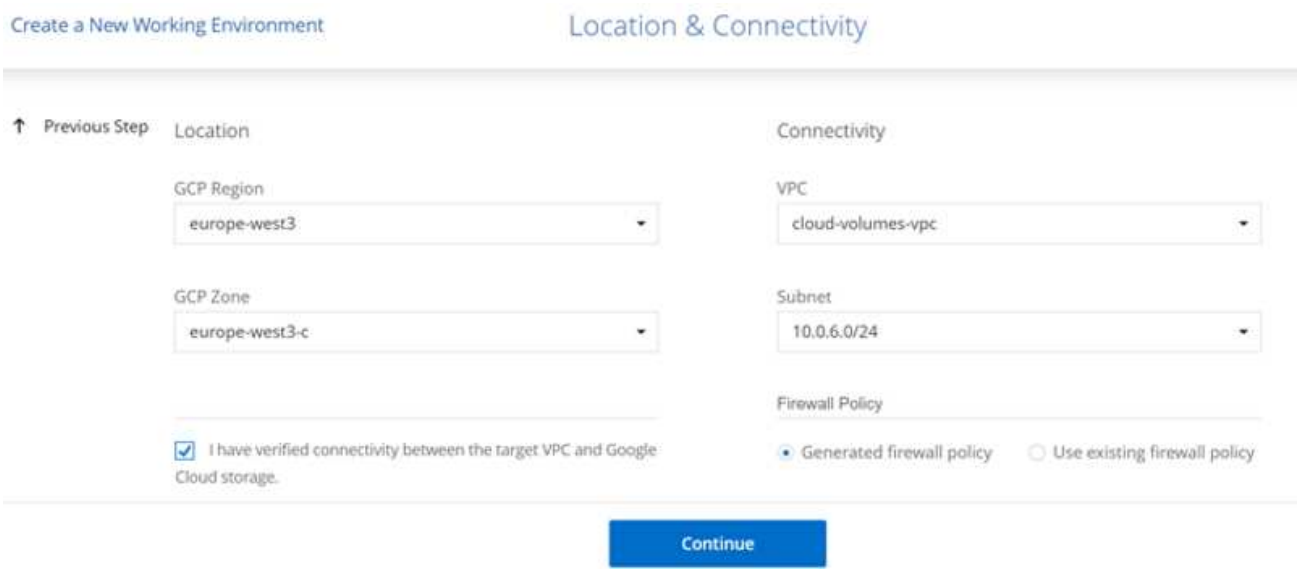


4. Seleccione o deseleccione los servicios complementarios para la implementación de Cloud Volumes ONTAP , incluidos Data Sense & Compliance o Backup to Cloud. Luego haga clic en Continuar.

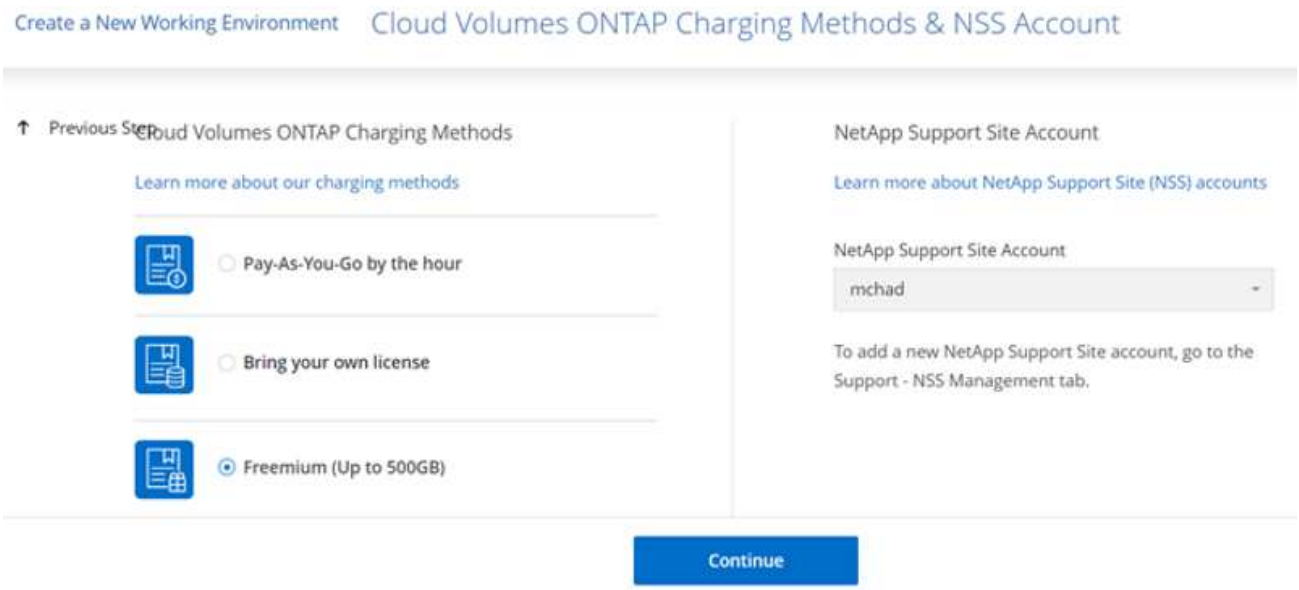
   SUGERENCIA: Se mostrará un mensaje emergente de verificación al desactivar servicios complementarios. Se pueden agregar o eliminar servicios complementarios después de la implementación de CVO; considere deseleccionarlos si no son necesarios desde el principio para evitar costos.



5. Seleccione una ubicación, elija una política de firewall y seleccione la casilla de verificación para confirmar la conectividad de red al almacenamiento de Google Cloud.



6. Seleccione la opción de licencia: Pago por uso o BYOL para utilizar una licencia existente. En este ejemplo, se utiliza la opción Freemium. Luego haga clic en Continuar.

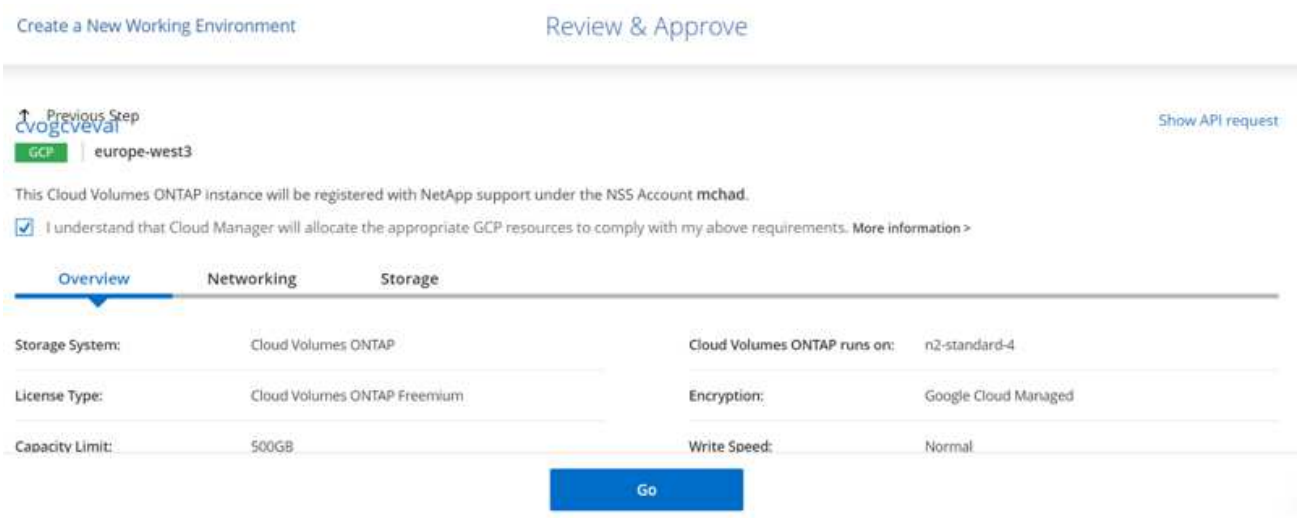


7. Seleccione entre varios paquetes preconfigurados disponibles según el tipo de carga de trabajo que se implementará en las máquinas virtuales que se ejecutan en VMware Cloud en AWS SDDC.

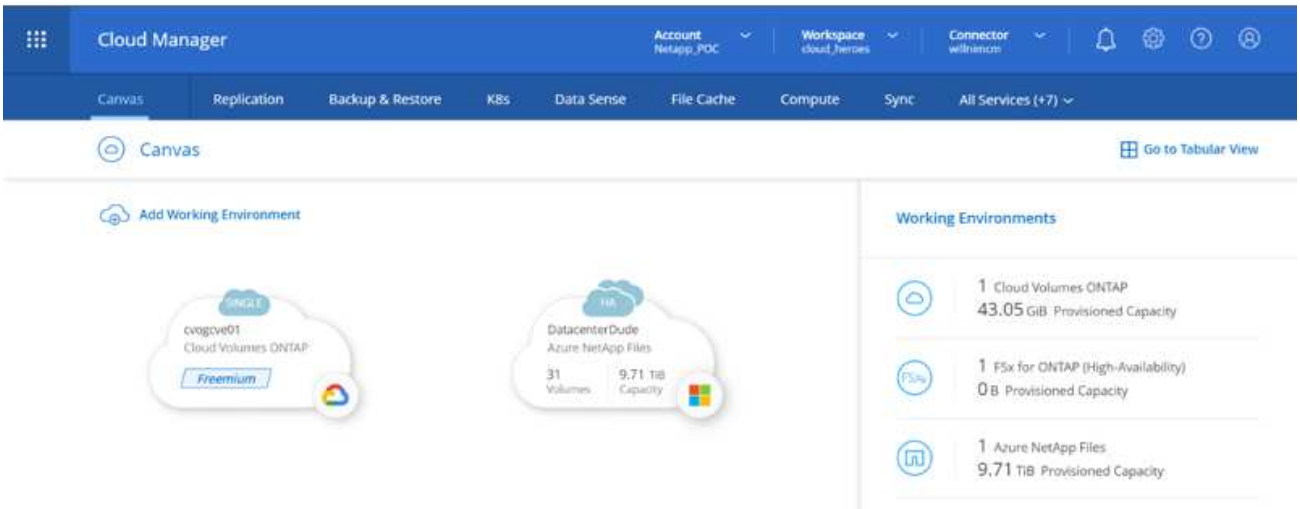
   SUGERENCIA: Pase el mouse sobre los mosaicos para obtener detalles o personalizar los componentes de CVO y la versión de ONTAP haciendo clic en Cambiar configuración.



8. En la página Revisar y aprobar, revise y confirme las selecciones. Para crear la instancia de Cloud Volumes ONTAP , haga clic en Ir.



9. Una vez aprovisionado Cloud Volumes ONTAP , aparece en los entornos de trabajo en la página Canvas.

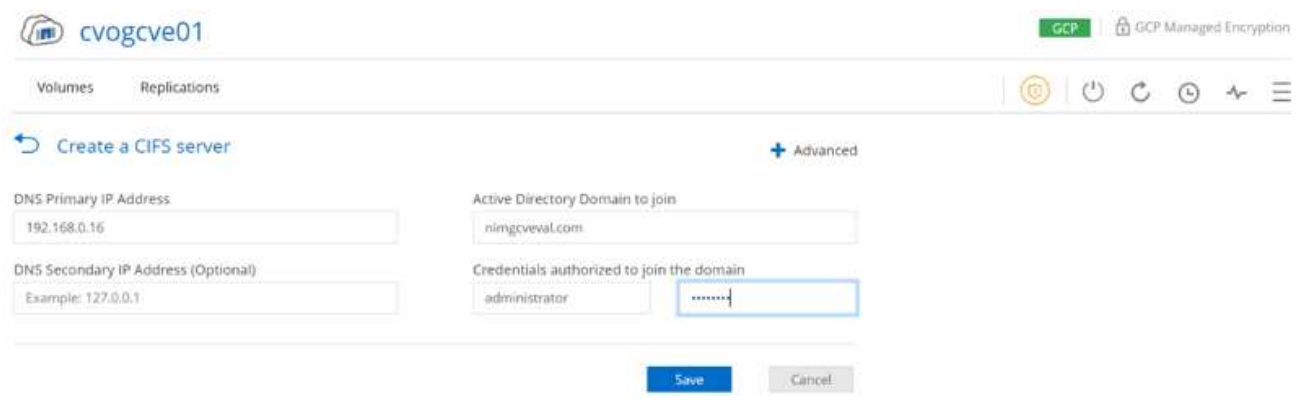


▼ Configuraciones adicionales para volúmenes SMB

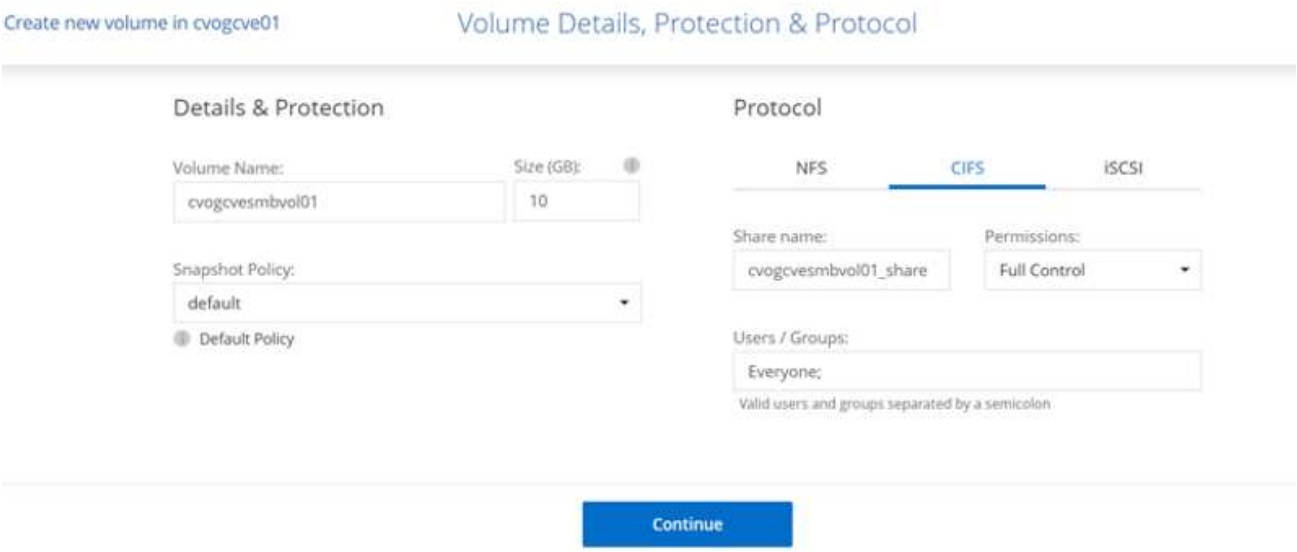
1. Una vez que el entorno de trabajo esté listo, asegúrese de que el servidor CIFS esté configurado con los parámetros de configuración de DNS y Active Directory adecuados. Este paso es necesario antes

de poder crear el volumen SMB.

SUGERENCIA: Haga clic en el ícono de Menú (º), seleccione Avanzado para mostrar más opciones y seleccione Configuración CIFS.



2. Crear el volumen SMB es un proceso sencillo. En Canvas, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP para crear y administrar volúmenes y haga clic en la opción Crear volumen. Elija el tamaño apropiado y el administrador de la nube elige el agregado contenedor o utiliza un mecanismo de asignación avanzado para colocarlo en un agregado específico. Para esta demostración, se selecciona CIFS/SMB como protocolo.



3. Una vez aprovisionado el volumen, estará disponible en el panel Volúmenes. Debido a que se aprovisiona un recurso compartido CIFS, otorgue a sus usuarios o grupos permiso para acceder a los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo. Este paso no es necesario si el volumen se replica desde un entorno local porque los permisos de archivos y carpetas se conservan como parte de la replicación de SnapMirror .

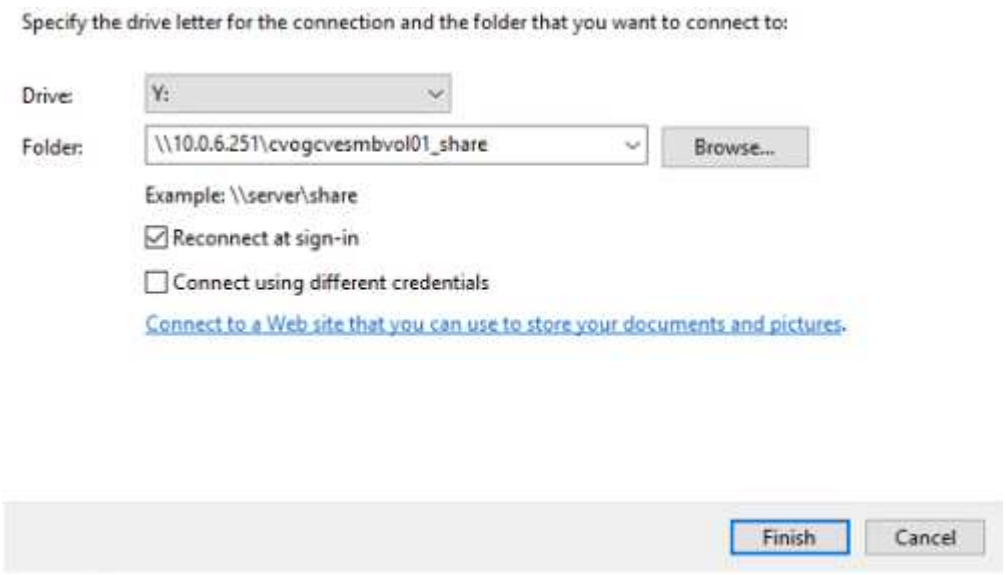
SUGERENCIA: Haga clic en el menú de volumen (º) para desplegar sus opciones.



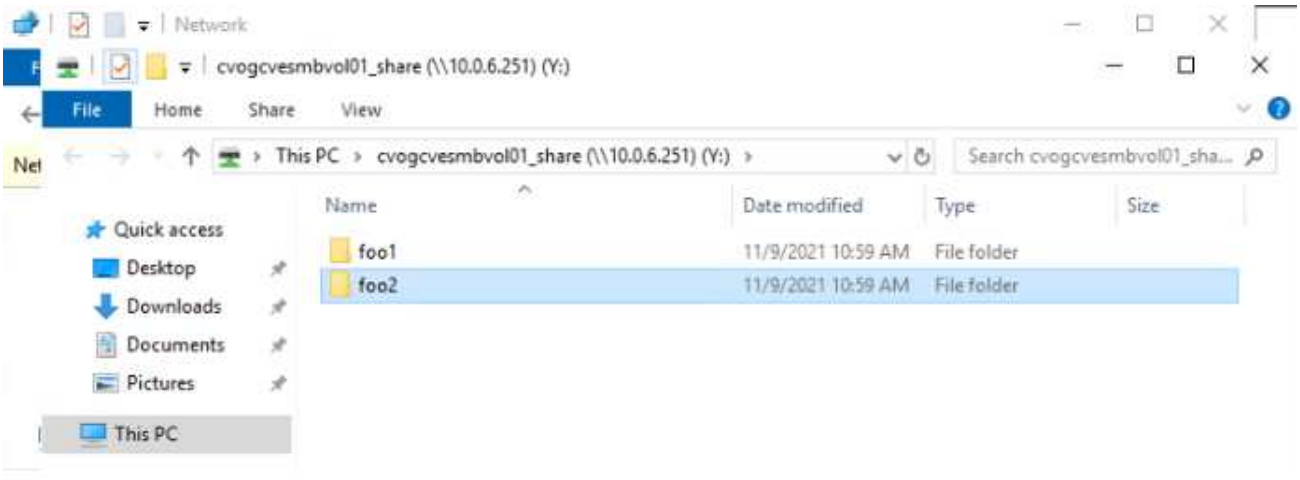
4. Una vez creado el volumen, utilice el comando mount para mostrar las instrucciones de conexión del volumen y, luego, conéctese al recurso compartido desde las máquinas virtuales en Google Cloud VMware Engine.



5. Copie la siguiente ruta y use la opción Asignar unidad de red para montar el volumen en la máquina virtual que se ejecuta en Google Cloud VMware Engine.



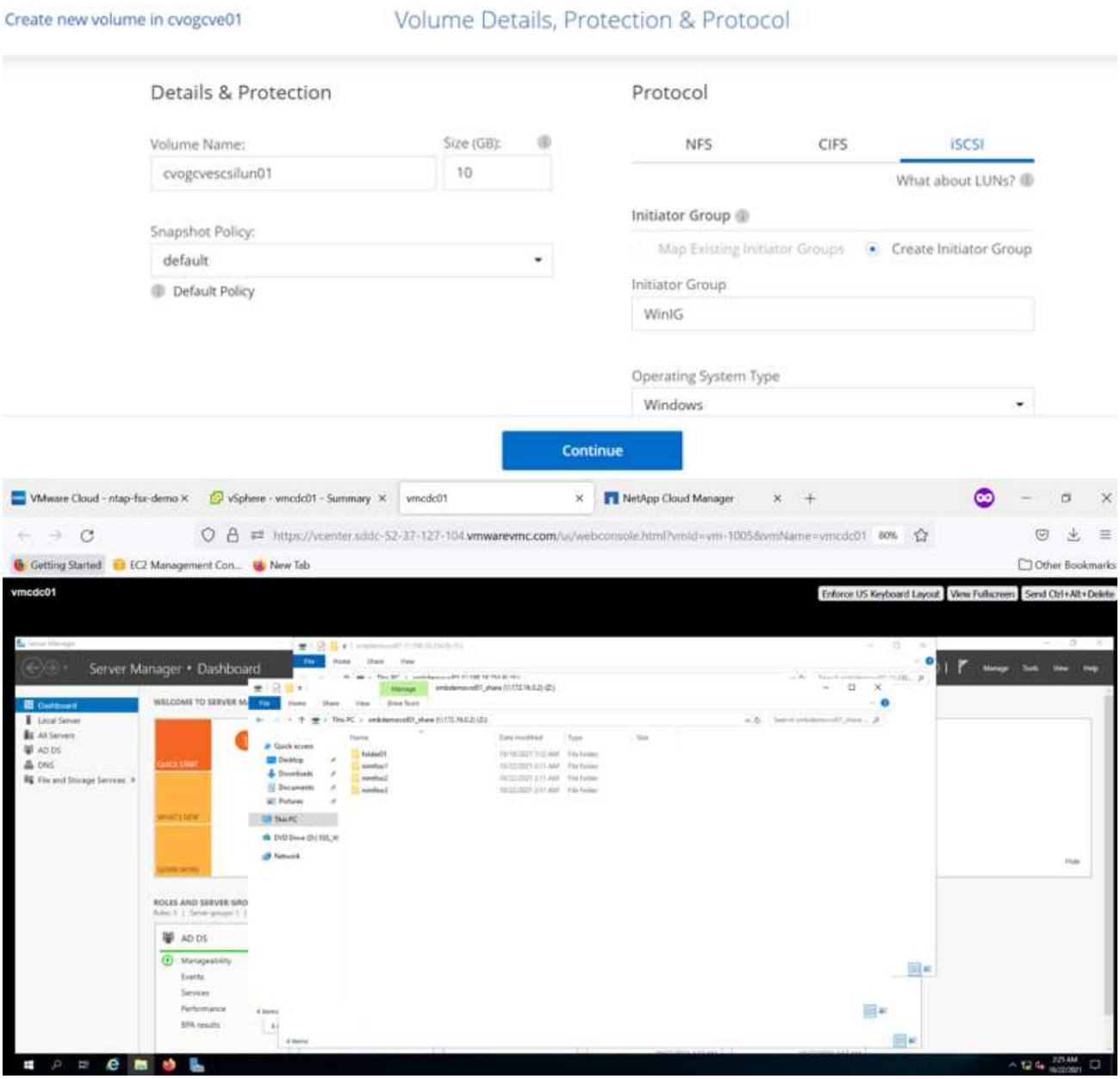
Una vez mapeado, se puede acceder fácilmente y se pueden configurar los permisos NTFS en consecuencia.



▼ **Conecte el LUN en Cloud Volumes ONTAP a un host**

Para conectar los volúmenes en la nube ONTAP LUN a un host, complete los siguientes pasos:

1. En la página Lienzo, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP para crear y administrar volúmenes.
2. Haga clic en Agregar volumen > Nuevo volumen y seleccione iSCSI y haga clic en Crear grupo de iniciadores. Haga clic en Continuar.



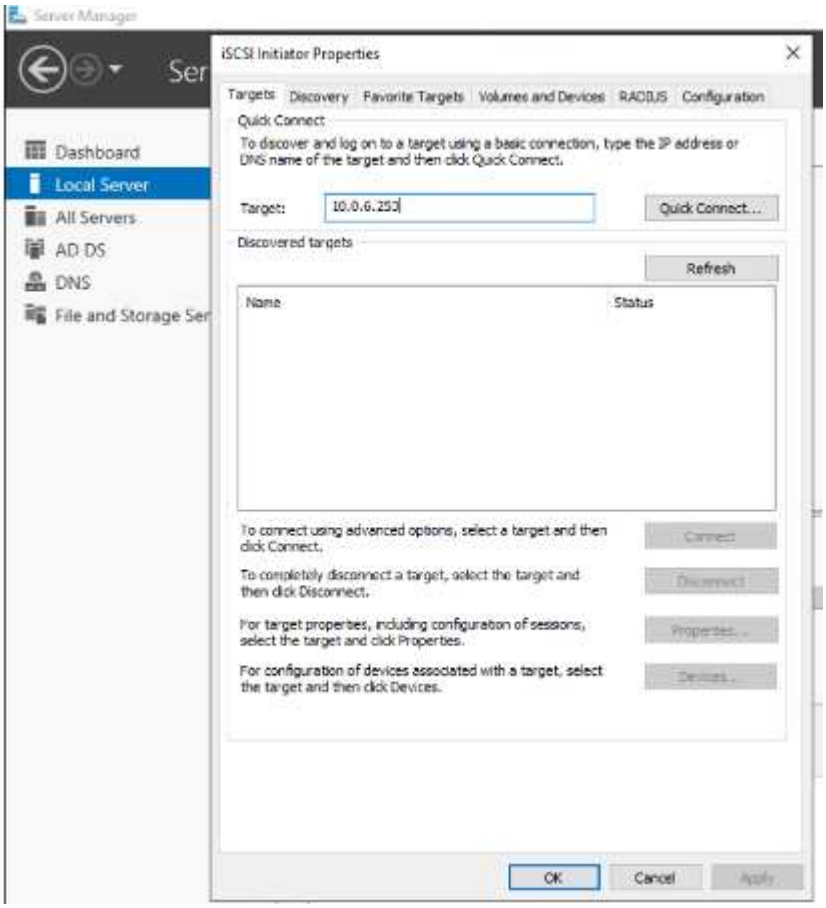
3. Una vez aprovisionado el volumen, seleccione el menú de volumen (º) y, a continuación, haga clic en Target iQN. Para copiar el nombre calificado iSCSI (iQN), haga clic en Copiar. Configure una conexión iSCSI desde el host al LUN.

Para lograr lo mismo para el host que reside en Google Cloud VMware Engine:

1. RDP a la máquina virtual alojada en Google Cloud VMware Engine.
2. Abra el cuadro de diálogo Propiedades del iniciador iSCSI: Administrador del servidor > Panel de control > Herramientas > Iniciador iSCSI.
3. Desde la pestaña Descubrimiento, haga clic en Descubrir portal o Agregar portal y luego ingrese la dirección IP del puerto de destino iSCSI.
4. Desde la pestaña Objetivos, seleccione el objetivo descubierto y luego haga clic en Iniciar sesión o Conectar.
5. Seleccione Habilitar múltiples rutas y, a continuación, seleccione Restaurar esta conexión automáticamente cuando se inicie el equipo o Agregar esta conexión a la lista de destinos favoritos.

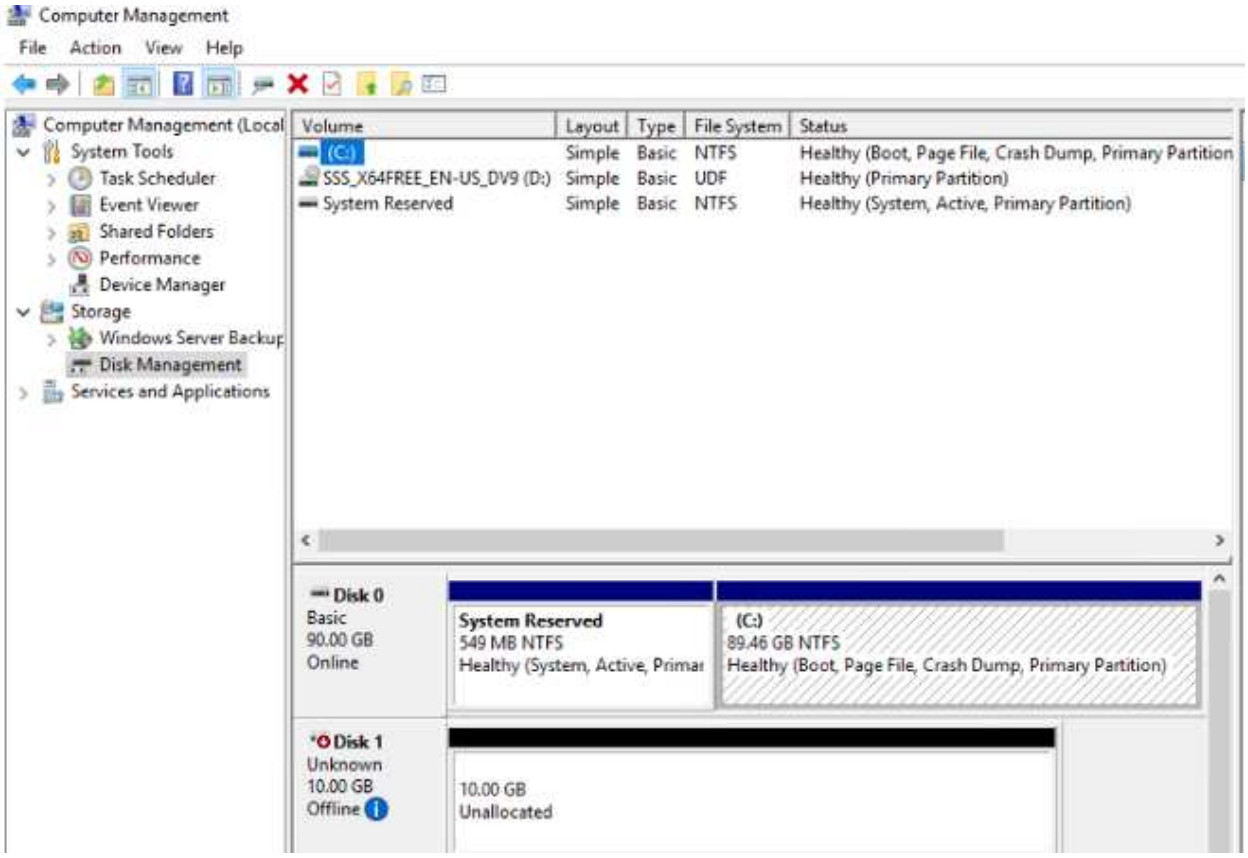
Haga clic en Avanzado.

El host de Windows debe tener una conexión iSCSI a cada nodo del clúster. El DSM nativo selecciona las mejores rutas a utilizar.



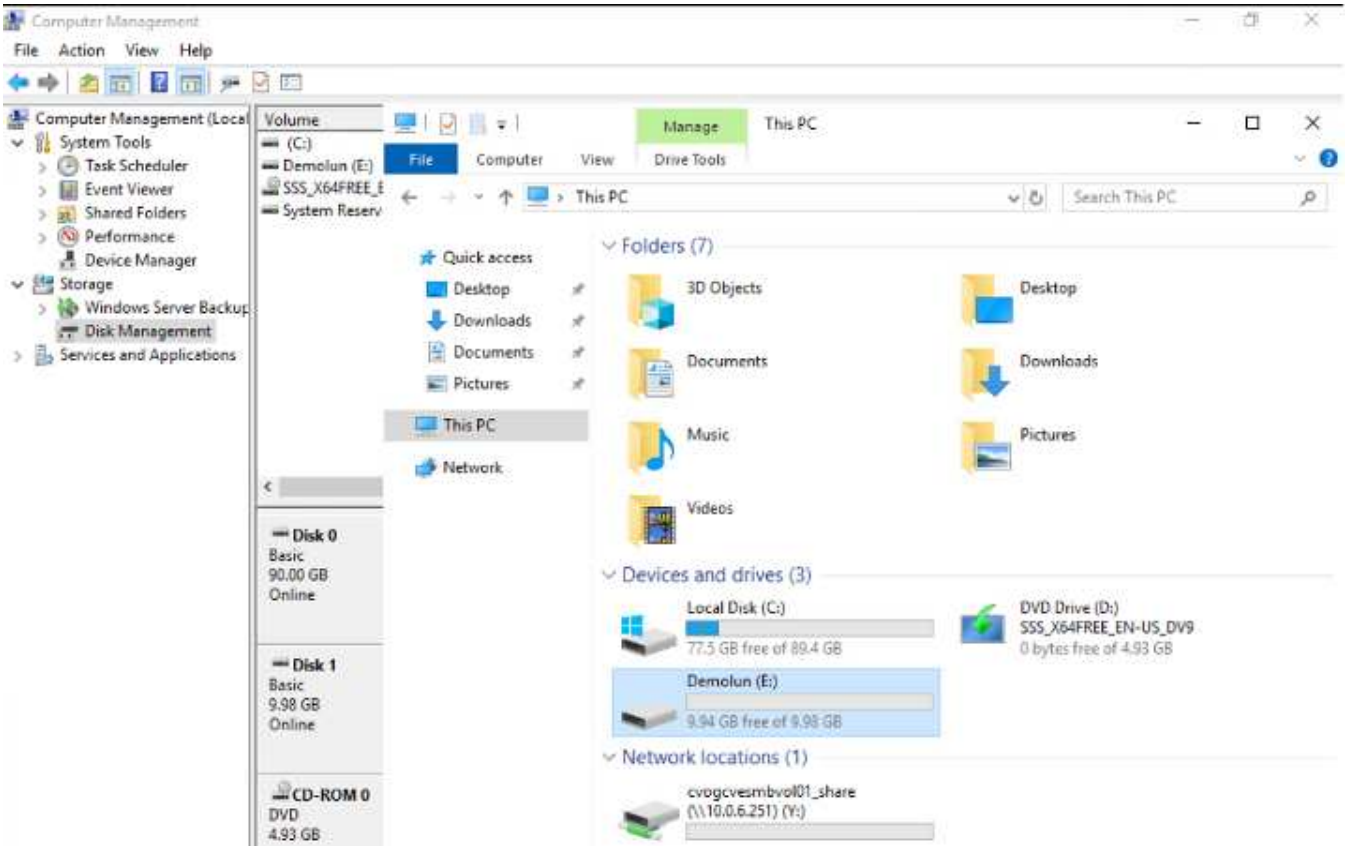
Los LUN en una máquina virtual de almacenamiento (SVM) aparecen como discos para el host de Windows. El host no detecta automáticamente ningún disco nuevo que se agregue. Active un nuevo escaneo manual para descubrir los discos completando los siguientes pasos:

a. Abra la utilidad de Administración de equipos de Windows: Inicio > Herramientas administrativas > Administración de equipos.
b. Expanda el nodo Almacenamiento en el árbol de navegación.
c. Haga clic en Administración de discos.
d. Haga clic en Acción > Volver a escanear discos.



Cuando el host de Windows accede por primera vez a un nuevo LUN, éste no tiene partición ni sistema de archivos. Inicialice el LUN y, opcionalmente, formatee el LUN con un sistema de archivos completando los siguientes pasos:

a. Inicie la Administración de discos de Windows.
b. Haga clic con el botón derecho en el LUN y luego seleccione el tipo de disco o partición requerido.
c. Siga las instrucciones del asistente. En este ejemplo, la unidad F: está montada.



En los clientes Linux, asegúrese de que el demonio iSCSI esté ejecutándose. Una vez aprovisionados los LUN, consulte la guía detallada sobre la configuración de iSCSI con Ubuntu como ejemplo aquí. Para verificar, ejecute lsblk cmd desde el shell.

```
nlyaz@nlmubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

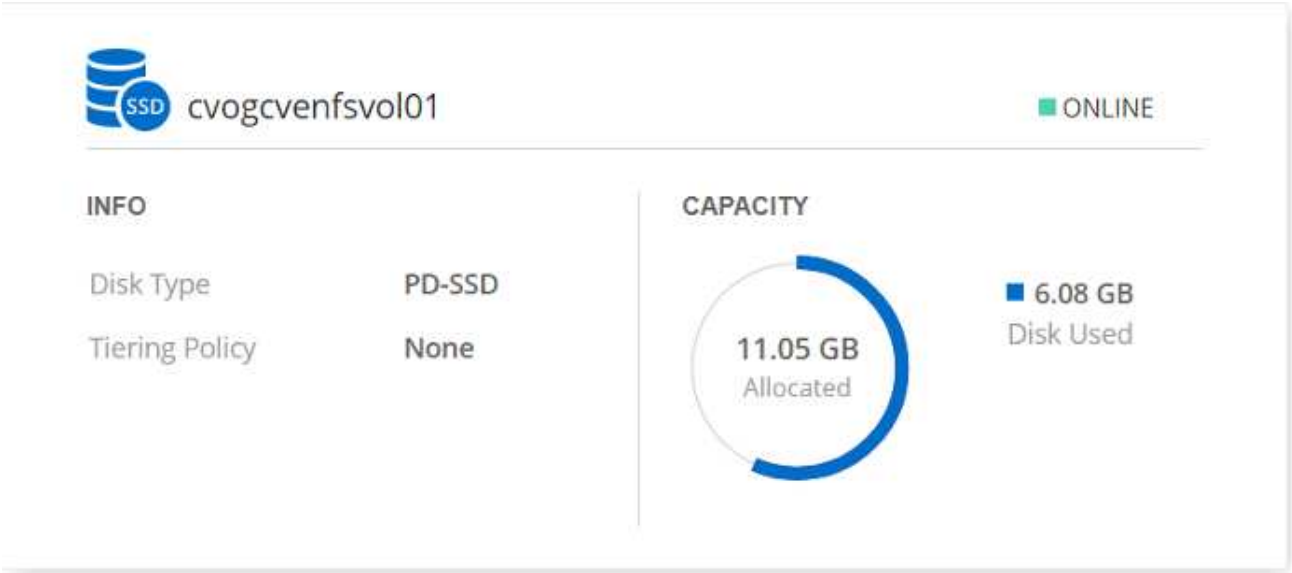
```
nlyaz@nlnubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M     0 100% /snap/snap-store/547
/dev/loop0       56M   56M     0 100% /snap/core18/2128
/dev/loop4       33M   33M     0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M   1% /boot/efi
tmpfs           394M   64K  394M   1% /run/user/1000
/dev/loop5       33M   33M     0 100% /snap/snapd/13640
/dev/loop6       56M   56M     0 100% /snap/core18/2246
/dev/loop7      128K  128K     0 100% /snap/bare/5
/dev/loop8       66M   66M     0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M   1% /mnt
```

▼ **Montar un volumen NFS de Cloud Volumes ONTAP en un cliente Linux**

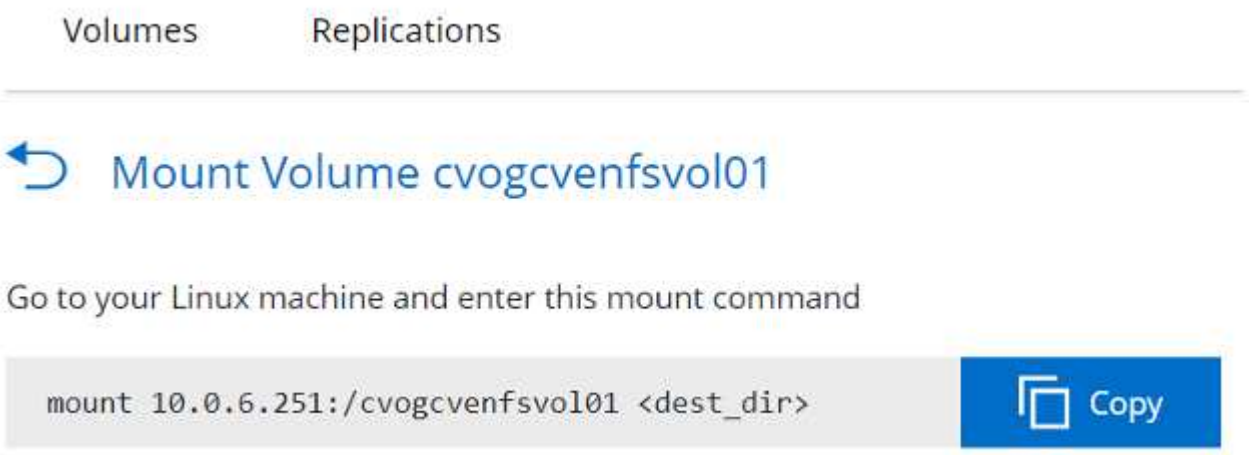
Para montar el sistema de archivos Cloud Volumes ONTAP (DIY) desde las máquinas virtuales dentro de Google Cloud VMware Engine, siga los pasos a continuación:

Aprovisione el volumen siguiendo los pasos a continuación

1. En la pestaña Volúmenes, haga clic en Crear nuevo volumen.
2. En la página Crear nuevo volumen, seleccione un tipo de volumen:



3. En la pestaña Volúmenes, coloque el cursor del mouse sobre el volumen, seleccione el ícono de menú (º) y luego haga clic en Comando de montaje.



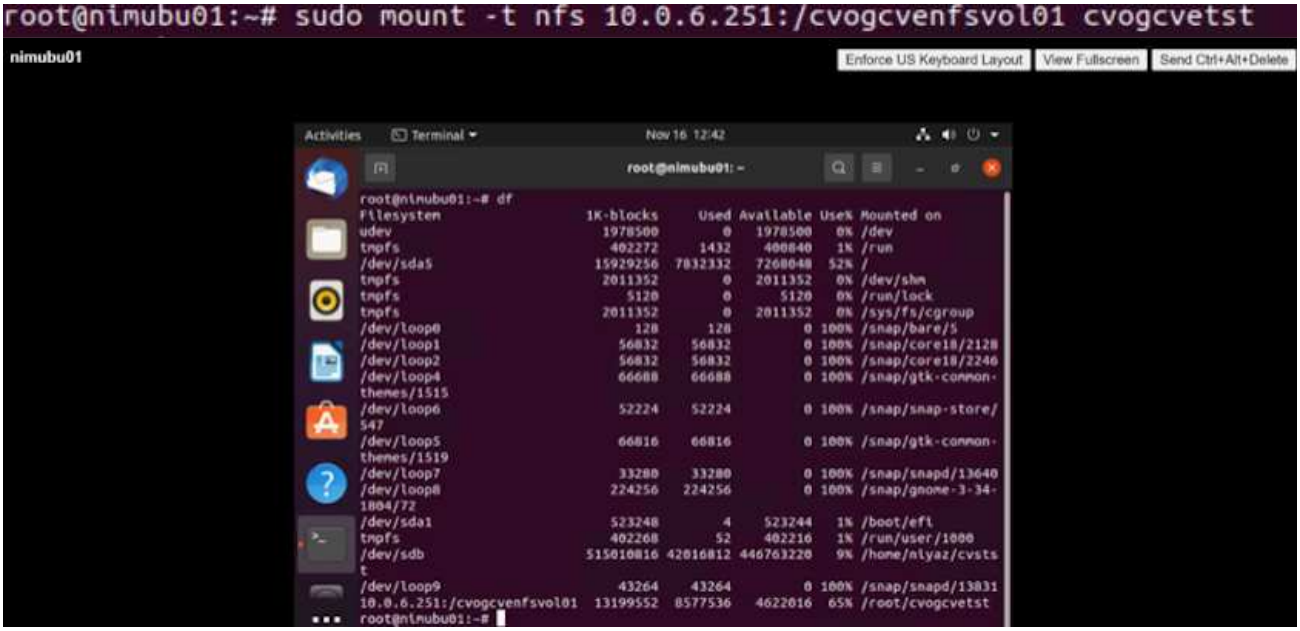
4. Haga clic en Copiar.
5. Conectarse a la instancia de Linux designada.
6. Abra una terminal en la instancia usando shell seguro (SSH) e inicie sesión con las credenciales adecuadas.
7. Cree un directorio para el punto de montaje del volumen con el siguiente comando.

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. Monte el volumen NFS de Cloud Volumes ONTAP en el directorio que se creó en el paso anterior.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



Google Cloud NetApp Volumes (Volúmenes NetApp)

Google Cloud NetApp Volumes (NetApp Volumes) es una cartera completa de servicios de datos para ofrecer soluciones de nube avanzadas. NetApp Volumes admite múltiples protocolos de acceso a archivos para los principales proveedores de nube (compatibilidad con NFS y SMB).

Otros beneficios y características incluyen: protección y restauración de datos con Snapshot; características especiales para replicar, sincronizar y migrar destinos de datos locales o en la nube; y un alto rendimiento constante al nivel de un sistema de almacenamiento flash dedicado.

Google Cloud NetApp Volumes (NetApp Volumes) como almacenamiento conectado para invitados

▼ Configurar volúmenes NetApp con VMware Engine

Los recursos compartidos de Google Cloud NetApp Volumes se pueden montar desde máquinas virtuales creadas en el entorno de VMware Engine. Los volúmenes también se pueden montar en el cliente Linux y mapear en el cliente Windows porque Google Cloud NetApp Volumes admite los protocolos SMB y NFS. Los volúmenes de Google Cloud NetApp Volumes se pueden configurar en pasos sencillos.

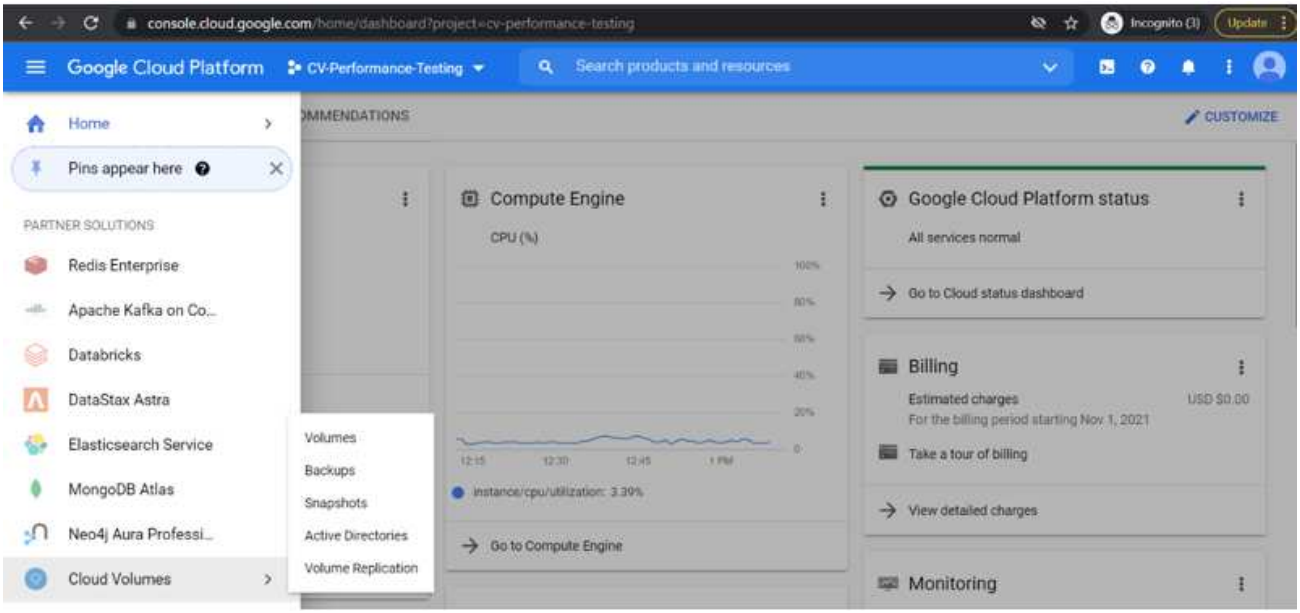
Los Google Cloud NetApp Volumes y la nube privada de Google Cloud VMware Engine deben estar en la misma región.

Para comprar, habilitar y configurar Google Cloud NetApp Volumes para Google Cloud desde Google Cloud Marketplace, siga esta información detallada."guía" .

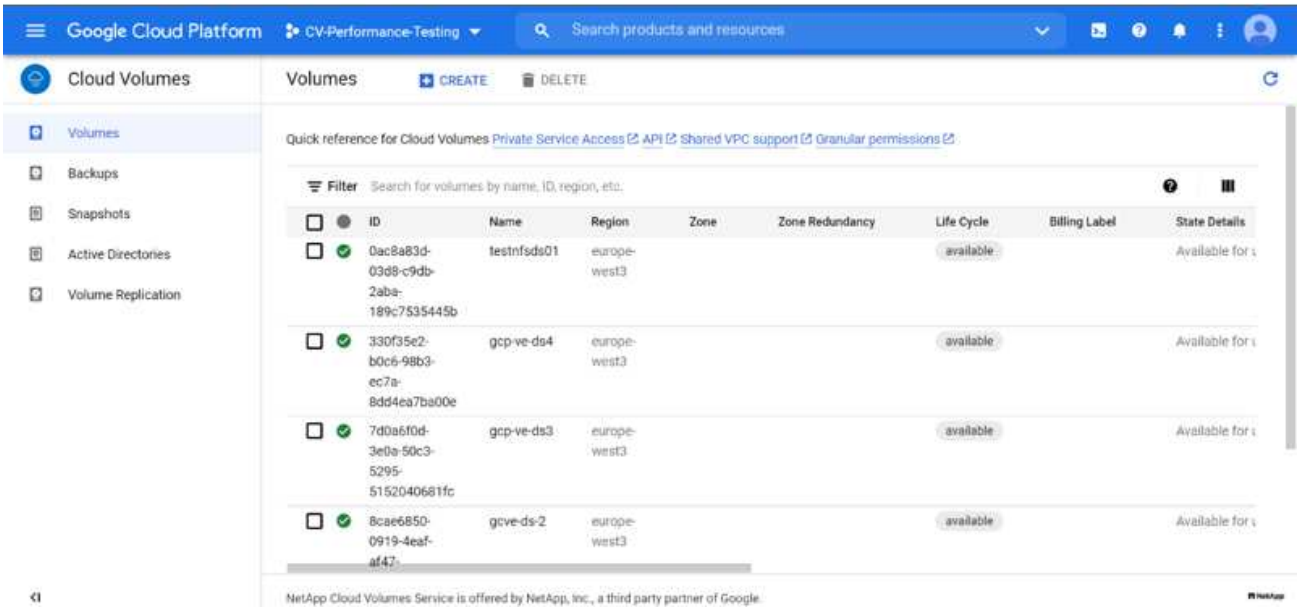
▼ Cree un volumen NFS de NetApp Volumes en la nube privada de GCVE

Para crear y montar volúmenes NFS, complete los siguientes pasos:

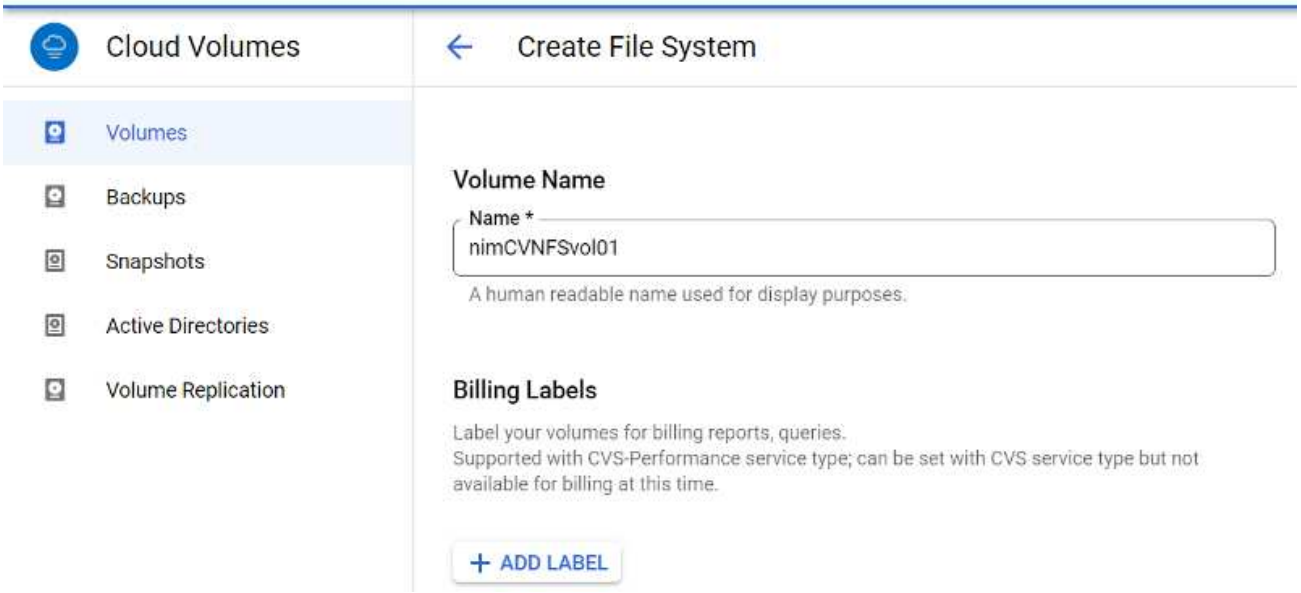
1. Acceda a Cloud Volumes desde Partner Solutions dentro de la consola de Google Cloud.



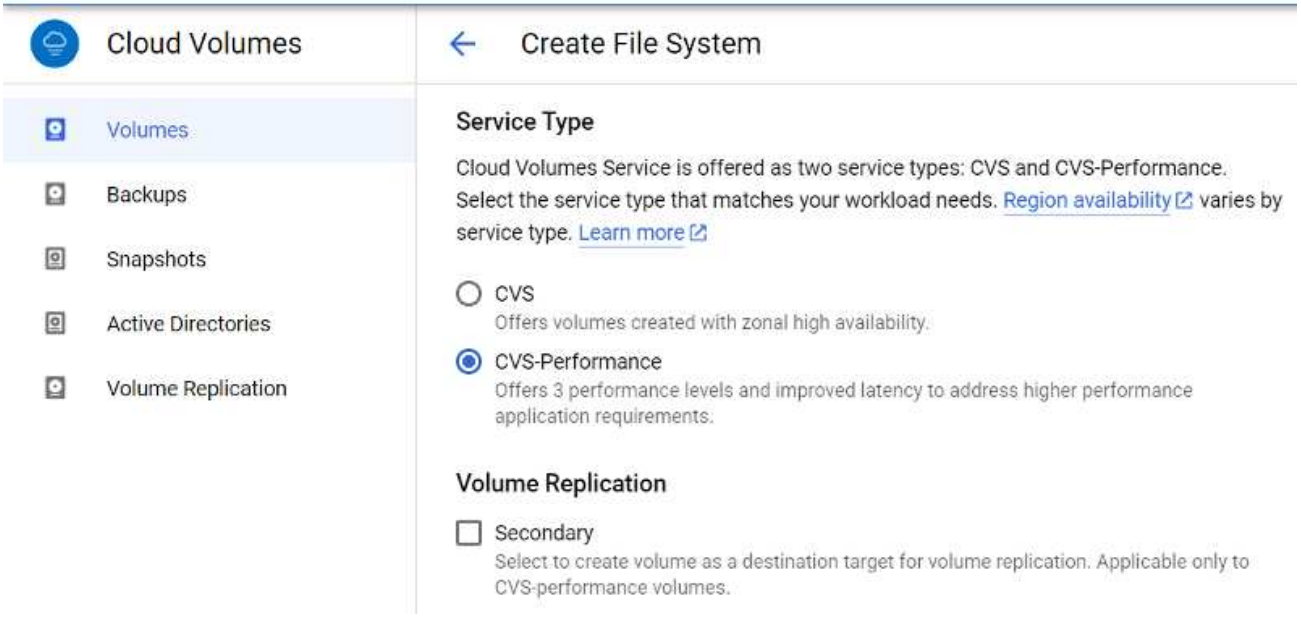
2. En la consola de Cloud Volumes, vaya a la página Volúmenes y haga clic en Crear.



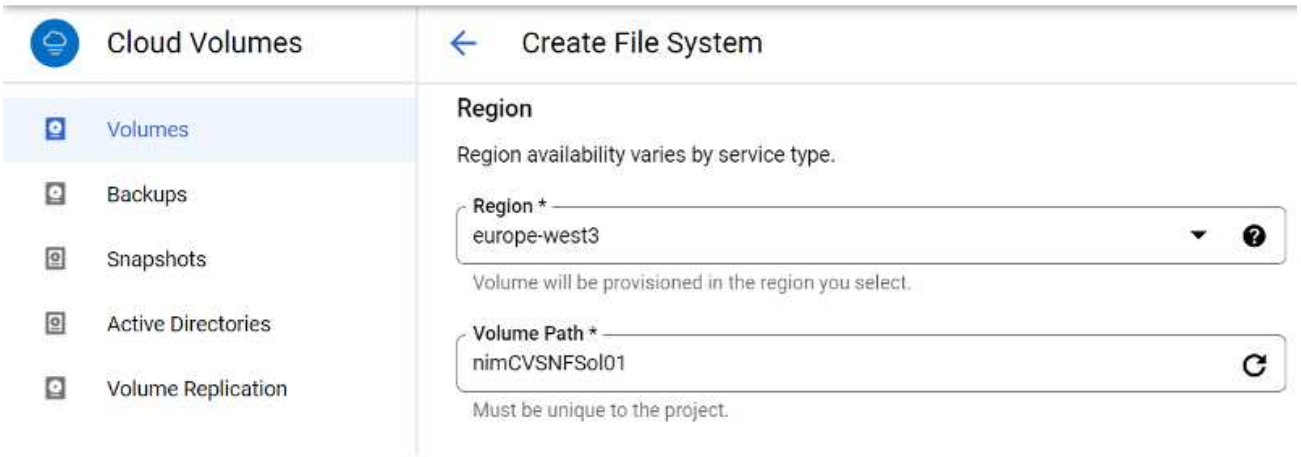
3. En la página Crear sistema de archivos, especifique el nombre del volumen y las etiquetas de facturación según sea necesario para los mecanismos de devolución de cargo.



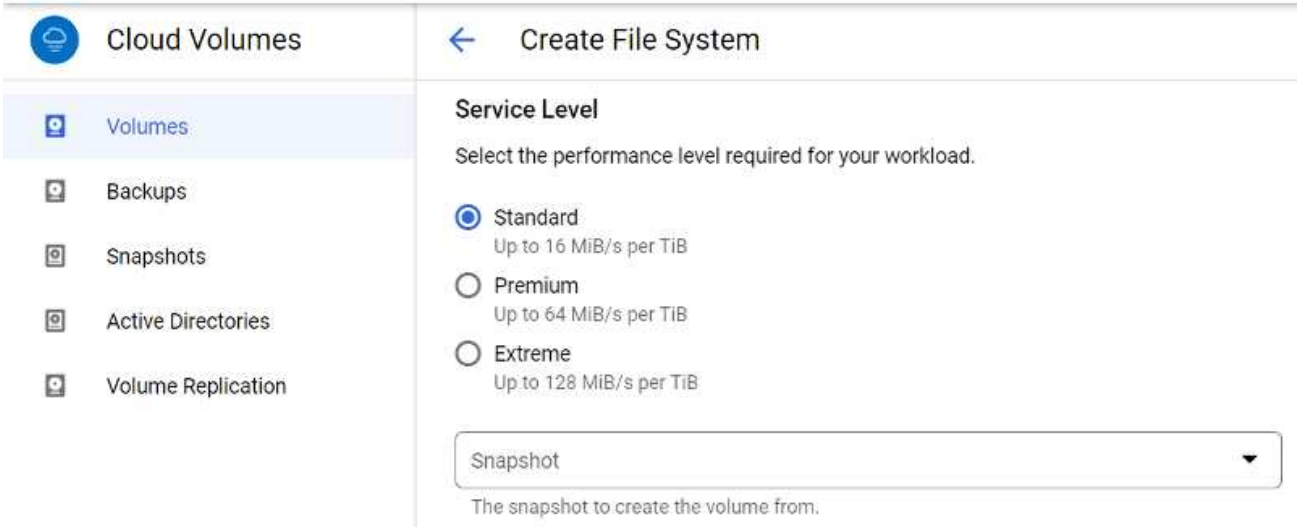
4. Seleccione el servicio apropiado. Para GCVE, elija NetApp Volumes-Performance y el nivel de servicio deseado para lograr una latencia mejorada y un mayor rendimiento según los requisitos de carga de trabajo de la aplicación.



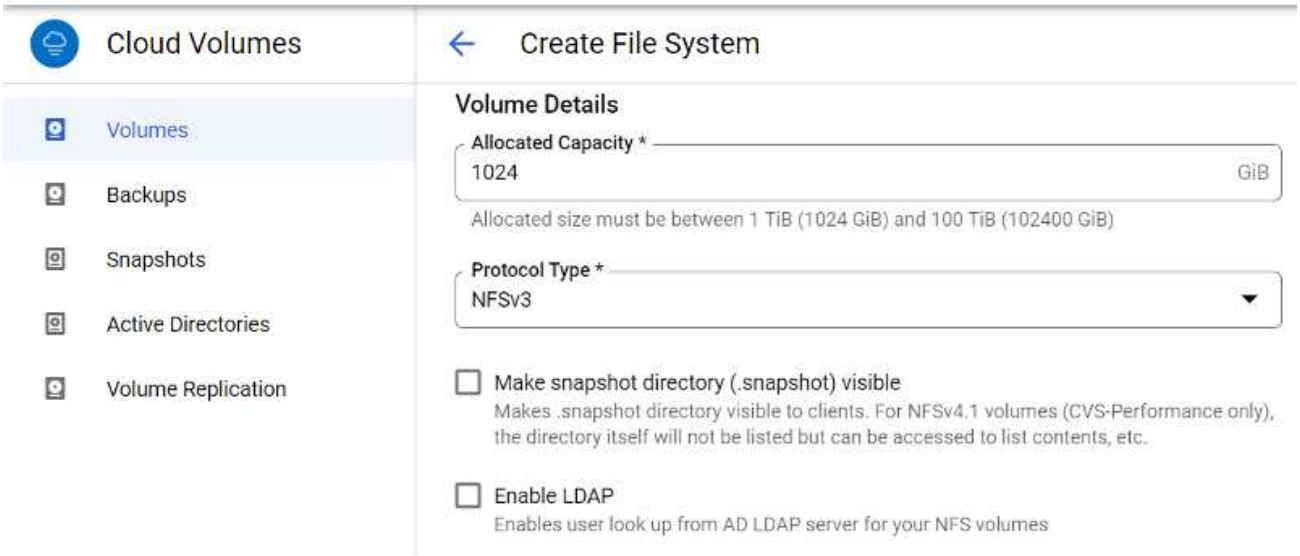
5. Especifique la región de Google Cloud para el volumen y la ruta del volumen (la ruta del volumen debe ser única en todos los volúmenes de nube del proyecto)



6. Seleccione el nivel de rendimiento para el volumen.

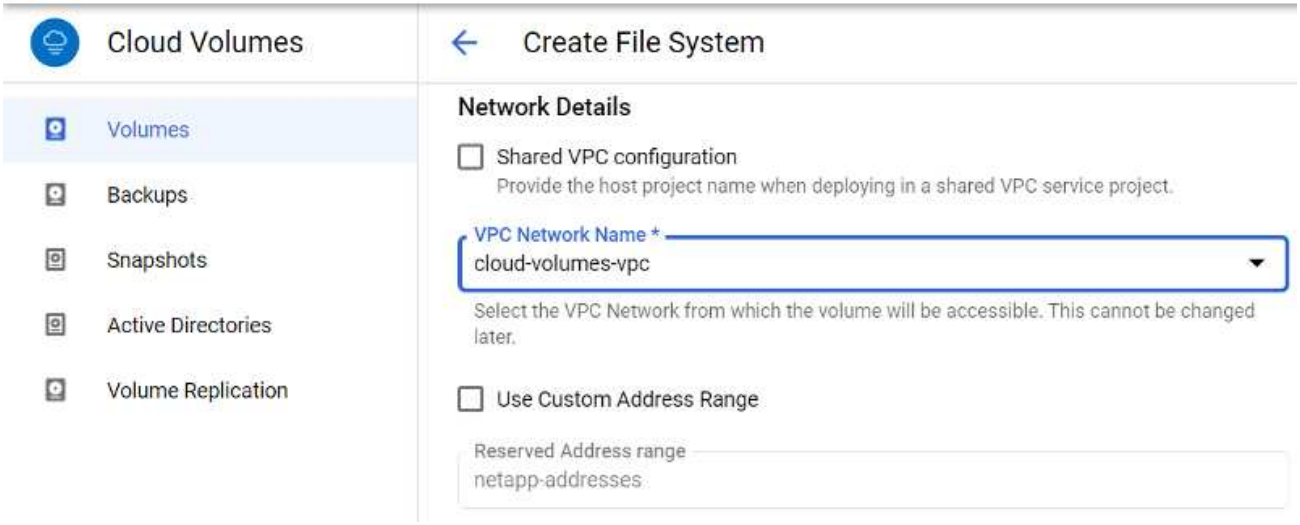


7. Especifique el tamaño del volumen y el tipo de protocolo. En esta prueba, se utiliza NFSv3.



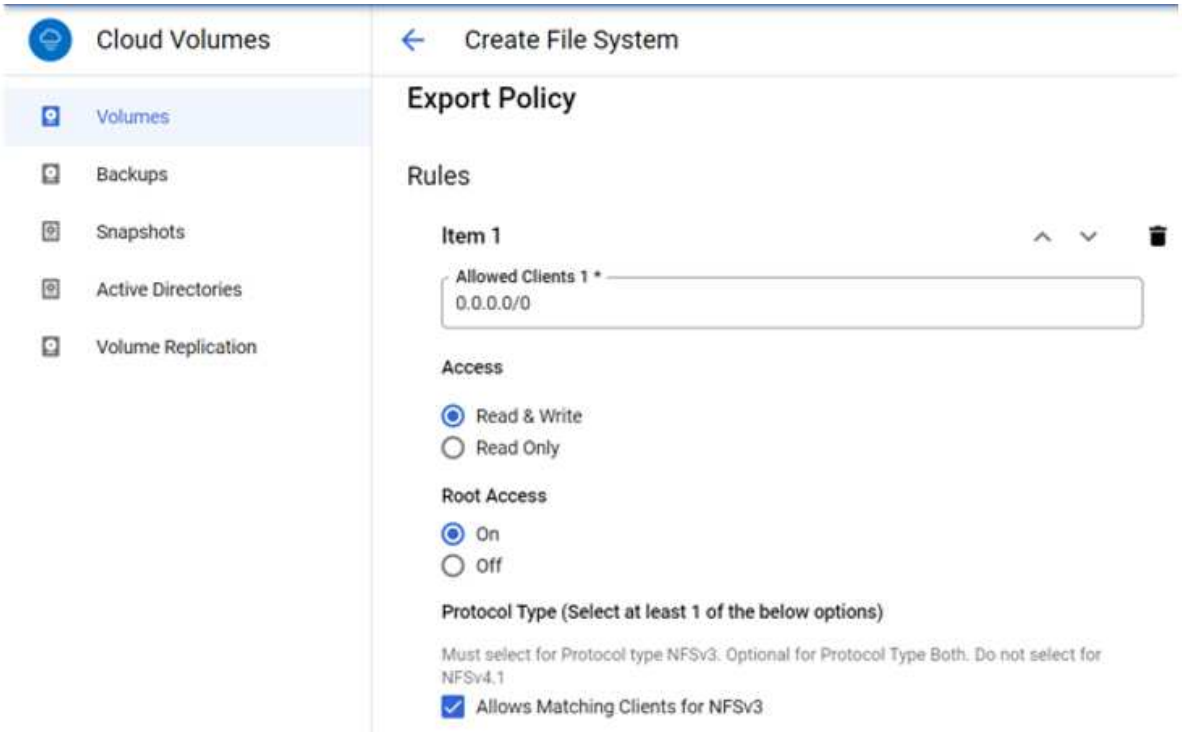
8. En este paso, seleccione la red VPC desde la cual se podrá acceder al volumen. Asegúrese de que el peering de VPC esté implementado.

   SUGERENCIA: Si no se ha realizado el emparejamiento de VPC, se mostrará un botón emergente para guiarlo a través de los comandos de emparejamiento. Abra una sesión de Cloud Shell y ejecute los comandos adecuados para emparejar su VPC con el productor de Google Cloud NetApp Volumes . En caso de que decida preparar el peering de VPC con antelación, consulte estas instrucciones.



9. Administre las reglas de la política de exportación agregando las reglas adecuadas y seleccionando la casilla de verificación para la versión de NFS correspondiente.

   Nota: El acceso a los volúmenes NFS no será posible a menos que se agregue una política de exportación.



10. Haga clic en Guardar para crear el volumen.



▼ **Montaje de exportaciones NFS en máquinas virtuales que se ejecutan en VMware Engine**

Antes de prepararse para montar el volumen NFS, asegúrese de que el estado de emparejamiento de la conexión privada aparezca como Activo. Una vez que el estado esté Activo, utilice el comando de montaje.

Para montar un volumen NFS, haga lo siguiente:

1. En Cloud Console, vaya a Volúmenes en la nube > Volúmenes.
2. Ir a la página de Volúmenes
3. Haga clic en el volumen NFS para el que desea montar exportaciones NFS.
4. Desplácese hacia la derecha, en Mostrar más, haga clic en Instrucciones de montaje.

Para realizar el proceso de montaje desde el sistema operativo invitado de la máquina virtual VMware, siga los pasos a continuación:

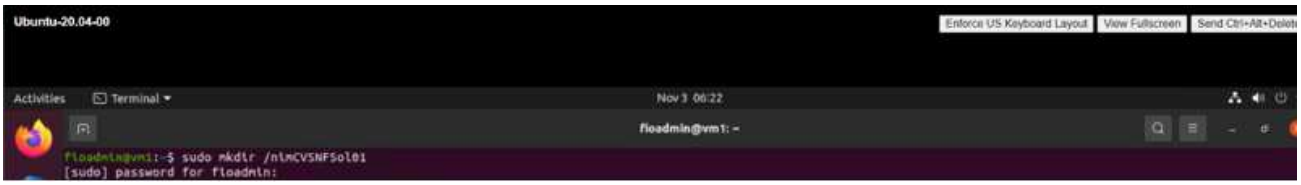
1. Utilice el cliente SSH y SSH a la máquina virtual.
2. Instale el cliente nfs en la instancia.
   a. En una instancia de Red Hat Enterprise Linux o SuSE Linux:

```
 sudo yum install -y nfs-utils
.. En una instancia de Ubuntu o Debian:
```

```
sudo apt-get install nfs-common
```

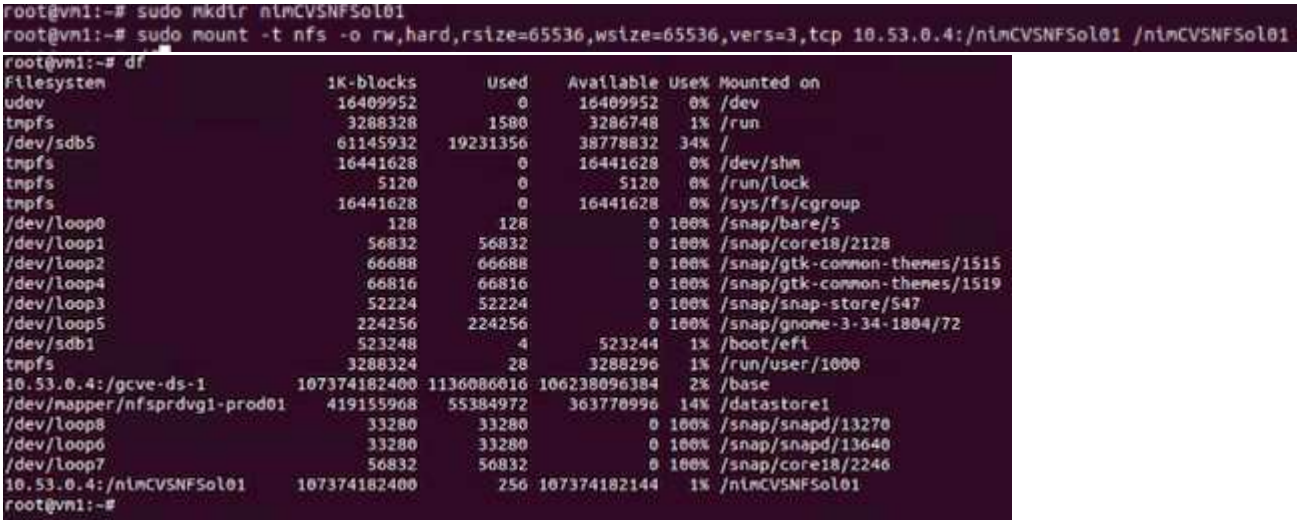
3. Cree un nuevo directorio en la instancia, como "/nimCVSNFSol01":

```
sudo mkdir /nimCVSNFSol01
```



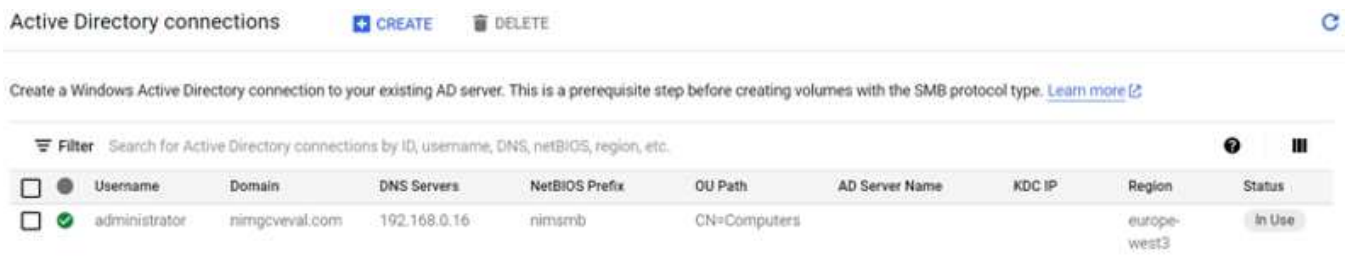
4. Monte el volumen utilizando el comando apropiado. A continuación se muestra un ejemplo de comando del laboratorio:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



▼ Creación y montaje de un recurso compartido SMB en máquinas virtuales que se ejecutan en VMware Engine

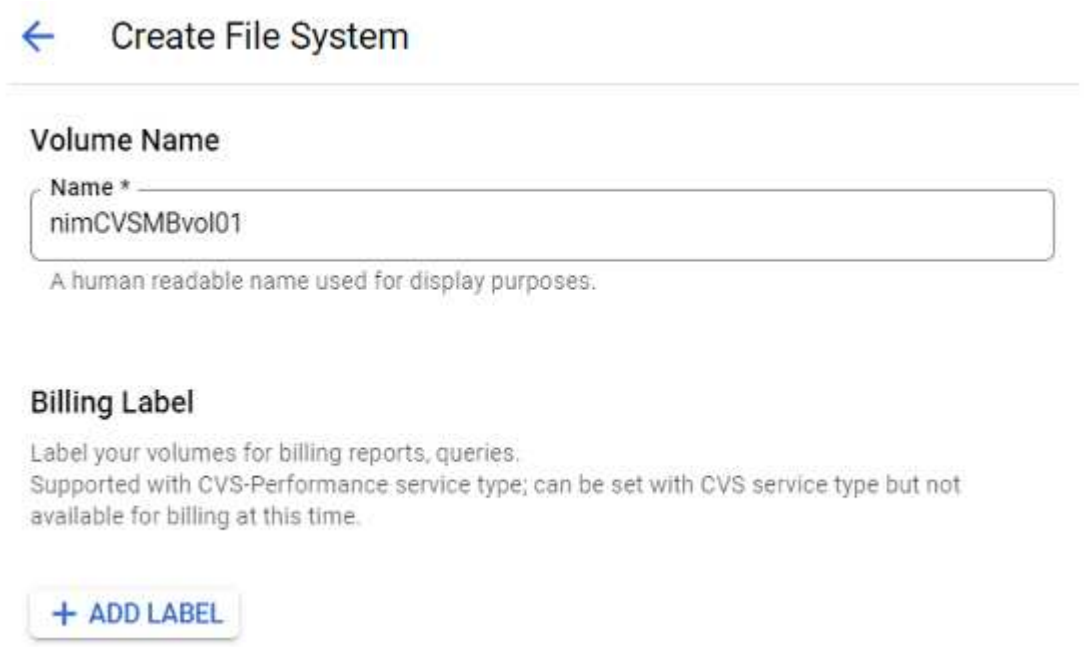
Para los volúmenes SMB, asegúrese de que las conexiones de Active Directory estén configuradas antes de crear el volumen SMB.



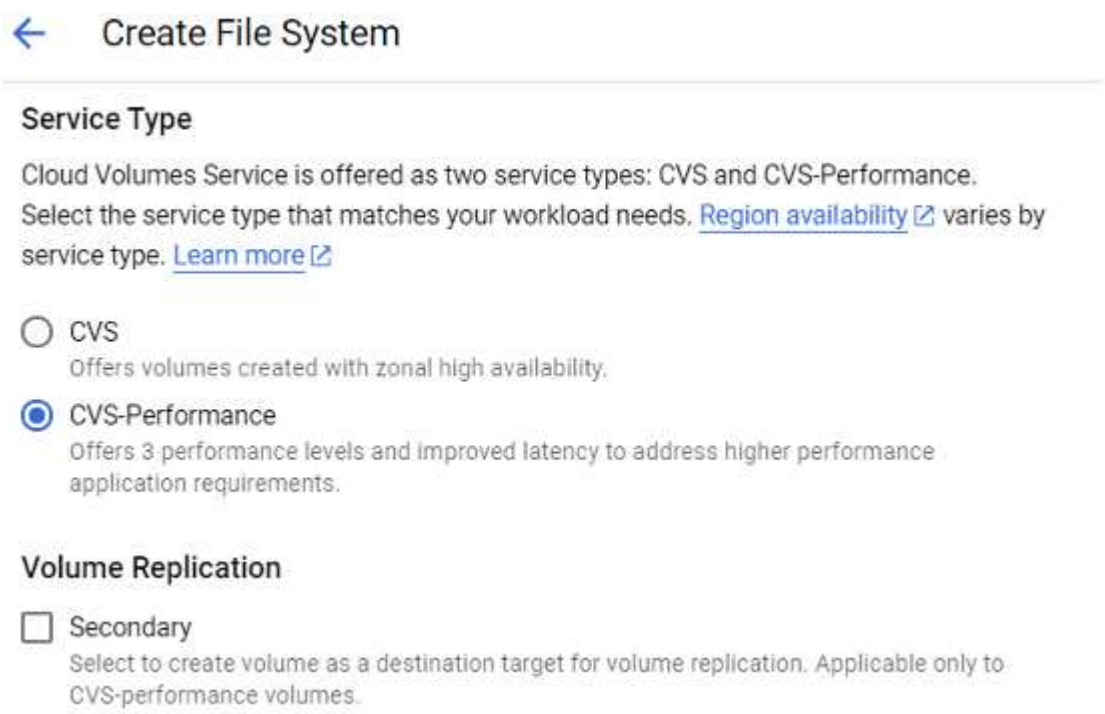
Una vez establecida la conexión AD, cree el volumen con el nivel de servicio deseado. Los pasos son como

crear un volumen NFS excepto que se selecciona el protocolo apropiado.

1. En la consola de Cloud Volumes, vaya a la página Volúmenes y haga clic en Crear.
2. En la página Crear sistema de archivos, especifique el nombre del volumen y las etiquetas de facturación según sea necesario para los mecanismos de devolución de cargo.



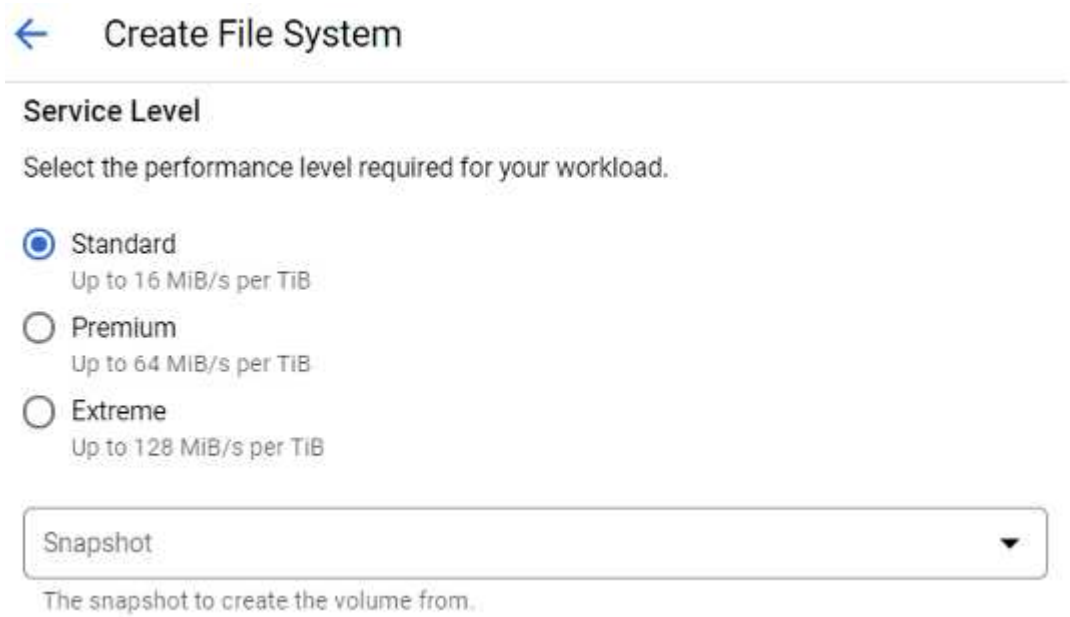
3. Seleccione el servicio apropiado. Para GCVE, elija NetApp Volumes-Performance y el nivel de servicio deseado para lograr una latencia mejorada y un mayor rendimiento según los requisitos de la carga de trabajo.



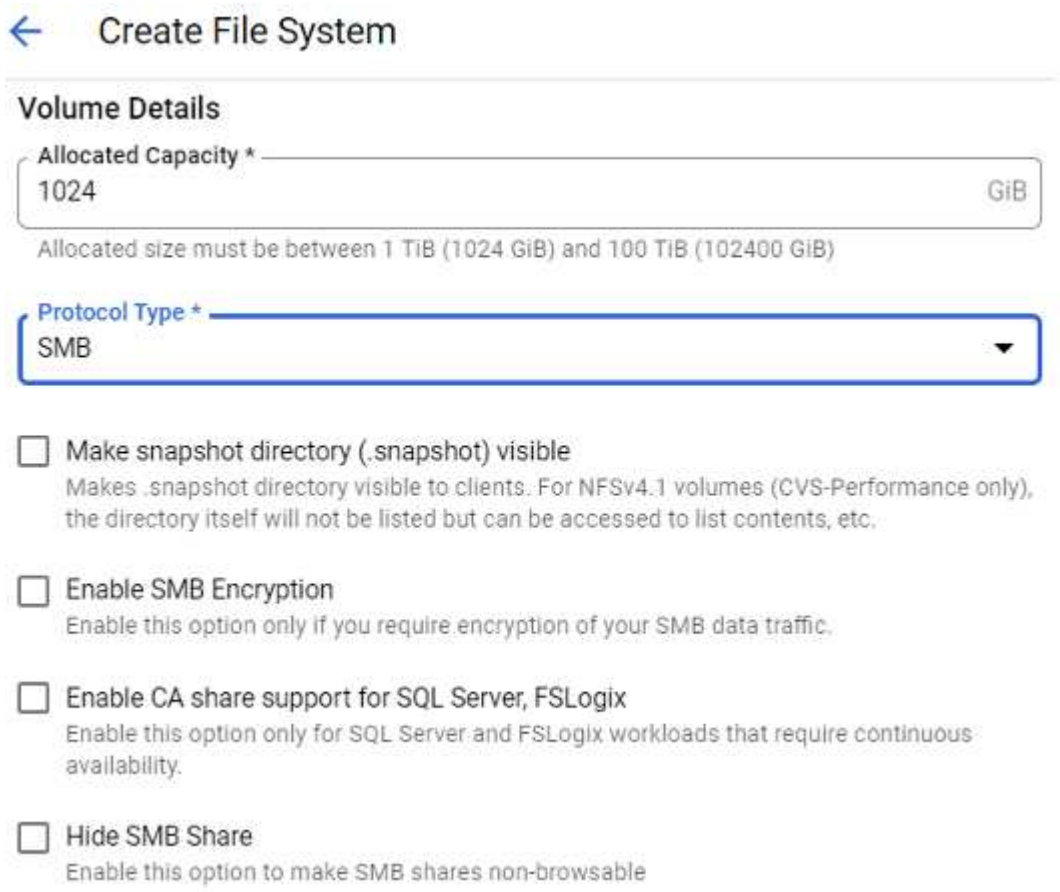
4. Especifique la región de Google Cloud para el volumen y la ruta del volumen (la ruta del volumen debe ser única en todos los volúmenes de nube del proyecto)



5. Seleccione el nivel de rendimiento para el volumen.

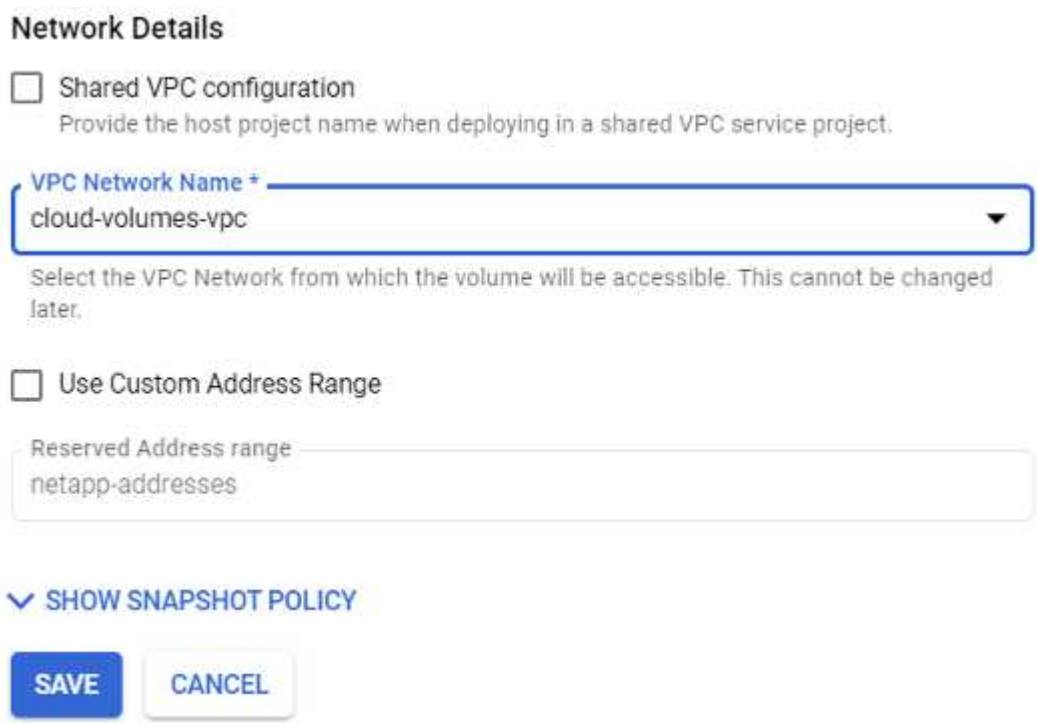


6. Especifique el tamaño del volumen y el tipo de protocolo. En esta prueba, se utiliza SMB.



7. En este paso, seleccione la red VPC desde la cual se podrá acceder al volumen. Asegúrese de que el peering de VPC esté implementado.

   SUGERENCIA: si aún no has configurado el emparejamiento de VPC, se mostrará un botón emergente para guiarte por los comandos de emparejamiento. Abre una sesión de Cloud Shell y ejecuta los comandos adecuados para emparejar tu VPC con el productor de Google Cloud NetApp Volumes. Si decides preparar de antemano el emparejamiento de VPC, consulta "instrucciones".



8. Haga clic en Guardar para crear el volumen.



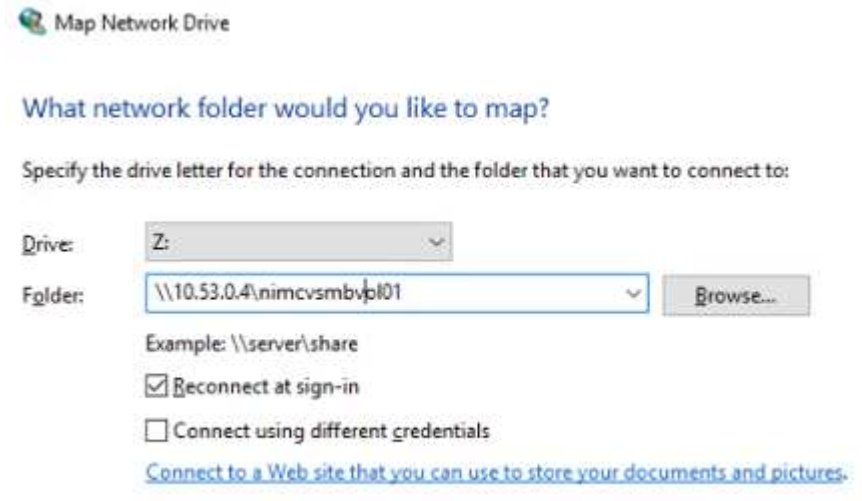
Para montar el volumen SMB, haga lo siguiente:

1. En Cloud Console, vaya a Volúmenes en la nube > Volúmenes.
2. Ir a la página de Volúmenes
3. Haga clic en el volumen SMB para el cual desea asignar un recurso compartido SMB.
4. Desplácese hacia la derecha, en Mostrar más, haga clic en Instrucciones de montaje.

Para realizar el proceso de montaje desde el sistema operativo invitado Windows de la máquina virtual VMware, siga los pasos a continuación:

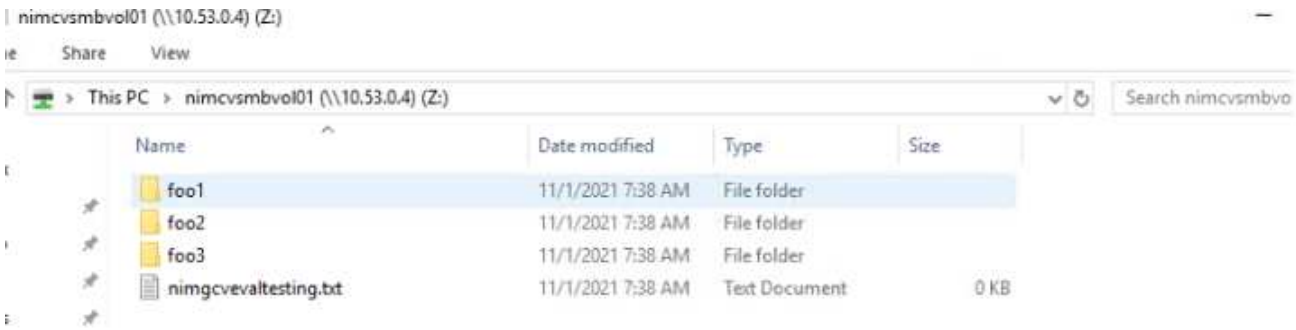
1. Haga clic en el botón Inicio y luego haga clic en Equipo.
2. Haga clic en Conectar a unidad de red.
3. En la lista de unidades, haga clic en cualquier letra de unidad disponible.
4. En el cuadro de carpeta, escriba:

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



Para conectarse cada vez que inicie sesión en su computadora, seleccione la casilla de verificación Reconectar al iniciar sesión.

5. Haga clic en Finalizar.



Resumen y conclusión: ¿Por qué NetApp Hybrid Multicloud con VMware?

NetApp Cloud Volumes junto con las soluciones VMware para los principales hiperescaladores ofrecen un gran potencial para las organizaciones que buscan aprovechar la nube híbrida. El resto de esta sección proporciona casos de uso que demuestran que la integración de NetApp Cloud Volumes permite verdaderas capacidades de multicloud híbrida.

Caso de uso n.° 1: Optimización del almacenamiento

Al realizar un ejercicio de dimensionamiento utilizando la salida de RVtools, siempre es evidente que la escala de potencia (vCPU/vMem) es paralela al almacenamiento. Muchas veces, las organizaciones se encuentran en una situación en la que el espacio de almacenamiento requerido aumenta el tamaño del clúster mucho más allá de lo necesario en términos de potencia.

Al integrar NetApp Cloud Volumes, las organizaciones pueden lograr una solución de nube basada en vSphere con un enfoque de migración simple, sin reorganización de la plataforma, sin cambios de IP y sin cambios arquitectónicos. Además, esta optimización le permite escalar la huella de almacenamiento mientras mantiene la cantidad de hosts en la mínima requerida en vSphere, pero sin cambios en la jerarquía de almacenamiento, la seguridad ni los archivos disponibles. Esto le permite optimizar la implementación y

reducir el TCO general entre un 35 y un 45 %. Esta integración también le permite escalar el almacenamiento desde un almacenamiento cálido hasta un rendimiento de nivel de producción en segundos.

Caso de uso n.° 2: Migración a la nube

Las organizaciones están bajo presión para migrar aplicaciones desde centros de datos locales a la nube pública por múltiples razones: un vencimiento de contrato de alquiler próximo, una directiva financiera para pasar del gasto de capital (capex) al gasto de gastos operativos (opex) o simplemente un mandato de arriba hacia abajo para mover todo a la nube.

Cuando la velocidad es crítica, solo un enfoque de migración optimizado es viable porque cambiar la plataforma y refactorizar las aplicaciones para adaptarse a la plataforma IaaS particular de la nube es lento y costoso, y a menudo lleva meses. Al combinar NetApp Cloud Volumes con la replicación SnapMirror de uso eficiente del ancho de banda para el almacenamiento conectado a invitados (incluidos RDM junto con copias Snapshot consistentes con la aplicación y HCX, migración específica de la nube (por ejemplo, Azure Migrate) o productos de terceros para replicar máquinas virtuales), esta transición es incluso más fácil que confiar en mecanismos de filtros de E/S que consumen mucho tiempo.

Caso de uso n.° 3: Expansión del centro de datos

Cuando un centro de datos alcanza los límites de capacidad debido a picos de demanda estacionales o simplemente a un crecimiento orgánico constante, pasar a VMware alojado en la nube junto con NetApp Cloud Volumes es una solución fácil. El aprovechamiento de NetApp Cloud Volumes permite la creación, replicación y expansión de almacenamiento con mucha facilidad al brindar alta disponibilidad en todas las zonas de disponibilidad y capacidades de escalamiento dinámico. El aprovechamiento de NetApp Cloud Volumes ayuda a minimizar la capacidad del clúster de host superando la necesidad de clústeres extendidos.

Caso de uso n.° 4: Recuperación ante desastres en la nube

En un enfoque tradicional, si ocurre un desastre, las máquinas virtuales replicadas en la nube requerirían una conversión a la plataforma de hipervisor propia de la nube antes de poder restaurarlas, una tarea que no se debe realizar durante una crisis.

Al utilizar NetApp Cloud Volumes para el almacenamiento conectado a invitados mediante la replicación de SnapCenter y SnapMirror desde las instalaciones locales junto con soluciones de virtualización de nube pública, se puede diseñar un mejor enfoque para la recuperación ante desastres que permite recuperar réplicas de máquinas virtuales en una infraestructura VMware SDDC totalmente consistente junto con herramientas de recuperación específicas de la nube (por ejemplo, Azure Site Recovery) o herramientas de terceros equivalentes como Veeam. Este enfoque también le permite realizar simulacros de recuperación ante desastres y recuperación de ransomware rápidamente. Esto también le permite escalar a producción completa para realizar pruebas o durante un desastre agregando hosts a pedido.

Caso de uso n.° 5: Modernización de aplicaciones

Una vez que las aplicaciones estén en la nube pública, las organizaciones querrán aprovechar los cientos de potentes servicios en la nube para modernizarlas y ampliarlas. Con el uso de NetApp Cloud Volumes, la modernización es un proceso sencillo porque los datos de la aplicación no están bloqueados en vSAN y permiten la movilidad de datos para una amplia gama de casos de uso, incluido Kubernetes.

Conclusión

Ya sea que su objetivo sea una nube completa o una nube híbrida, NetApp Cloud Volumes ofrece excelentes opciones para implementar y administrar las cargas de trabajo de las aplicaciones junto con los servicios de archivos y los protocolos de bloque, al tiempo que reduce el TCO al hacer que los requisitos de datos se

integren perfectamente con la capa de aplicación.

Cualquiera que sea el caso de uso, elija su nube/hiperescalador favorito junto con NetApp Cloud Volumes para obtener rápidamente los beneficios de la nube, una infraestructura y operaciones consistentes en las instalaciones y en múltiples nubes, portabilidad bidireccional de cargas de trabajo y capacidad y rendimiento de nivel empresarial.

Es el mismo proceso y procedimientos familiares que se utilizan para conectar el almacenamiento. Recuerde que lo único que cambió con los nuevos nombres fue la posición de los datos; las herramientas y los procesos siguen siendo los mismos y NetApp Cloud Volumes ayuda a optimizar la implementación general.

Casos de uso de la nube híbrida de VMware

Casos de uso de NetApp Hybrid Multicloud con VMware

Una descripción general de los casos de uso importantes para la organización de TI al planificar implementaciones de nube híbrida o de nube primero.

Casos de uso populares

Los casos de uso incluyen:

- Recuperación ante desastres,
- Cargas de trabajo de alojamiento durante el mantenimiento del centro de datos, * picos repentinos en los que se requieren recursos adicionales a los que están aprovisionados en el centro de datos local,
- Expansión del sitio de VMware,
- Migración rápida a la nube,
- Desarrollo/prueba, y
- Modernización de aplicaciones aprovechando tecnologías complementarias de la nube.

A lo largo de esta documentación, se detallarán referencias de carga de trabajo en la nube utilizando los casos de uso de VMware. Estos casos de uso son:

- Proteger (incluye recuperación ante desastres y copia de seguridad/restauración)
- Emigrar
- Extender

Dentro del viaje de TI

La mayoría de las organizaciones están en un viaje hacia la transformación y la modernización. Como parte de este proceso, las empresas están intentando utilizar sus inversiones existentes en VMware mientras aprovechan los beneficios de la nube y exploran formas de hacer que el proceso de migración sea lo más fluido posible. Este enfoque haría que sus esfuerzos de modernización fueran muy fáciles porque los datos ya están en la nube.

La respuesta más fácil a este escenario son las ofertas de VMware en cada hiperescalador. Al igual que NetApp Cloud Volumes, VMware ofrece una manera de trasladar o ampliar los entornos locales de VMware a cualquier nube, lo que le permite conservar los activos, las habilidades y las herramientas locales existentes mientras ejecuta cargas de trabajo de forma nativa en la nube. Esto reduce el riesgo porque no habrá interrupciones del servicio ni necesidad de cambios de IP y proporciona al equipo de TI la capacidad de

operar como lo hace localmente utilizando habilidades y herramientas existentes. Esto puede conducir a migraciones a la nube aceleradas y a una transición mucho más fluida hacia una arquitectura multicloud híbrida.

Comprender la importancia de las opciones de almacenamiento NFS suplementarias

Si bien VMware en cualquier nube ofrece capacidades híbridas únicas para cada cliente, las opciones limitadas de almacenamiento NFS complementario han restringido su utilidad para las organizaciones con cargas de trabajo con gran capacidad de almacenamiento. Debido a que el almacenamiento está directamente vinculado a los hosts, la única forma de escalar el almacenamiento es agregar más hosts, y eso puede aumentar los costos entre un 35 y un 40 por ciento o más para cargas de trabajo intensivas en almacenamiento. Estas cargas de trabajo solo necesitan almacenamiento adicional, no potencia adicional. Pero eso significa pagar por hosts adicionales.

Consideremos este escenario:

Un cliente requiere solo cinco hosts para CPU y memoria, pero tiene muchas necesidades de almacenamiento y necesita 12 hosts para satisfacer los requisitos de almacenamiento. Este requisito termina inclinando realmente la balanza financiera al tener que comprar caballos de fuerza adicionales, cuando solo necesitan incrementar el almacenamiento.

Al planificar la adopción y las migraciones a la nube, siempre es importante evaluar el mejor enfoque y tomar el camino más fácil que reduzca las inversiones totales. El enfoque más común y sencillo para cualquier migración de aplicaciones es el rehosting (también conocido como lift and shift) donde no hay una máquina virtual (VM) ni conversión de datos. El uso de NetApp Cloud Volumes con el centro de datos definido por software (SDDC) de VMware, además de complementar vSAN, proporciona una opción sencilla de elevación y traslado.

Soluciones NetApp para VMware en hiperescaladores

Obtenga más información sobre las soluciones que NetApp aporta al entorno VMware en cada uno de los hiperescaladores: desde la migración de flujos de trabajo, la extensión/explosión a la nube, el backup/restauración y la recuperación ante desastres.

Soluciones NetApp para entornos VMware

Ya sea que opere en un modelo de nube híbrida o un modelo de "nube primero", NetApp ofrece una amplia variedad de soluciones para abordar los casos de uso más comunes para administrar cargas de trabajo en un modelo de nube o nube híbrida.

NetApp también ofrece soluciones de almacenamiento aprovisionadas como almacenamiento invitado (conectado a invitado) o como un almacén de datos NFS complementario en cada uno de los hiperescaladores. Todas las soluciones se clasifican al unísono con la clasificación de VMware de cargas de trabajo en la nube. Estas clasificaciones incluyen:

- Proteger (incluye recuperación ante desastres y copia de seguridad/restauración)
- Emigrar
- Extender

Para obtener más detalles sobre las soluciones disponibles para cada hiperescalador, visite:

- "Soluciones para AWS/VMC"

- "Soluciones para Azure/AVS"
- "Soluciones para GCP/GCVE"

Soluciones de NetApp para Amazon VMware Managed Cloud (VMC)

Obtenga más información sobre las soluciones que NetApp aporta a AWS.

VMware define las cargas de trabajo en la nube en una de tres categorías:

- Proteger (incluyendo recuperación ante desastres y copia de seguridad/restauración)
- Emigrar
- Extender

Explore las soluciones disponibles en las siguientes secciones.

Proteger

- "Recuperación ante desastres con VMC en AWS (conexión de invitado)"
- "Veeam Backup Restore en VMC con FSx ONTAP"
- "Recuperación ante desastres (DRO) con FSx ONTAP y VMC"
- "Uso de Veeam Replication y FSx ONTAP para la recuperación ante desastres en VMware Cloud en AWS"

Emigrar

- "Migrar cargas de trabajo al almacén de datos de FSx ONTAP mediante VMware HCX"

Extender

¡¡MUY PRONTO!!

Soluciones NetApp para Azure VMware Solution (AVS)

Obtenga más información sobre las soluciones que NetApp aporta a Azure.

VMware define las cargas de trabajo en la nube en una de tres categorías:

- Proteger (incluyendo recuperación ante desastres y copia de seguridad/restauración)
- Emigrar
- Extender

Explore las soluciones disponibles en las siguientes secciones.

Proteger

- "Recuperación ante desastres con ANF y JetStream (almacén de datos NFS complementario)"
- "Recuperación ante desastres con ANF y CVO (almacenamiento conectado para invitados)"
- "Recuperación ante desastres (DRO) con ANF y AVS"
- "Uso de Veeam Replication y el almacén de datos de Azure NetApp Files para la recuperación ante

desastres en Azure VMware Solution"

Emigrar

- "Migrar cargas de trabajo al almacén de datos de Azure NetApp Files mediante VMware HCX"

Extender

¡¡MUY PRONTO!!

Soluciones de NetApp para Google Cloud VMware Engine (GCVE)

Obtenga más información sobre las soluciones que NetApp aporta a GCP.

VMware define las cargas de trabajo en la nube en una de tres categorías:

- Proteger (incluyendo recuperación ante desastres y copia de seguridad/restauración)
- Emigrar
- Extender

Explore las soluciones disponibles en las siguientes secciones.

Proteger

- "Recuperación ante desastres de aplicaciones con SnapCenter, Cloud Volumes ONTAP y Veeam Replication"
- "Recuperación ante desastres consistente con aplicaciones con NetApp SnapCenter y Veeam Replication en NetApp Volumes en GCVE"

Emigrar

- "Migración de carga de trabajo mediante VMware HCX al almacén de datos NFS de Google Cloud NetApp Volumes"
- "Replicación de máquinas virtuales mediante Veeam en el almacén de datos NFS de Google Cloud NetApp Volumes"

Extender

¡¡MUY PRONTO!!

NetApp para AWS/VMC

Capacidades de NetApp para AWS VMC

Obtenga más información sobre las capacidades que NetApp aporta a AWS VMware Cloud (VMC), desde NetApp como un dispositivo de almacenamiento conectado invitado o un almacén de datos NFS complementario hasta la migración de flujos de trabajo, la extensión/ampliación a la nube, la copia de seguridad/restauración y la recuperación ante desastres.

Salte a la sección del contenido deseado seleccionando entre las siguientes opciones:

- "Configuración de VMC en AWS"
- "Opciones de almacenamiento de NetApp para VMC"
- "Soluciones en la nube NetApp /VMware"

Configuración de VMC en AWS

Al igual que en las instalaciones locales, la planificación de un entorno de virtualización basado en la nube es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

Esta sección describe cómo configurar y administrar VMware Cloud on AWS SDDC y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .



El almacenamiento en el host es el único método compatible para conectar Cloud Volumes ONTAP a AWS VMC.

El proceso de configuración se puede dividir en los siguientes pasos:

- Implementar y configurar VMware Cloud para AWS
- Conecte VMware Cloud a FSx ONTAP

Ver el detalle"Pasos de configuración para VMC" .

Opciones de almacenamiento de NetApp para VMC

El almacenamiento de NetApp se puede utilizar de varias maneras, ya sea como almacenamiento conectado a una instancia específica o como un almacén de datos NFS complementario, dentro de AWS VMC.

Por favor visite"Opciones de almacenamiento de NetApp compatibles" Para más información.

AWS admite el almacenamiento de NetApp en las siguientes configuraciones:

- FSx ONTAP como almacenamiento conectado para invitados
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- FSx ONTAP como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para VMC" . Ver el detalle"Opciones de almacén de datos NFS complementario para VMC" .

Casos de uso de soluciones

Con las soluciones de nube de NetApp y VMware, muchos casos de uso son fáciles de implementar en su AWS VMC. Se definen casos de uso para cada una de las áreas de nube definidas por VMware:

- Proteger (incluye recuperación ante desastres y copia de seguridad/restauración)
- Extender
- Emigrar

"Explorar las soluciones de NetApp para AWS VMC"

Proteja las cargas de trabajo en AWS/VMC

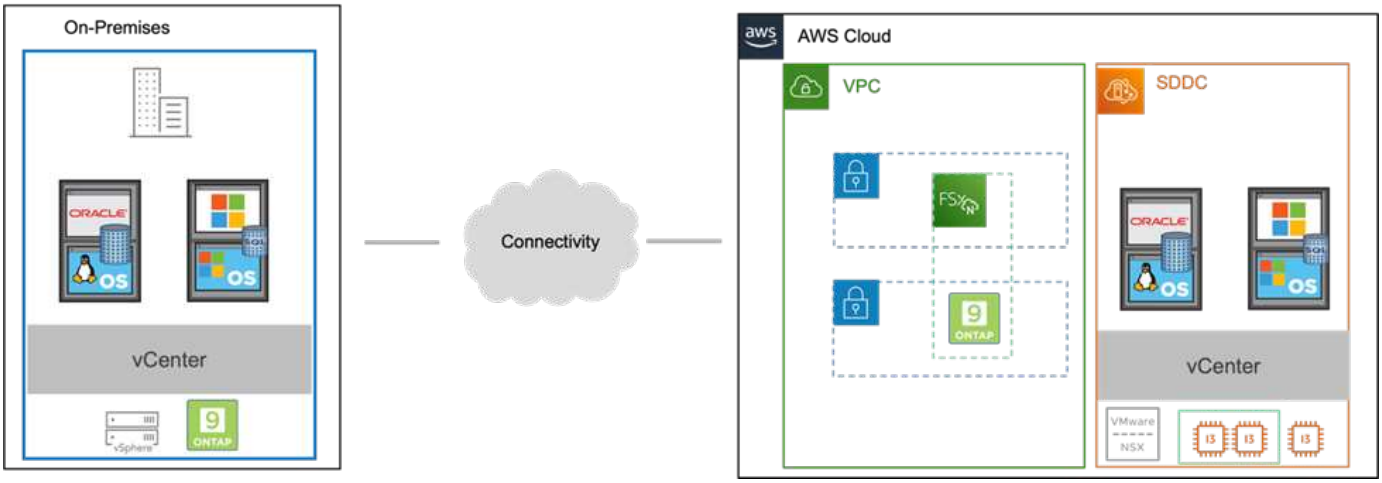
TR-4931: Recuperación ante desastres con VMware Cloud en Amazon Web Services y Guest Connect

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.

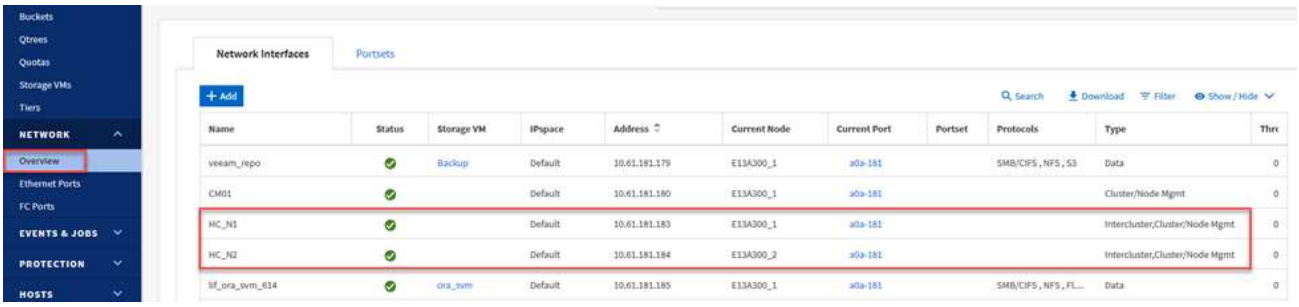
Los siguientes pasos son necesarios para configurar las relaciones de SnapMirror entre un sistema ONTAP local y FSx ONTAP:

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.
```

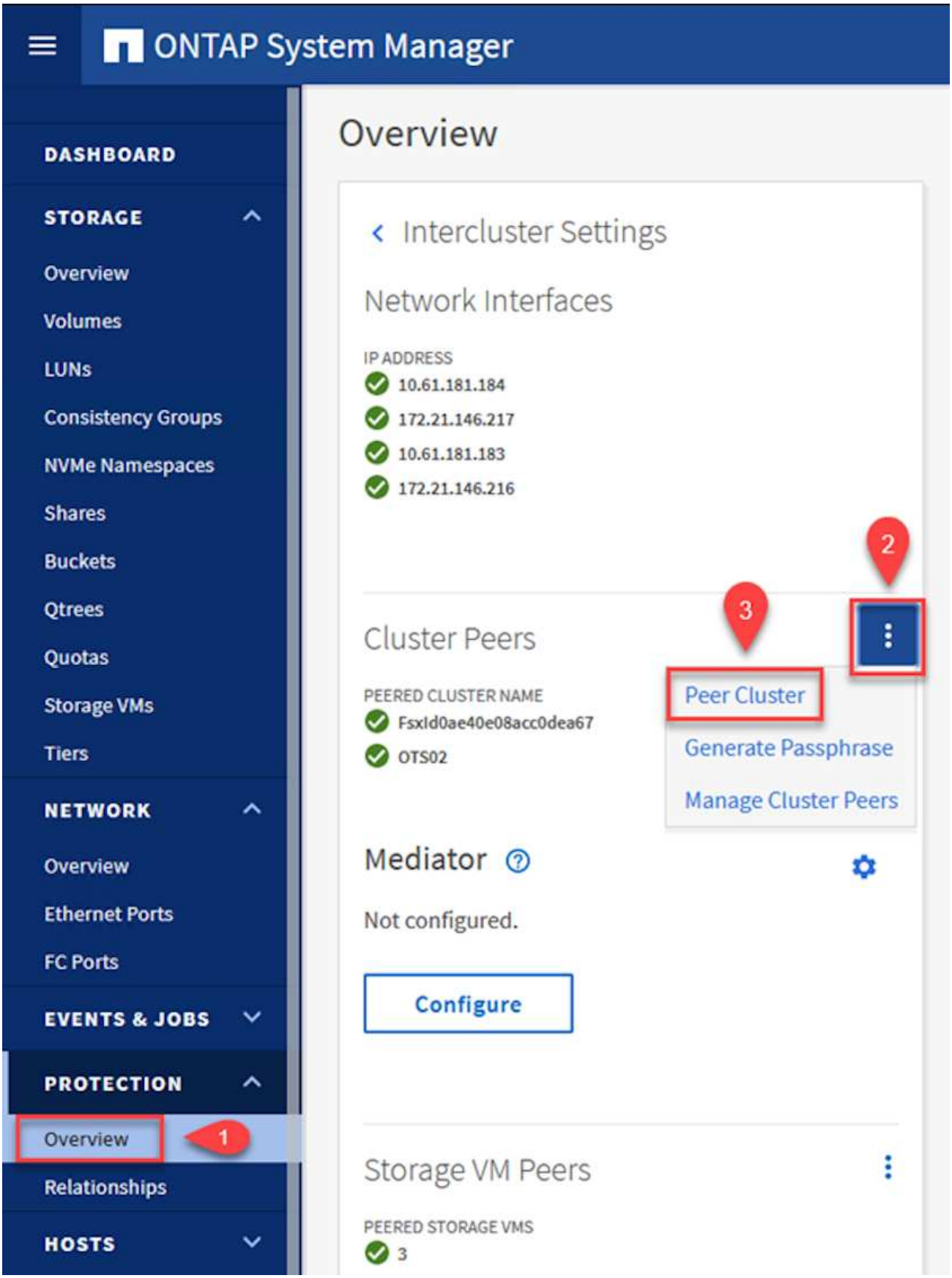
▼ **Establecer peering de clúster entre ONTAP y FSx**

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.



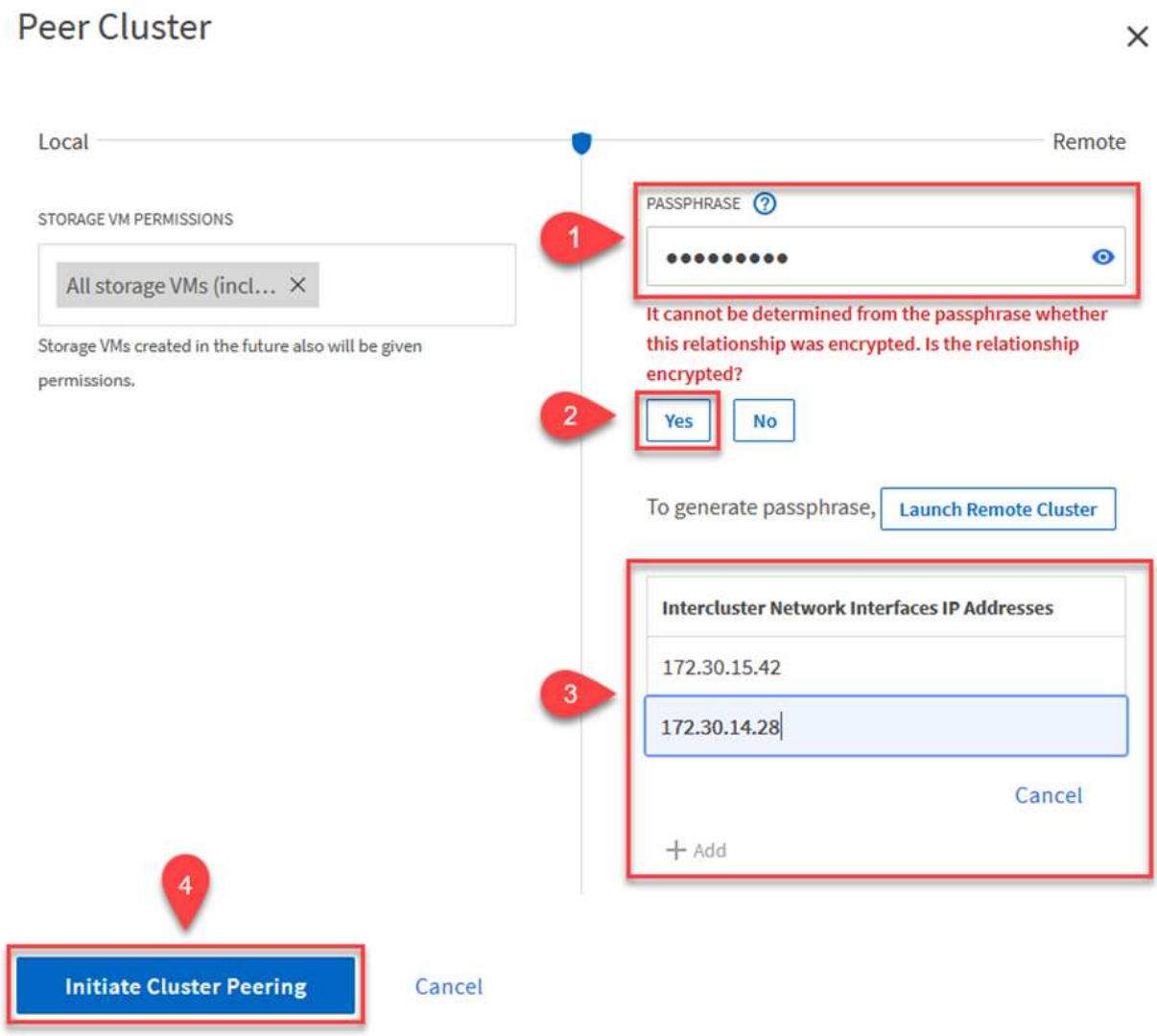
3. En el cuadro de diálogo Clúster de pares, complete la información requerida:
   a. Ingrese la frase de contraseña que se utilizó para establecer la relación de clúster de pares en el

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**

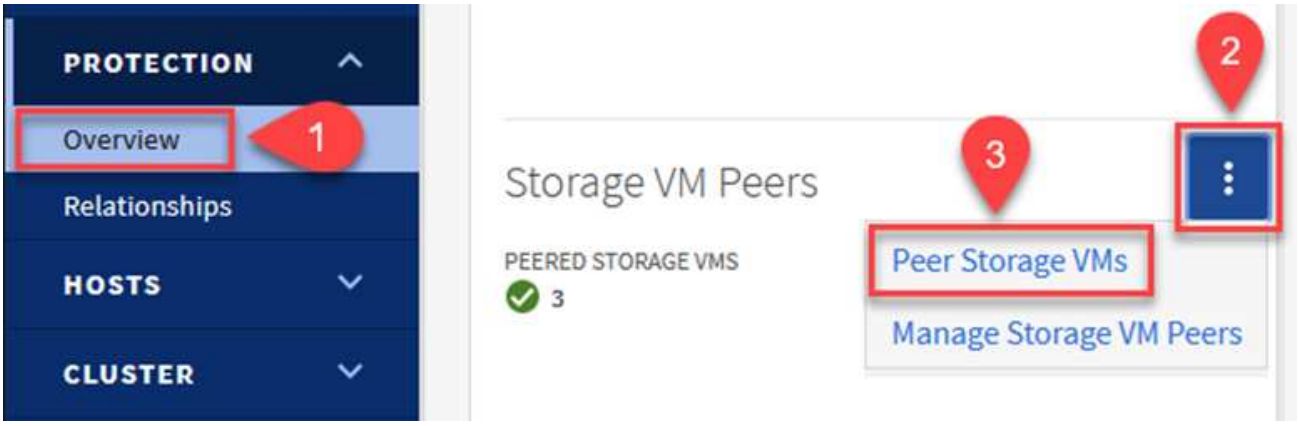
El siguiente paso es configurar una relación SVM entre las máquinas virtuales de almacenamiento de

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.

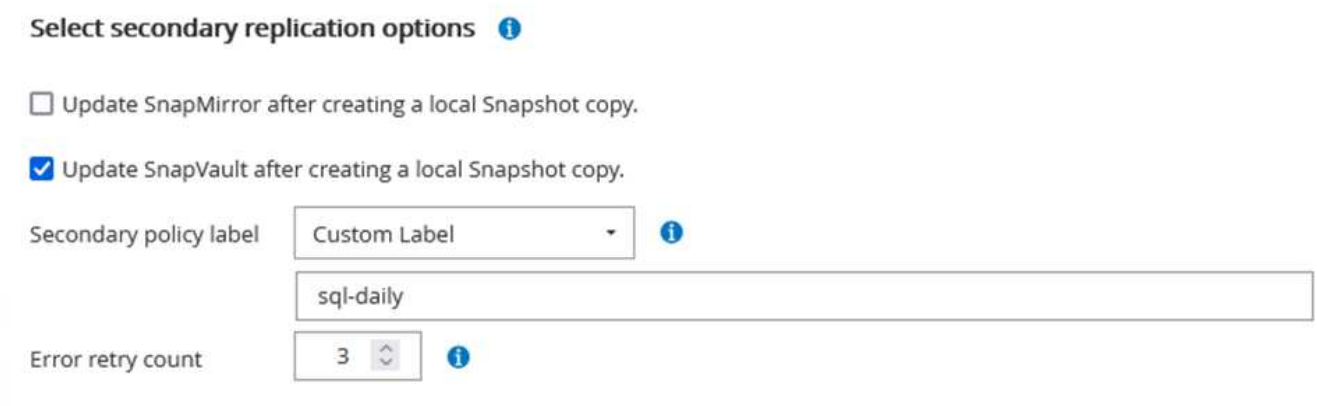
▼ **Crear una política de retención de instantáneas**

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" .

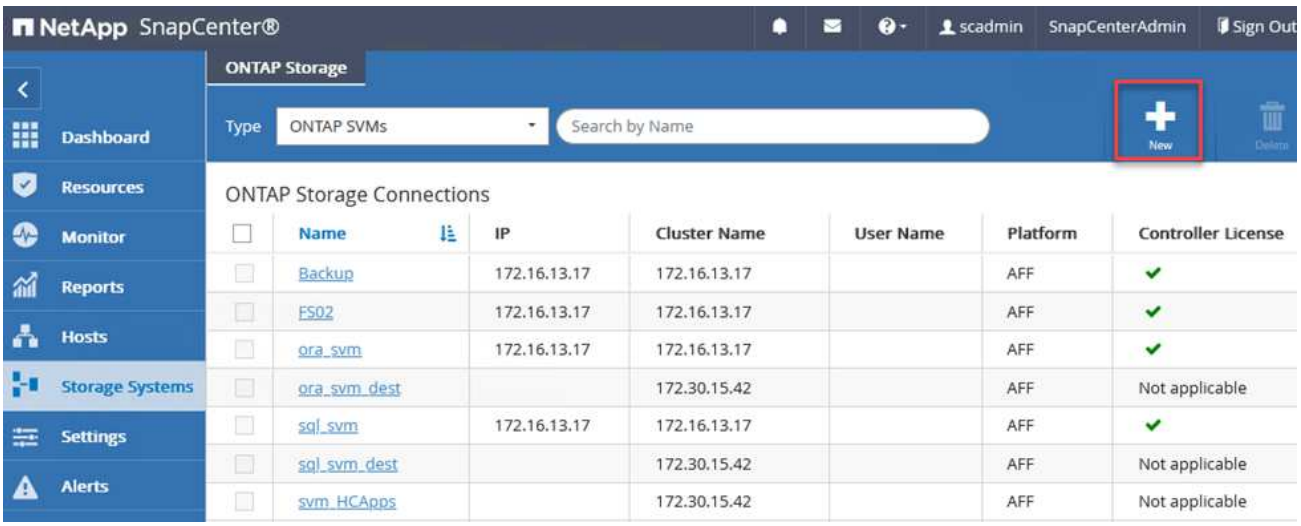
Una vez instalado, puede acceder a la consola de SnapCenter desde un navegador web usando *https://Virtual_Cluster_IP_or_FQDN:8146*.

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.

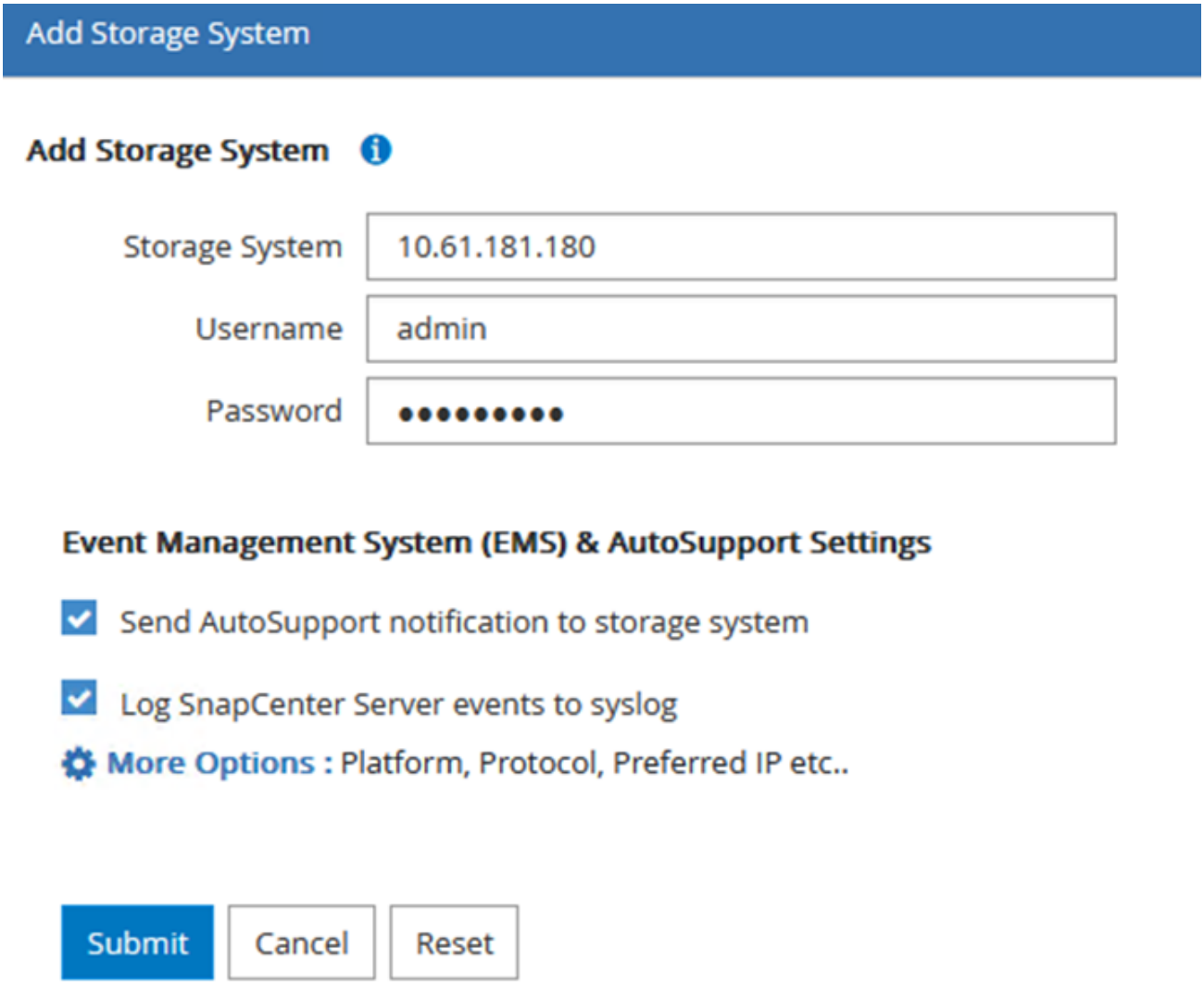
▼ Agregar controladores de almacenamiento a SnapCenter

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

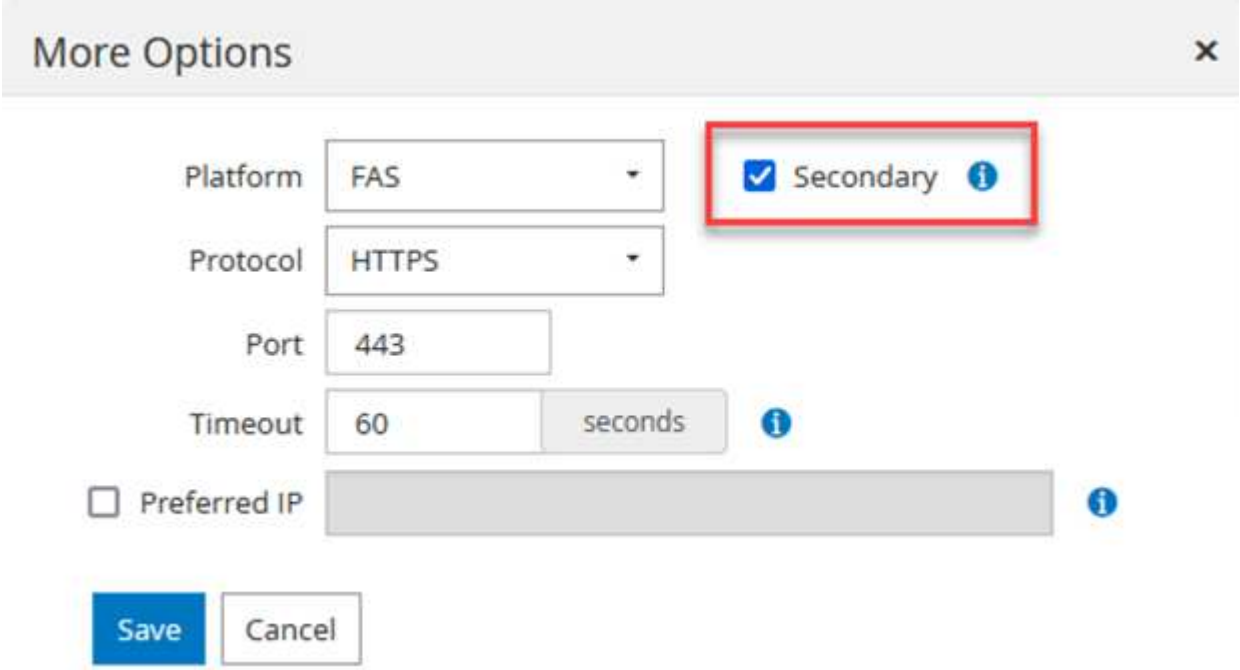
1. En el menú de la izquierda, seleccione Sistemas de almacenamiento y luego haga clic en Nuevo para comenzar el proceso de agregar sus controladores de almacenamiento a SnapCenter.



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.

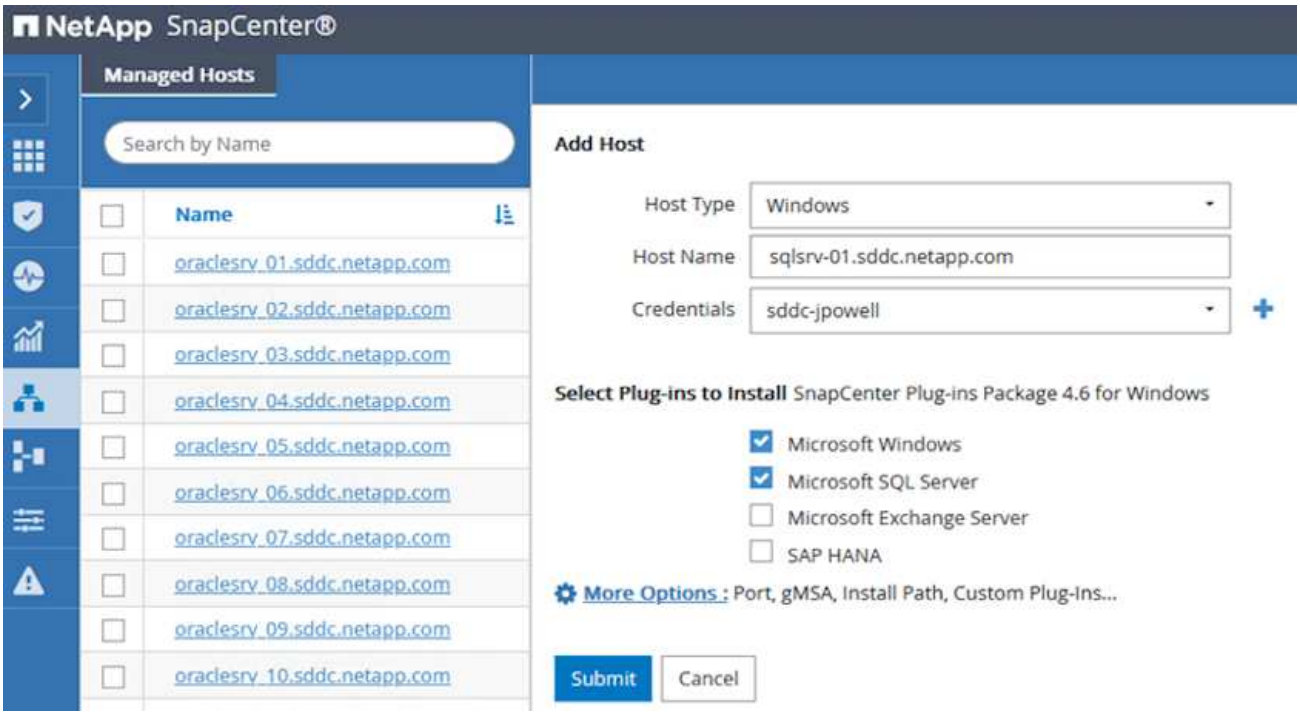


Para obtener más información relacionada con la adición de sistemas de almacenamiento a SnapCenter, consulte la documentación en "este enlace" .

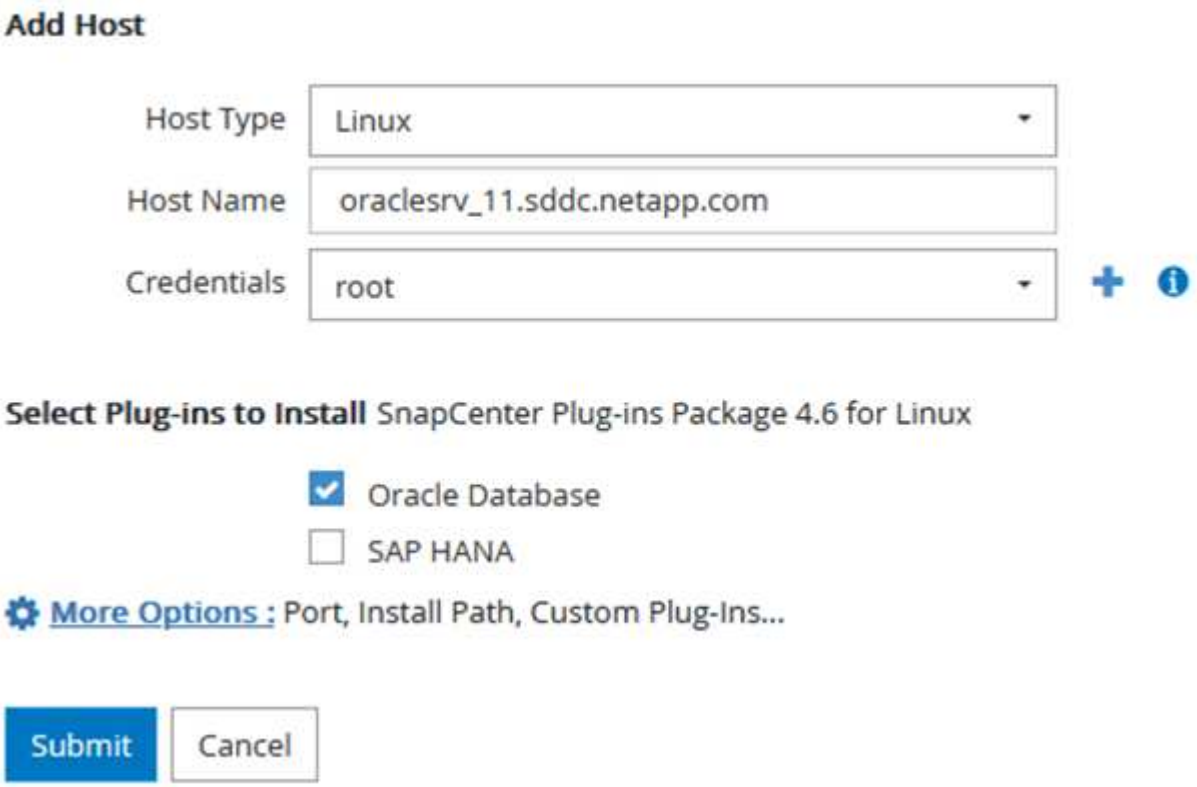
▼ **Agregar hosts a SnapCenter**

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.



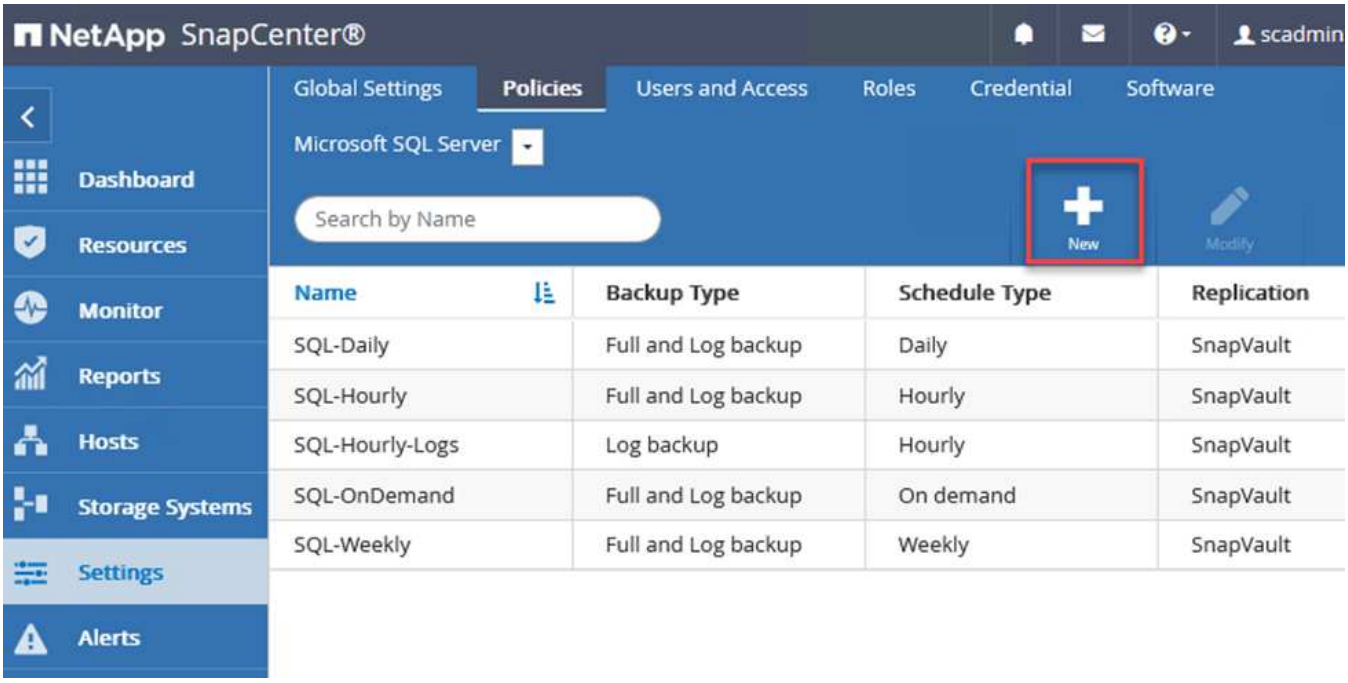
3. Para Oracle, complete los campos obligatorios en el cuadro de diálogo Agregar host y marque la casilla del complemento de Oracle Database. A continuación, haga clic en Enviar para iniciar el proceso de descubrimiento y agregar el host a SnapCenter.



▼ **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 .



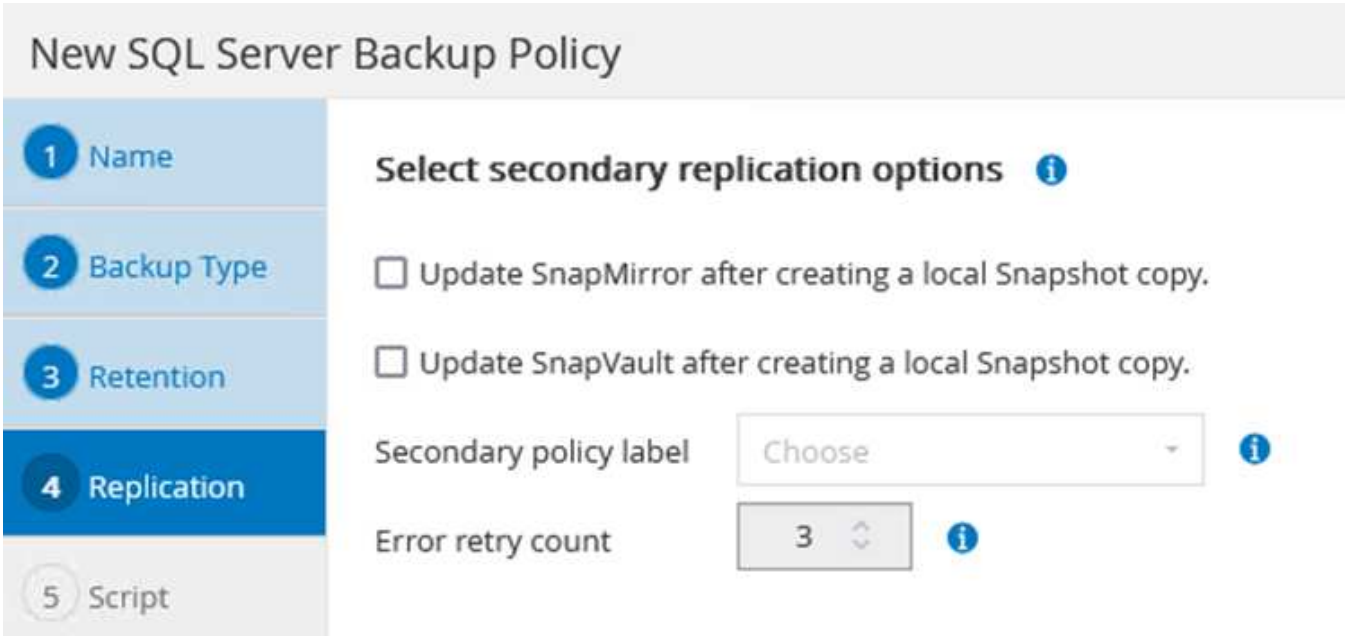
Para obtener información completa sobre la creación de políticas para copias de seguridad de SQL Server, consulte la "Documentación de SnapCenter" .

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.

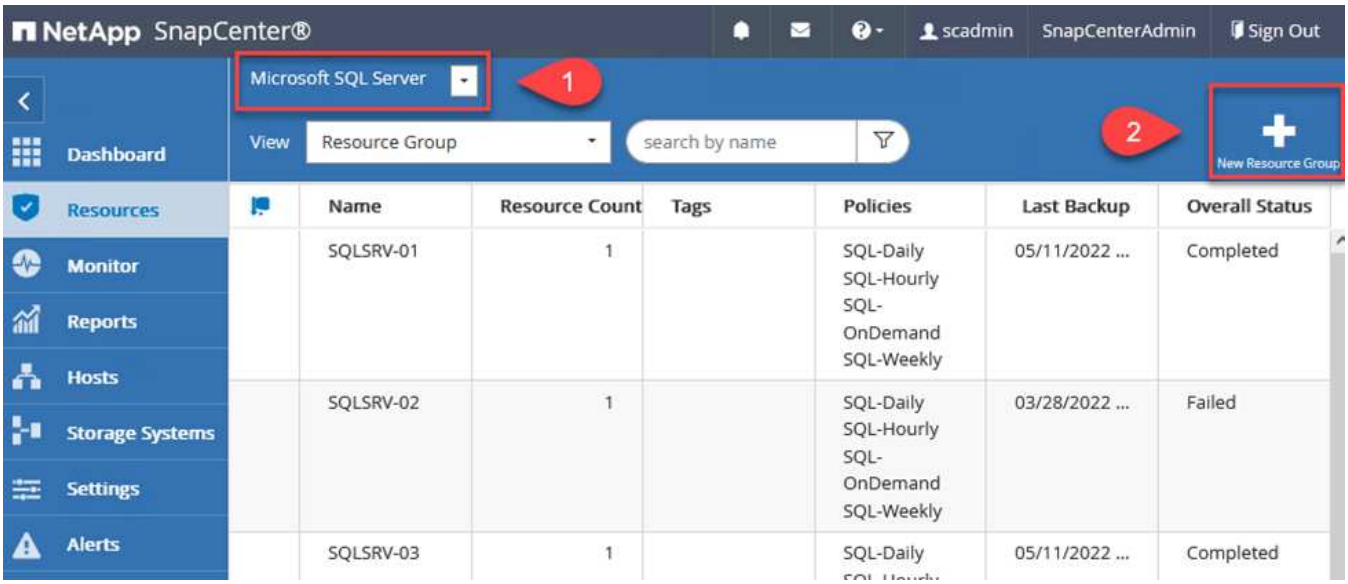
La siguiente imagen muestra las opciones anteriores y cómo se ven en el asistente de política de respaldo.



▼ **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.

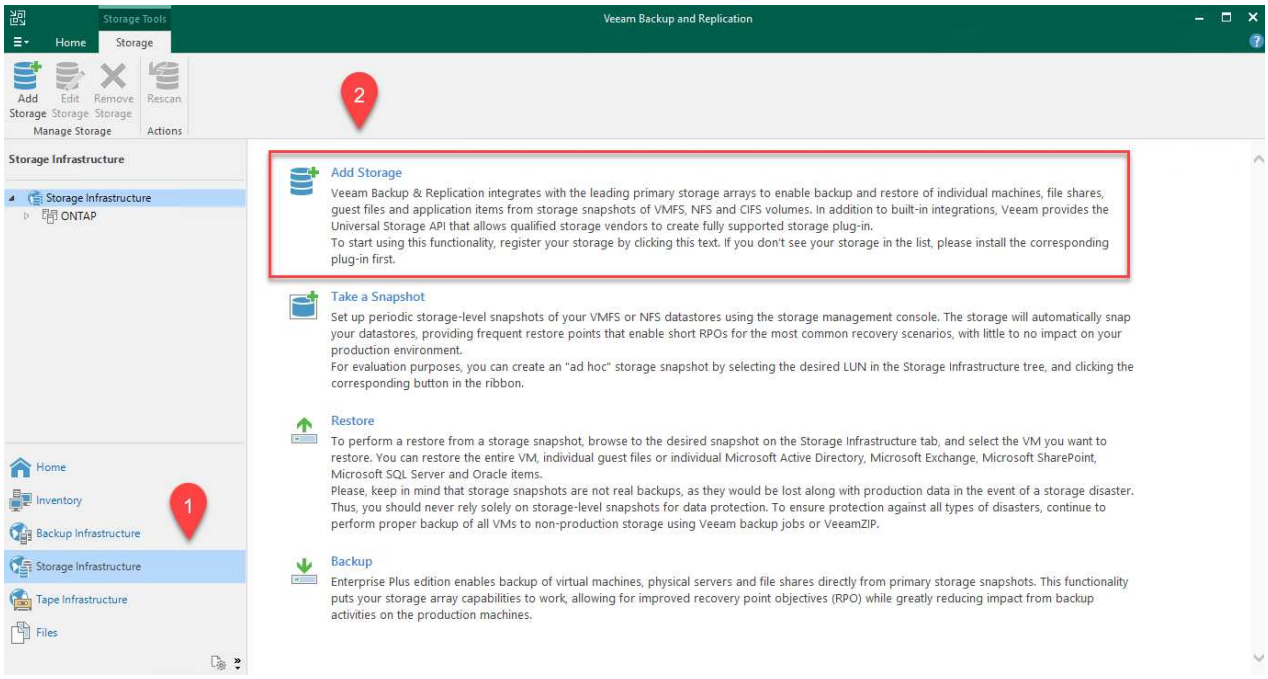
Consulte los siguientes requisitos previos antes de comenzar.

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.

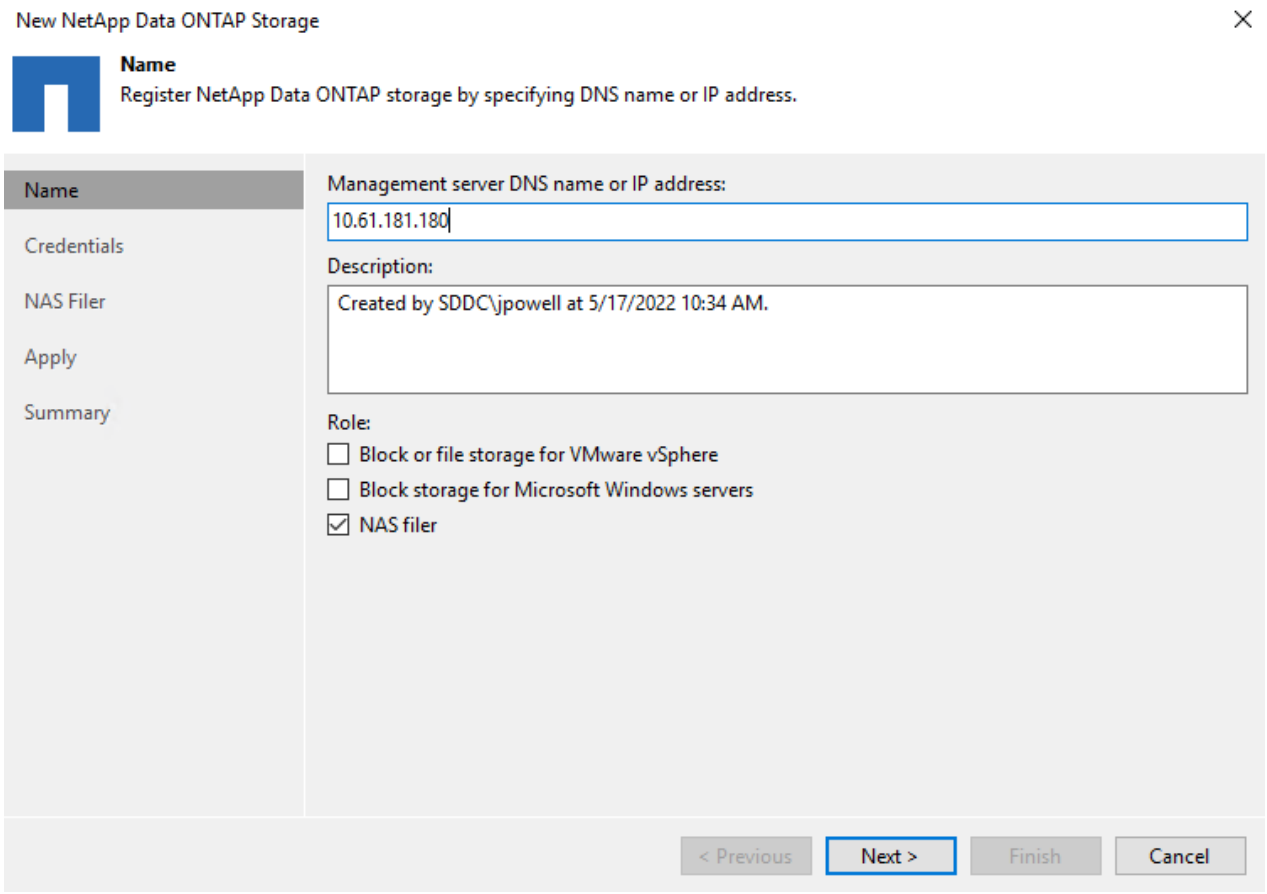
▼ **Agregue almacenamiento ONTAP a Veeam**

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

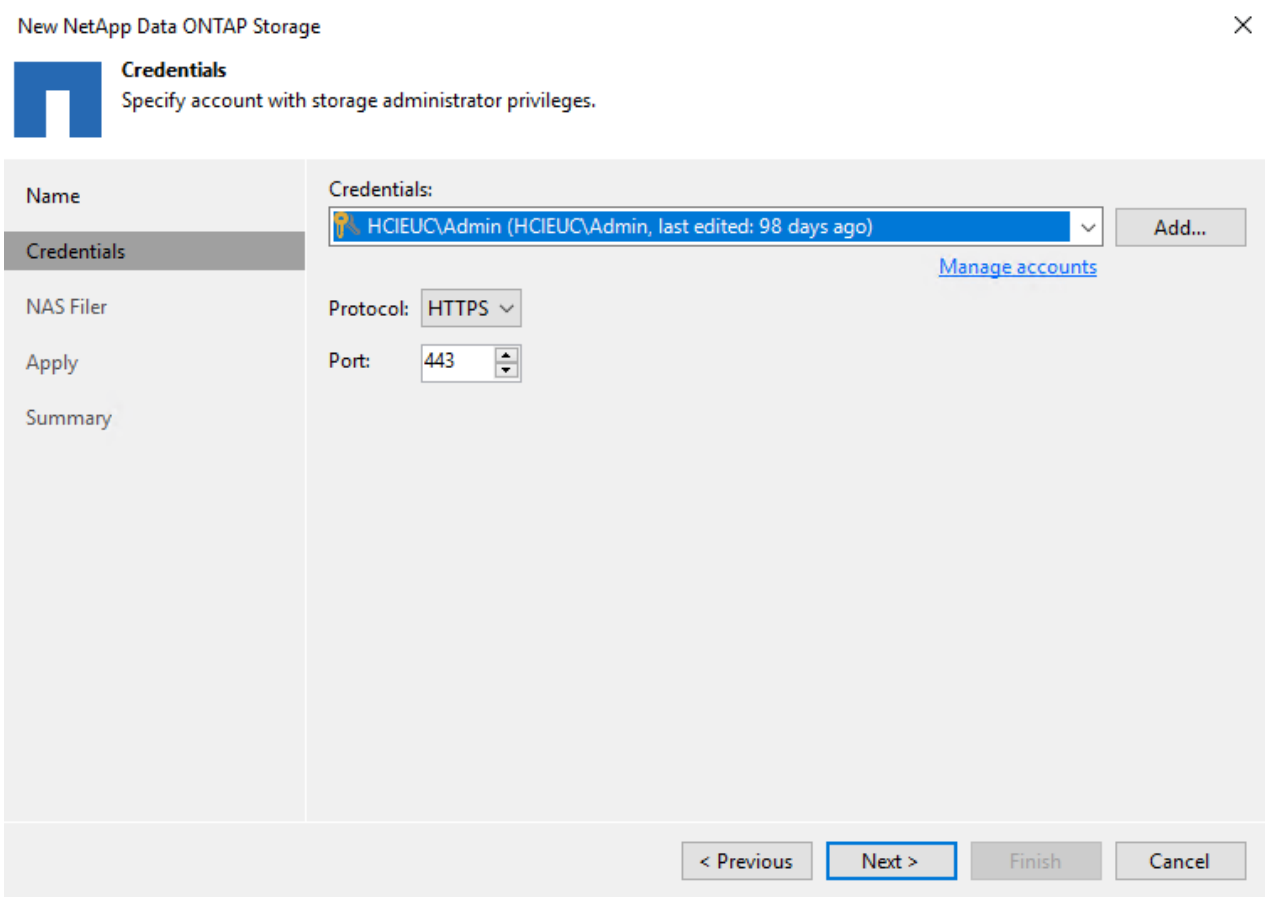
1. Abra la consola de Veeam e inicie sesión. Navegue hasta Infraestructura de almacenamiento y luego seleccione Agregar almacenamiento.



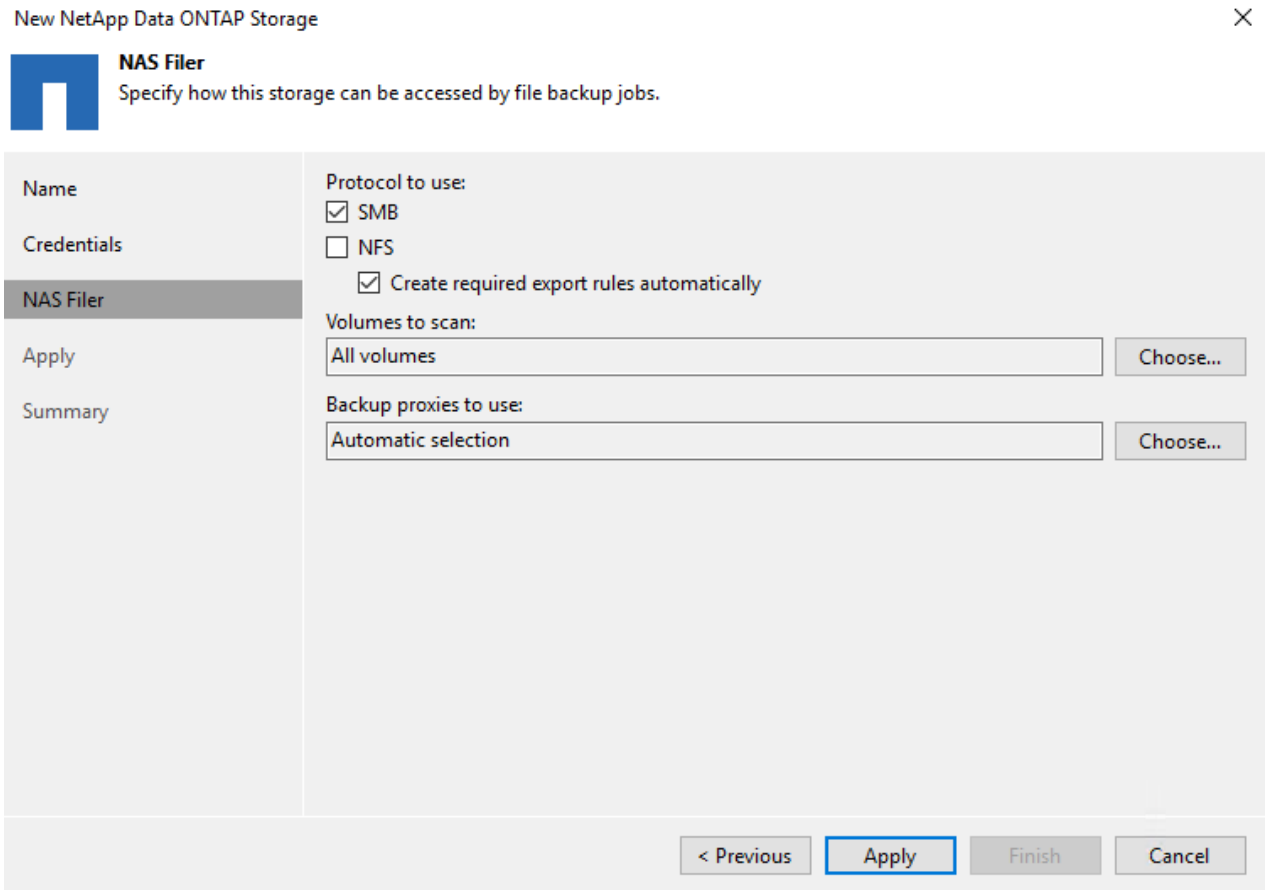
2. En el asistente Agregar almacenamiento, seleccione NetApp como proveedor de almacenamiento y luego seleccione Data ONTAP.
3. Introduzca la dirección IP de administración y marque la casilla NAS Filer. Haga clic en Siguiente.



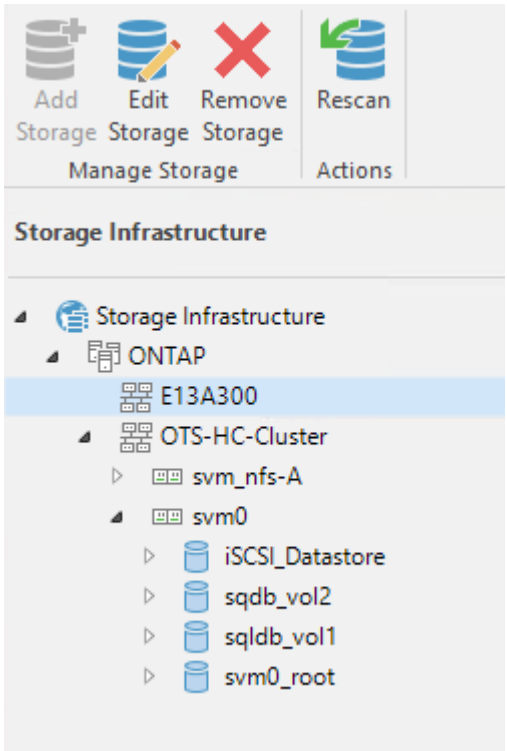
4. Agregue sus credenciales para acceder al clúster ONTAP .



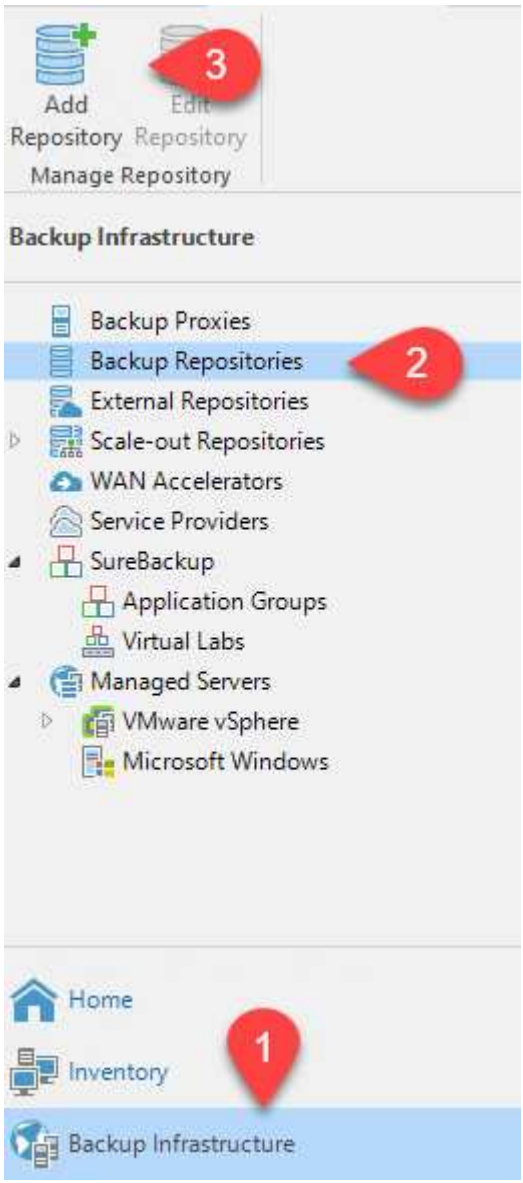
5. En la página NAS Filer, seleccione los protocolos que desea escanear y seleccione Siguiente.



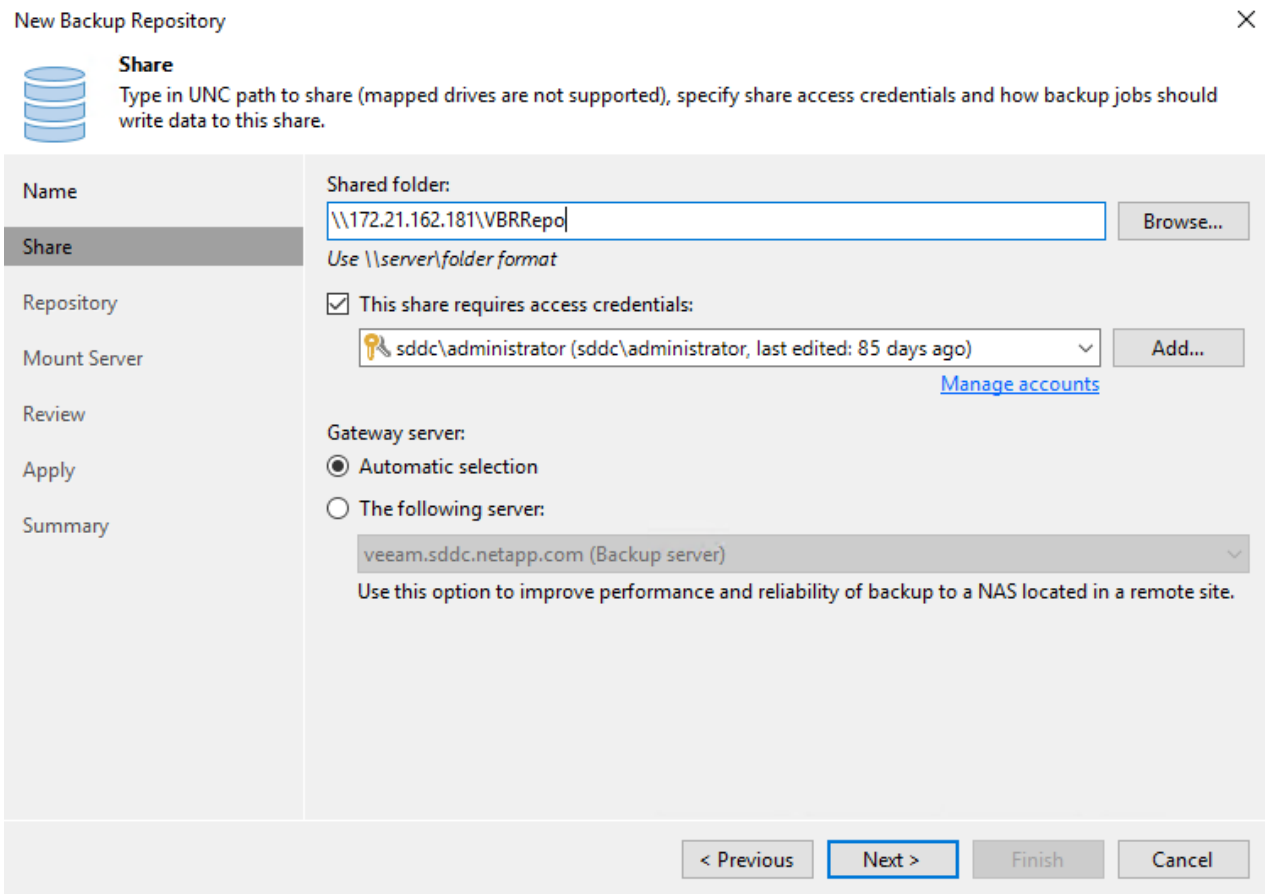
6. Complete las páginas Aplicar y Resumen del asistente y haga clic en Finalizar para comenzar el proceso de descubrimiento de almacenamiento. Una vez finalizado el escaneo, se agrega el clúster ONTAP junto con los archivadores NAS como recursos disponibles.



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.



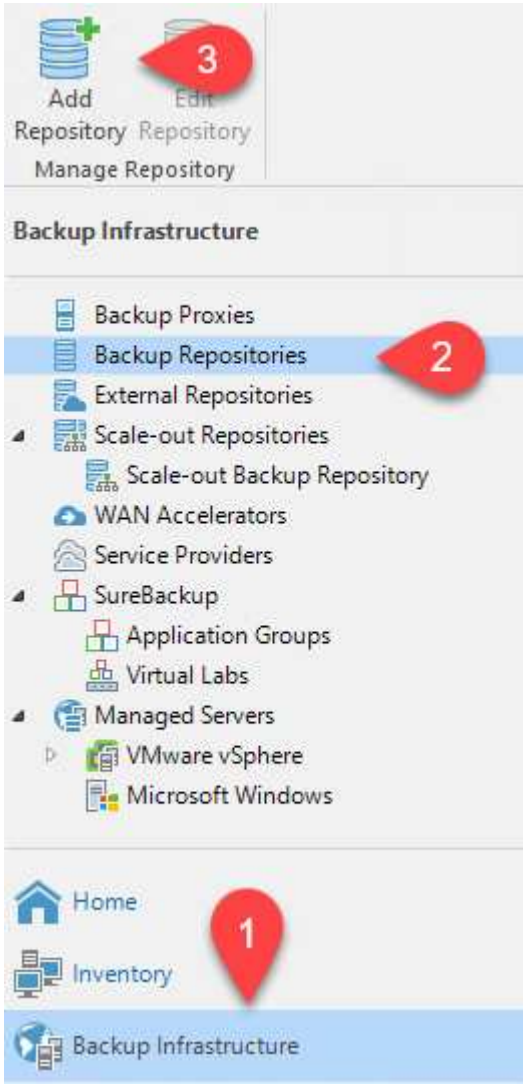
8. Siga todos los pasos del Asistente para nuevo repositorio de copia de seguridad para crear el repositorio. Para obtener información detallada sobre la creación de repositorios de Veeam Backup, consulte la "Documentación de Veeam" .



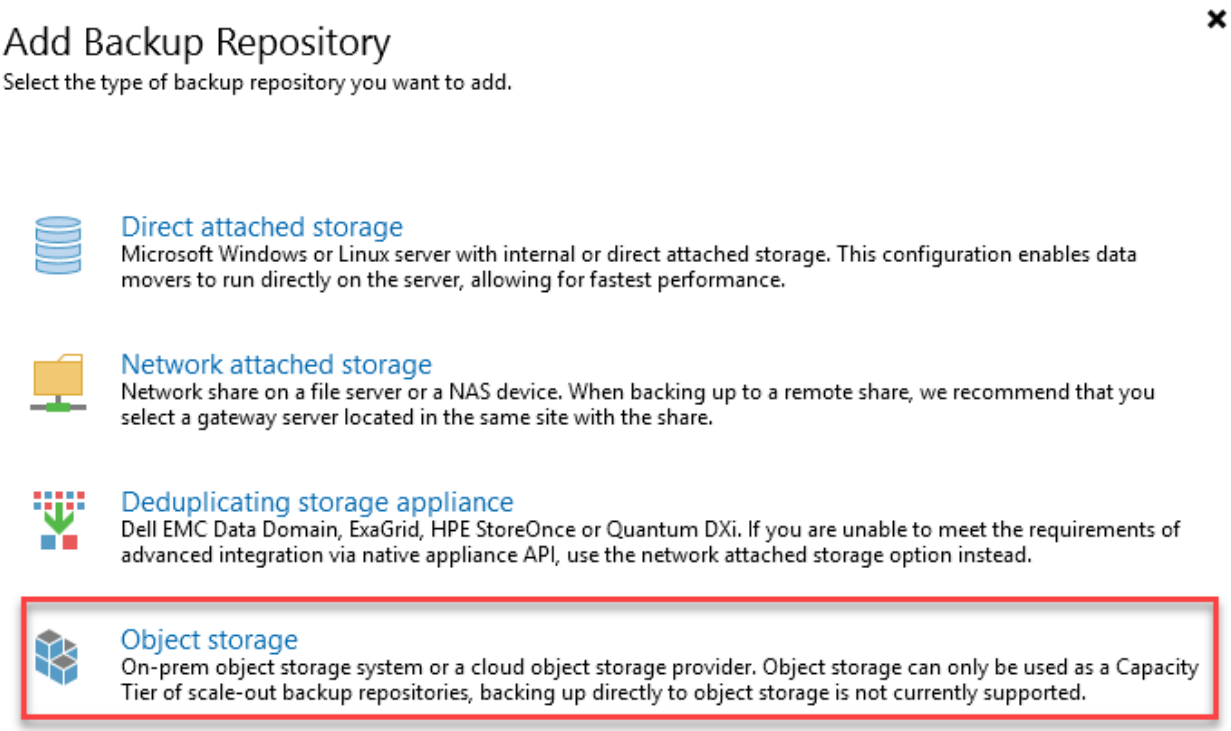
▼ **Agregue el bucket de Amazon S3 como repositorio de respaldo**

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

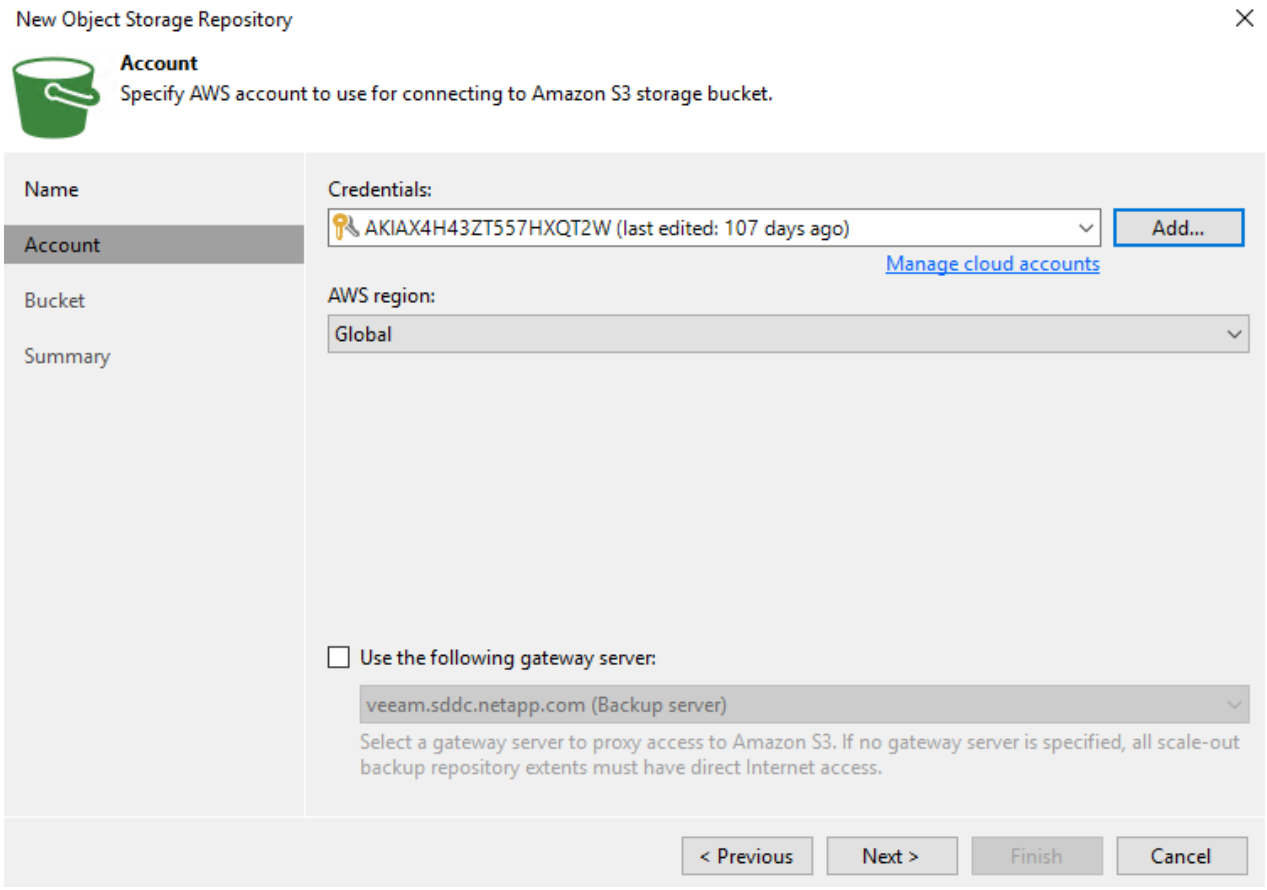
1. Vaya a Infraestructura de respaldo > Repositorios de respaldo. Haga clic en Agregar repositorio.



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.

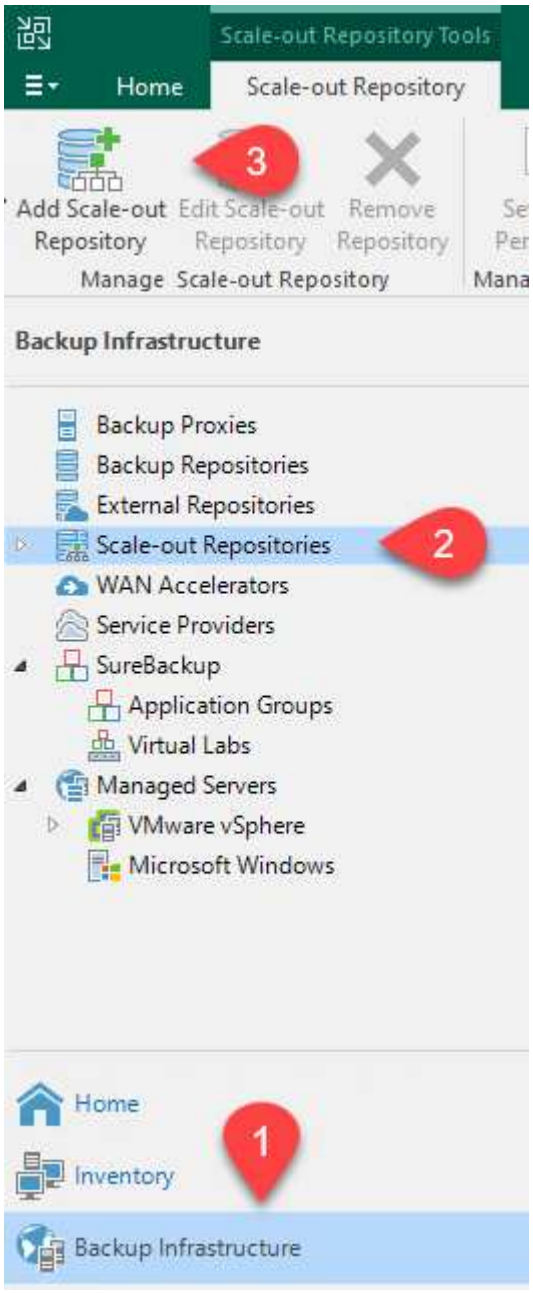


5. Después de que se cargue la configuración de Amazon, elija su centro de datos, depósito y carpeta y haga clic en Aplicar. Por último, haga clic en Finalizar para cerrar el asistente.

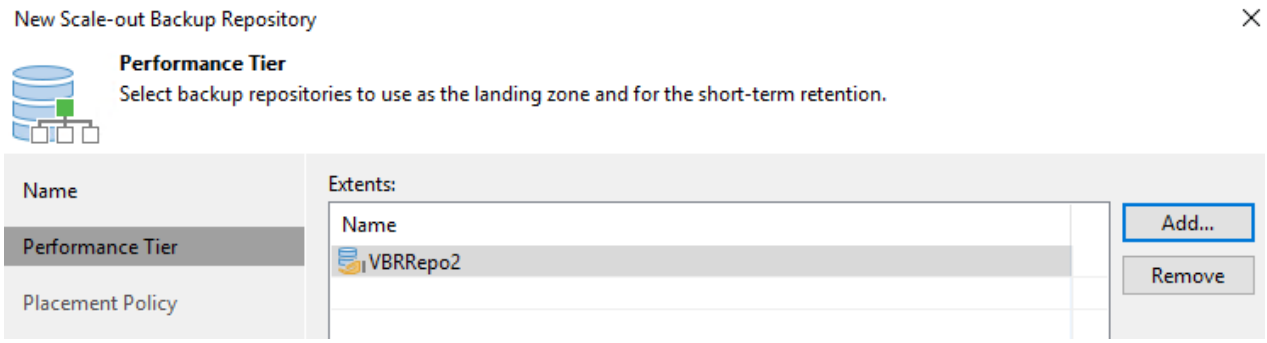
▼ **Crear un repositorio de respaldo escalable**

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.

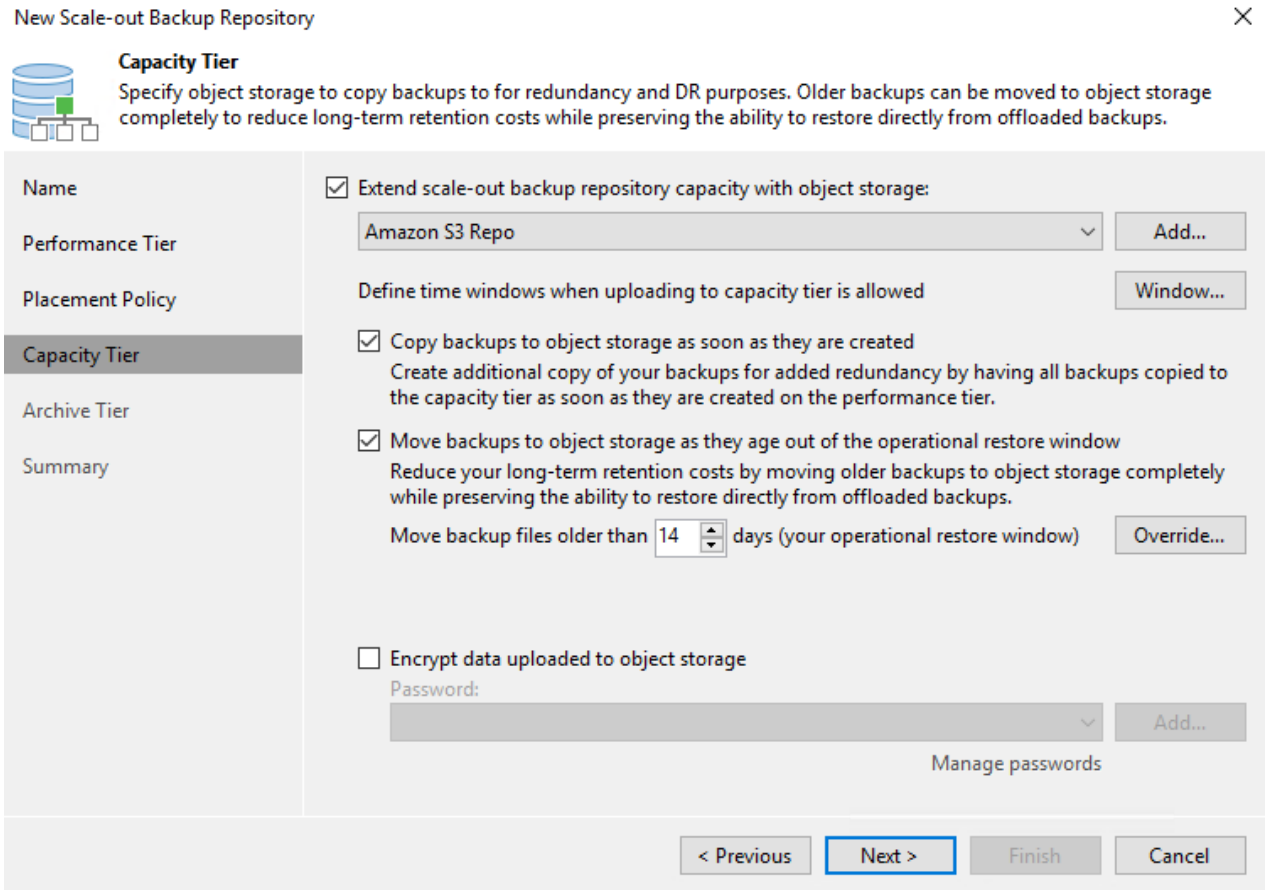
1. En Infraestructura de respaldo, seleccione Repositorios de escalamiento horizontal y luego haga clic en el elemento de menú Agregar repositorio de escalamiento horizontal.



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" .

NetApp herramientas y configuración de 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**

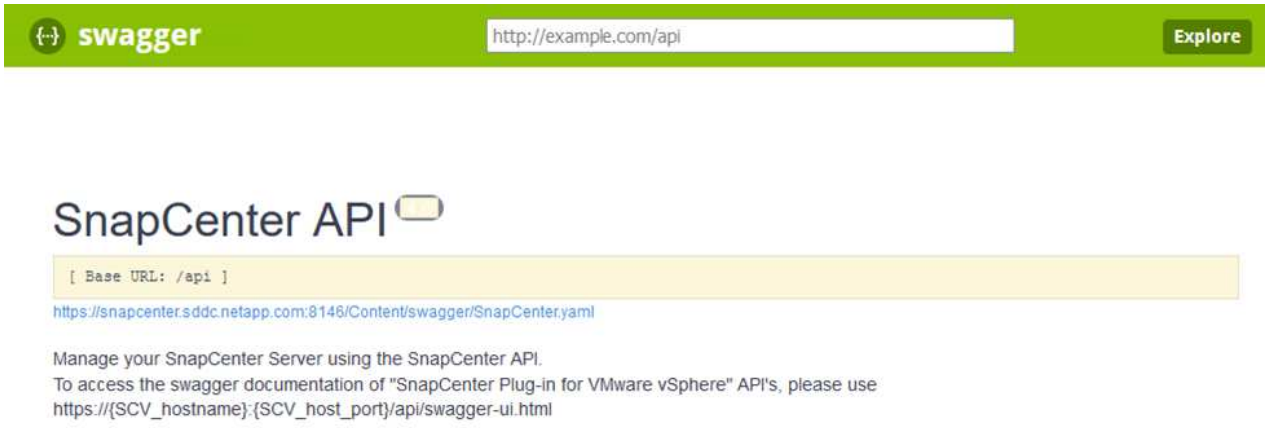
SnapCenter proporciona una interfaz de cliente web para ejecutar comandos de API REST. Para obtener información sobre cómo acceder a las API REST a través de Swagger, consulte la documentación de SnapCenter en "este enlace" .

▼ **Inicie sesión en Swagger y obtenga el token de autorización**

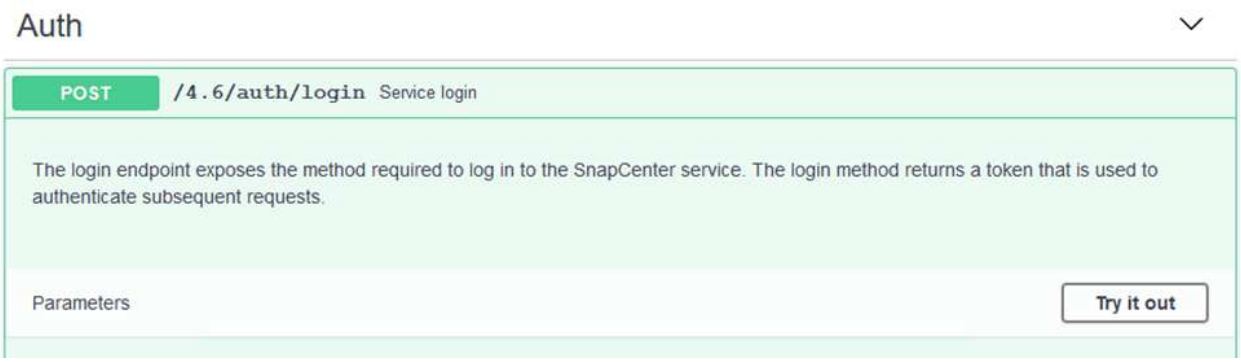
Después de navegar a la página Swagger, debe recuperar un token de autorización para iniciar el

proceso de restauración de la base de datos.

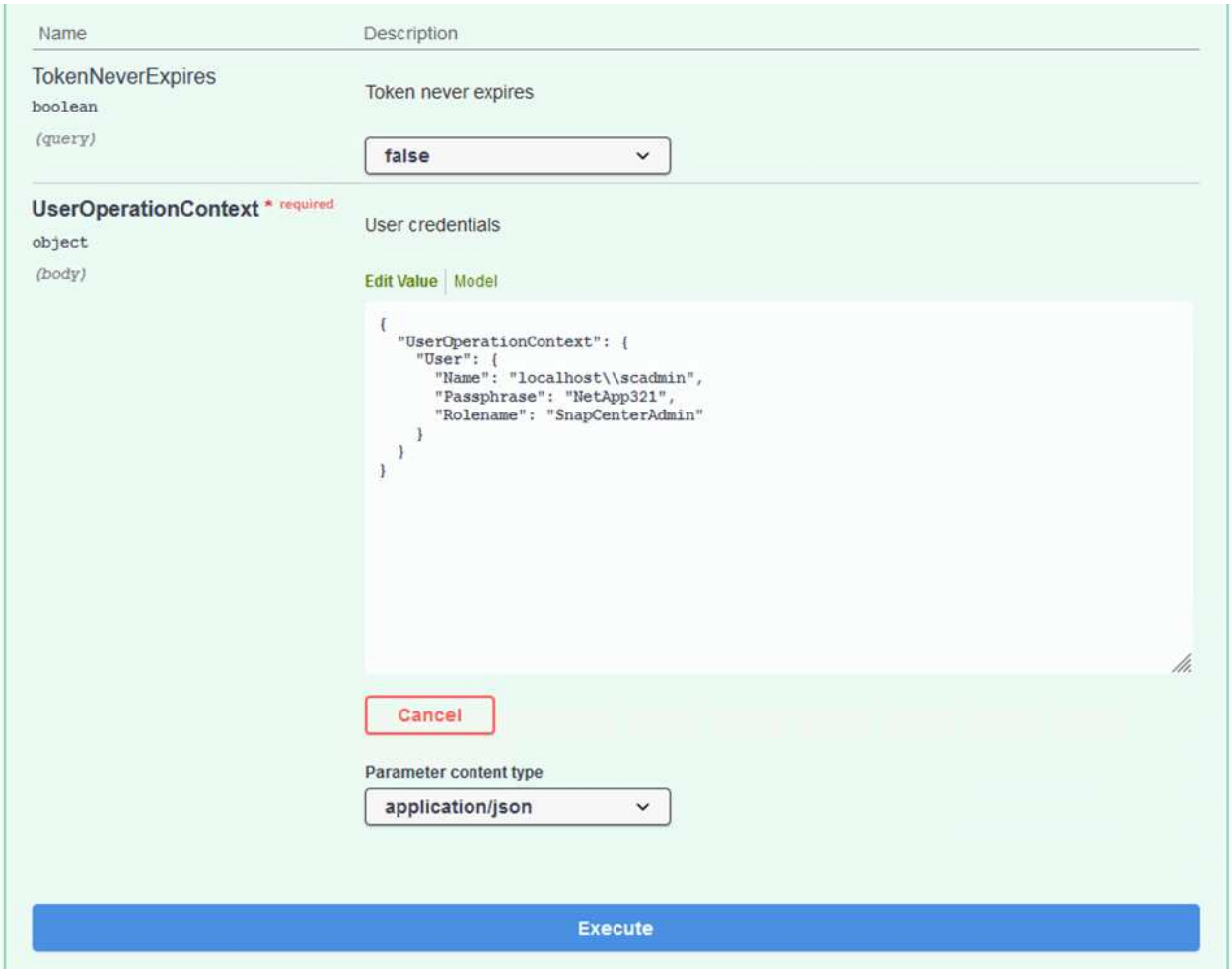
1. Acceda a la página web de la API Swagger de SnapCenter en *https://< IP del servidor SnapCenter >:8146/swagger/*.



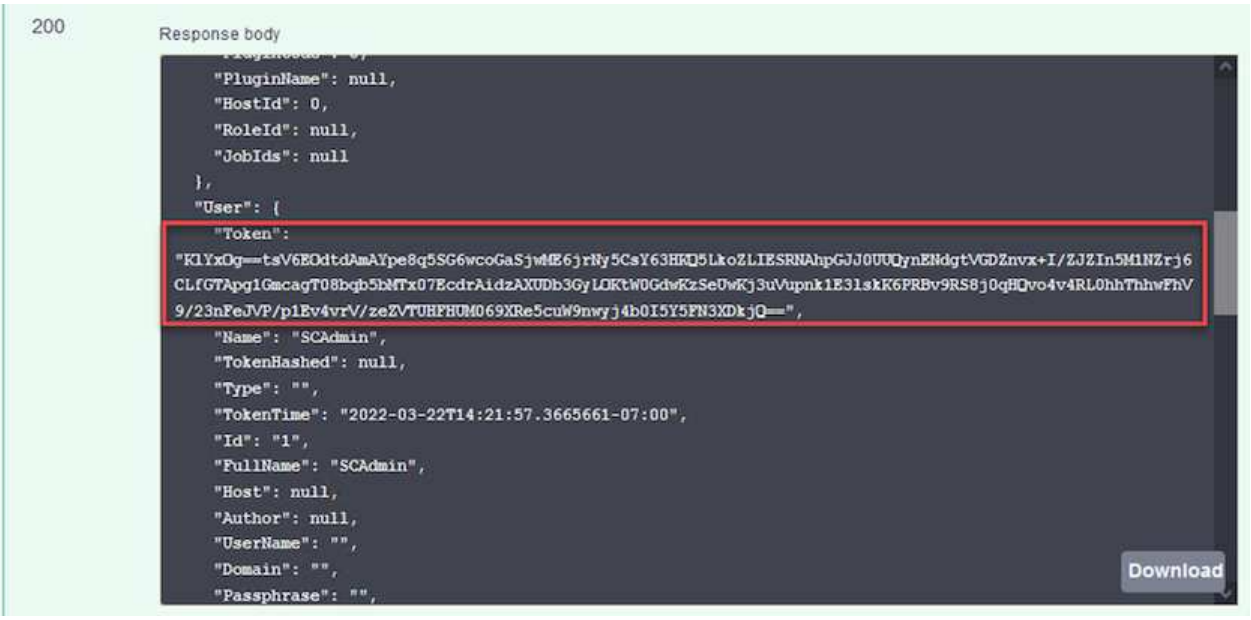
2. Expande la sección Autenticación y haz clic en Probarlo.



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



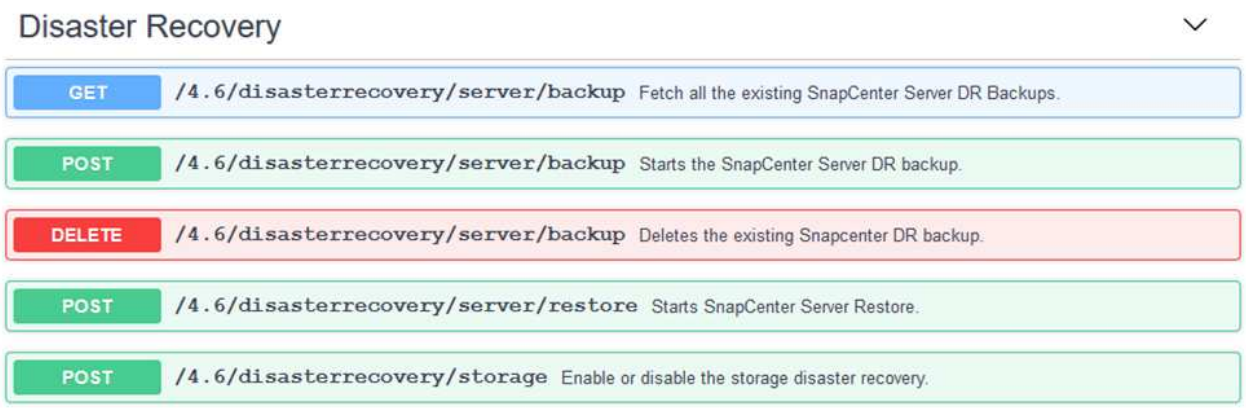
4. En el cuerpo de respuesta a continuación, puedes ver el token. Copie el texto del token para la autenticación al ejecutar el proceso de copia de seguridad.



▼ **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.

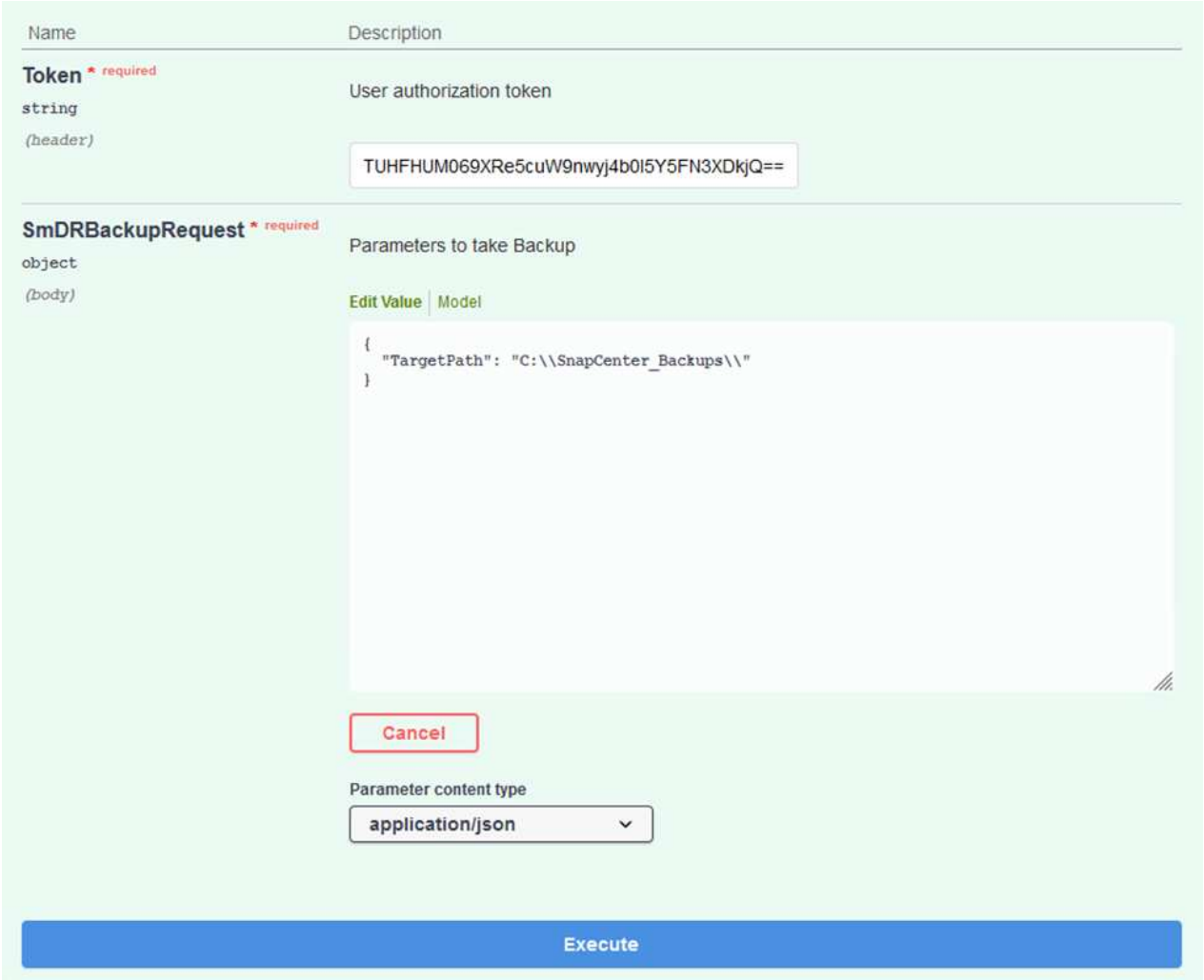


2. Ampliar el `/4.6/disasterrecovery/server/backup` sección y haga clic en Probarlo.



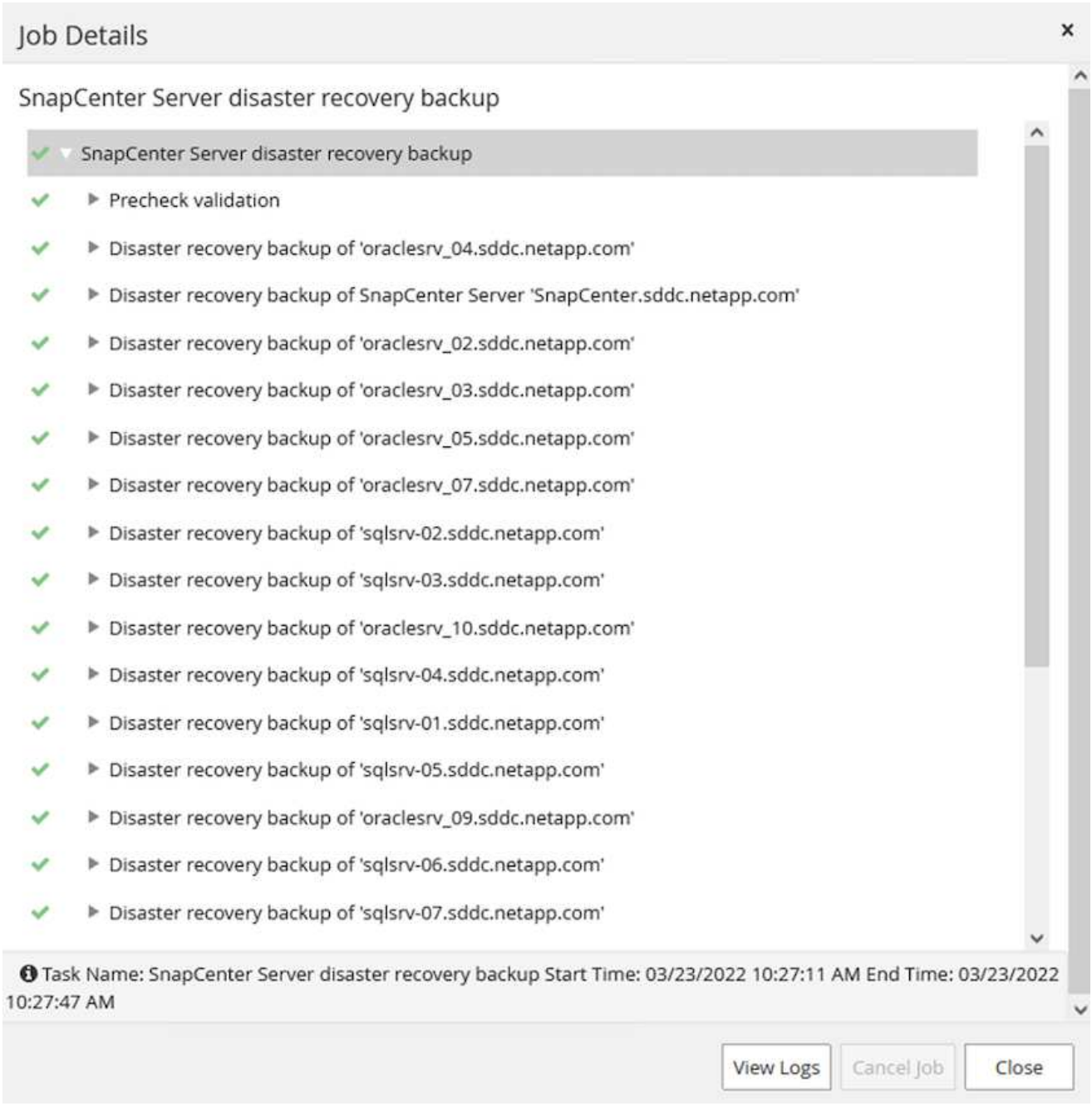
3. En la sección SmDRBackupRequest, agregue la ruta de destino local correcta y seleccione Ejecutar para iniciar la copia de seguridad de la base de datos y la configuración de SnapCenter .

> El proceso de copia de seguridad no permite realizar copias de seguridad directamente en un recurso compartido de archivos NFS o CIFS.



▼ **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**

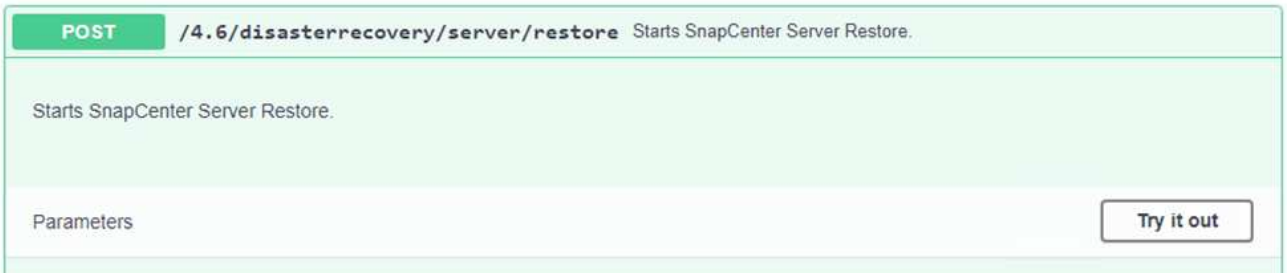
SnapCenter admite escenarios de recuperación ante desastres al permitir la copia de seguridad y la restauración de su base de datos MySQL y sus archivos de configuración. Esto permite que un administrador mantenga copias de seguridad periódicas de la base de datos de SnapCenter en el centro de datos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

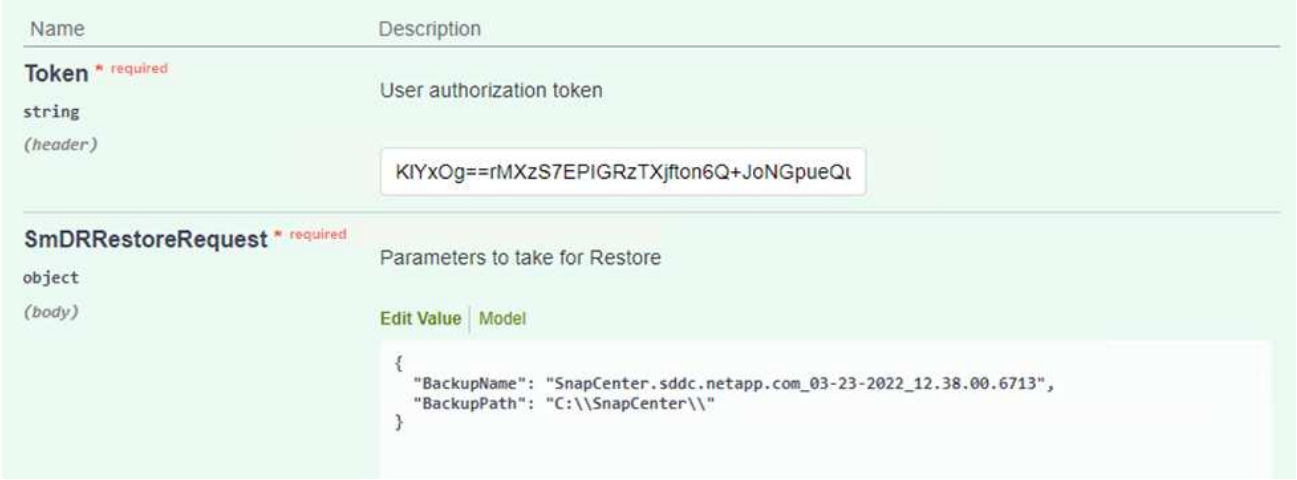
1. Romper la relación SnapMirror del clúster FSx, lo que hace que el volumen sea de lectura y escritura.
2. Cree un servidor CIFS (si es necesario) y cree un recurso compartido CIFS que apunte a la ruta de unión del volumen clonado.
3. Utilice xcopy para copiar los archivos de respaldo a un directorio 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:

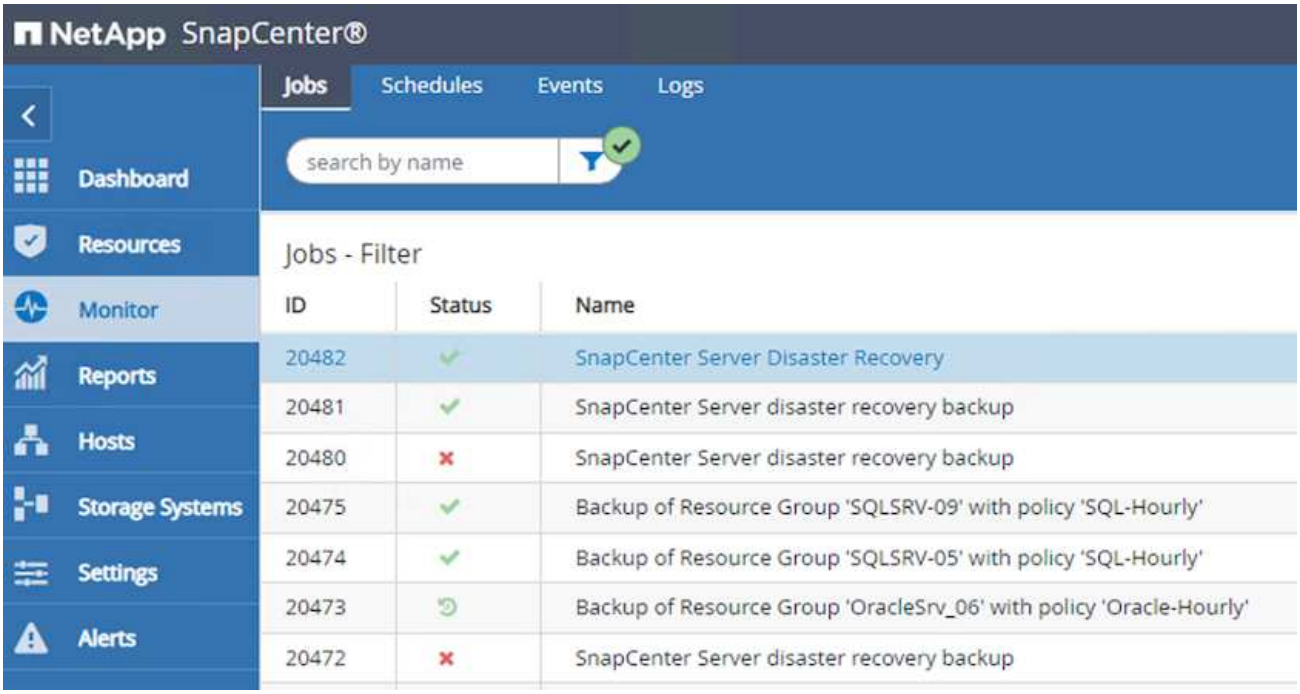
1. Navegue a la página web de la API de Swagger para el servidor secundario SnapCenter y siga las instrucciones anteriores para obtener un token de autorización.
2. Vaya a la sección Recuperación ante desastres de la página Swagger, seleccione `/4.6/disasterrecovery/server/restore` y haga clic en Probarlo.

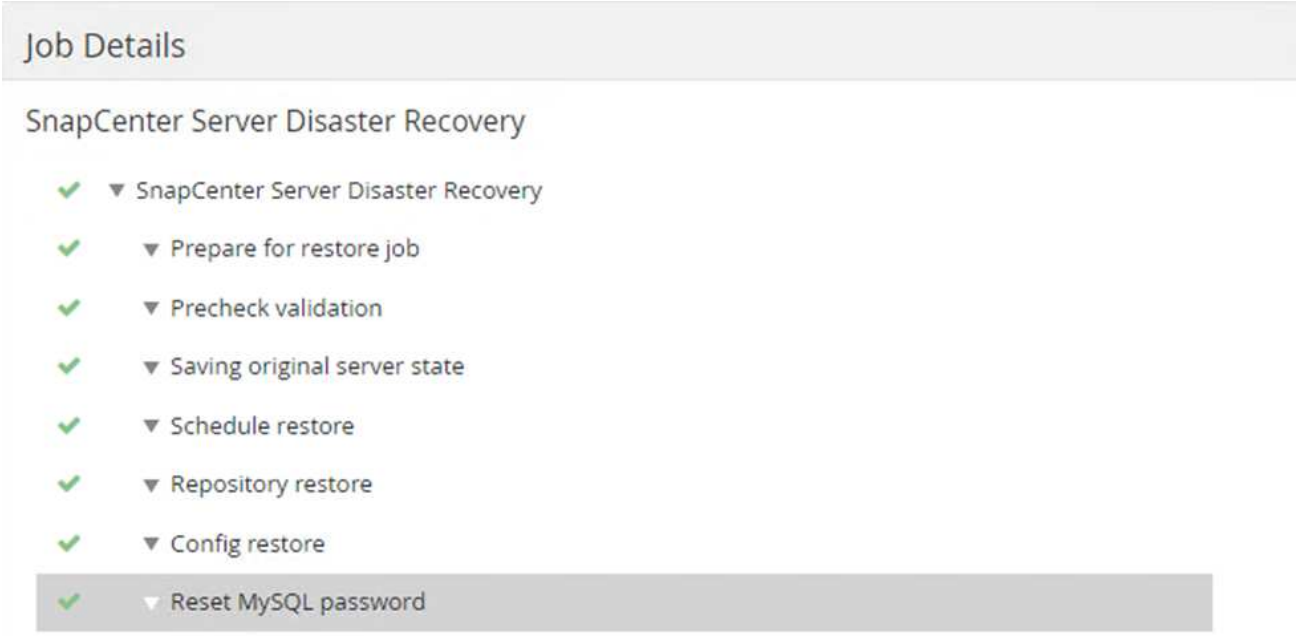


3. Pegue su token de autorización y, en la sección SmDRResterRequest, pegue el nombre de la copia de seguridad y el directorio local en el servidor secundario de SnapCenter .



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.





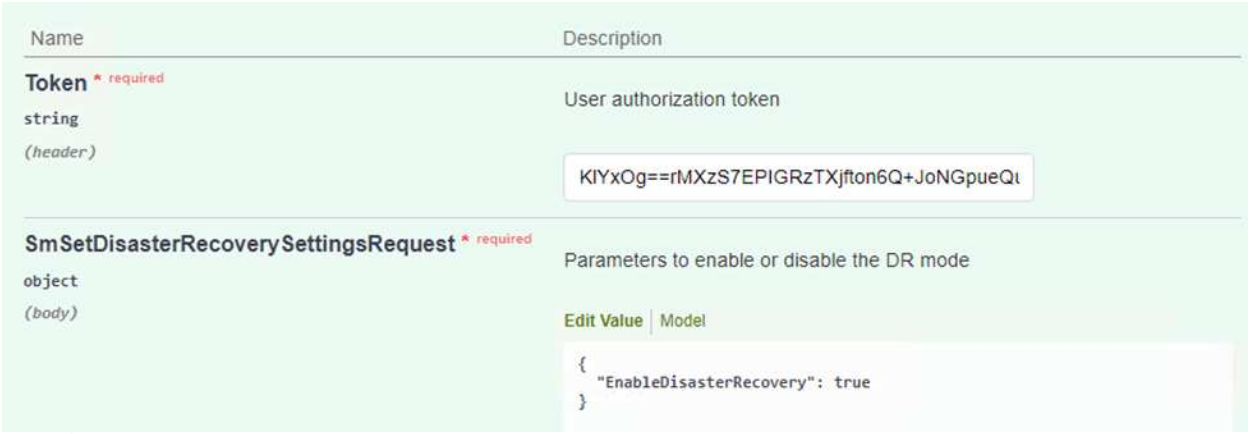
6. Para habilitar las restauraciones de SQL Server desde el almacenamiento secundario, debe alternar la base de datos de SnapCenter al modo de recuperación ante desastres. Esto se realiza como una operación separada y se inicia en la página web de la API de Swagger.

   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.

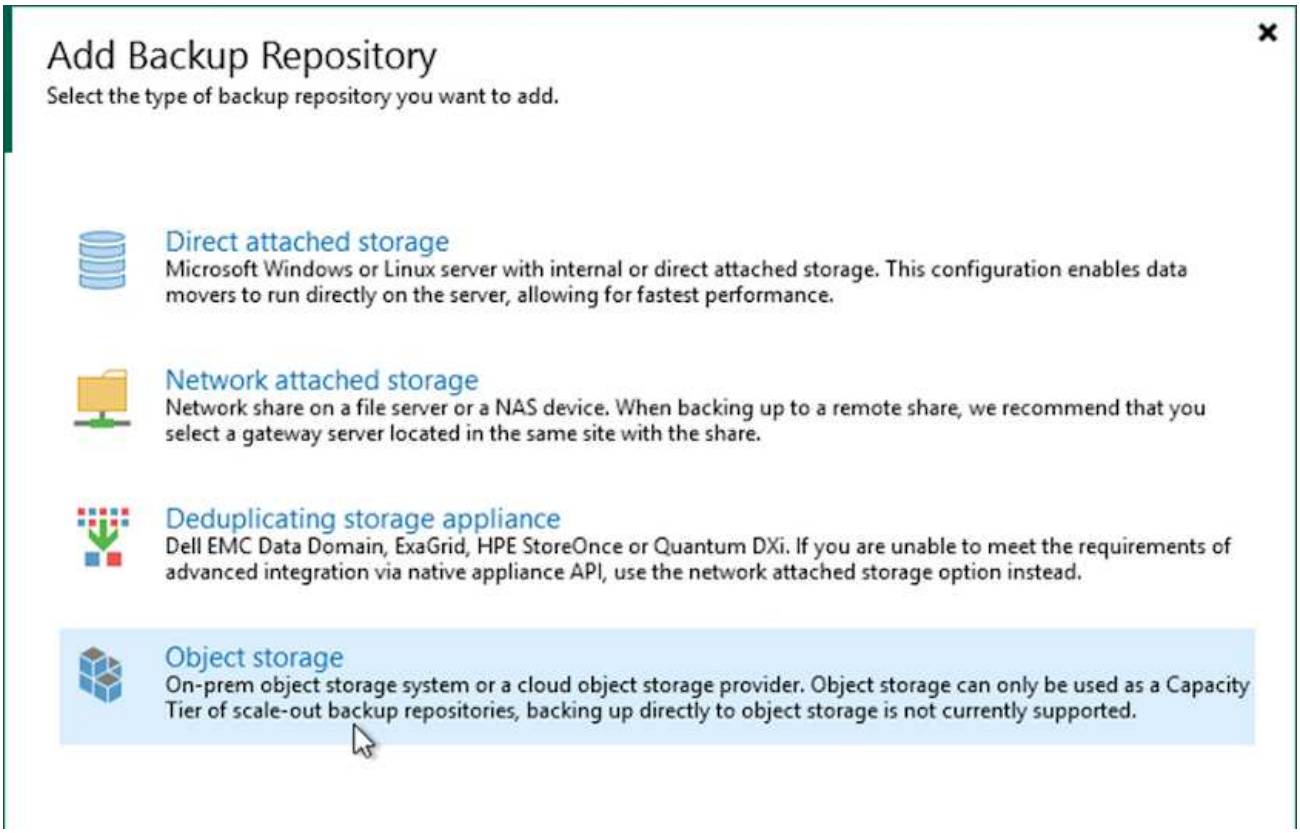
Restaurar máquinas virtuales de aplicaciones con la restauración completa de Veeam

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

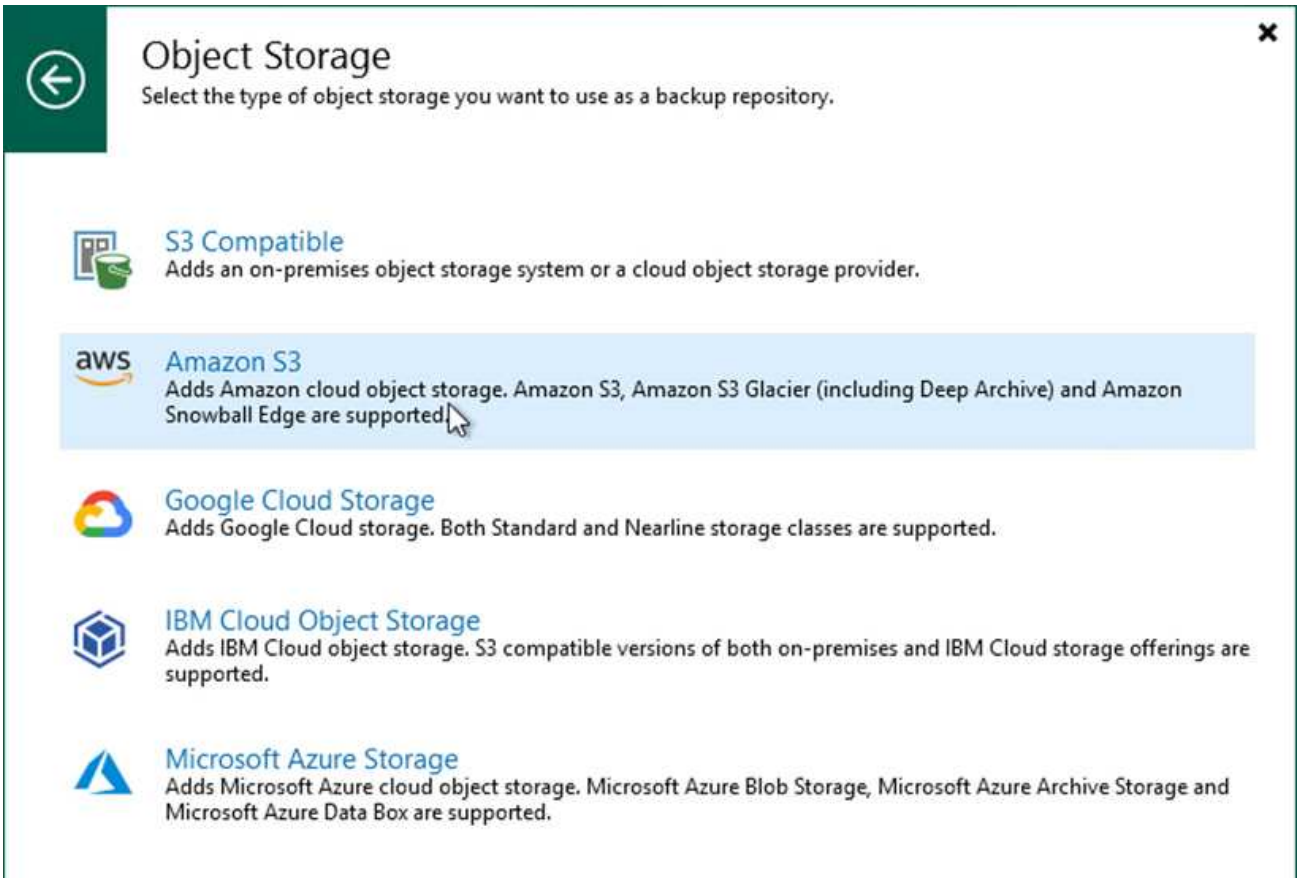
Desde el servidor secundario de Veeam, importe las copias de seguridad del almacenamiento S3 y restaure las máquinas virtuales de SQL Server y Oracle en su clúster de VMware Cloud.

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:

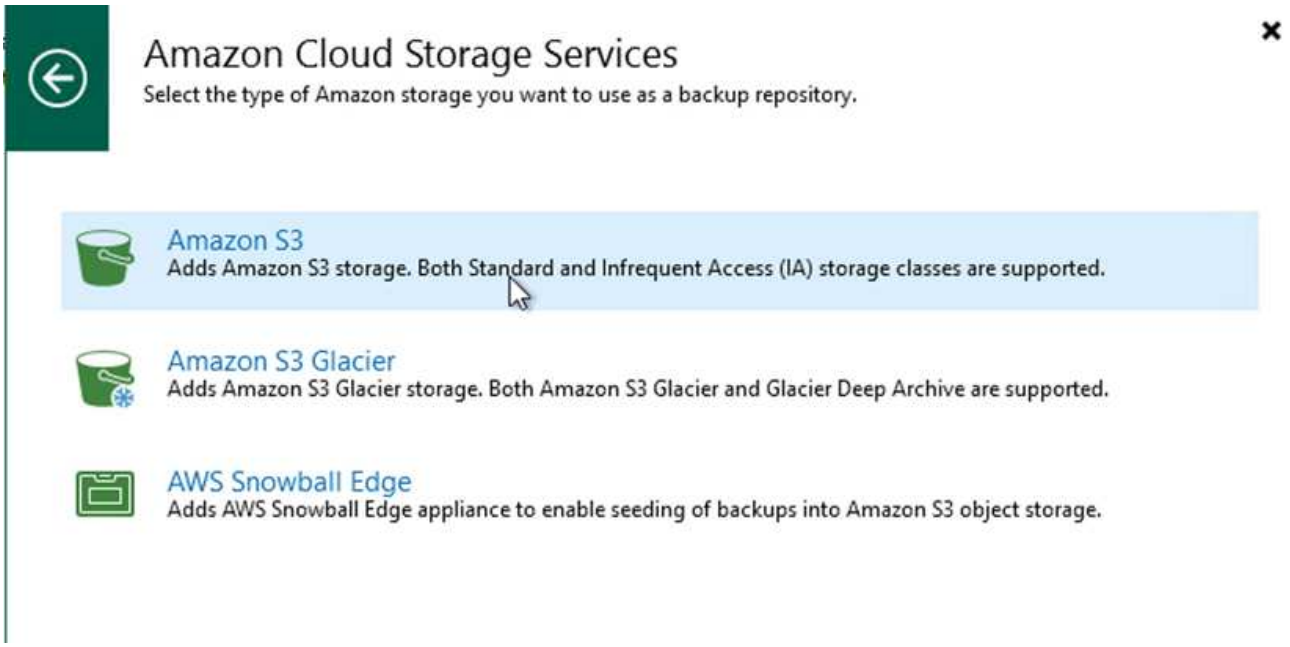
1. Vaya a Repositorios de respaldo y haga clic en Agregar repositorio en el menú superior para iniciar el asistente Agregar repositorio de respaldo. En la primera página del asistente, seleccione Almacenamiento de objetos como tipo de repositorio de respaldo.



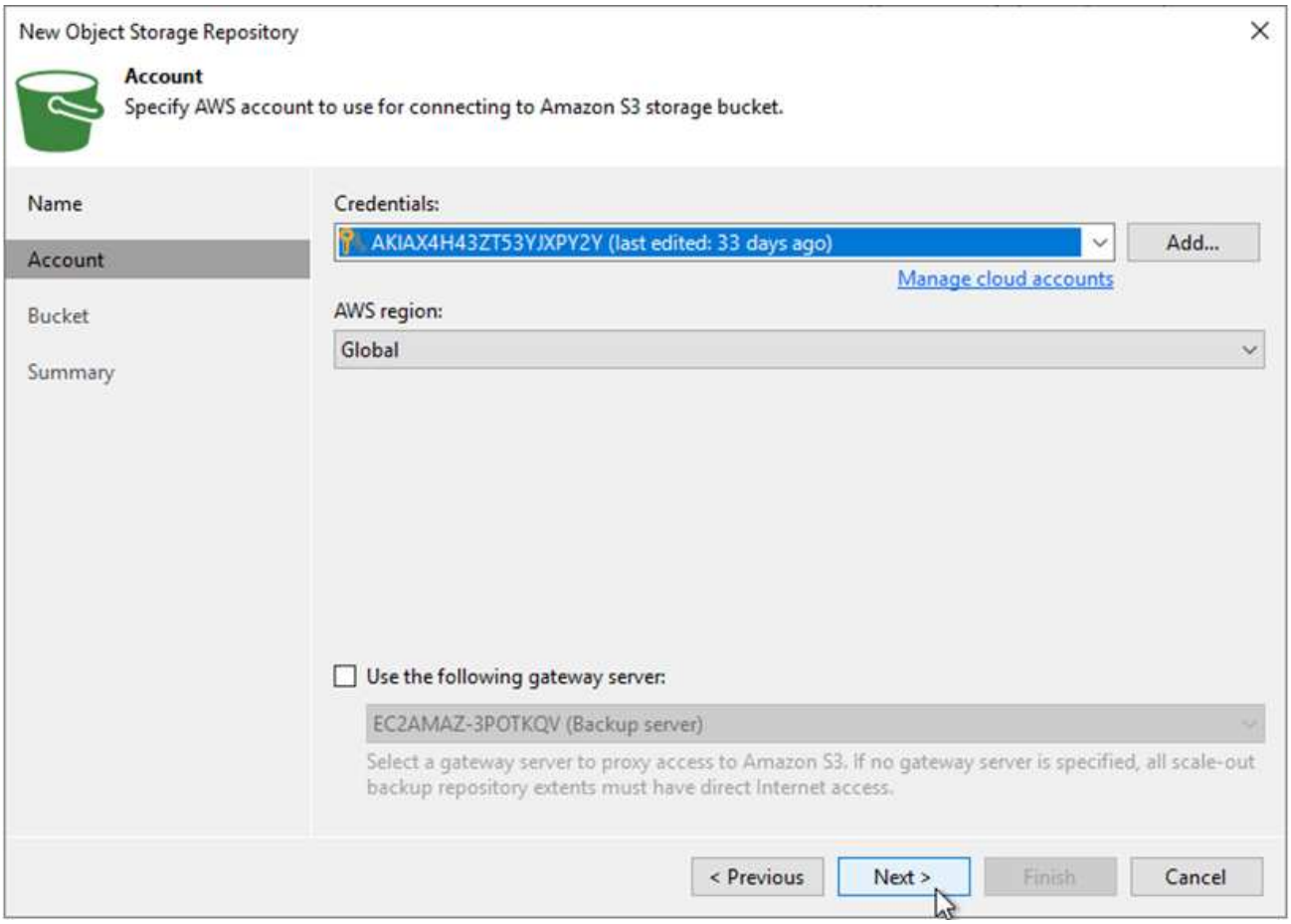
2. Seleccione Amazon S3 como tipo de almacenamiento de objetos.



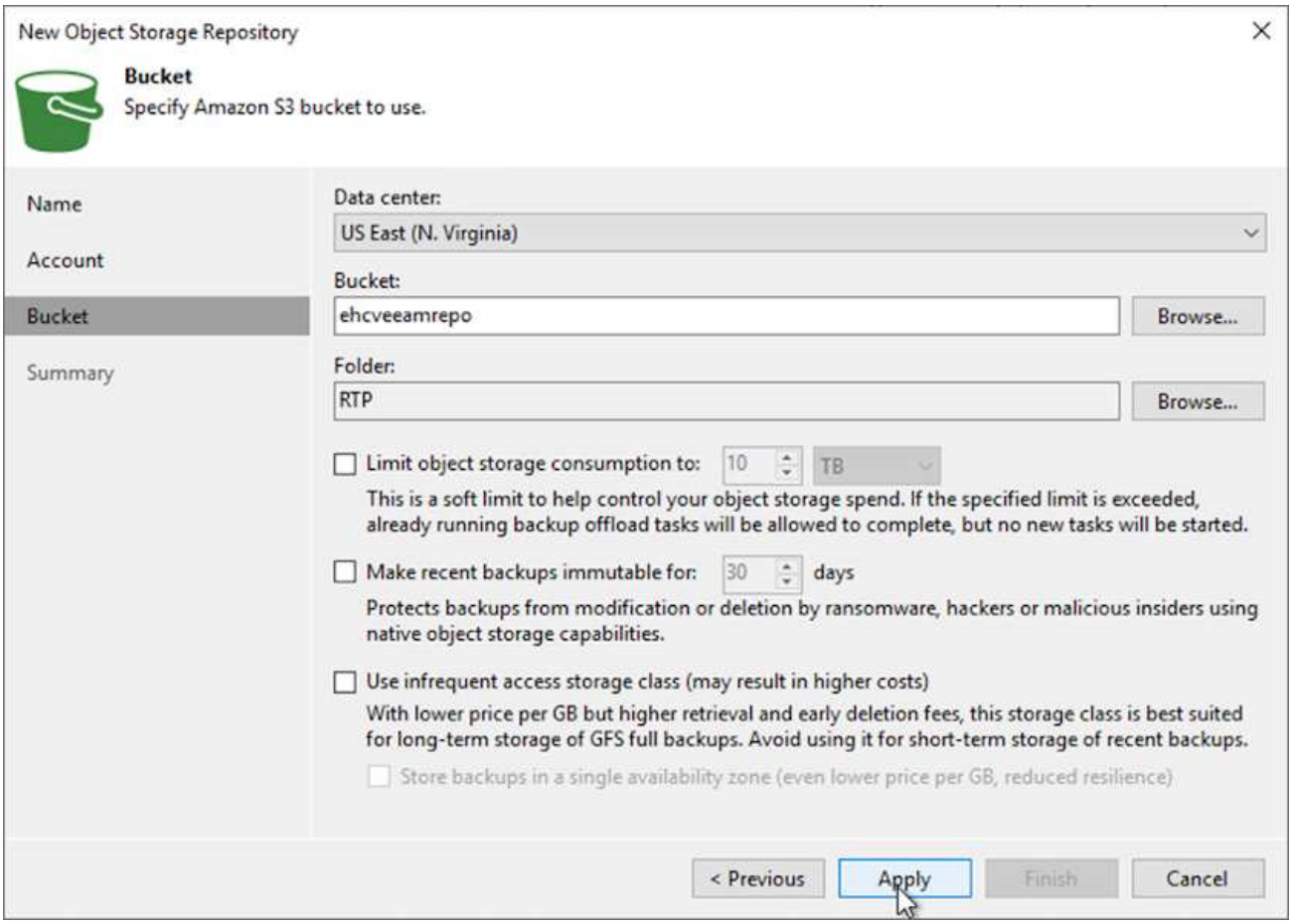
3. De la lista de servicios de almacenamiento en la nube de Amazon, seleccione Amazon S3.



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.

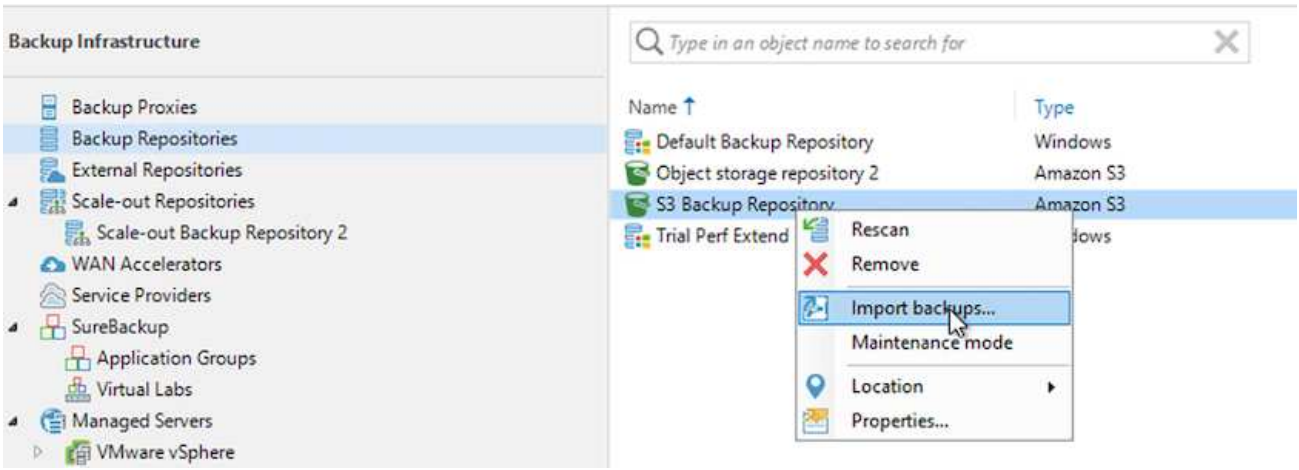


6. Por último, seleccione Finalizar para completar el proceso y agregar el repositorio.

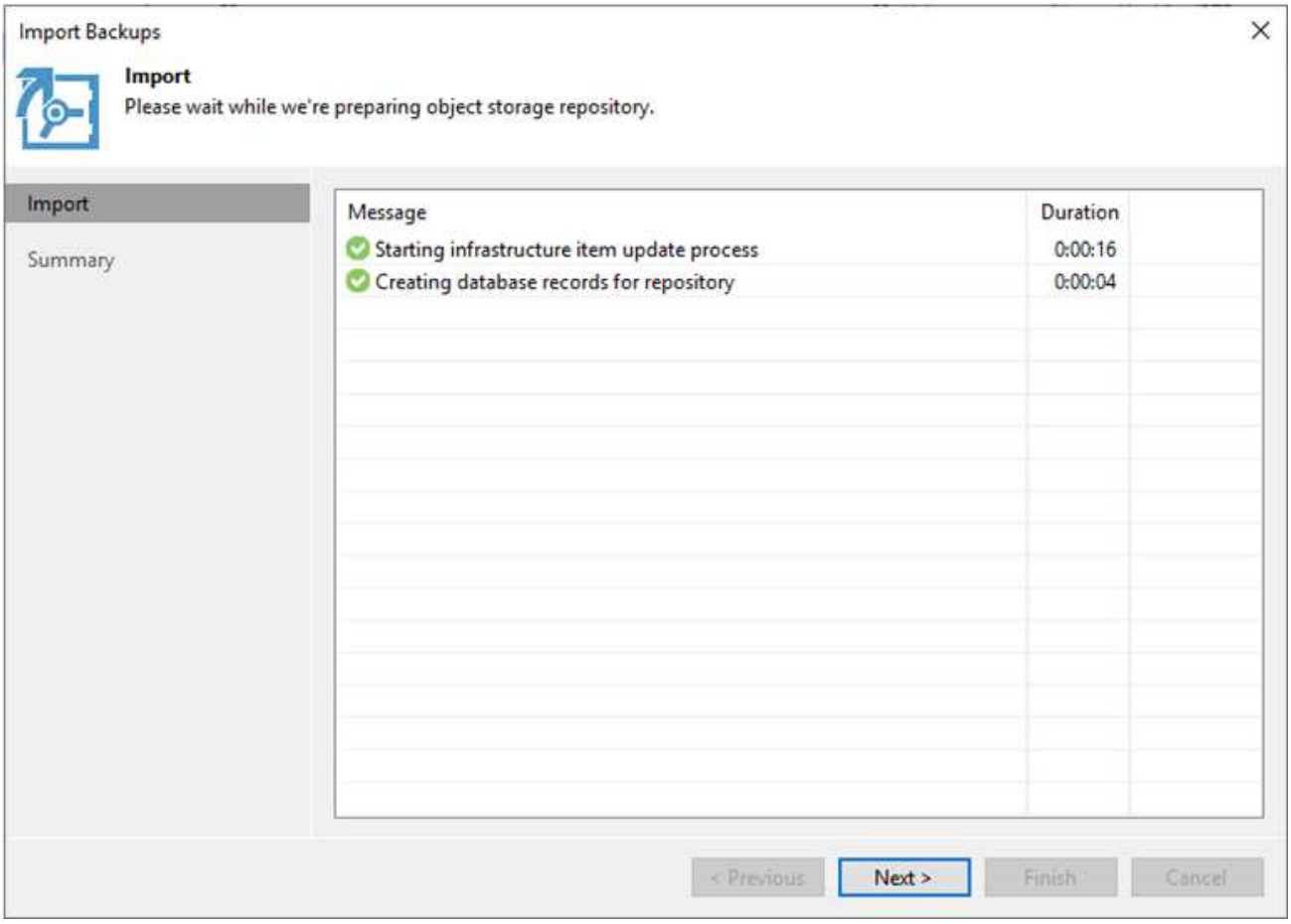
▼ **Importar copias de seguridad desde el almacenamiento de objetos S3**

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

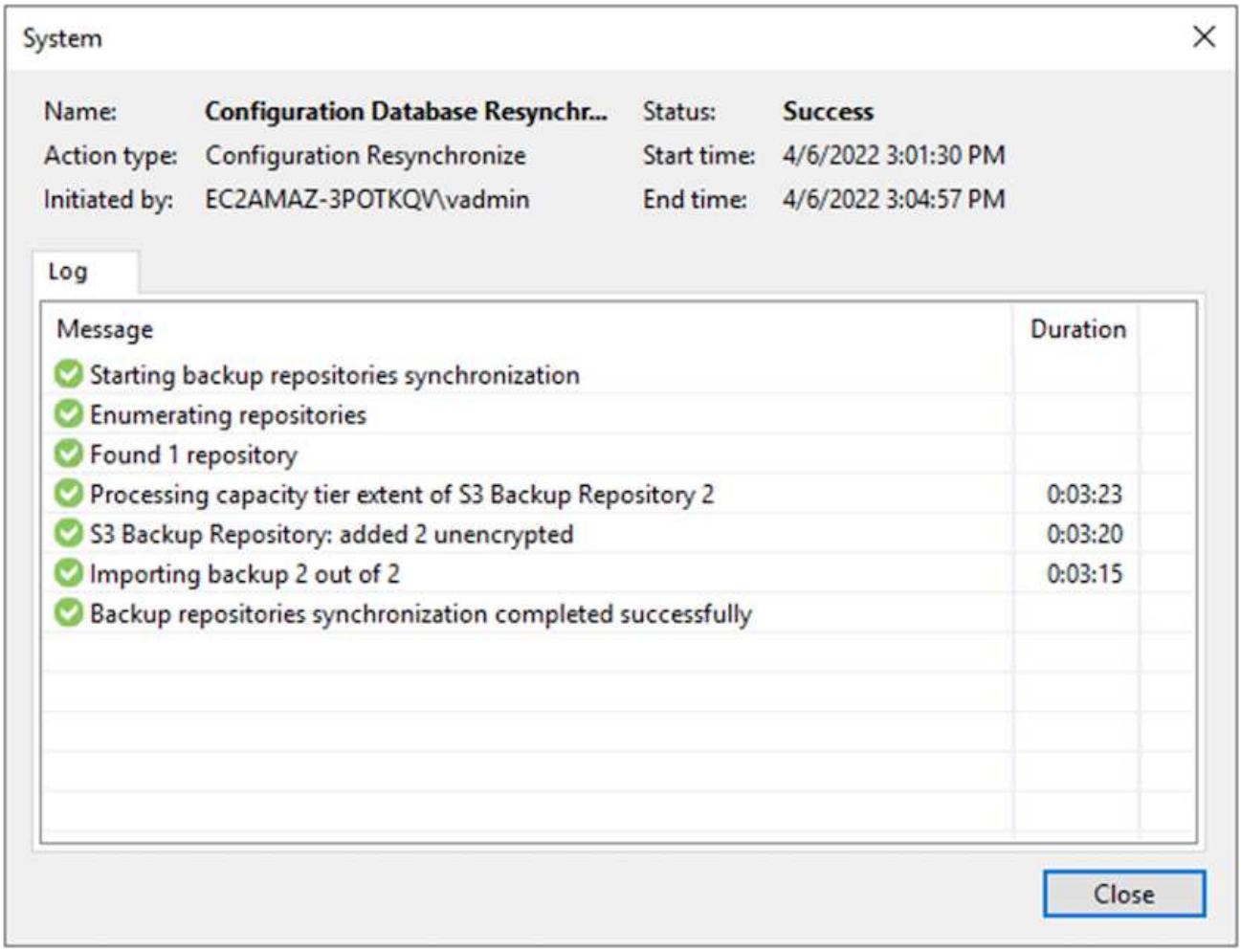
1. Desde el repositorio de copias de seguridad de S3, seleccione Importar copias de seguridad para iniciar el asistente de importación de copias de seguridad.



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.



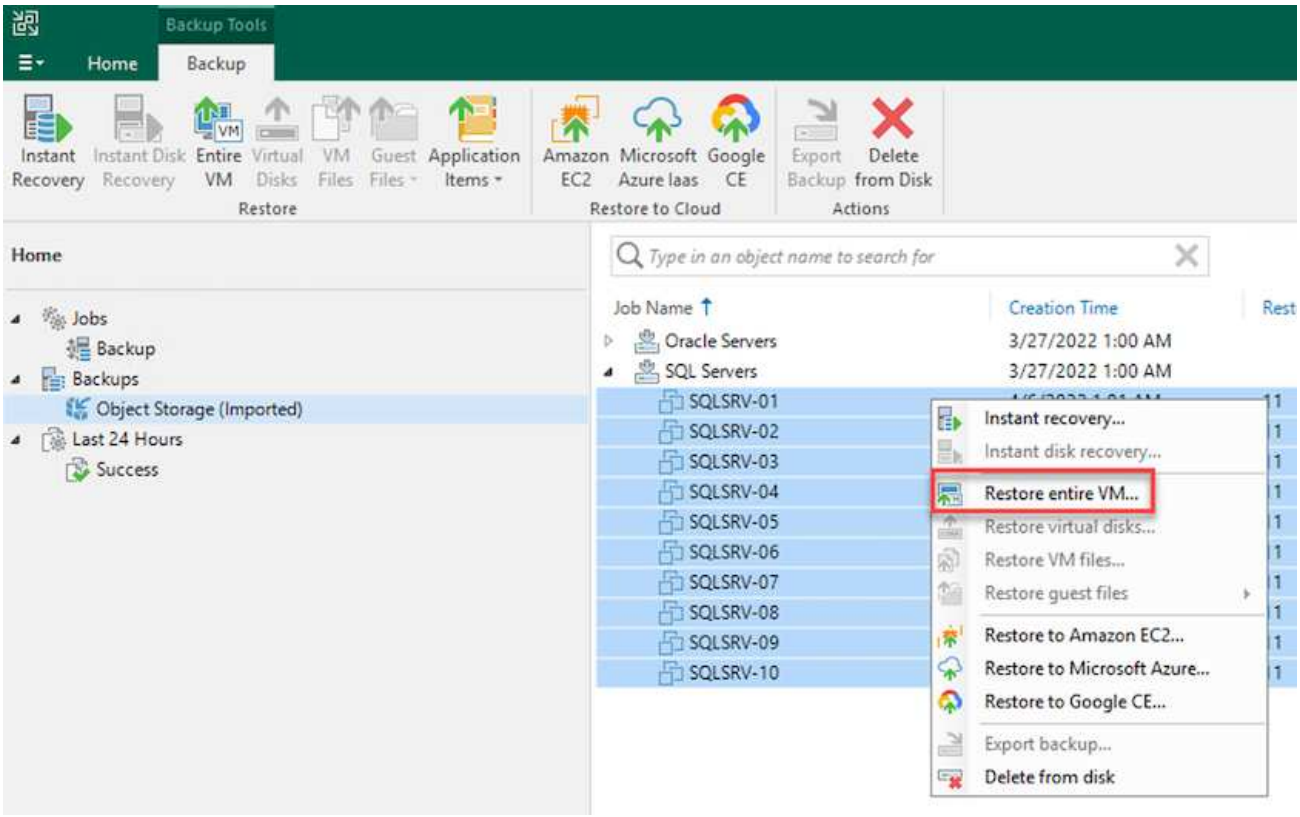
3. Una vez completada la importación, puede restaurar las máquinas virtuales en el clúster de VMware Cloud.



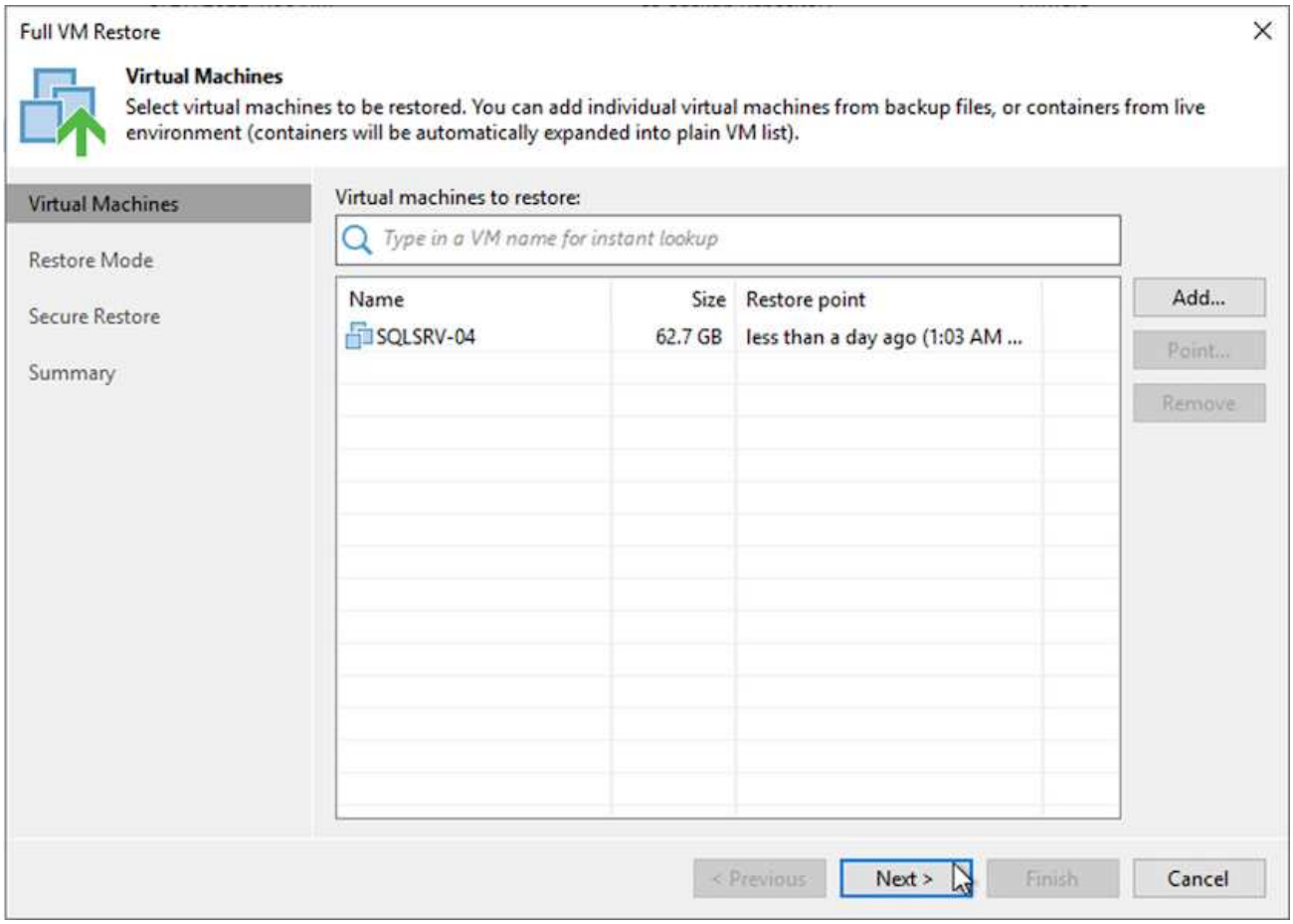
▼ **Restaurar máquinas virtuales de aplicaciones con la restauración completa de Veeam en VMware Cloud**

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.

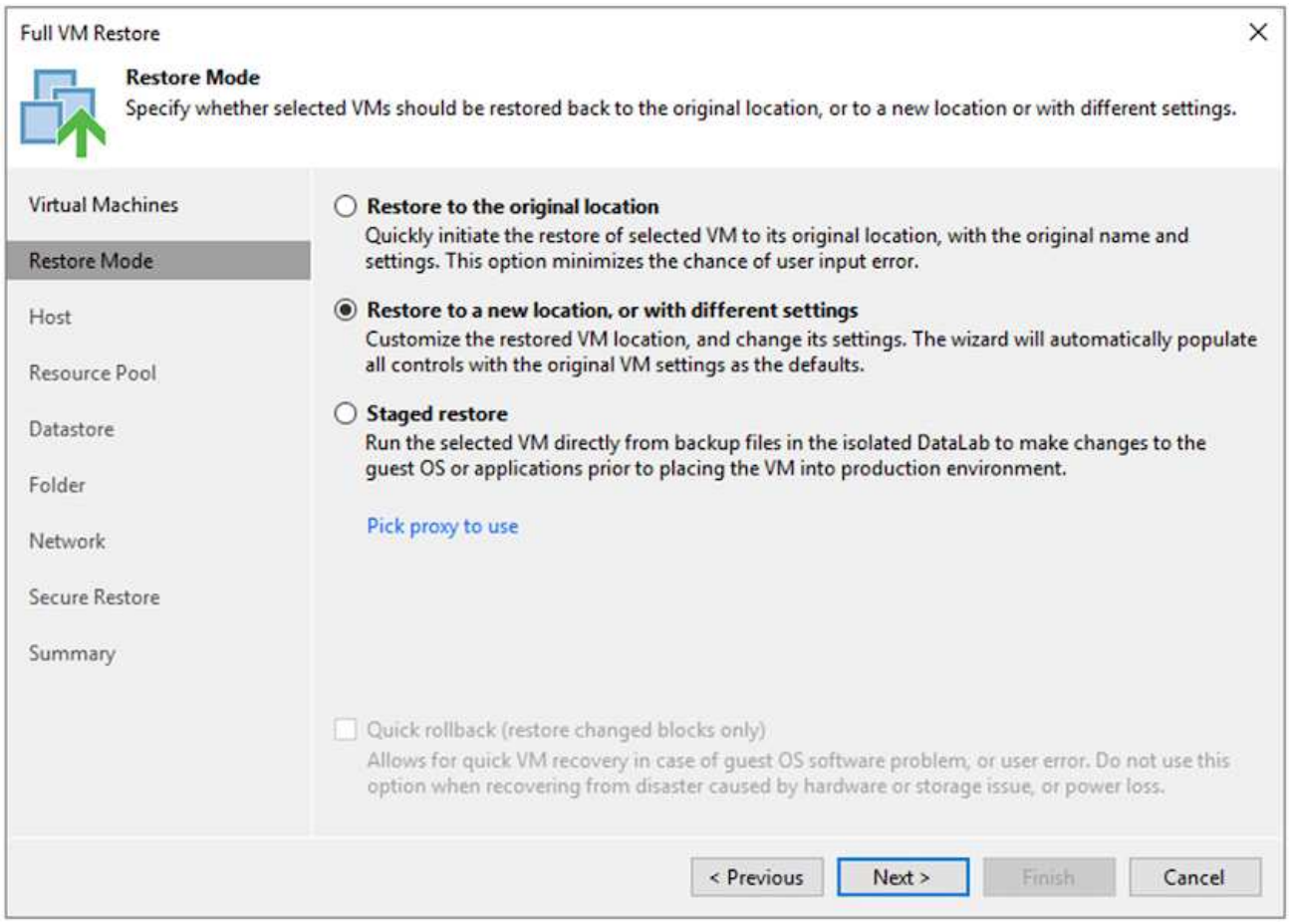
1. Desde la página de inicio de Veeam, seleccione el almacenamiento de objetos que contiene las copias de seguridad importadas, seleccione las máquinas virtuales que desea restaurar y, a continuación, haga clic con el botón derecho y seleccione Restaurar máquina virtual completa.



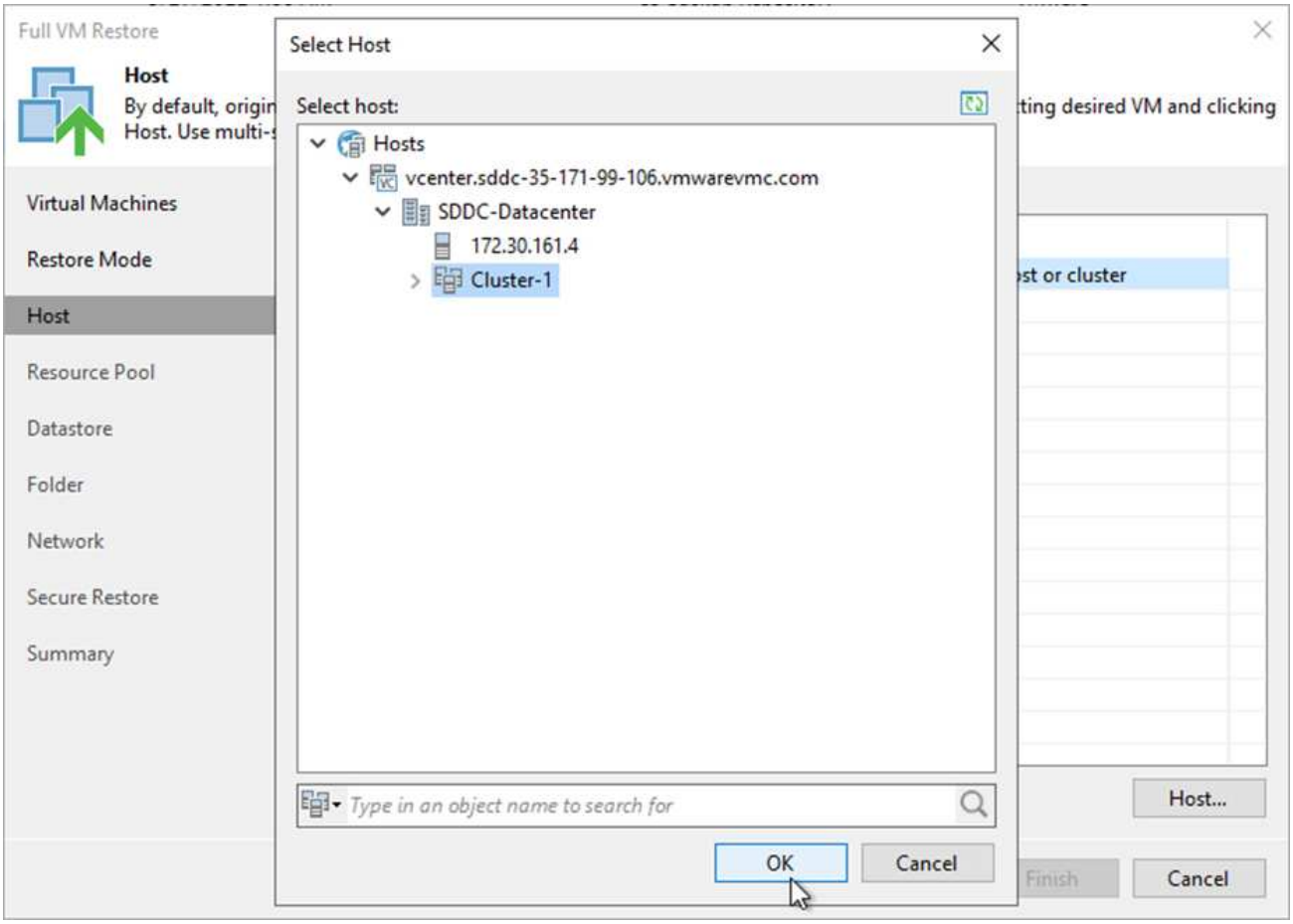
2. En la primera página del asistente de restauración completa de máquinas virtuales, modifique las máquinas virtuales de las que desea realizar una copia de seguridad y seleccione Siguiente.



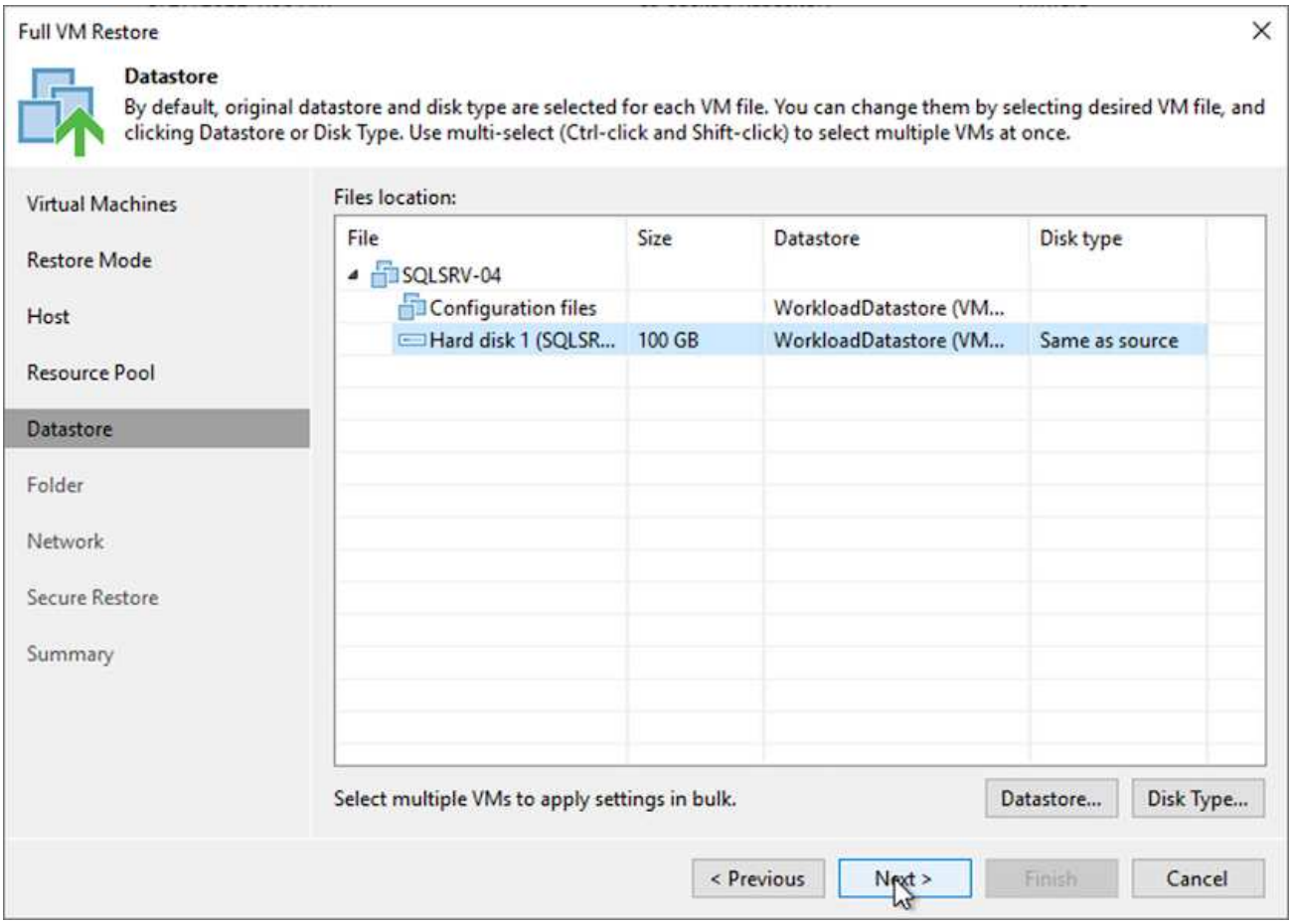
3. En la página Modo de restauración, seleccione Restaurar en una nueva ubicación o con configuraciones diferentes.



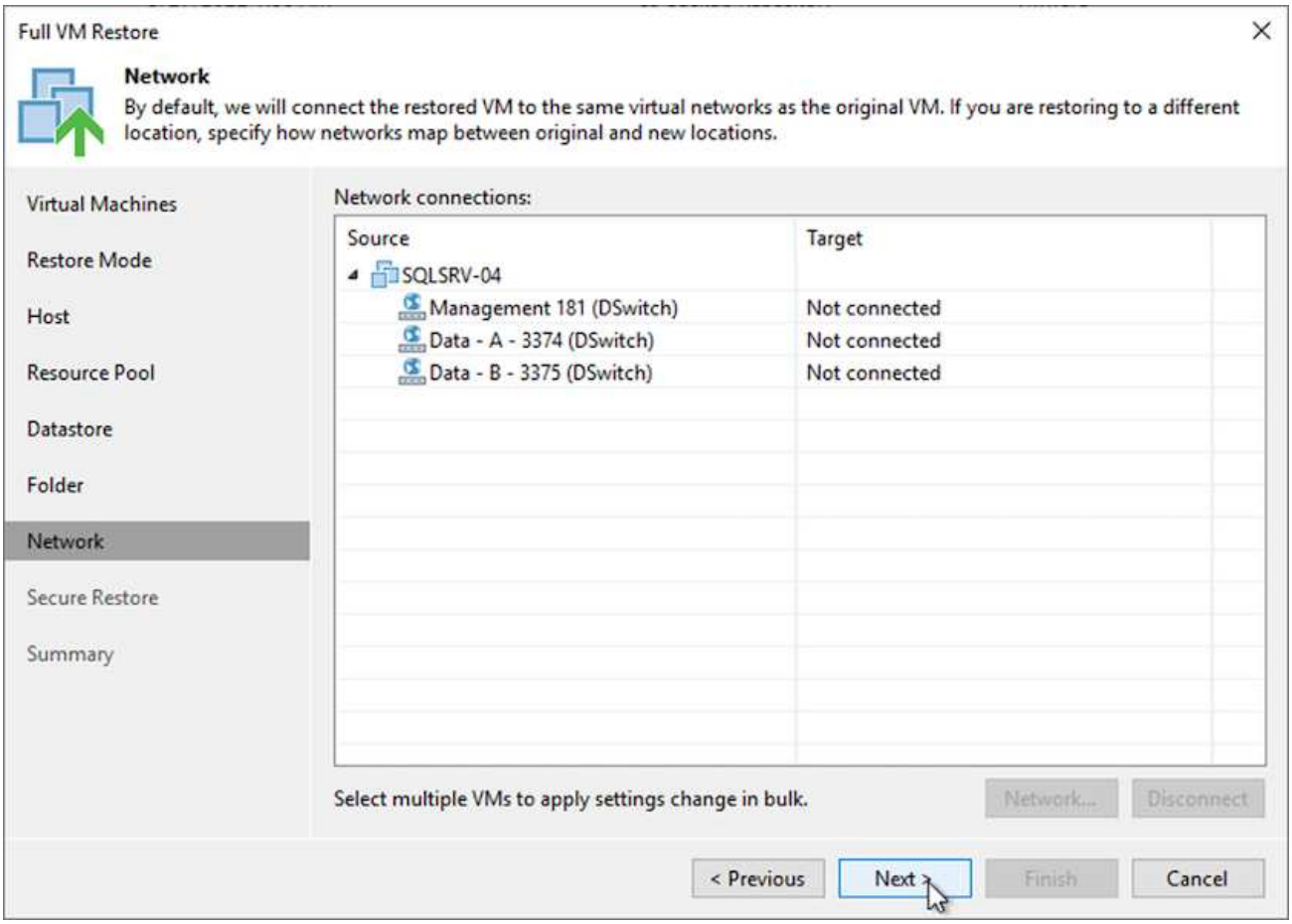
4. En la página del host, seleccione el host o clúster ESXi de destino donde restaurar la máquina virtual.

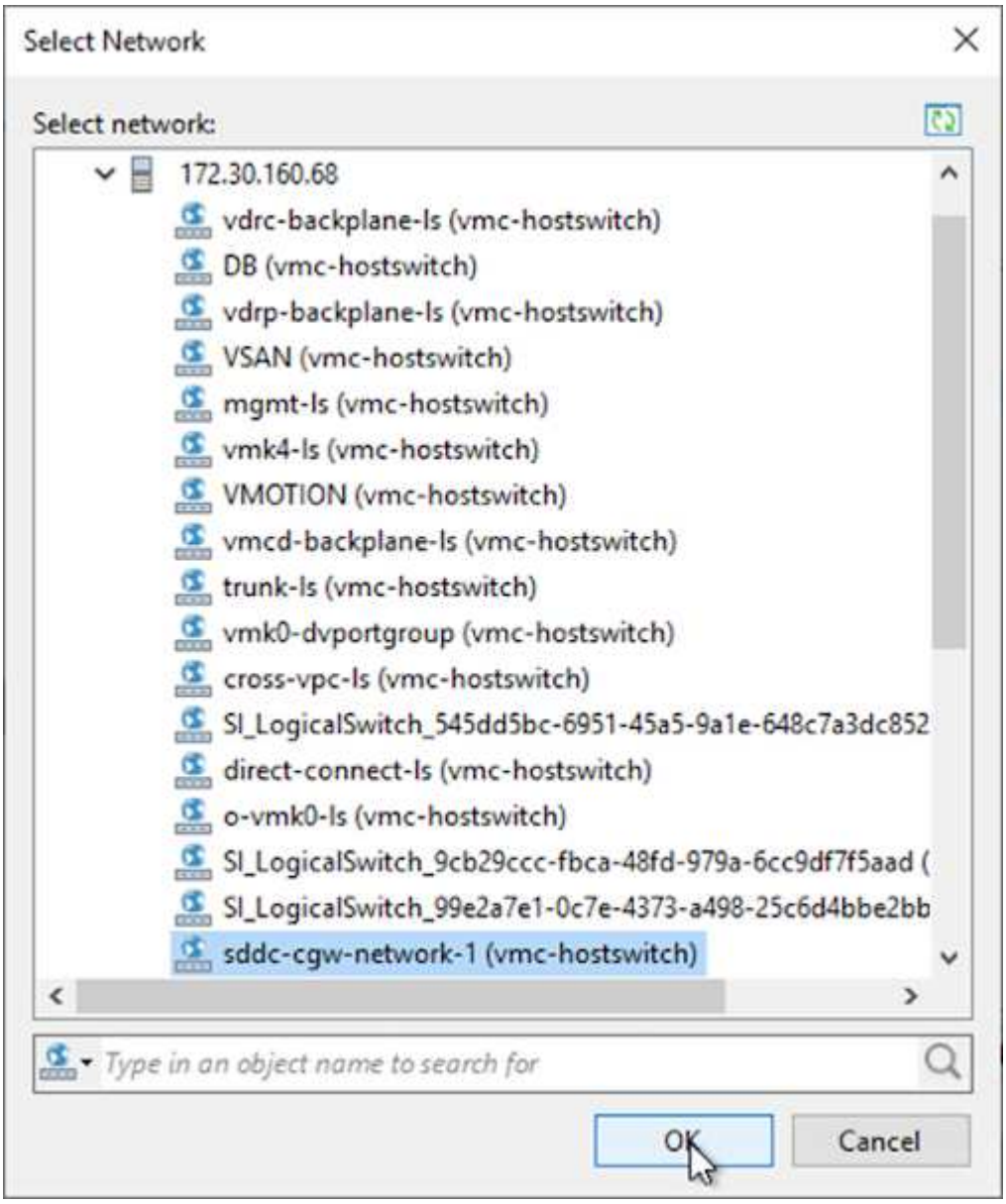


5. En la página Almacenes de datos, seleccione la ubicación del almacén de datos de destino para los archivos de configuración y el disco duro.



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:

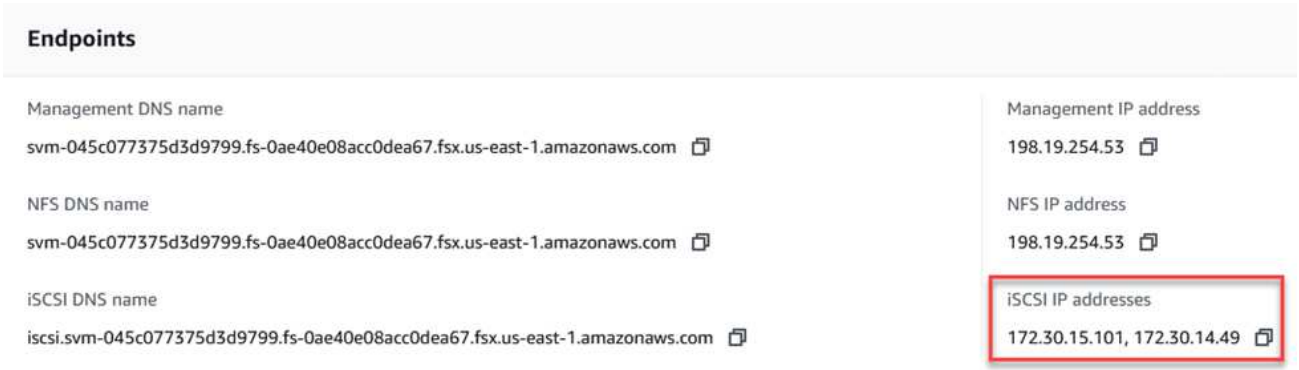
```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

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

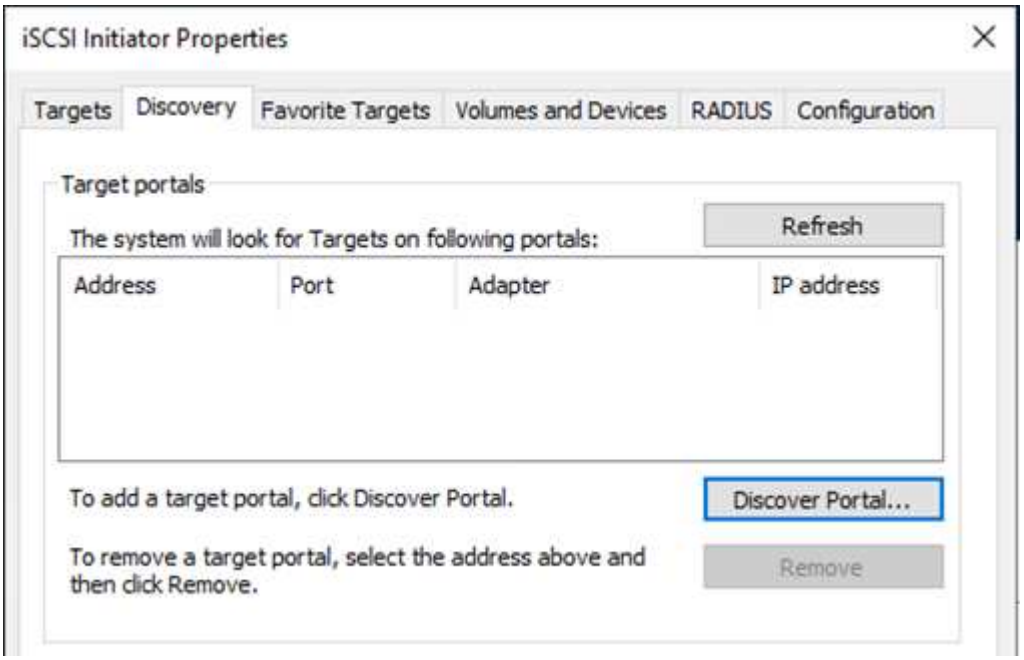
▼ Configurar la máquina virtual de Windows para el acceso iSCSI y descubrir los sistemas de archivos

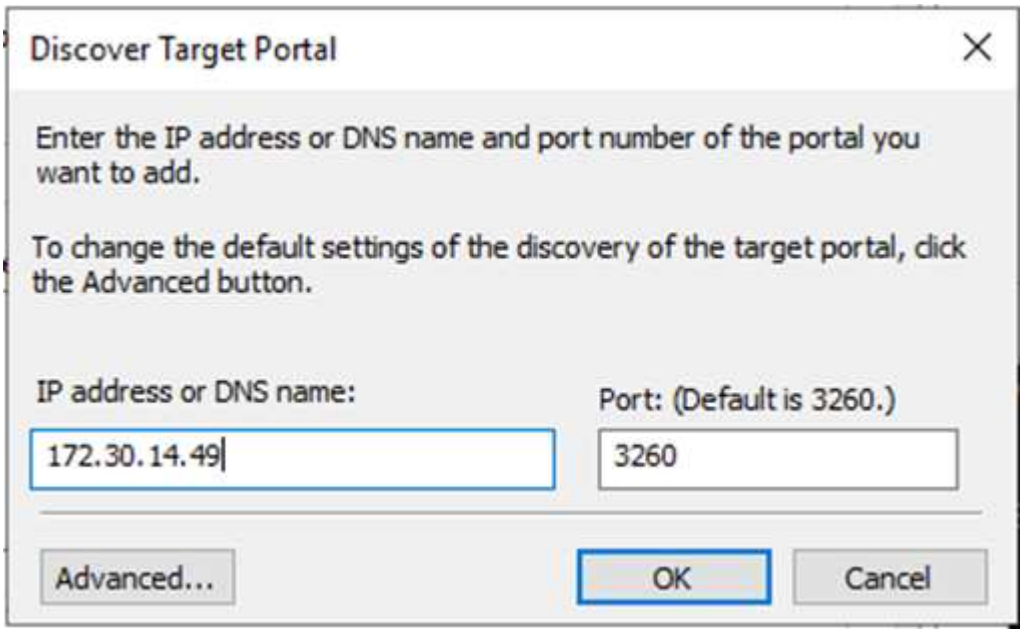
1. Desde la máquina virtual de SQL Server, configure su adaptador de red iSCSI para comunicarse en el grupo de puertos VMware que se ha establecido con conectividad a las interfaces de destino iSCSI en su instancia FSx.
2. Abra la utilidad Propiedades del iniciador iSCSI y borre las configuraciones de 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.

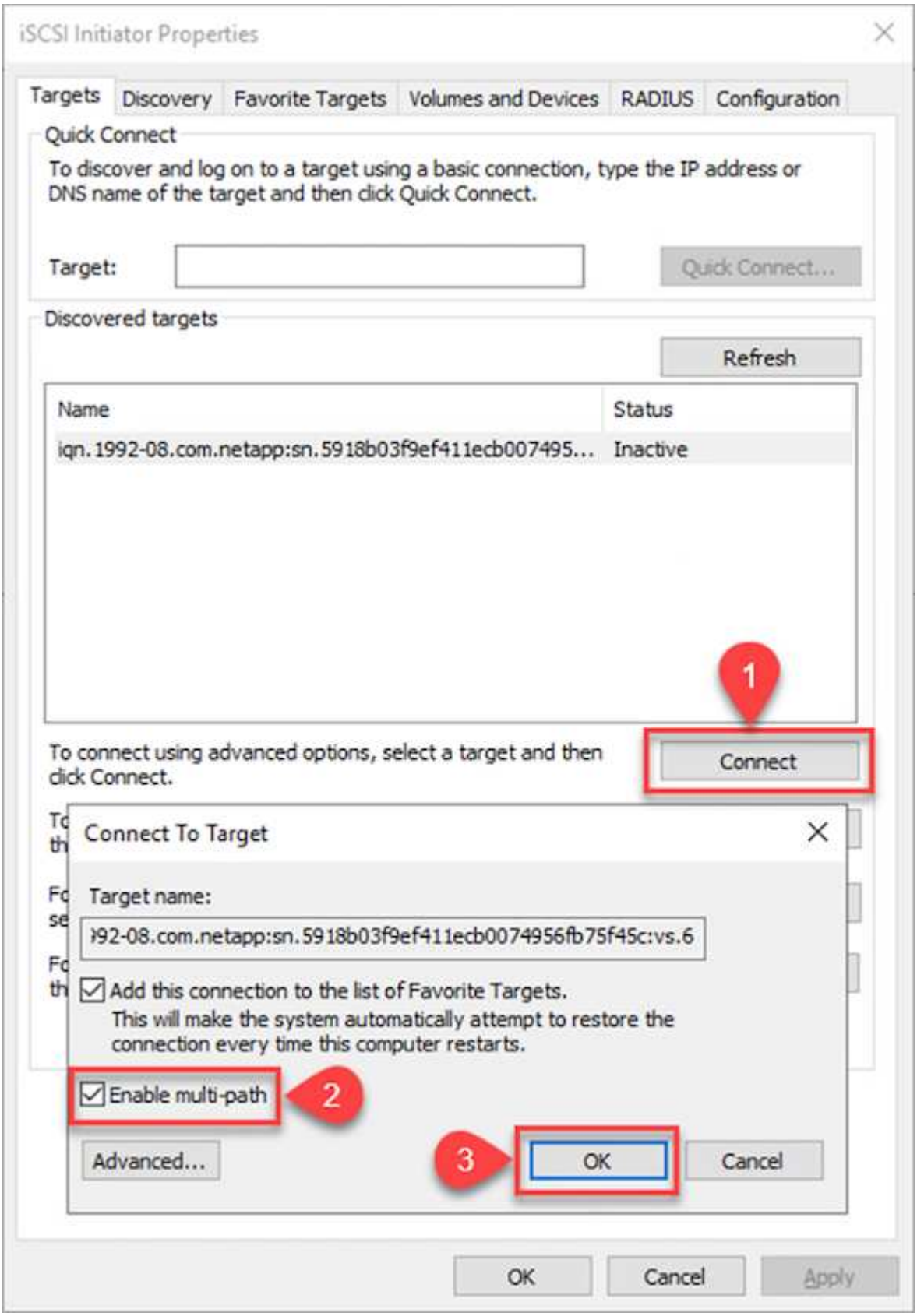


4. Desde la pestaña Descubrimiento, haga clic en Portal de descubrimiento e ingrese las direcciones IP para sus objetivos iSCSI de FSx.

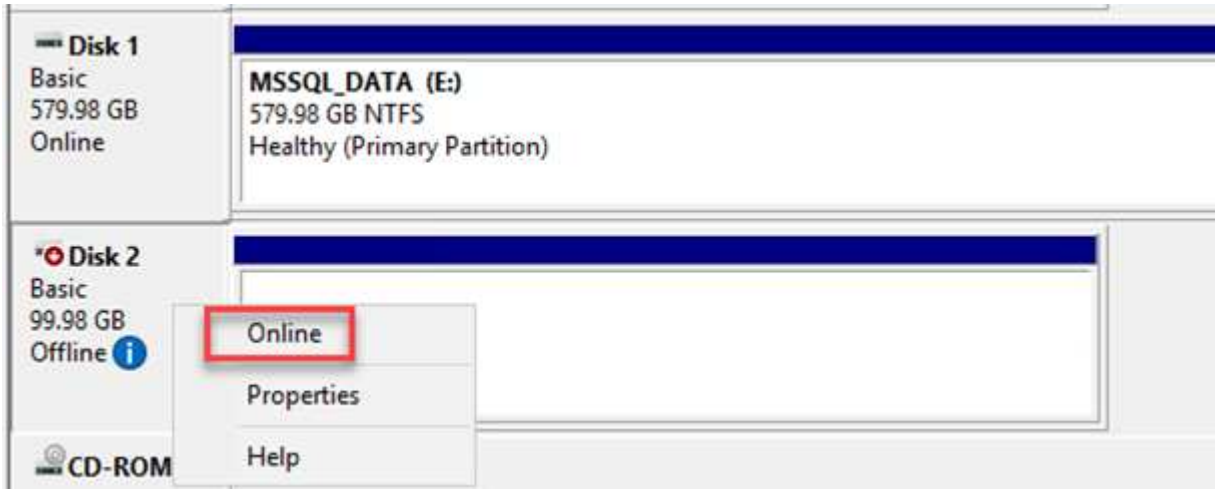




5. En la pestaña Destino, haga clic en Conectar, seleccione Habilitar múltiples rutas si corresponde a su configuración y luego haga clic en Aceptar para conectarse al destino.

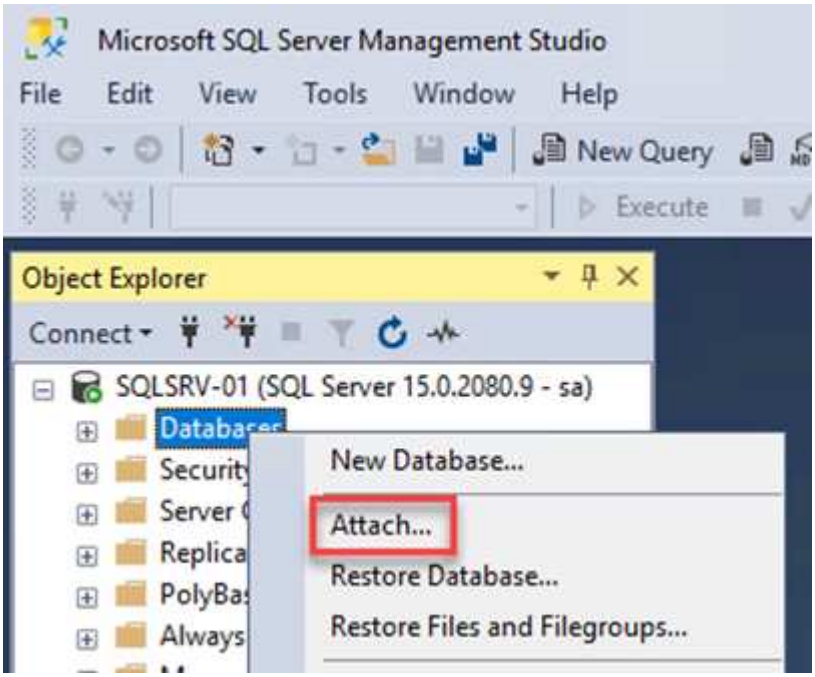


6. Abra la utilidad de Administración de equipos y ponga los discos en línea. Verifique que conserven las mismas letras de unidad que tenían anteriormente.

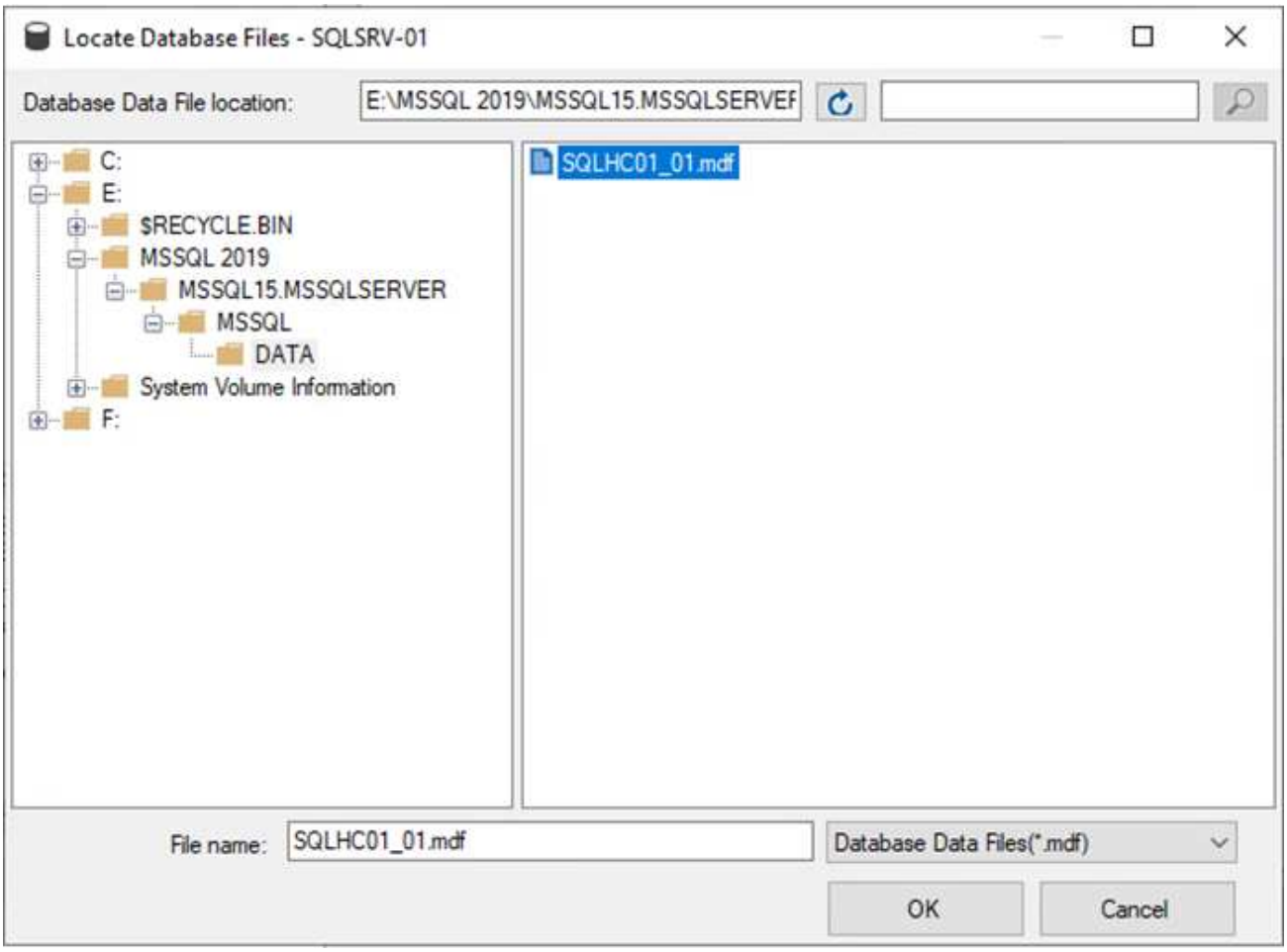


▼ **Adjuntar las bases de datos de SQL Server**

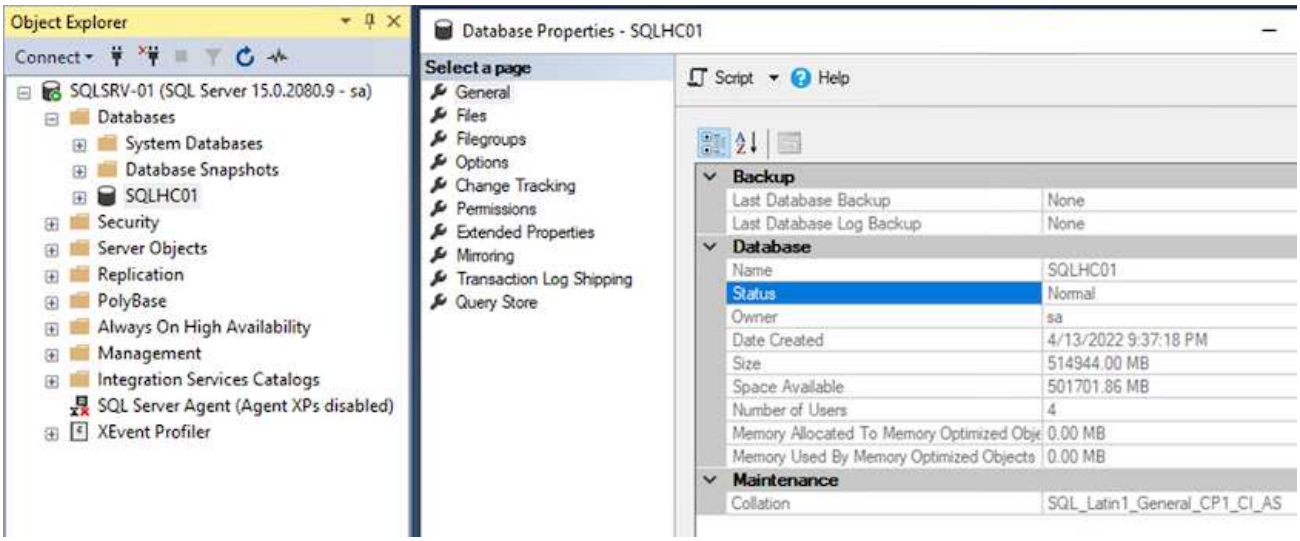
1. Desde la máquina virtual de SQL Server, abra Microsoft SQL Server Management Studio y seleccione Conectar para iniciar el proceso de conexión a la base de datos.



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.

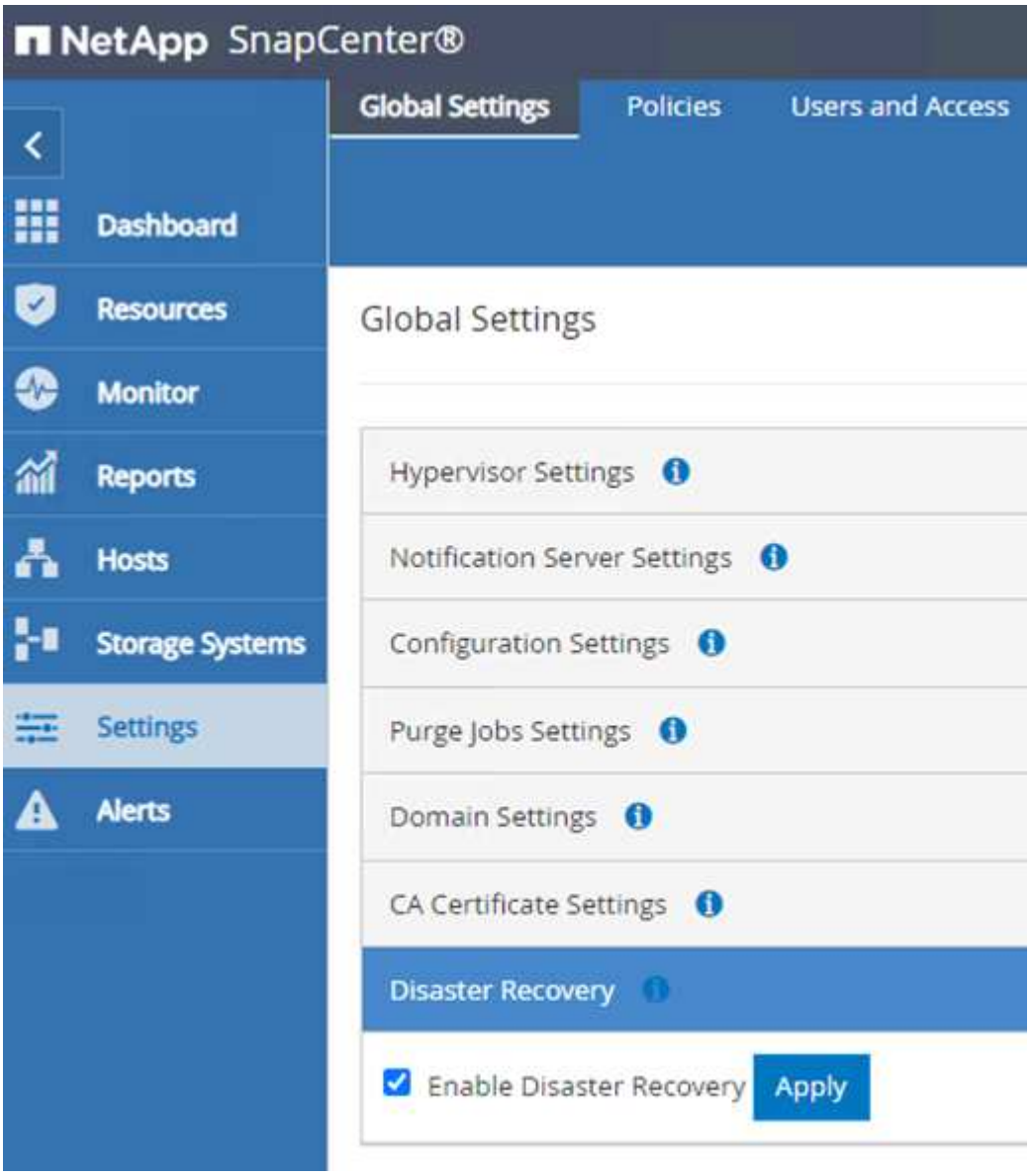


▼ **Confirmar la comunicación de SnapCenter con el complemento de SQL Server**

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::>
```

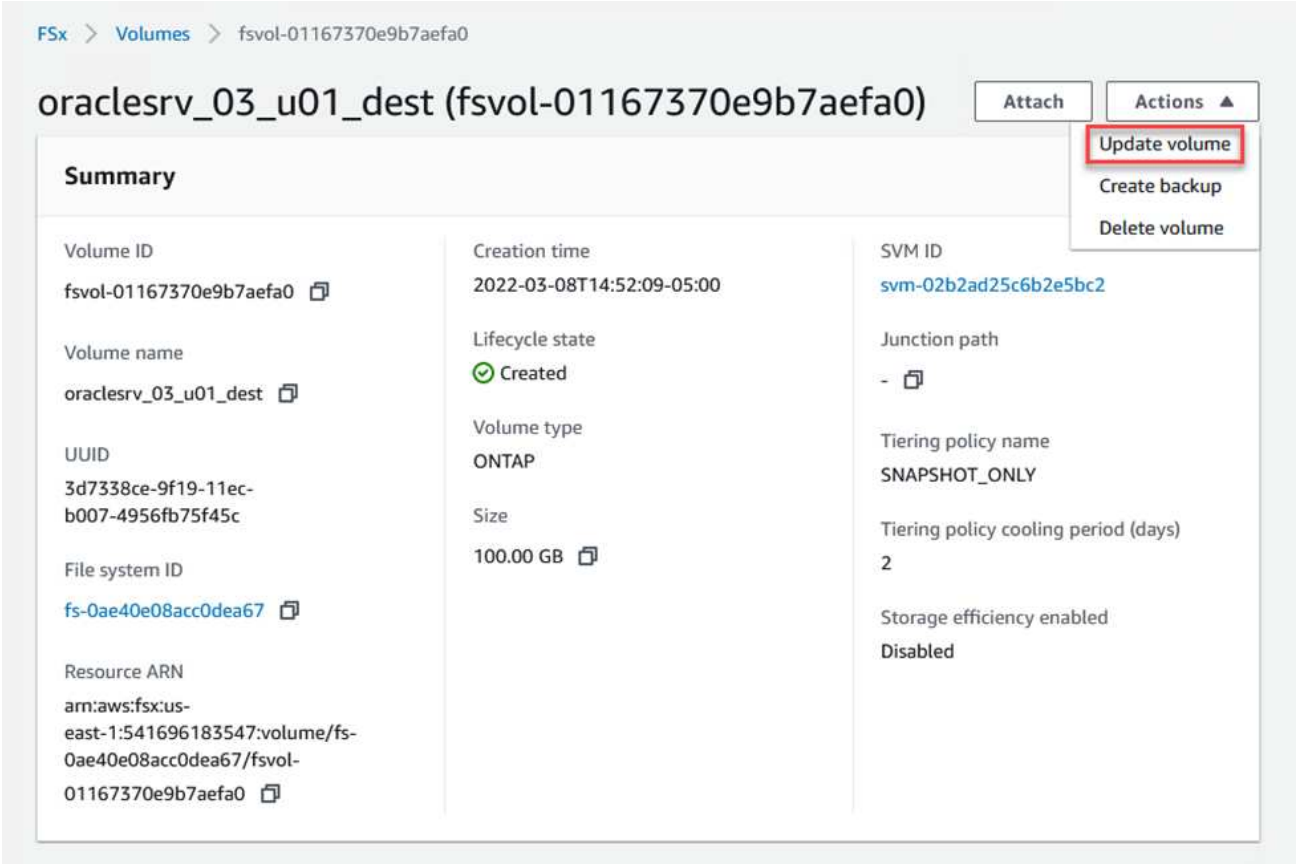
2. Ejecute el siguiente comando para romper las relaciones SnapMirror existentes.

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

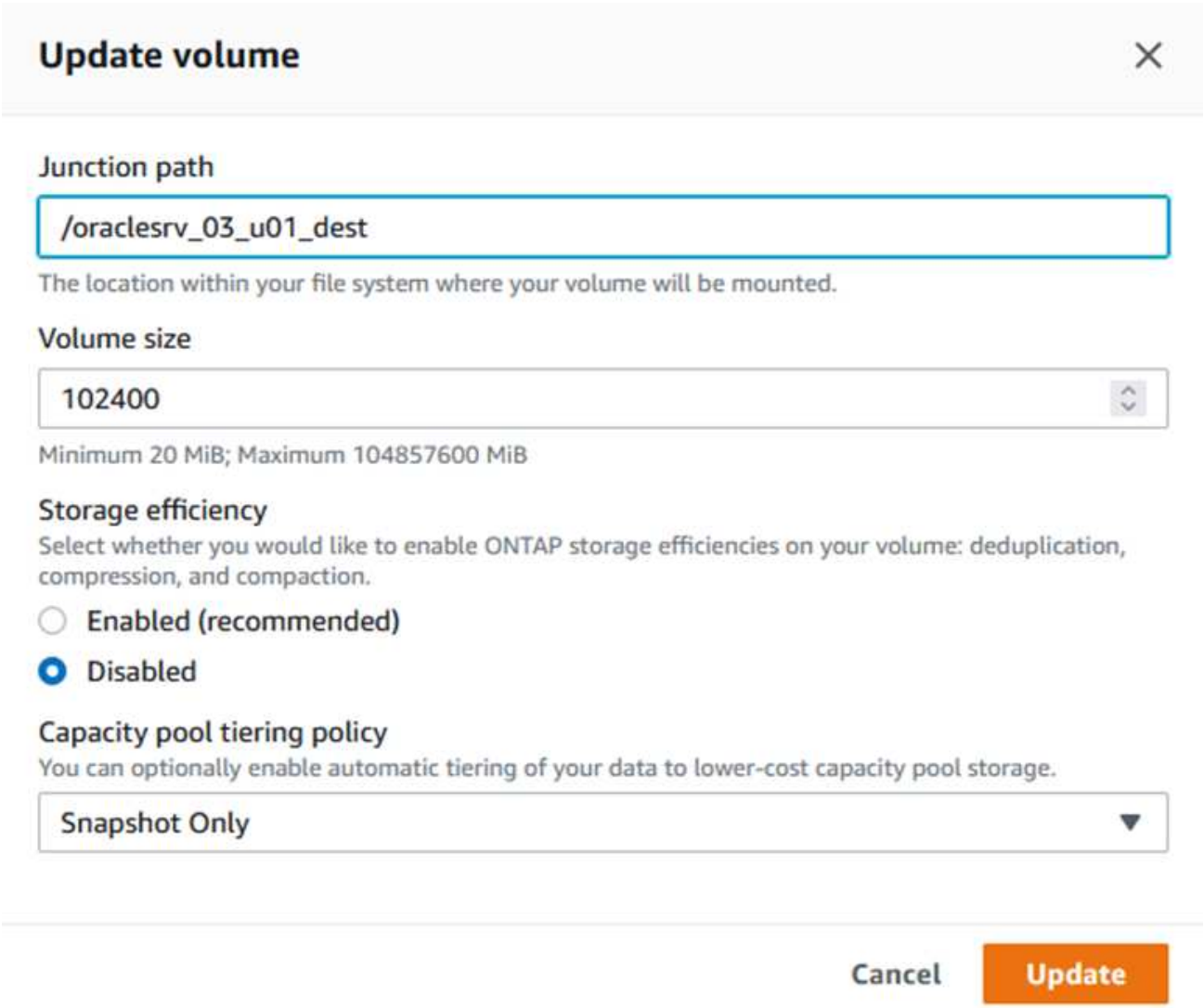
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

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 :



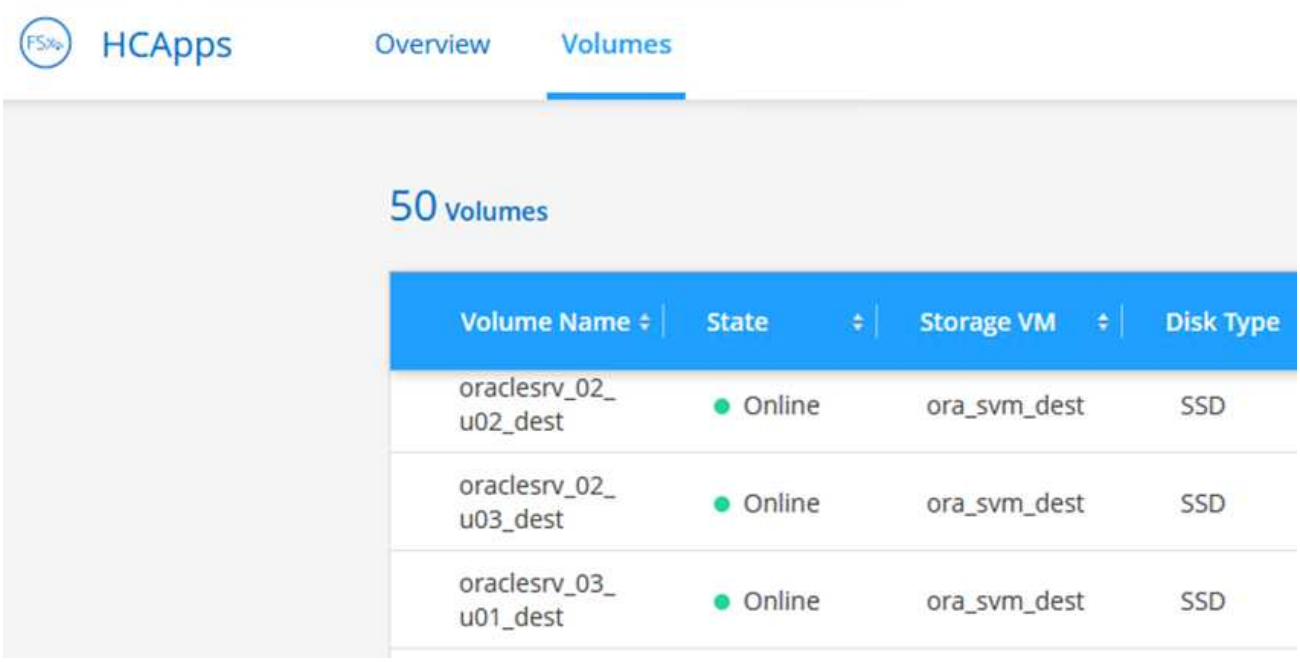
4. Agregue el nombre de la ruta de unión y haga clic en Actualizar. Especifique esta ruta de unión al montar el volumen NFS desde el servidor Oracle.



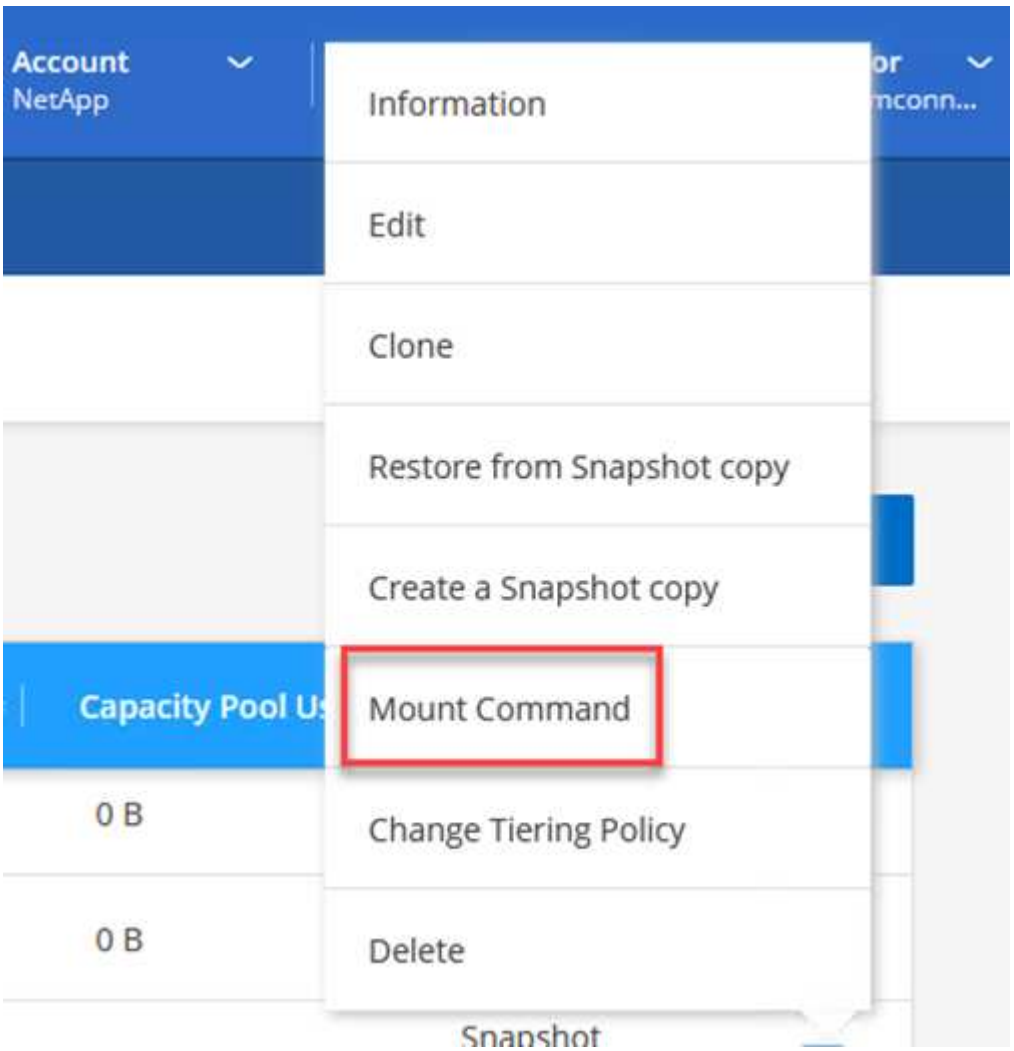
▼ **Montar volúmenes NFS en Oracle Server**

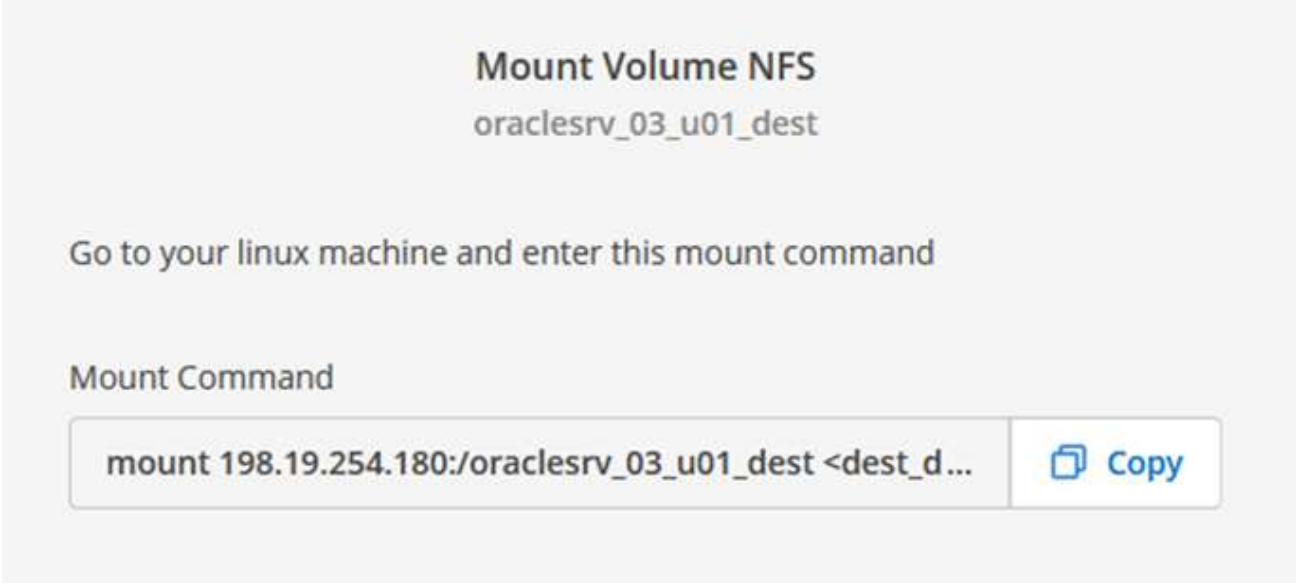
En Cloud Manager, puede obtener el comando de montaje con la dirección IP LIF de NFS correcta para montar los volúmenes NFS que contienen los archivos y registros de la base de datos de Oracle.

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.

Veeam Backup & Restore en VMware Cloud, con Amazon FSx ONTAP

Veeam Backup & Replication es una solución eficaz y confiable para proteger datos en VMware Cloud. Esta solución demuestra la configuración adecuada para usar Veeam Backup and Replication para realizar copias de seguridad y restaurar máquinas virtuales de aplicaciones que residen en almacenes de datos NFS de FSx ONTAP en VMware Cloud.

Descripción general

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

Casos de uso

Esta solución aborda los siguientes casos de uso:

- Copia de seguridad y restauración de máquinas virtuales Windows y Linux alojadas en VMC utilizando FSx ONTAP como repositorio de copia de seguridad.
- Copia de seguridad y restauración de datos de aplicaciones de Microsoft SQL Server utilizando FSx ONTAP como repositorio de copia de seguridad.
- Copia de seguridad y restauración de datos de aplicaciones Oracle utilizando FSx ONTAP como repositorio de copia de seguridad.

Almacenes de datos NFS que utilizan Amazon FSx ONTAP

Todas las máquinas virtuales de esta solución residen en almacenes de datos NFS complementarios de FSx ONTAP . El uso de FSx ONTAP como un almacén de datos NFS complementario tiene varios beneficios. Por ejemplo, le permite:

- Cree un sistema de archivos escalable y de alta disponibilidad en la nube sin necesidad de configuración y gestión complejas.
- Se integra con su entorno VMware existente, lo que le permite utilizar herramientas y procesos familiares para administrar sus recursos en la nube.
- Benefíciese de las funciones avanzadas de gestión de datos que ofrece ONTAP, como instantáneas y replicación, para proteger sus datos y garantizar su disponibilidad.

▼ Descripción general de la implementación de la solución

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

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

▼ Prerrequisitos

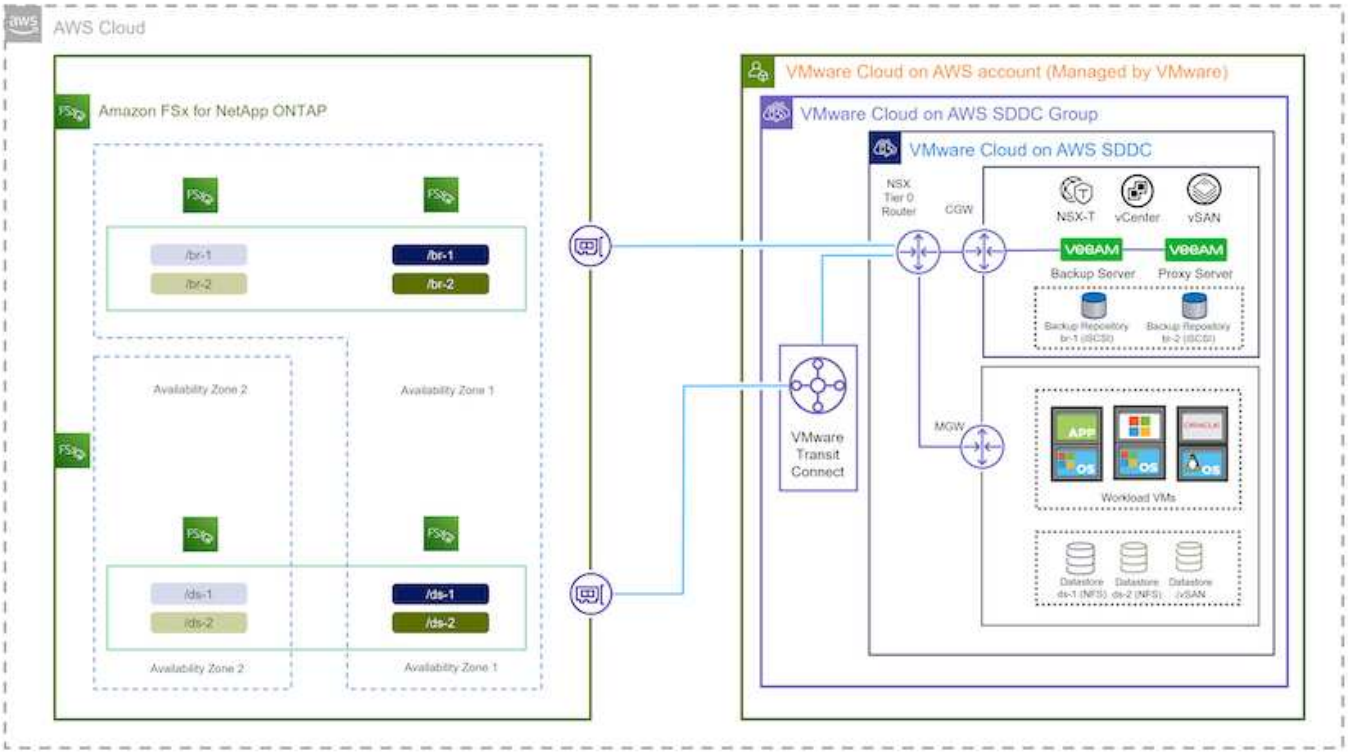
El propósito de esta solución es demostrar la protección de datos de las máquinas virtuales que se ejecutan en VMware Cloud y se encuentran en almacenes de datos NFS alojados por FSx ONTAP. Esta solución asume que los siguientes componentes están configurados y listos para usar:

1. Sistema de archivos FSx ONTAP con uno o más almacenes de datos NFS conectados a VMware Cloud.
2. Máquina virtual Microsoft Windows Server con el software Veeam Backup & Replication instalado.
    - El servidor de Veeam Backup & Replication descubrió el servidor vCenter mediante su dirección IP o nombre de dominio completo.
3. Máquina virtual de Microsoft Windows Server que se instalará con 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 almacenes de datos NFS de FSx ONTAP . Para esta solución teníamos dos bases de datos SQL en dos VMDK separados.
    - Nota: Como práctica recomendada, los archivos de base de datos y de registro de transacciones se colocan en unidades separadas, ya que esto mejorará el rendimiento y la confiabilidad. Esto se debe en parte al hecho de que los registros de transacciones se escriben secuencialmente, mientras que los archivos de base de datos se escriben aleatoriamente.
5. Máquinas virtuales de Oracle Database con VMDK y datos de aplicaciones que residen en almacenes de datos NFS de FSx ONTAP .
6. Máquinas virtuales de servidor de archivos Linux y Windows con VMDK que residen en almacenes de datos NFS de FSx ONTAP .
7. Veeam requiere puertos TCP específicos para la comunicación entre servidores y componentes en el entorno de respaldo. En los componentes de infraestructura de respaldo de Veeam, las reglas de firewall necesarias se crean automáticamente. Para obtener una lista completa de los requisitos del puerto de red, consulte la sección Puertos del "Guía del usuario de Veeam Backup and Replication para

VMware vSphere" .

Arquitectura de alto nivel

La prueba/validación de esta solución se realizó en un laboratorio que puede o no coincidir con el entorno de implementación final. Para obtener más información, consulte las siguientes secciones.



▼ **Componentes de hardware/software**

El propósito de esta solución es demostrar la protección de datos de las máquinas virtuales que se ejecutan en VMware Cloud y se encuentran en almacenes de datos NFS alojados por FSx ONTAP. Esta solución asume que los siguientes componentes ya están configurados y listos para usar:

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

Implementación de la solución

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

Revisaremos la creación del sistema de archivos FSx ONTAP , el montaje de volúmenes iSCSI para usarlos como repositorios de respaldo, la creación y ejecución de trabajos de respaldo y la realización de

restauraciones de máquinas virtuales y bases de datos.

Para obtener información detallada sobre FSx ONTAP, consulte "Guía del usuario de FSx ONTAP" .

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

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

Implementar el servidor proxy de Veeam

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

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

Para calcular el número de servidores proxy y sus requisitos de sistema, consulte la "Guía de mejores prácticas de Veeam VMware vSphere" .

Veeam Data Mover es un componente del Veeam Proxy Server y utiliza un modo de transporte como método para obtener datos de la máquina virtual desde la fuente 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 las copias de seguridad de los almacenes de datos NFS mediante el acceso directo al almacenamiento.

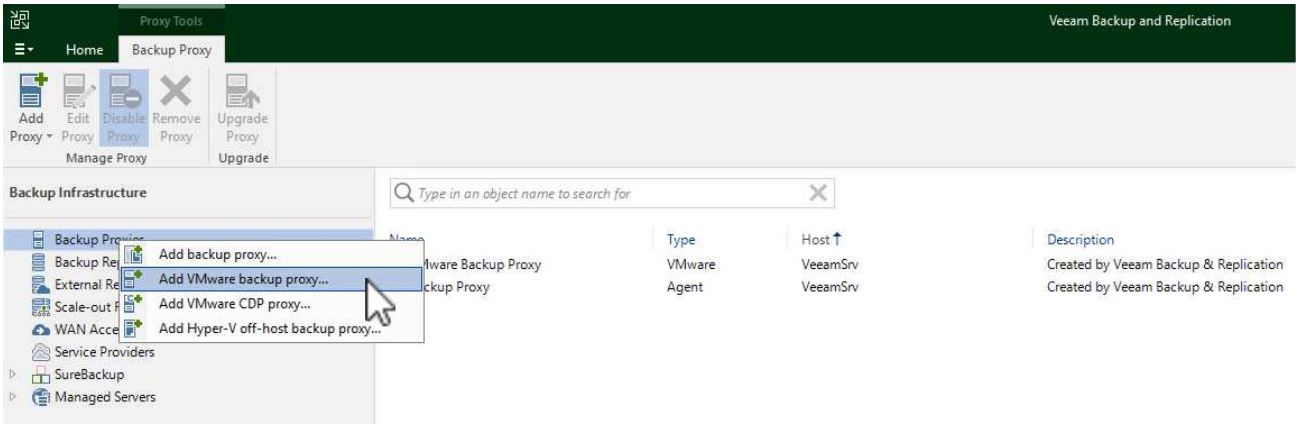
Para obtener más información sobre los modos de transporte, consulte la "Guía del usuario de Veeam Backup and Replication para VMware vSphere" .

En el siguiente paso, cubrimos la implementación del servidor proxy Veeam en una máquina virtual Windows en VMware Cloud SDDC.

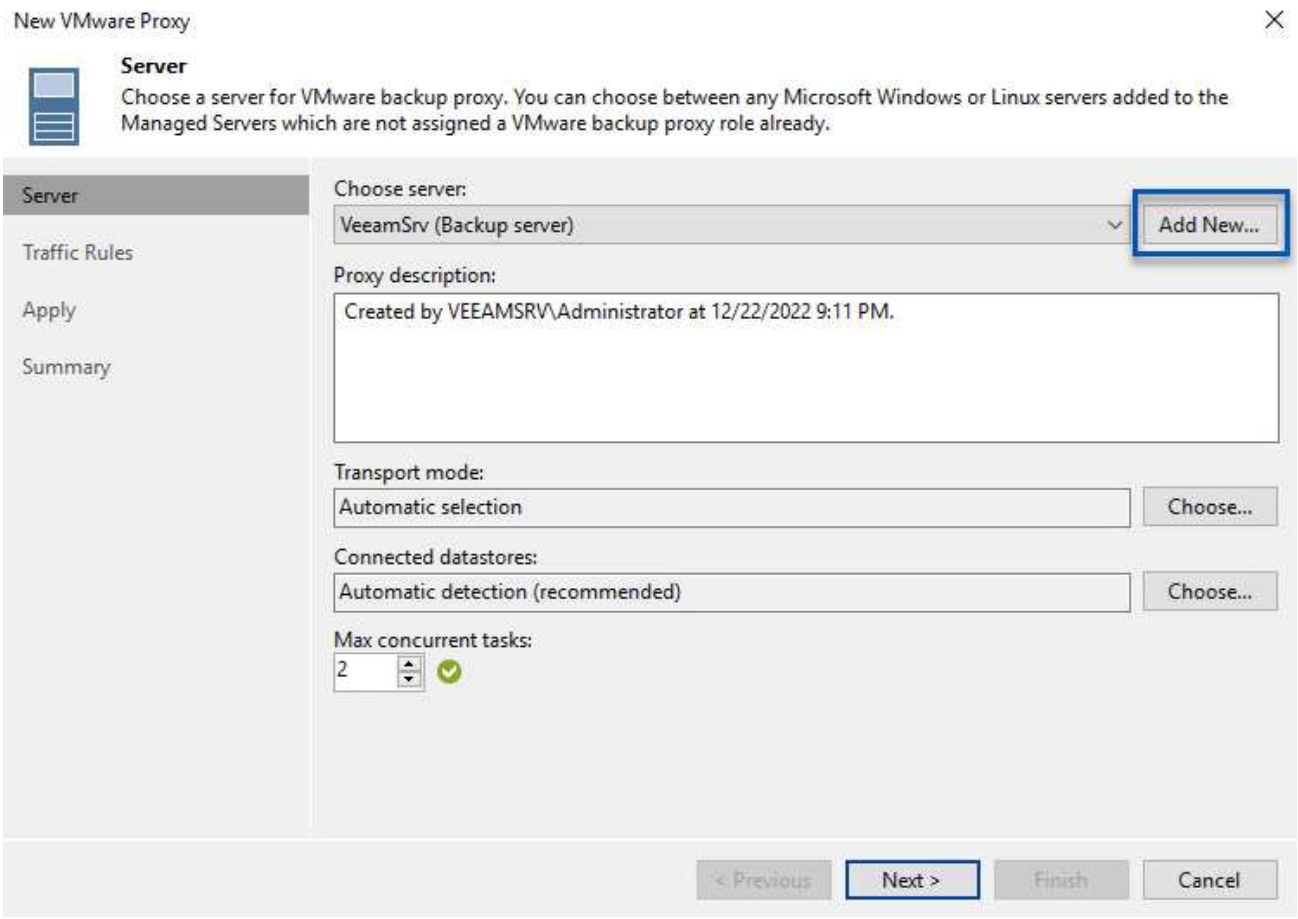
▼ **Implementar Veeam Proxy para distribuir cargas de trabajo de respaldo**

En este paso, el Veeam Proxy se implementa en una máquina virtual Windows existente. Esto permite que los trabajos de respaldo se distribuyan entre el servidor de respaldo Veeam principal y el proxy Veeam.

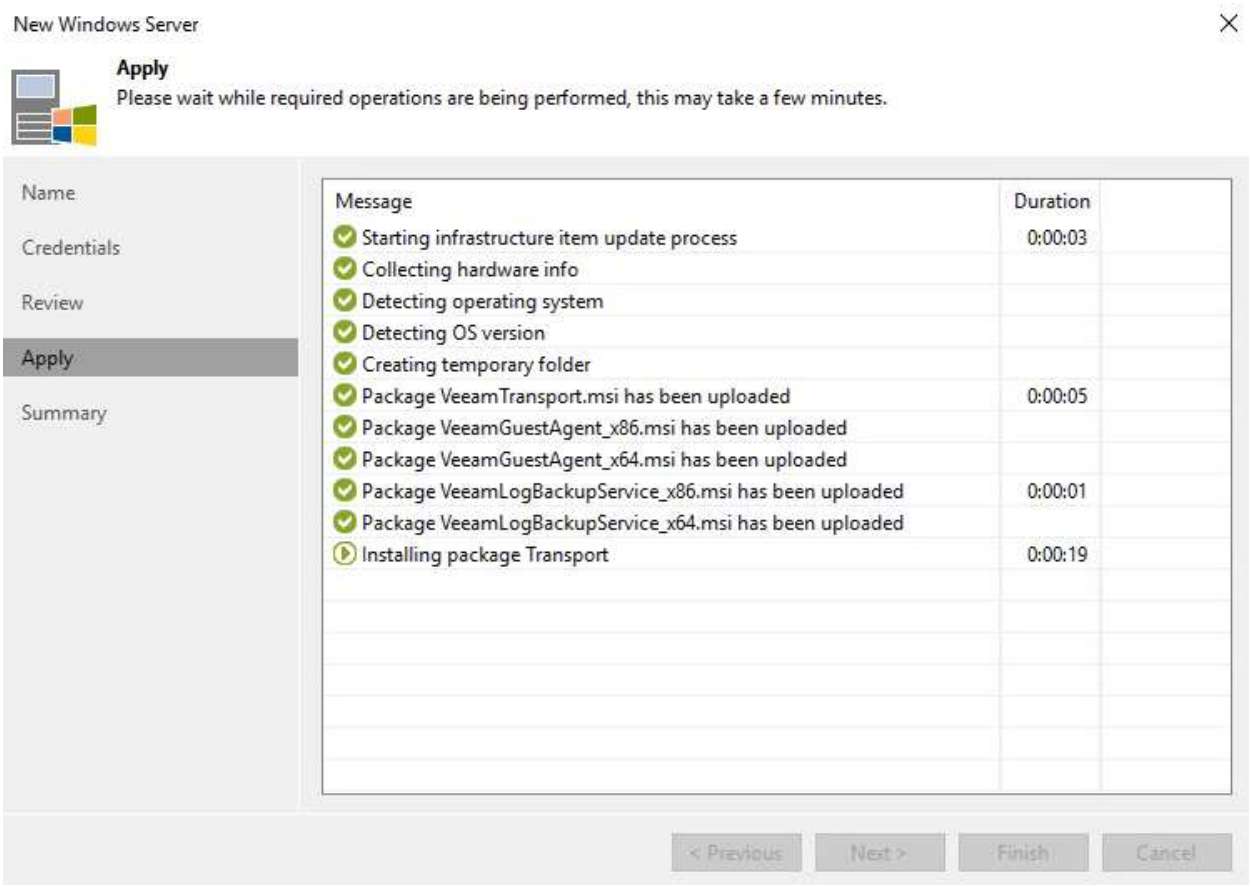
1. En el servidor de Veeam Backup and Replication, abra la consola de administración y seleccione **Infraestructura de respaldo** en el menú inferior izquierdo.
2. Haga clic derecho en **Proxies de respaldo** y haga clic en **Agregar proxy de respaldo de VMware…** para abrir el asistente.



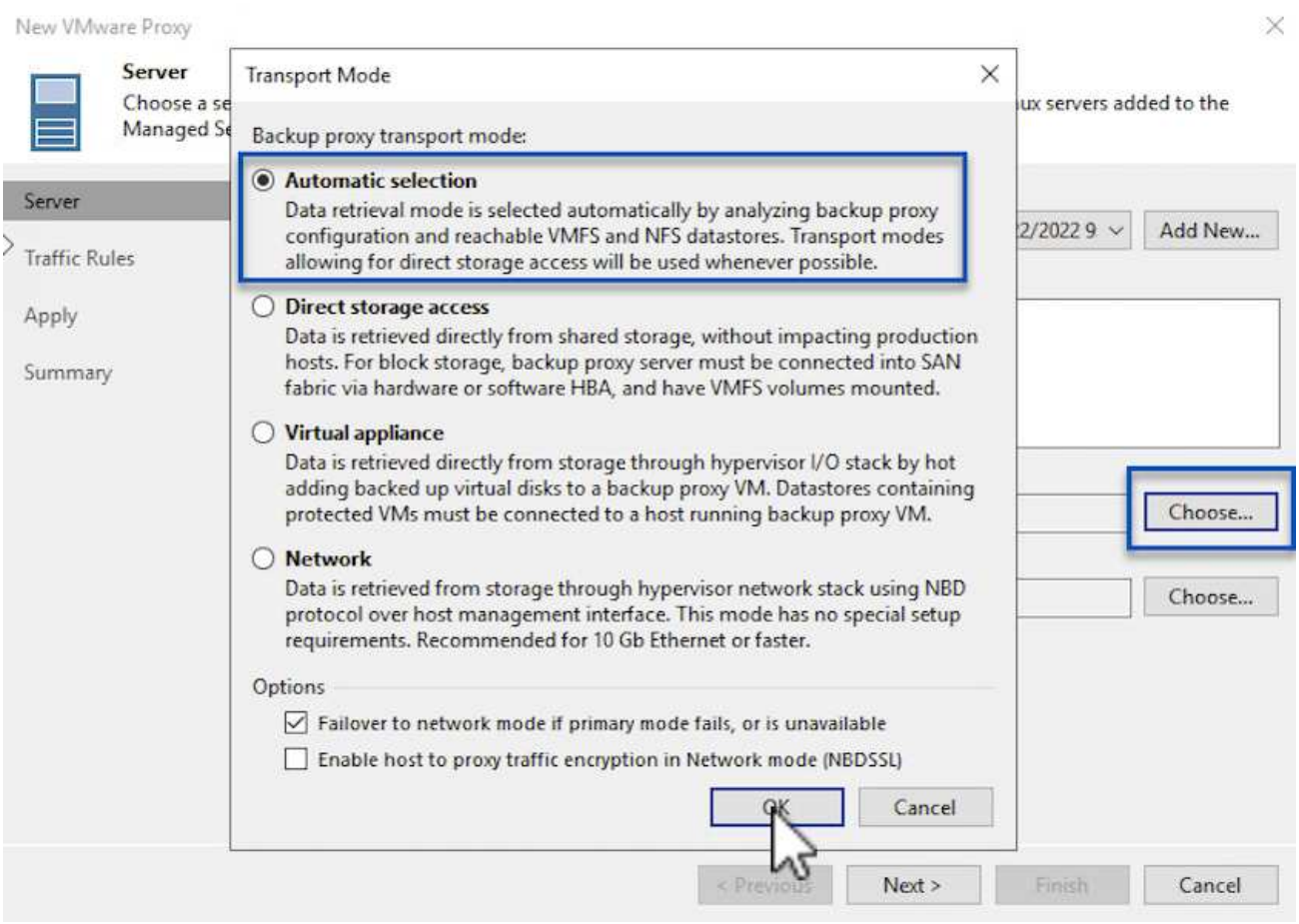
3. En el asistente **Agregar proxy VMware**, haga clic en el botón **Agregar nuevo…** para agregar un nuevo servidor proxy.



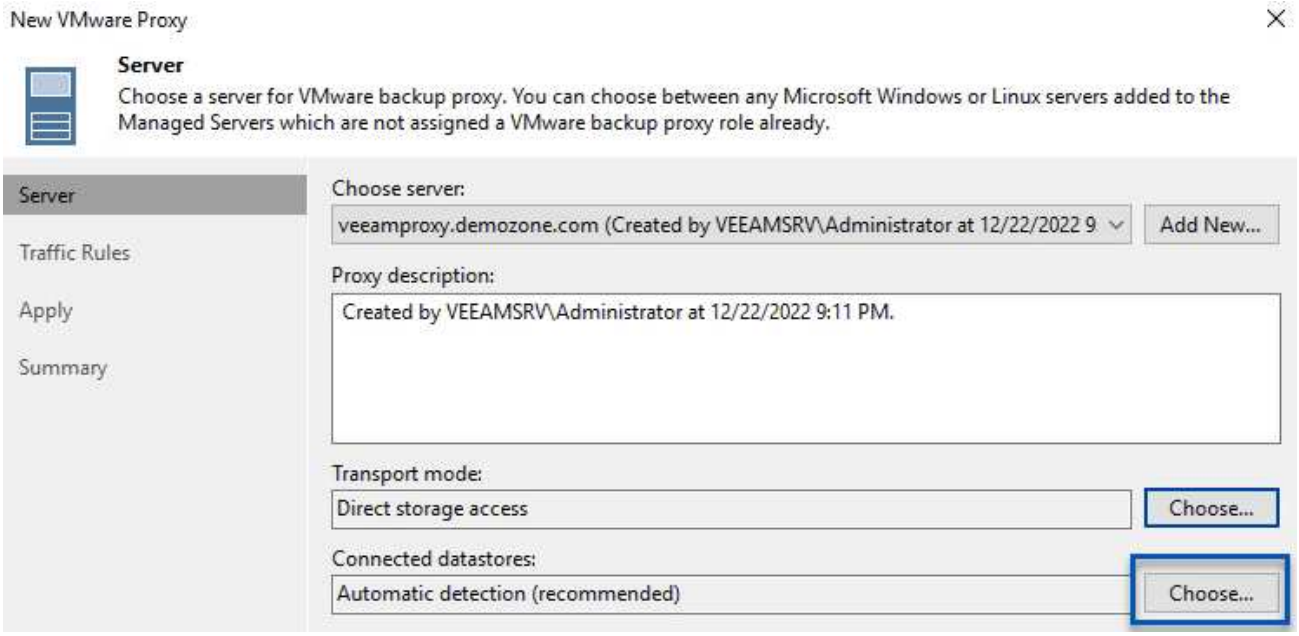
4. Seleccione para agregar Microsoft Windows y siga las instrucciones para agregar el servidor:
   - Complete el nombre DNS o la dirección IP
   - Seleccione una cuenta para usar como credenciales en el nuevo sistema o agregue nuevas credenciales
   - Revise los componentes que se instalarán y luego haga clic en **Aplicar** para comenzar la implementación.

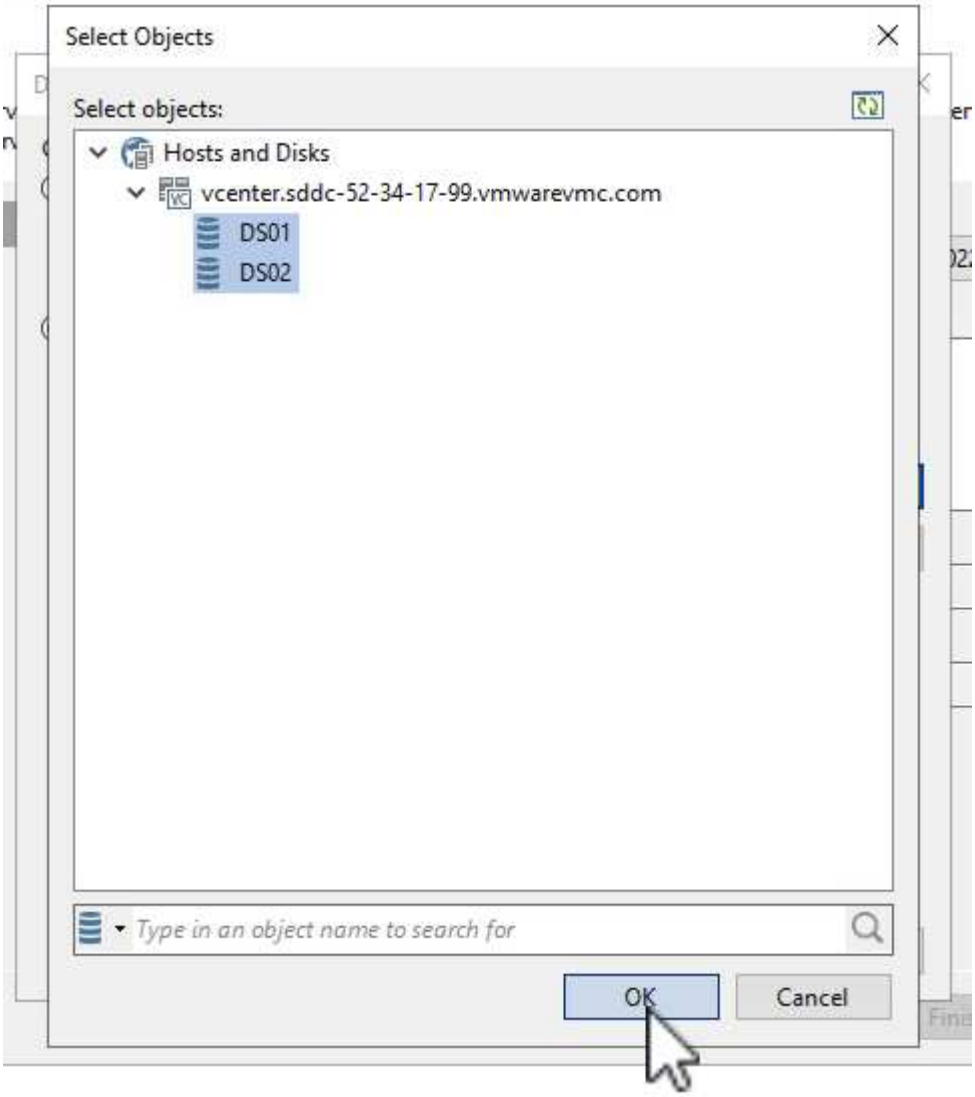


5. De vuelta en el asistente **Nuevo proxy VMware**, elija un Modo de transporte. En nuestro caso elegimos **Selección automática**.

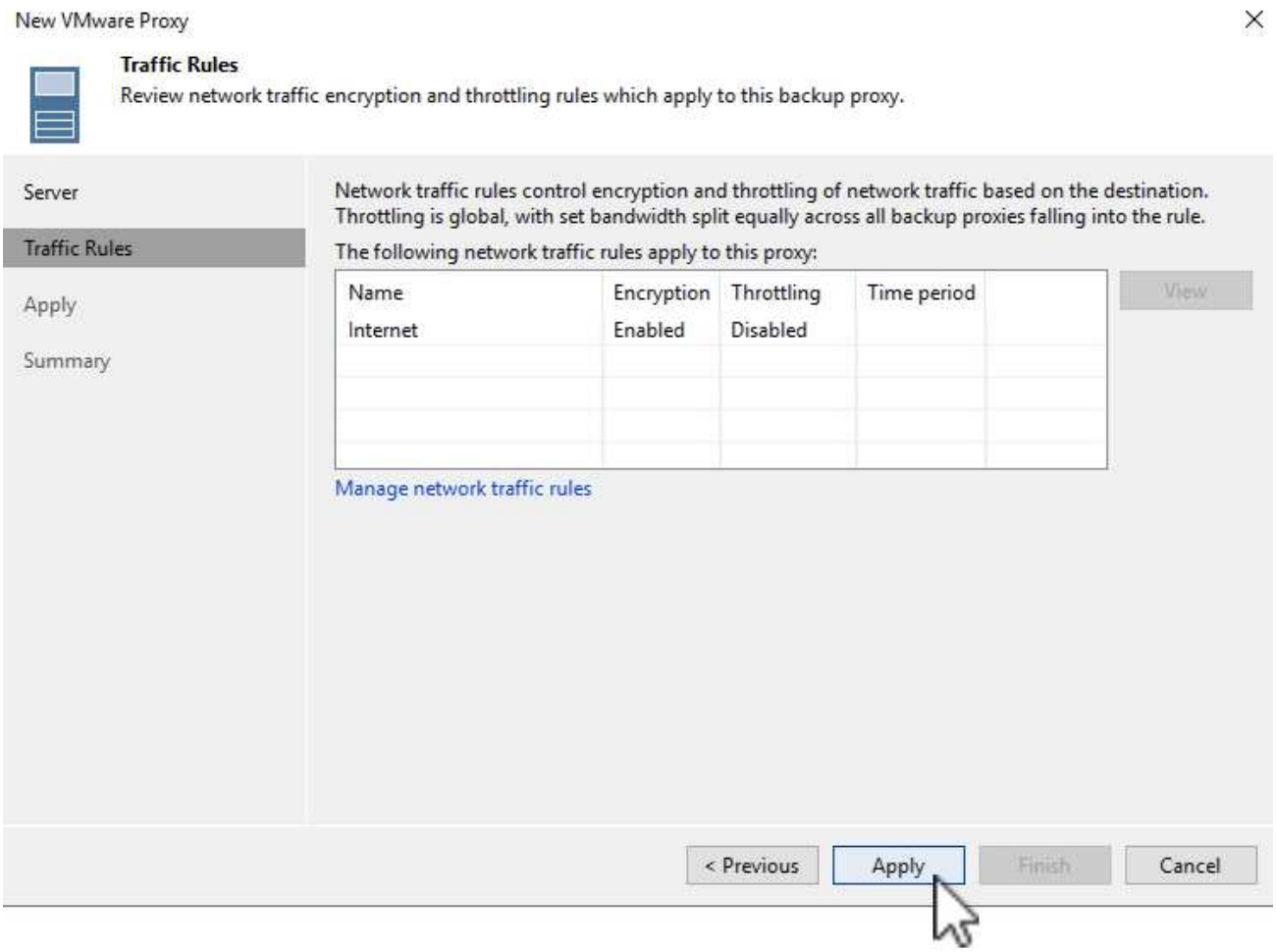


6. Seleccione los almacenes de datos conectados a los que desea que el proxy VMware tenga acceso directo.





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



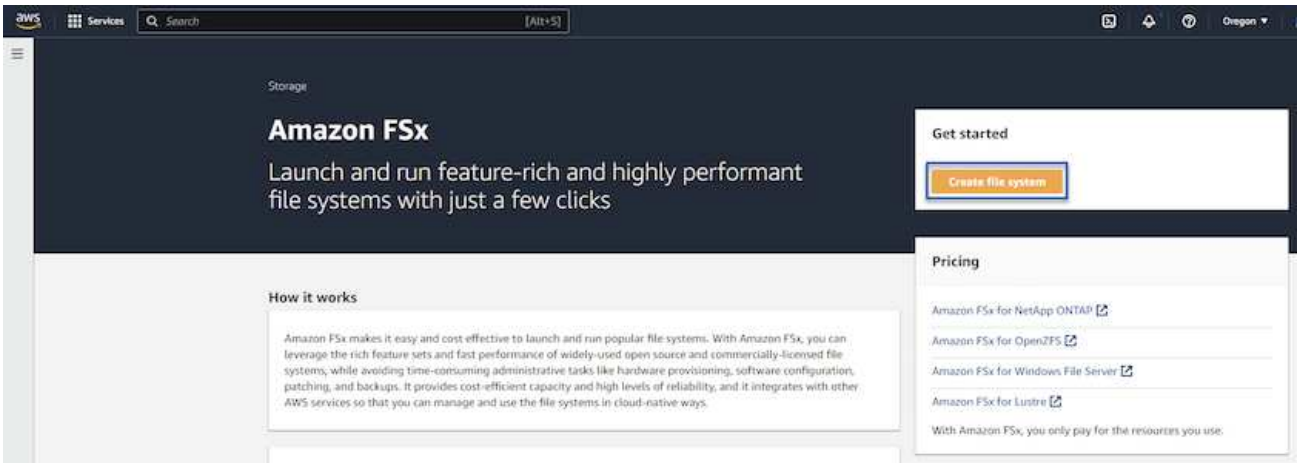
Configurar repositorios de almacenamiento y de respaldo

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

▼ Crear el sistema de archivos FSx ONTAP

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

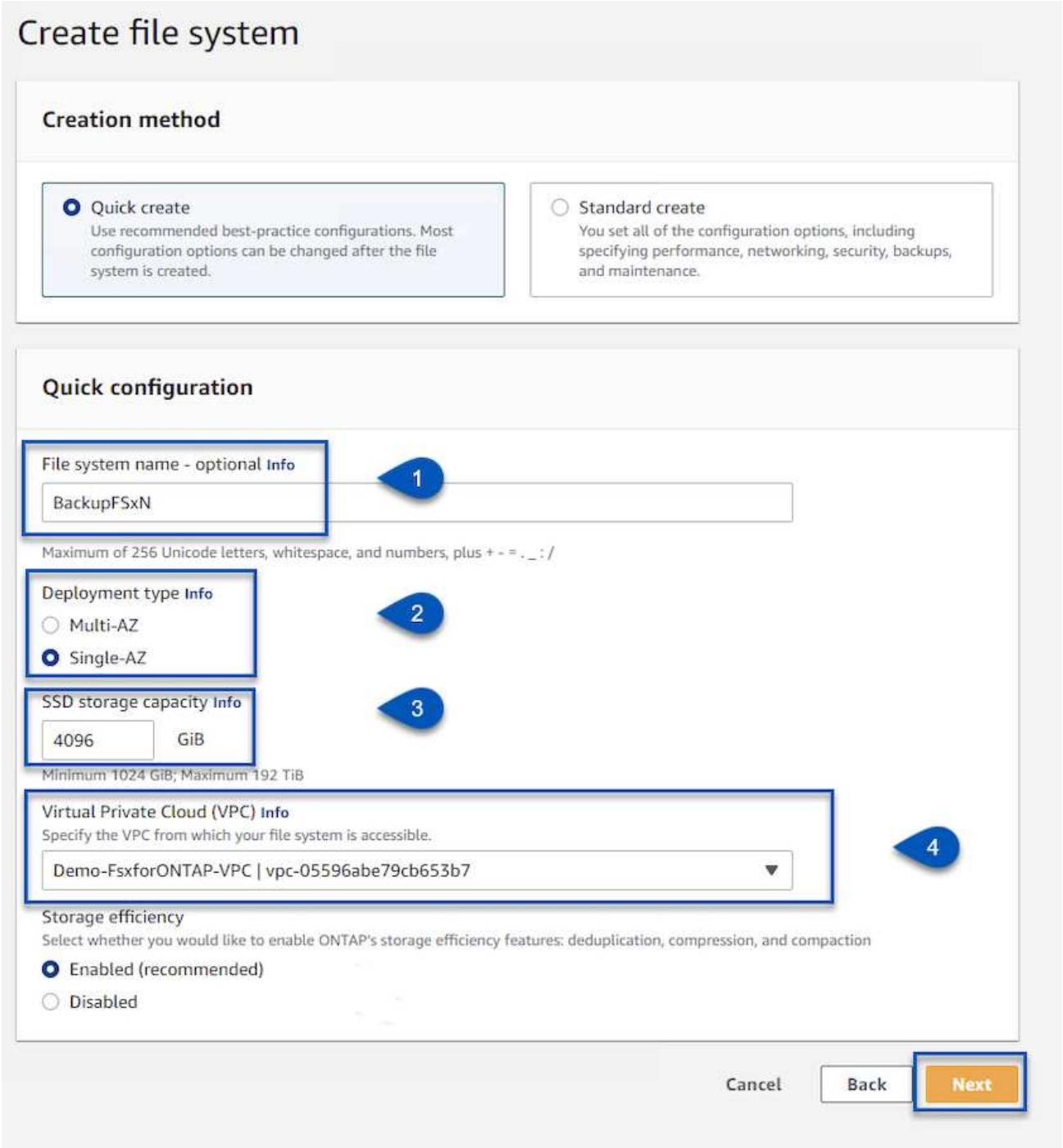
1. En la consola de AWS, vaya a FSx y luego **Crear sistema de archivos**



2. Seleccione * Amazon FSx ONTAP* y luego * Siguiente * para continuar.



3. Complete el nombre del sistema de archivos, el tipo de implementación, la capacidad de almacenamiento SSD y la VPC en la que residirá el clúster FSx ONTAP . Esta debe ser una VPC configurada para comunicarse con la red de máquinas virtuales 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.

▼ **Configurar y montar LUN iSCSI**

Cree y configure los LUN iSCSI en FSx ONTAP y móntelos en los servidores proxy y de respaldo de Veeam. Estos LUN se utilizarán más adelante para crear repositorios de respaldo de Veeam.

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

ⓘ Para obtener más información sobre el uso de FSx ONTAP, consulte la "Guía del usuario de

FSx ONTAP" .

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

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

2. Cree LUN utilizando los volúmenes creados 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. Otorgue acceso a los LUN mediante la creación de un grupo de iniciadores que contenga el IQN iSCSI de los servidores proxy y de respaldo de Veeam:

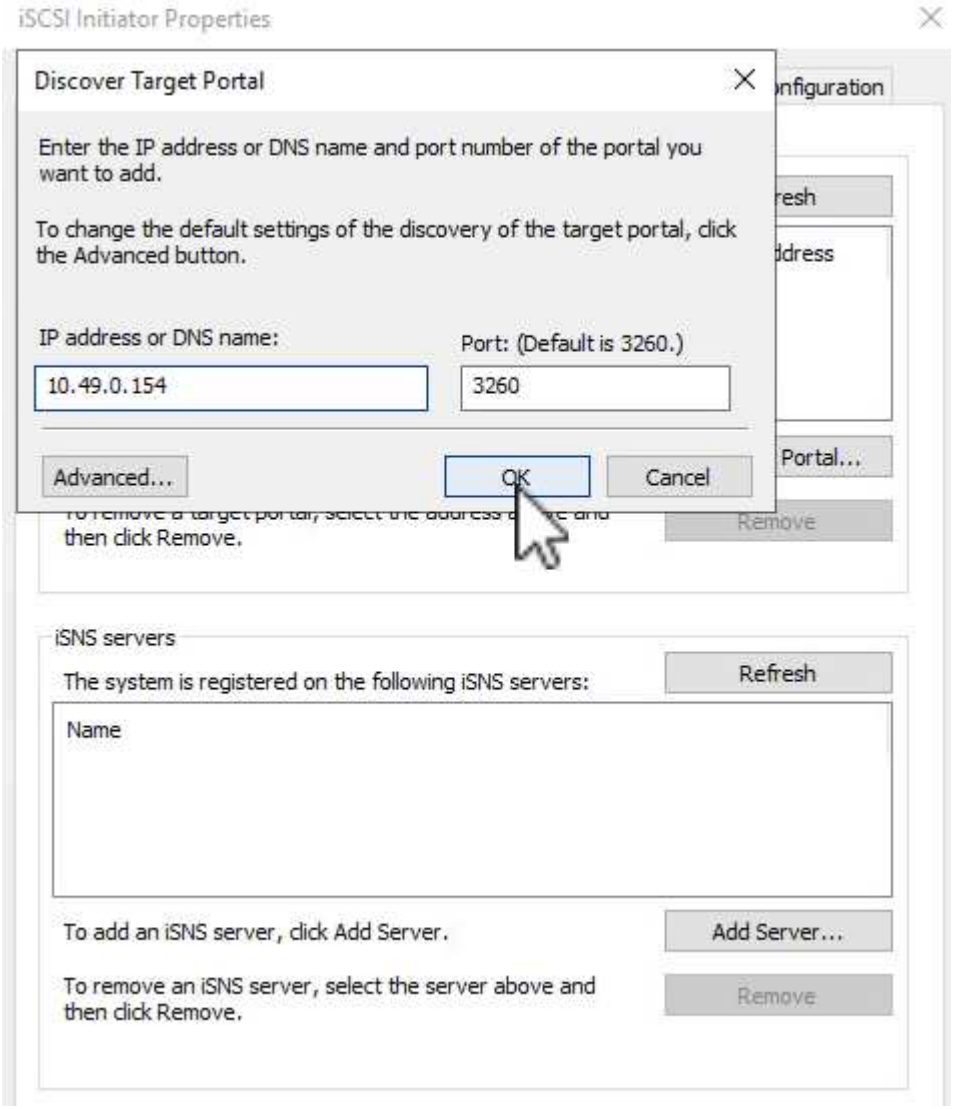
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

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

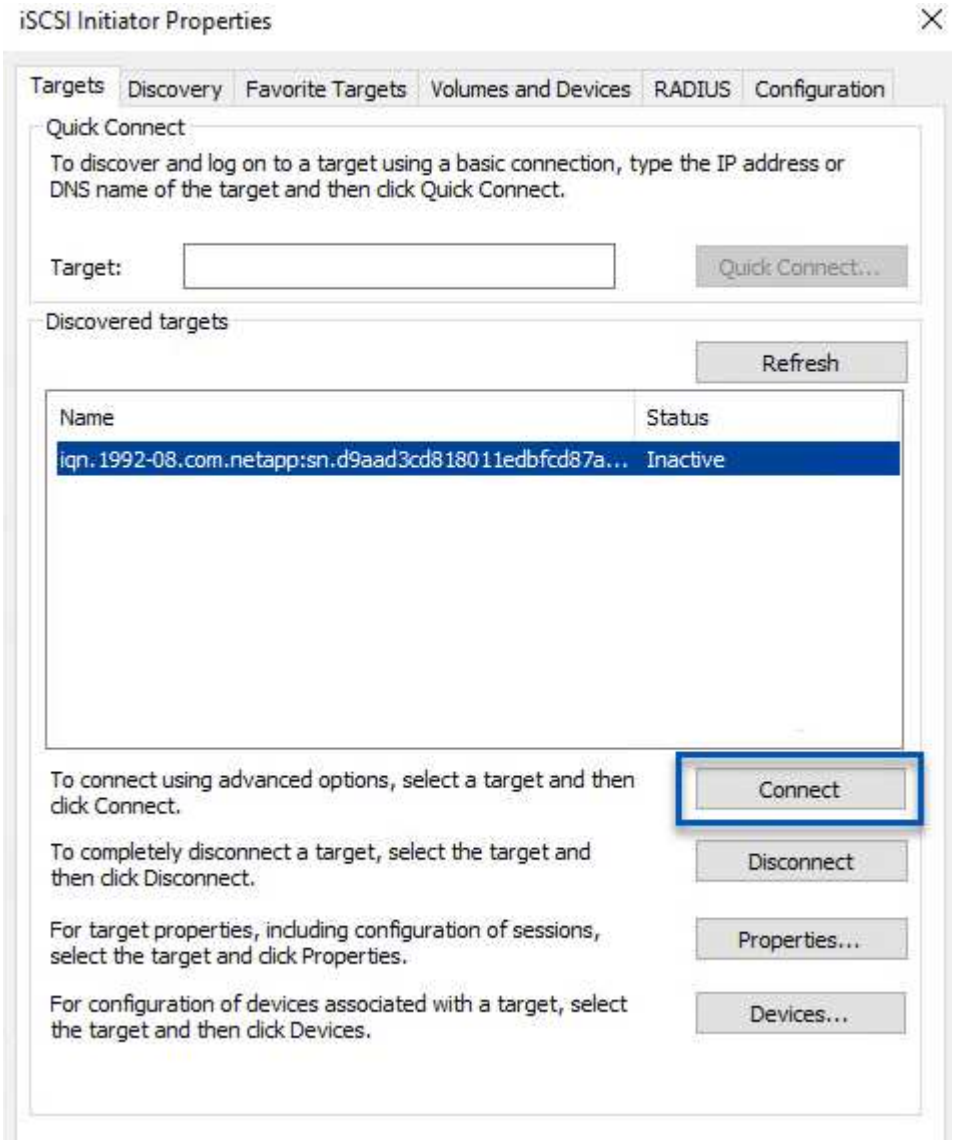
4. Por último, asigne los LUN al grupo de iniciadores que acaba de crear:

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

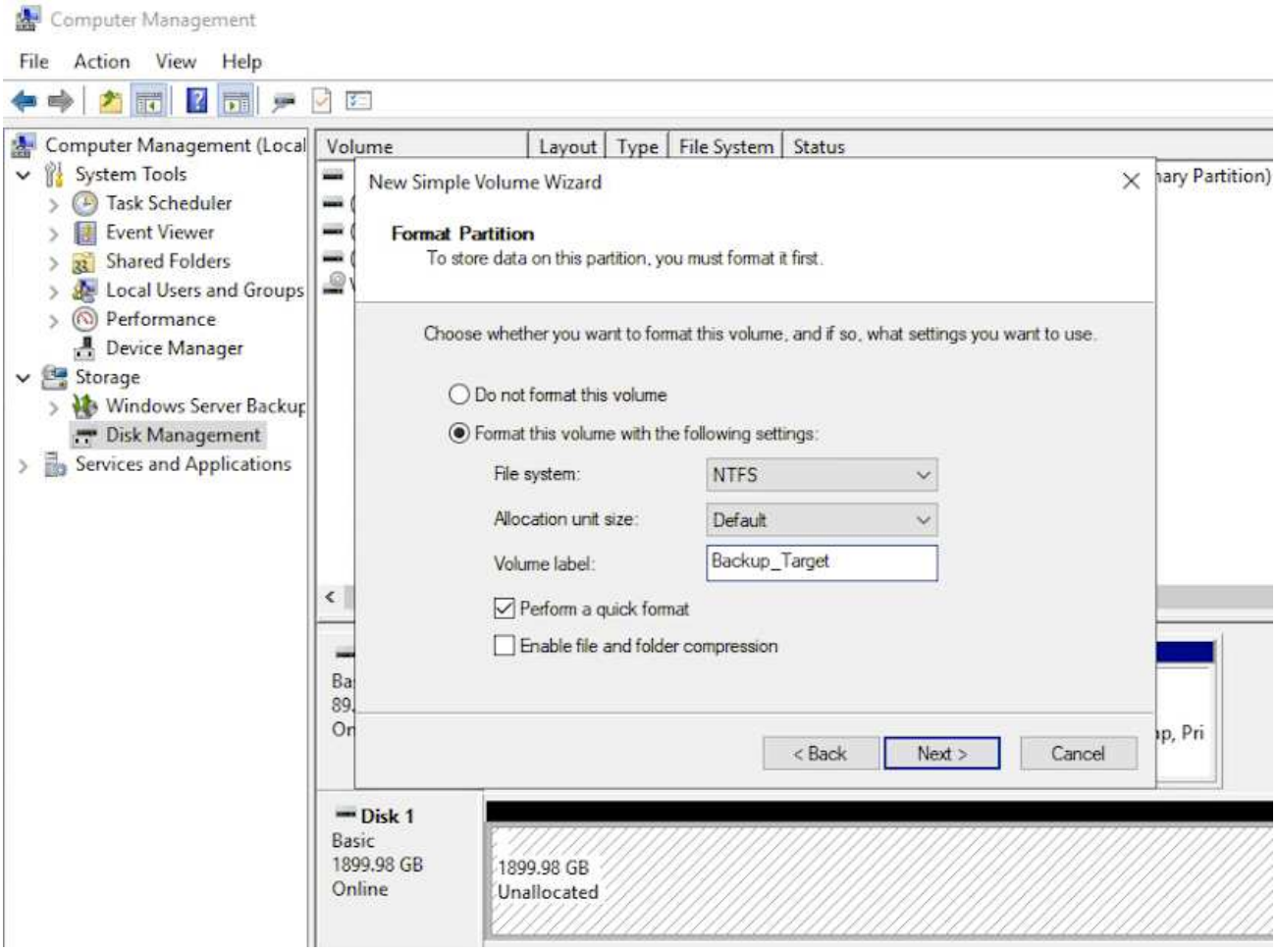
5. Para montar los LUN iSCSI, inicie sesión en Veeam Backup & Replication Server y abra Propiedades del iniciador iSCSI. Vaya a la pestaña **Descubrir** e ingrese la dirección IP de destino iSCSI.



6. En la pestaña **Objetivos**, resalte el LUN inactivo y haga clic en **Conectar**. Marque la casilla **Habilitar múltiples rutas** y haga clic en **Aceptar** para conectarse al LUN.



7. En la utilidad de Administración de discos, inicialice el nuevo LUN y cree un volumen con el nombre y la letra de unidad deseados. Marque la casilla **Habilitar múltiples rutas** y haga clic en **Aceptar** para conectarse al LUN.

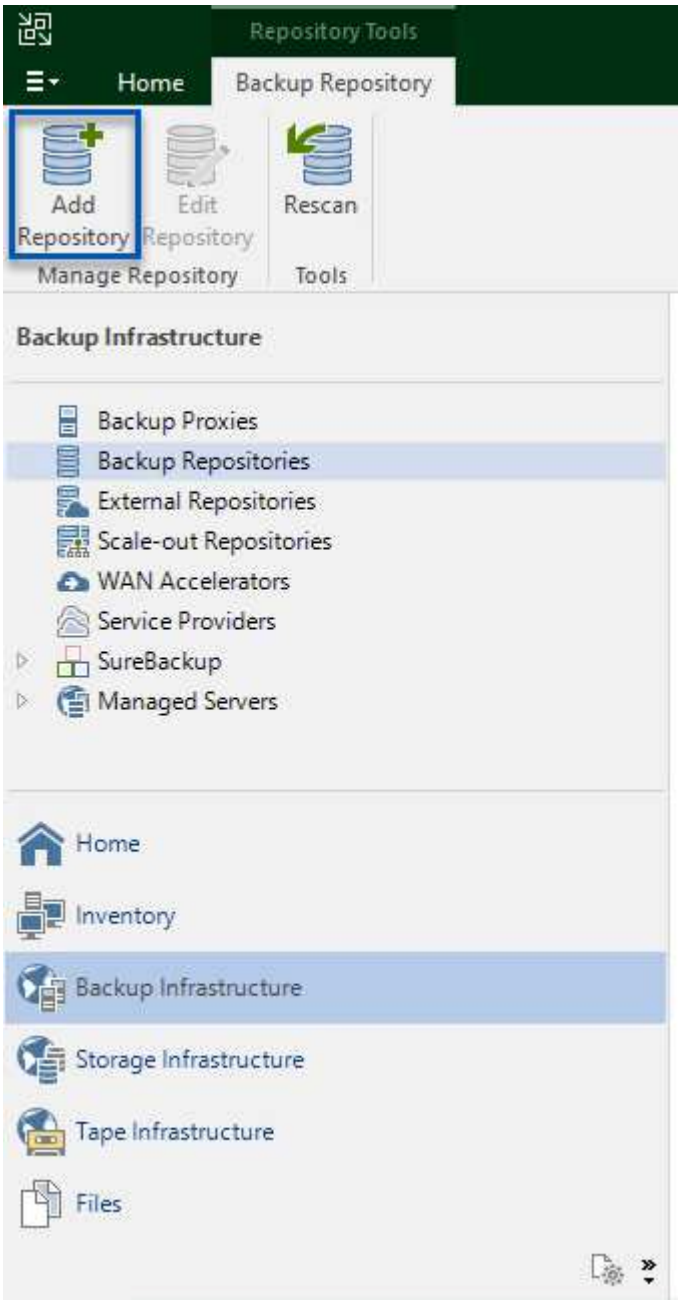


8. Repita estos pasos para montar los volúmenes iSCSI en el servidor proxy de Veeam.

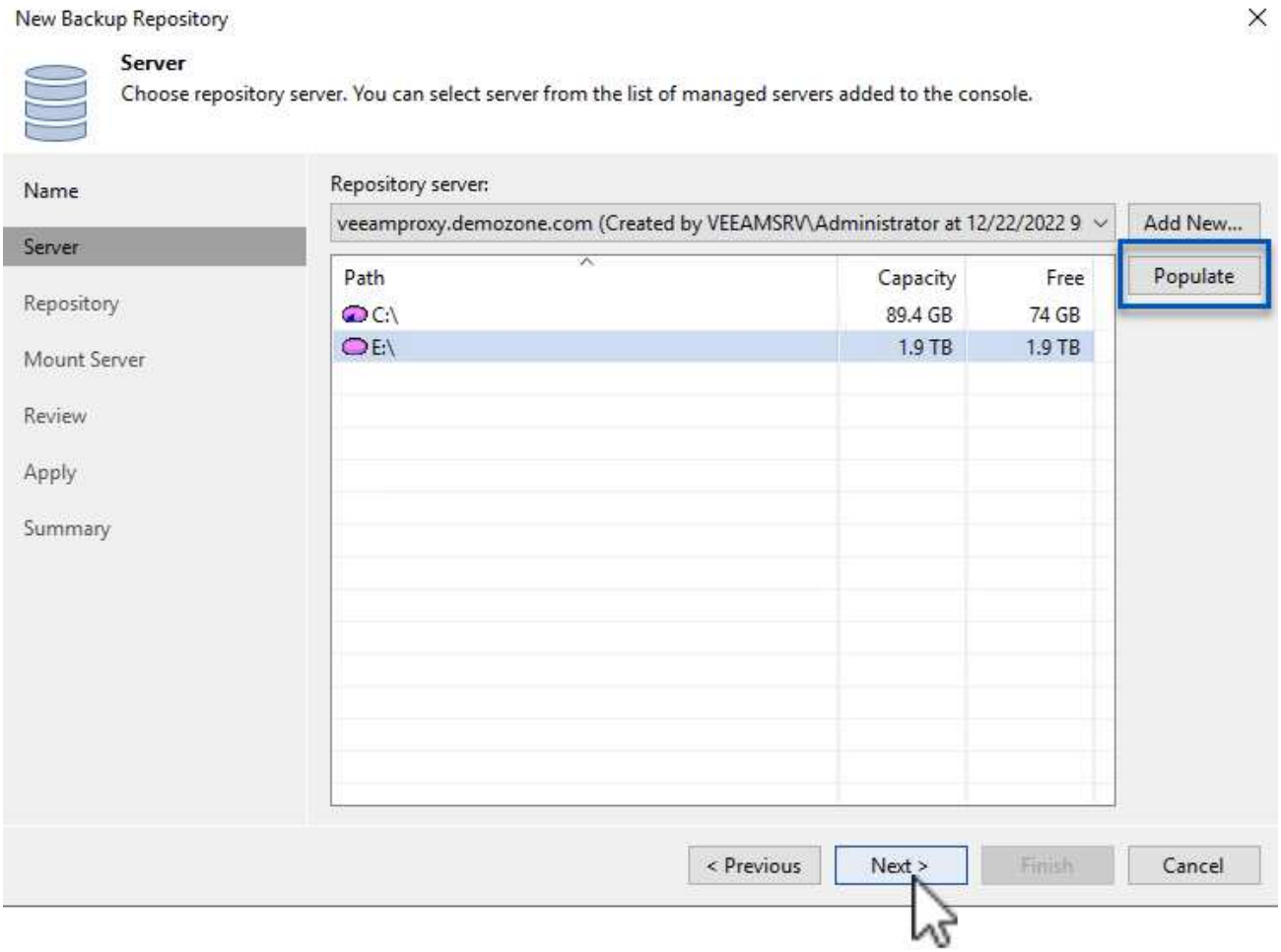
▼ **Crear repositorios de Veeam Backup**

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

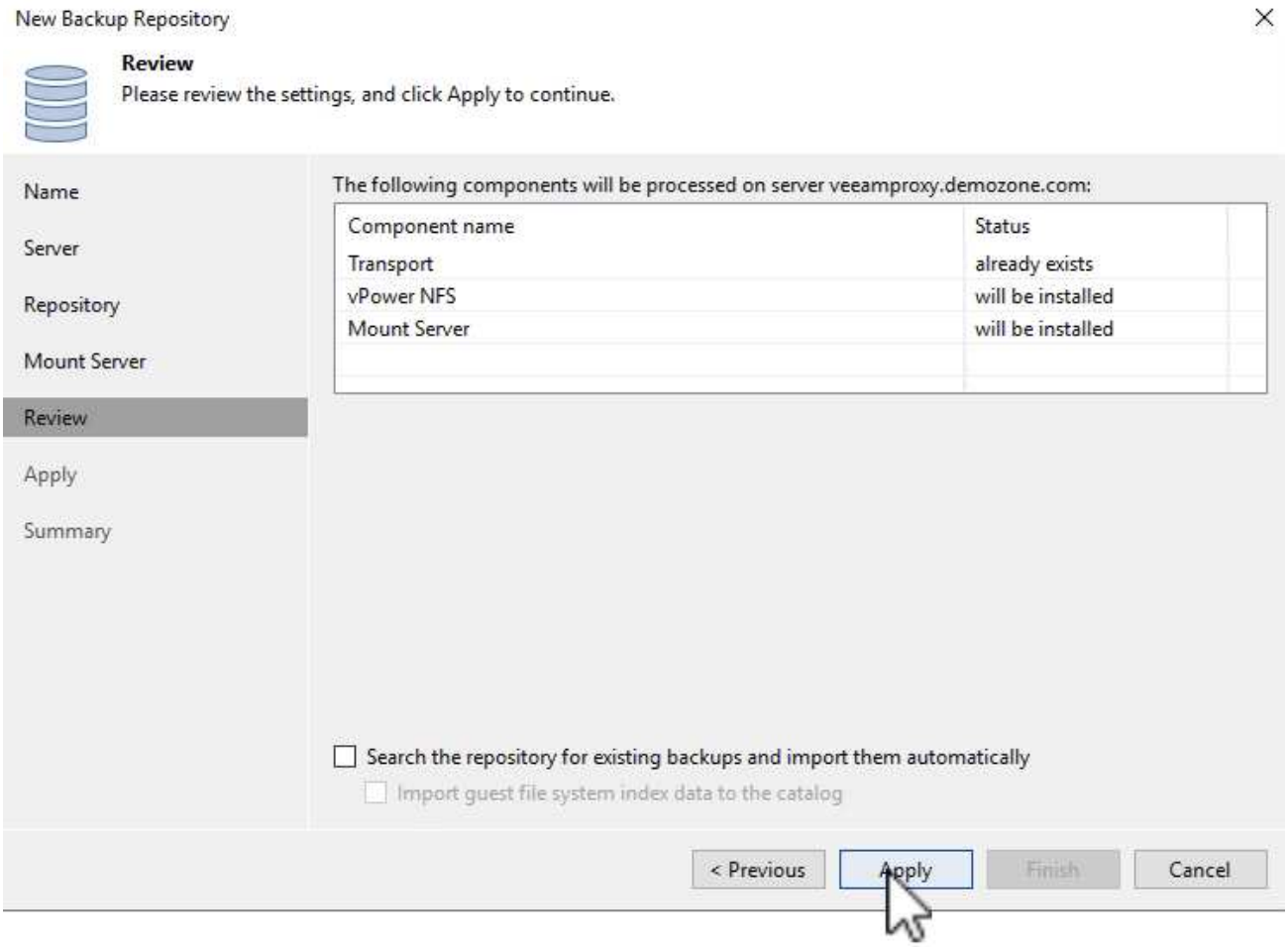
1. En la consola de Veeam Backup and Replication, haga clic en **Infraestructura de respaldo** en la parte inferior izquierda y luego seleccione **Agregar repositorio**



2. En el asistente Nuevo repositorio de respaldo, ingrese un nombre para el repositorio y luego seleccione el servidor de la lista desplegable y haga clic en el botón **Rellenar** para elegir el volumen NTFS que se utilizará.



3. En la página siguiente, seleccione un servidor de montaje que se utilizará para montar copias de seguridad cuando se realicen restauraciones avanzadas. De forma predeterminada, 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 respaldo.



5. Repita estos pasos para cualquier servidor proxy adicional.

Configurar trabajos de respaldo de Veeam

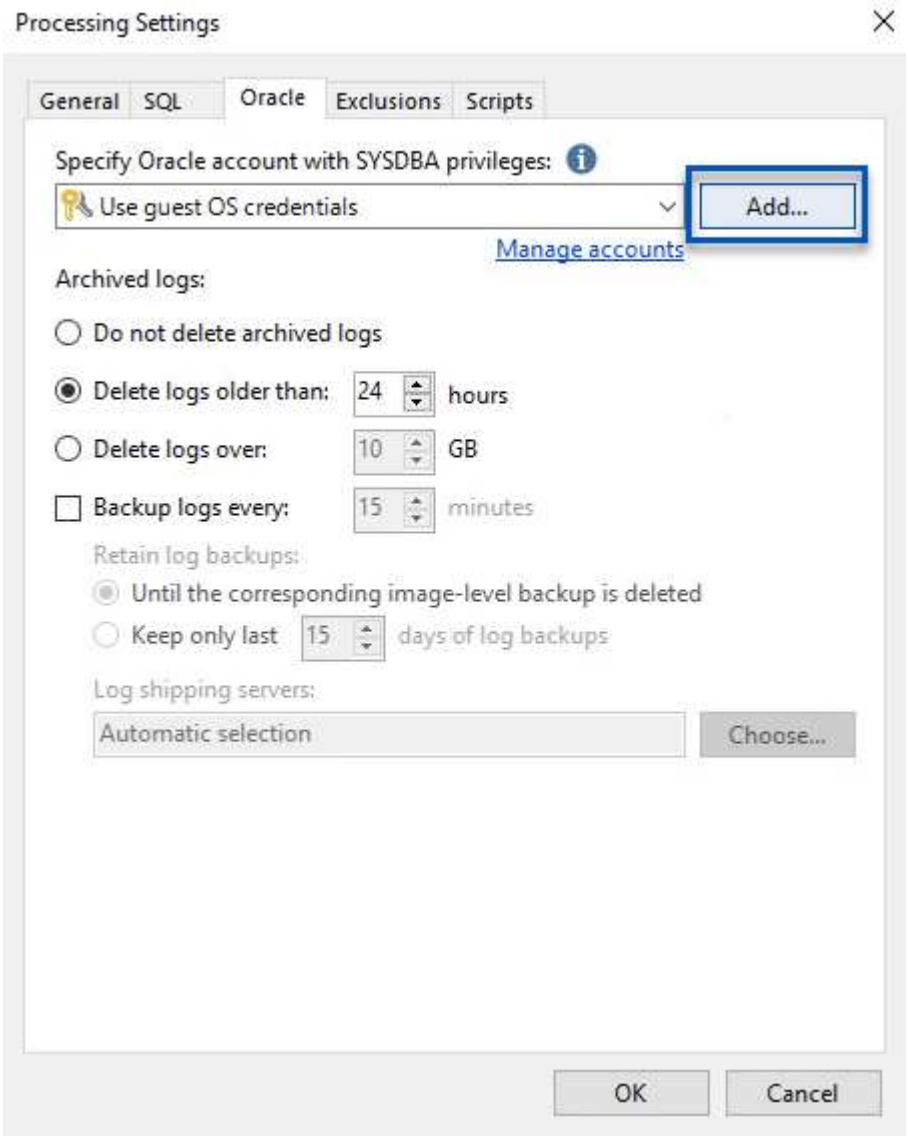
Los trabajos de respaldo deben crearse utilizando los repositorios de respaldo en la sección anterior. La creación de trabajos de respaldo es una parte normal del repertorio de cualquier administrador de almacenamiento y no cubrimos todos los pasos aquí. Para obtener información más completa sobre la creación de trabajos de respaldo en Veeam, consulte la "Documentación técnica del Centro de ayuda de Veeam" .

En esta solución se crearon trabajos de respaldo independientes para:

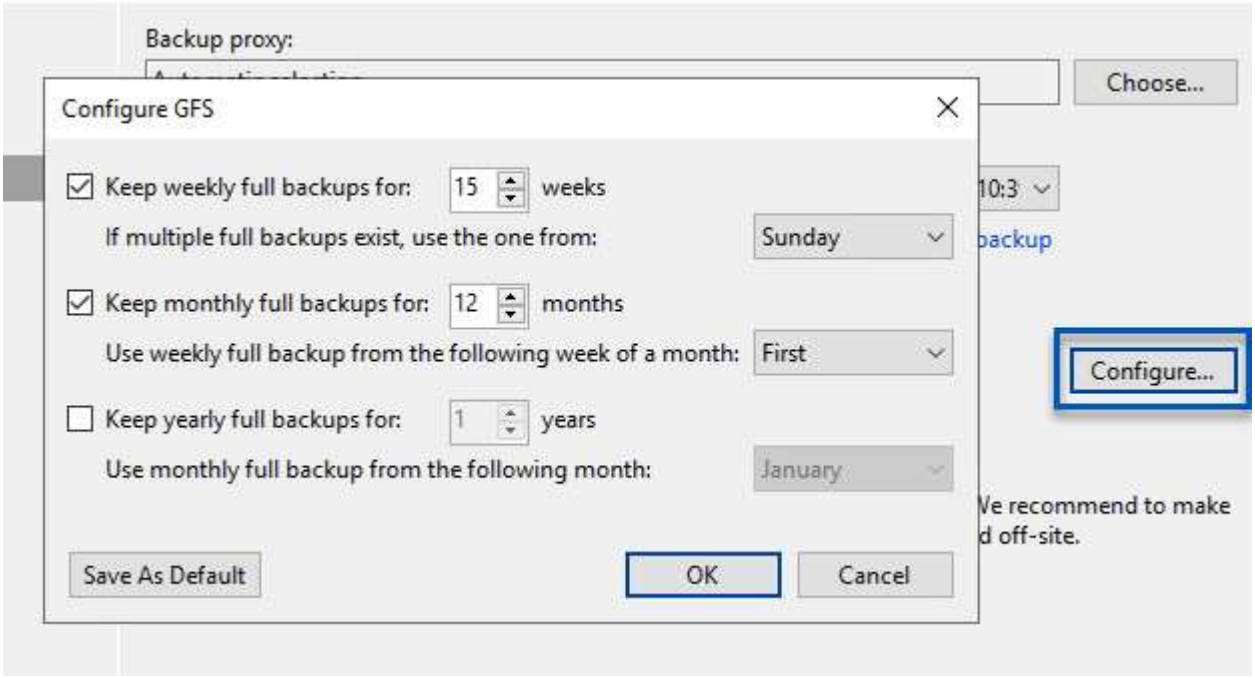
- Servidores SQL de Microsoft Windows
- servidores de bases de datos Oracle
- servidores de archivos de Windows
- servidores de archivos Linux

▼ Consideraciones generales al configurar trabajos de backup de Veeam

1. Habilite el procesamiento consciente de la aplicación para crear copias de seguridad consistentes y realizar el procesamiento del registro de transacciones.
2. Después de habilitar el procesamiento consciente de la aplicación, agregue las credenciales correctas con privilegios de administrador a la aplicación, ya que pueden ser diferentes de las credenciales del sistema operativo invitado.



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



Restaurar máquinas virtuales de aplicaciones con la restauración completa de Veeam

Realizar una restauración completa con Veeam es el primer paso para realizar una restauración de una aplicación. Validamos que las restauraciones completas de nuestras máquinas virtuales se encendieron y que todos los servicios funcionaron normalmente.

Restaurar servidores es una parte normal del repertorio de cualquier administrador 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" .

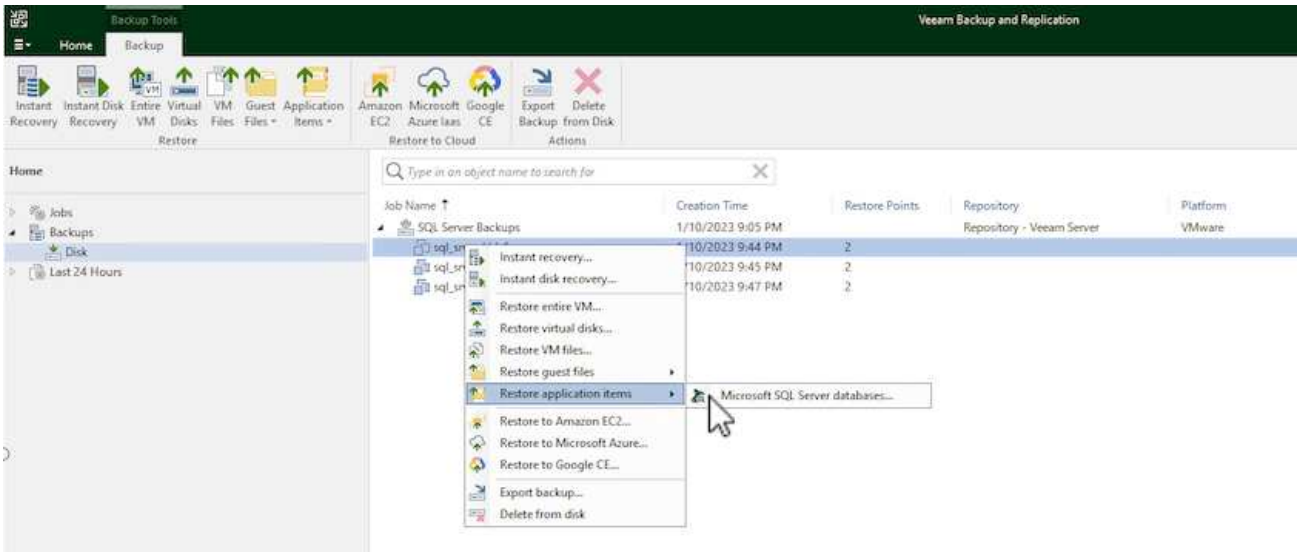
Restaurar bases de datos de SQL Server

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

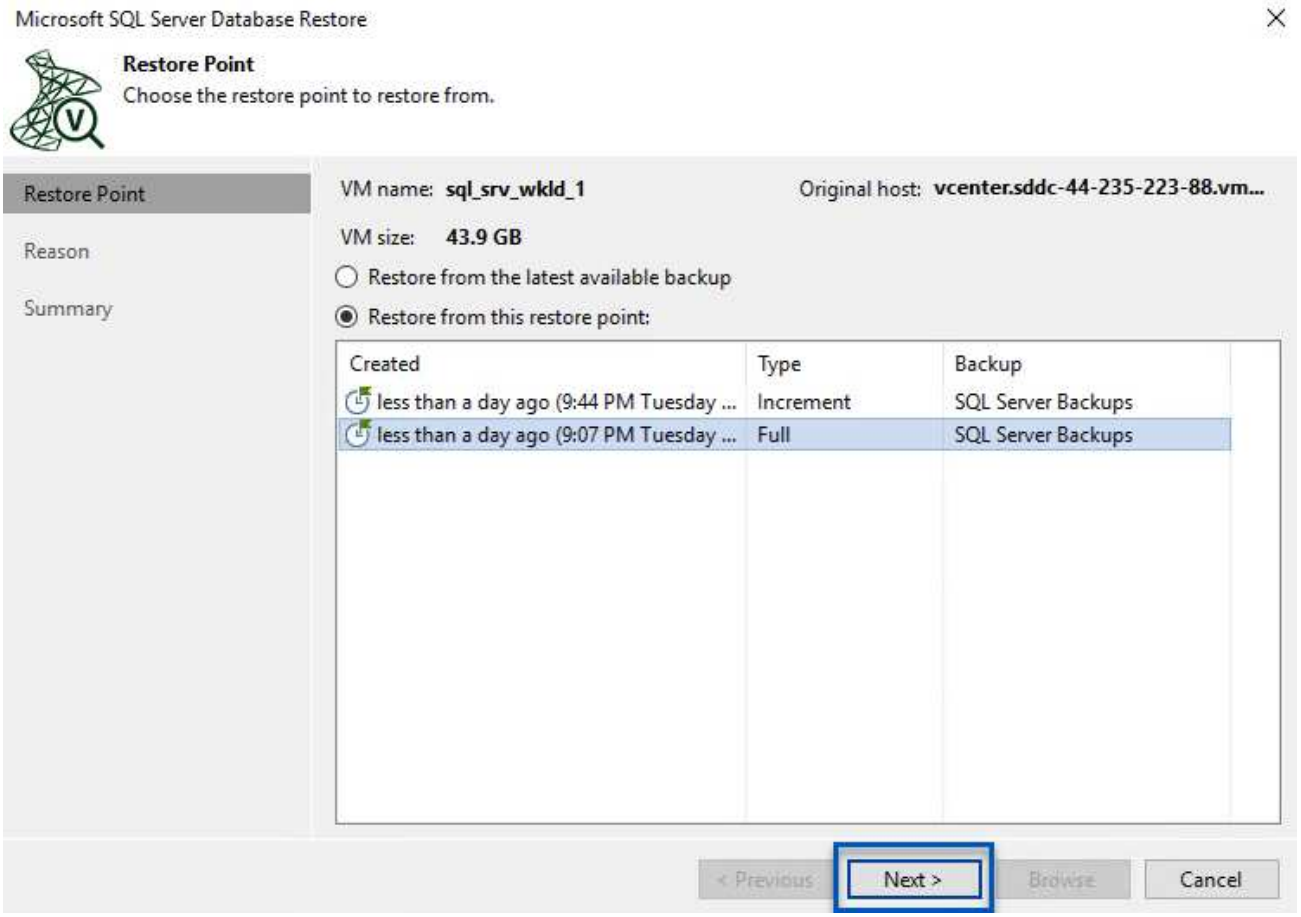
- Veeam Explorer **monta la copia de seguridad** que contiene la base de datos de SQL Server que se va a restaurar.
- El software **publica la base de datos** directamente desde los archivos montados, lo que la hace accesible como una base de datos temporal en la instancia de SQL Server de destino.
- Mientras la base de datos temporal está en uso, Veeam Explorer **redirige las consultas de los usuarios** a esta base de datos, lo que garantiza 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 de la base de datos original.
- Una vez que se completa la restauración completa de la base de datos, Veeam Explorer **cambia las consultas del usuario a la base de datos original** y elimina la base de datos temporal.

▼ Restaurar la base de datos de SQL Server con Veeam Explorer Instant Recovery

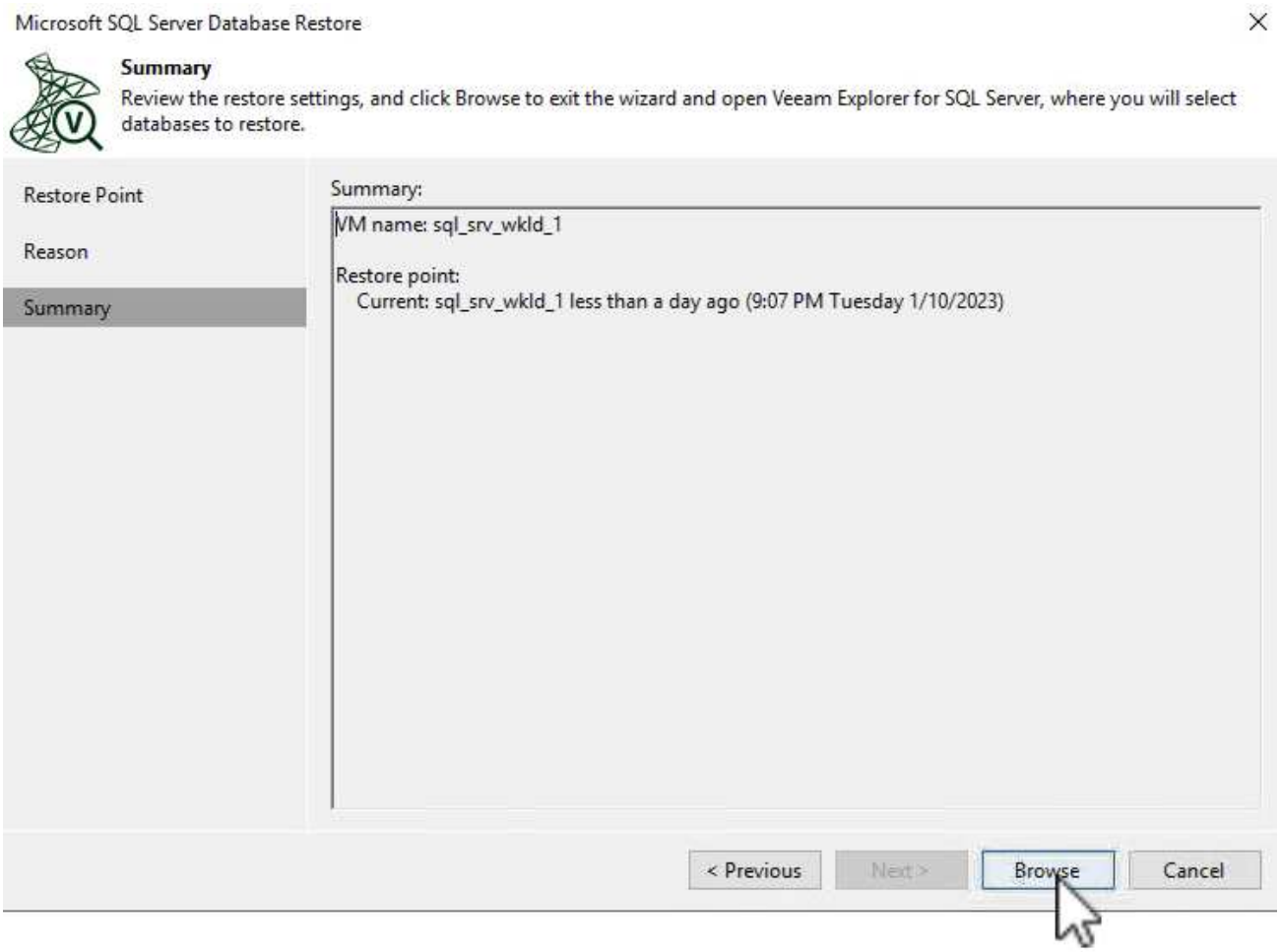
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de SQL Server, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de aplicación** y luego **Bases de datos de Microsoft SQL Server…**.



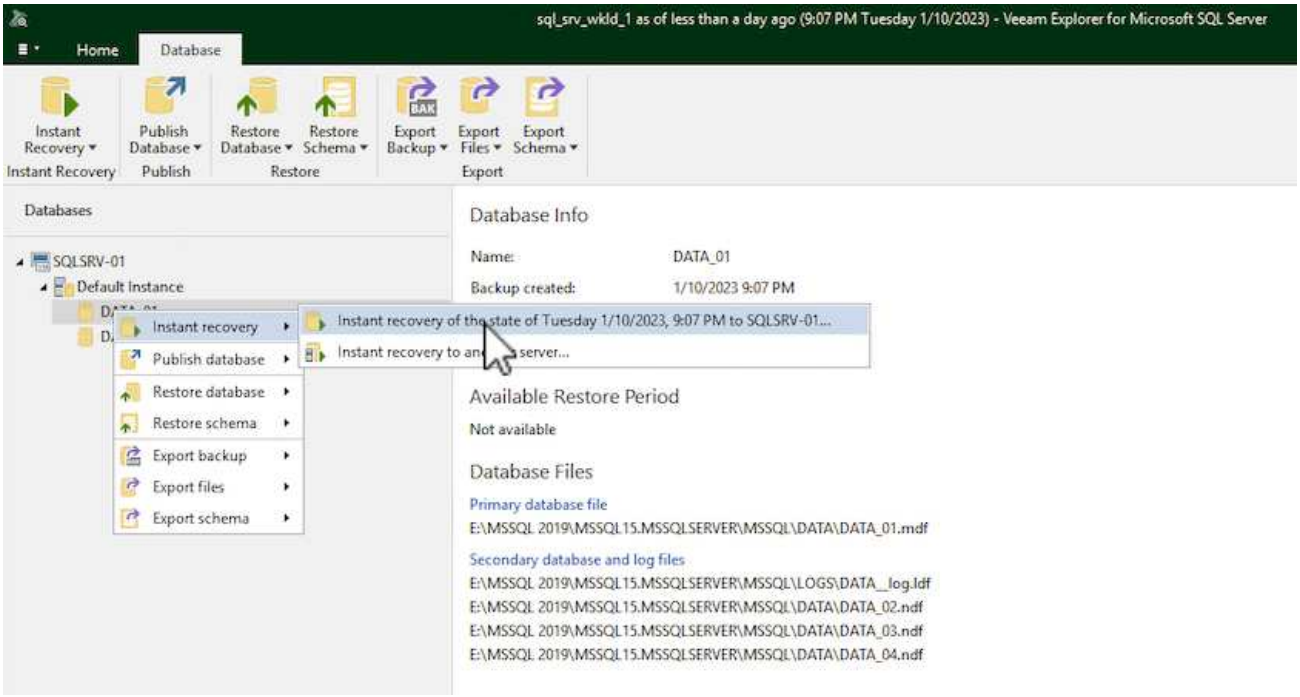
2. En el Asistente para restauración de bases de datos de Microsoft SQL Server, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.



3. Ingrese un **Motivo de restauración** si lo desea y luego, en la página Resumen, haga clic en el botón **Explorar** para iniciar Veeam Explorer para Microsoft SQL Server.

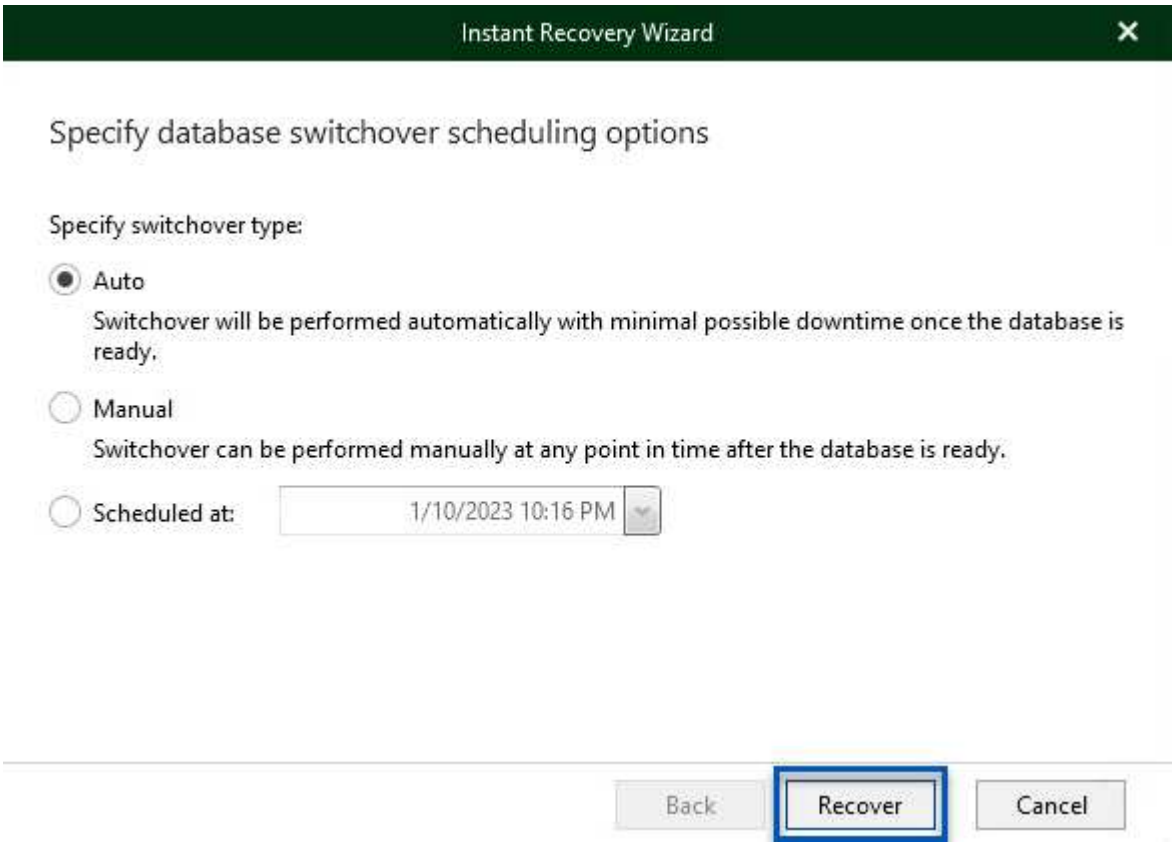


4. En Veeam Explorer, expanda la lista de instancias de base de datos, haga clic derecho y seleccione **Recuperación instantánea** y luego el punto de restauración específico al que recuperar.

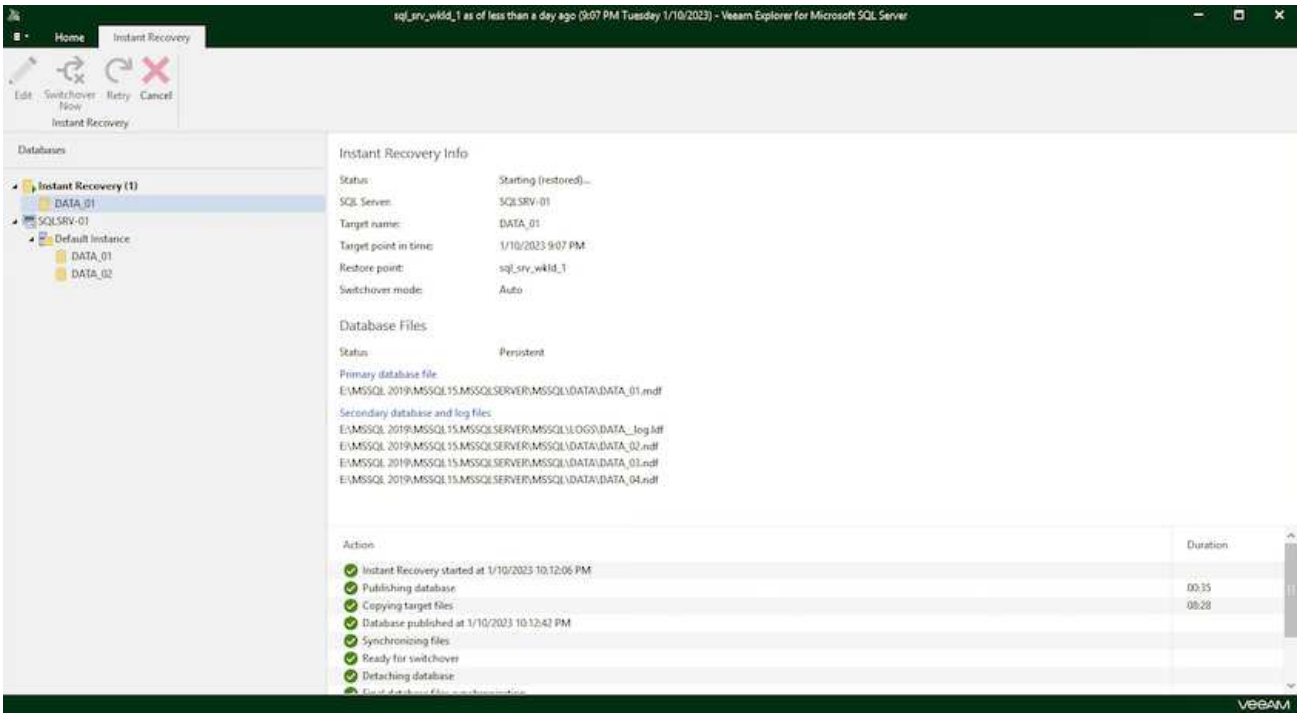


5. En el Asistente de recuperación instantánea, especifique el tipo de cambio. Esto puede hacerse de

forma automática, con un tiempo de inactividad mínimo, de forma manual o en un momento específico. 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 el "Guía del usuario de Veeam Explorers" .

Restaurar bases de datos de Oracle con Veeam Explorer

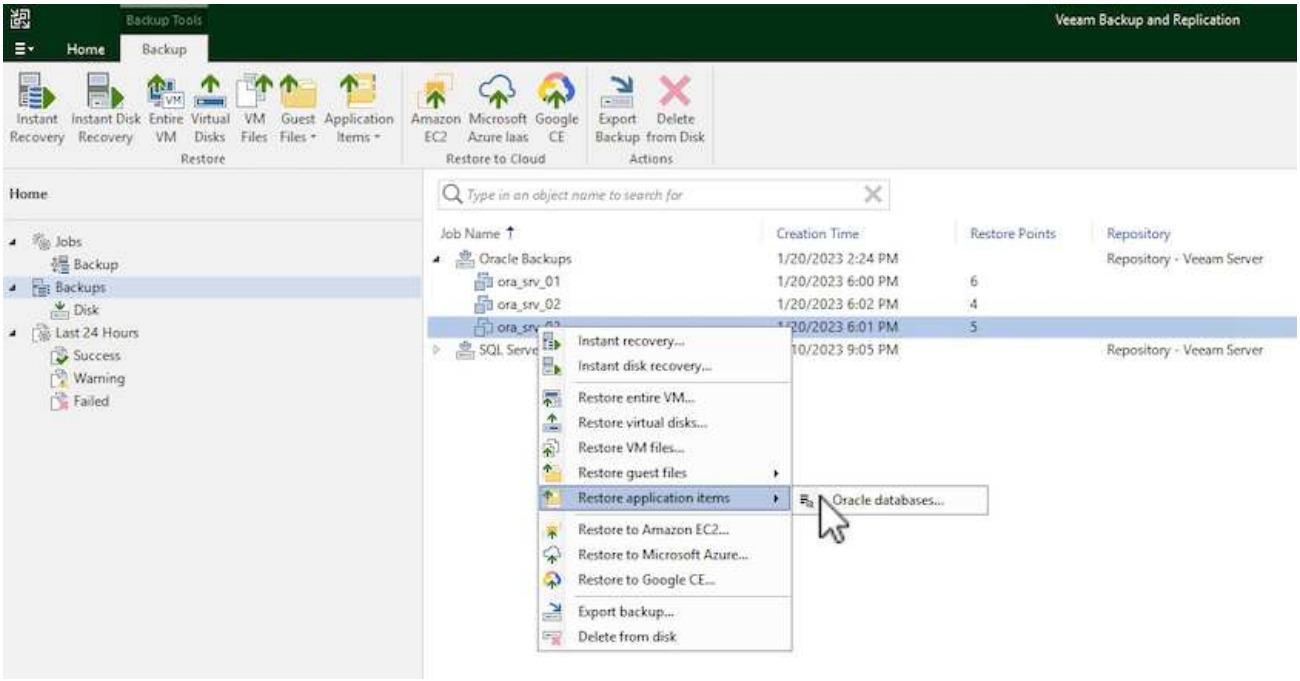
Veeam Explorer para bases de datos Oracle brinda la capacidad de realizar una restauración de base de datos Oracle estándar o una restauración ininterrumpida mediante Instant Recovery. También admite la publicación de bases de datos para un acceso rápido, la recuperación de bases de datos de Data Guard y restauraciones desde 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 de Oracle en el "Guía del usuario de Veeam Explorers" .

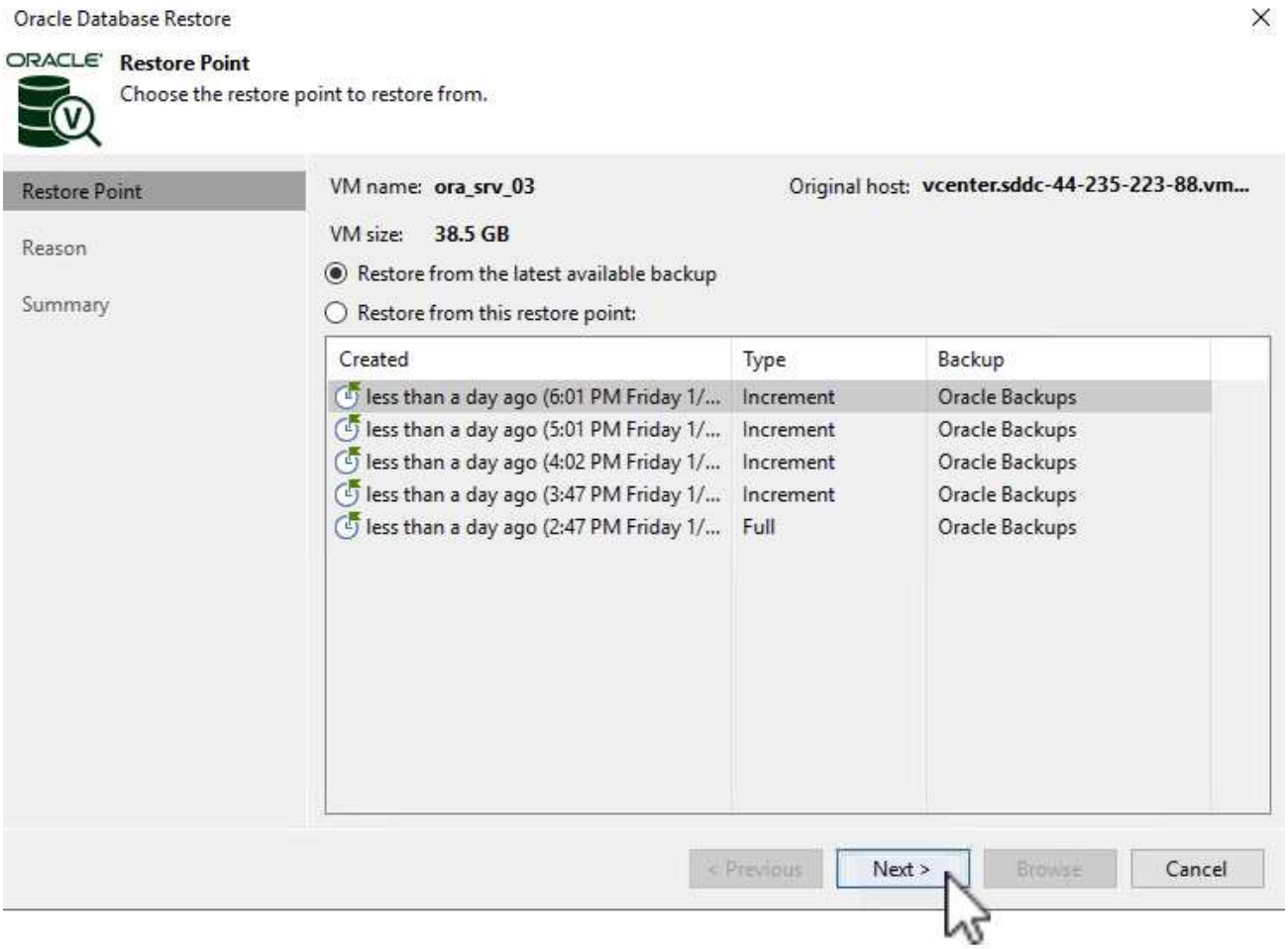
▼ **Restaurar la base de datos de Oracle con Veeam Explorer**

En esta sección se cubre la restauración de una base de datos Oracle a un servidor diferente utilizando Veeam Explorer.

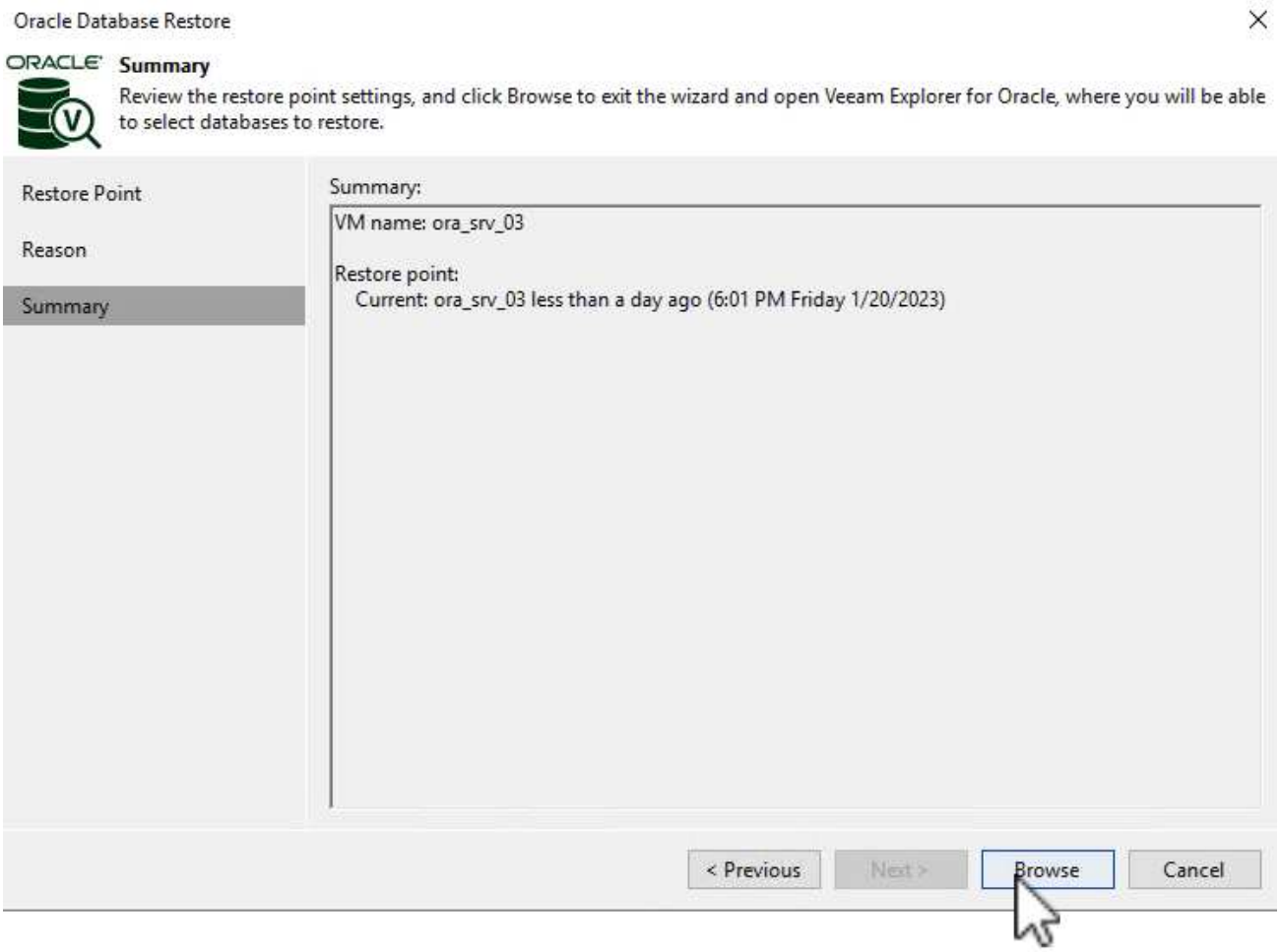
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de Oracle, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de la aplicación** y luego **Bases de datos Oracle…**.



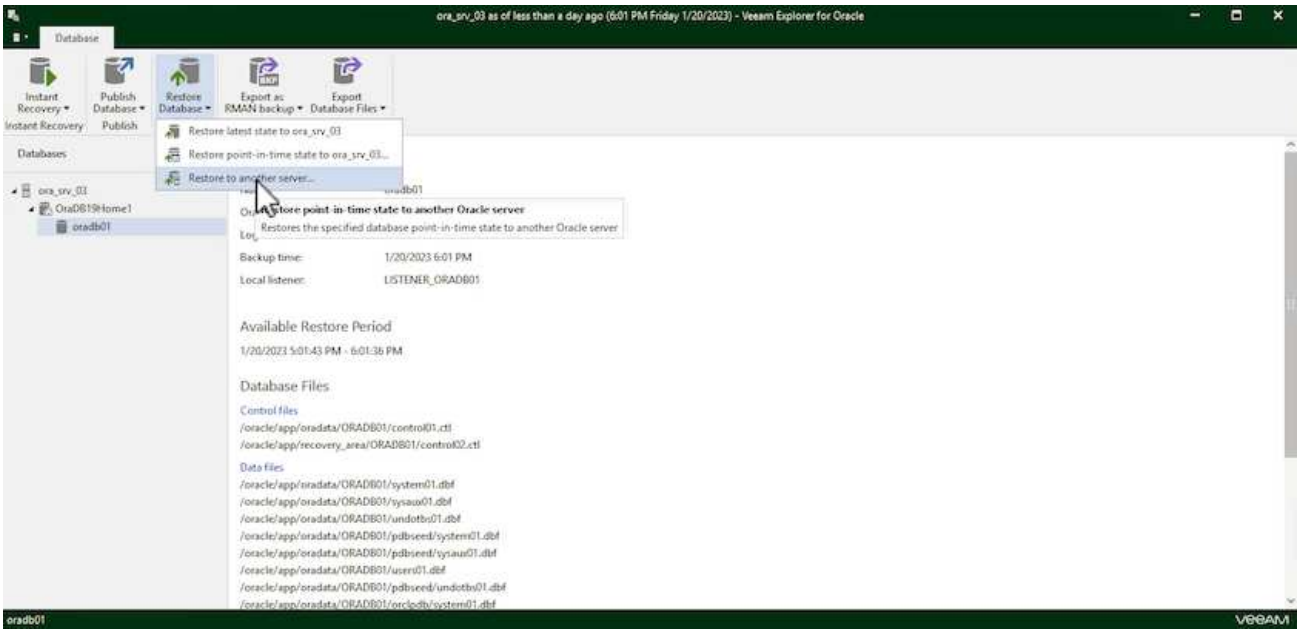
2. En el Asistente de restauración de base de datos de Oracle, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.



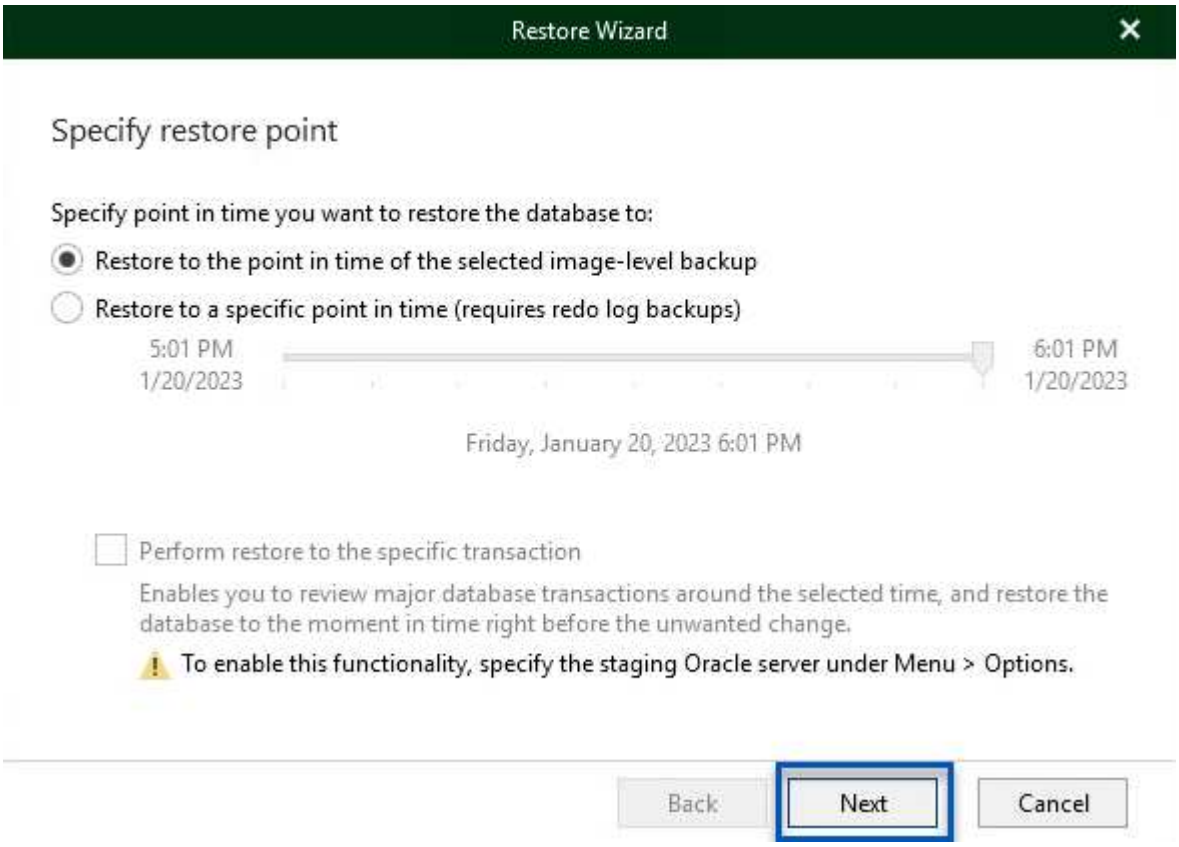
3. Ingrese un **Motivo de restauración** si lo desea y luego, en la página Resumen, haga clic en el botón **Explorar** para iniciar Veeam Explorer para Oracle.



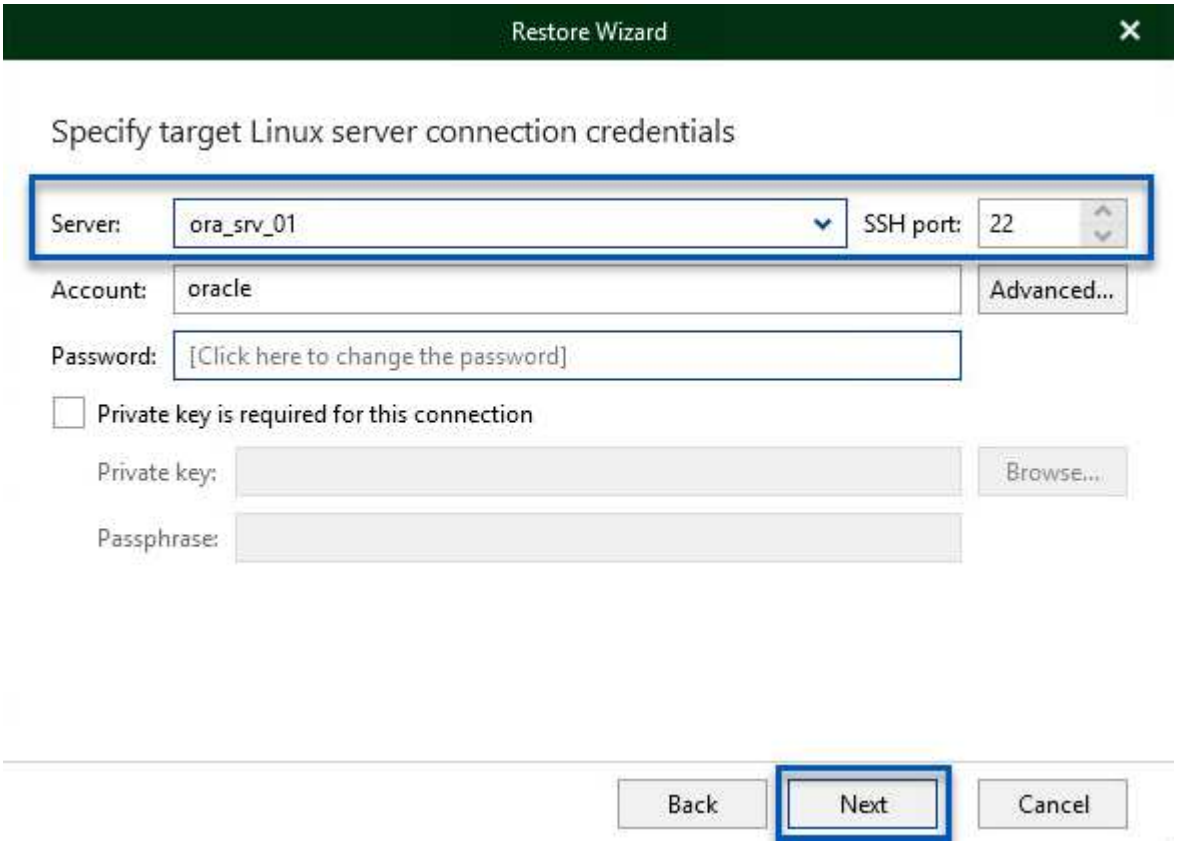
4. En Veeam Explorer, expanda la lista de instancias de base de datos, haga clic en la base de datos que desea restaurar y luego, en el menú desplegable **Restaurar base de datos** en la parte superior, seleccione **Restaurar a otro servidor…**.



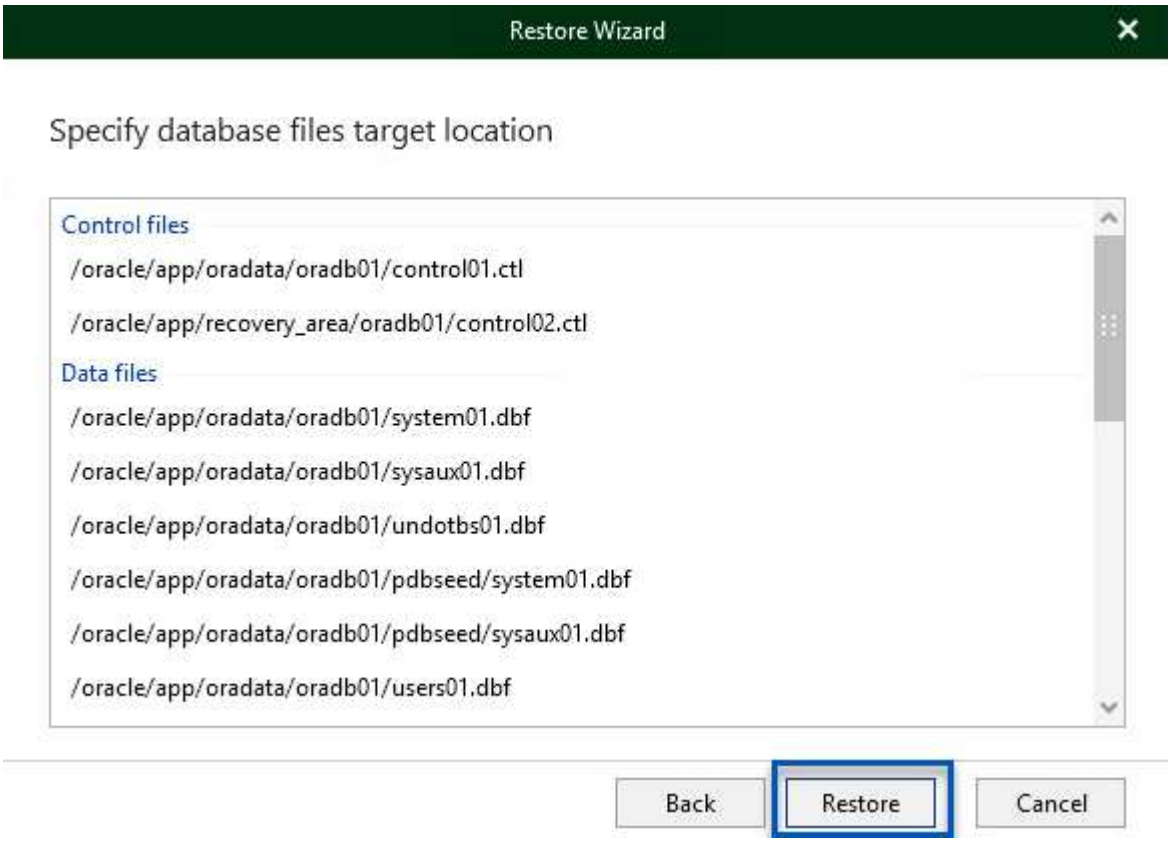
5. En el Asistente de restauración, especifique el punto de restauración desde el que desea restaurar y haga clic en **Siguiente**.



6. Especifique el servidor de destino en el 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 la base de datos y haga clic en el botón **Restaurar** para iniciar el proceso de restauración.

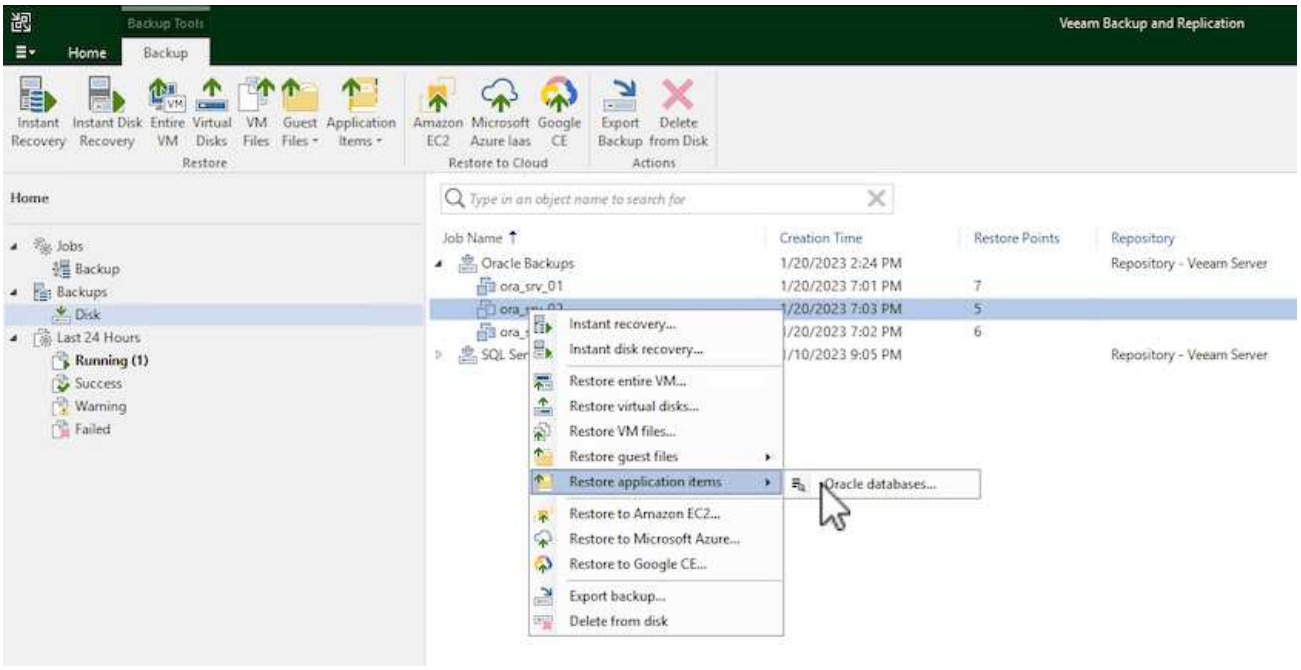


8. Una vez completada la recuperación de la base de datos, verifique que la base de datos Oracle se inicie correctamente en el servidor.

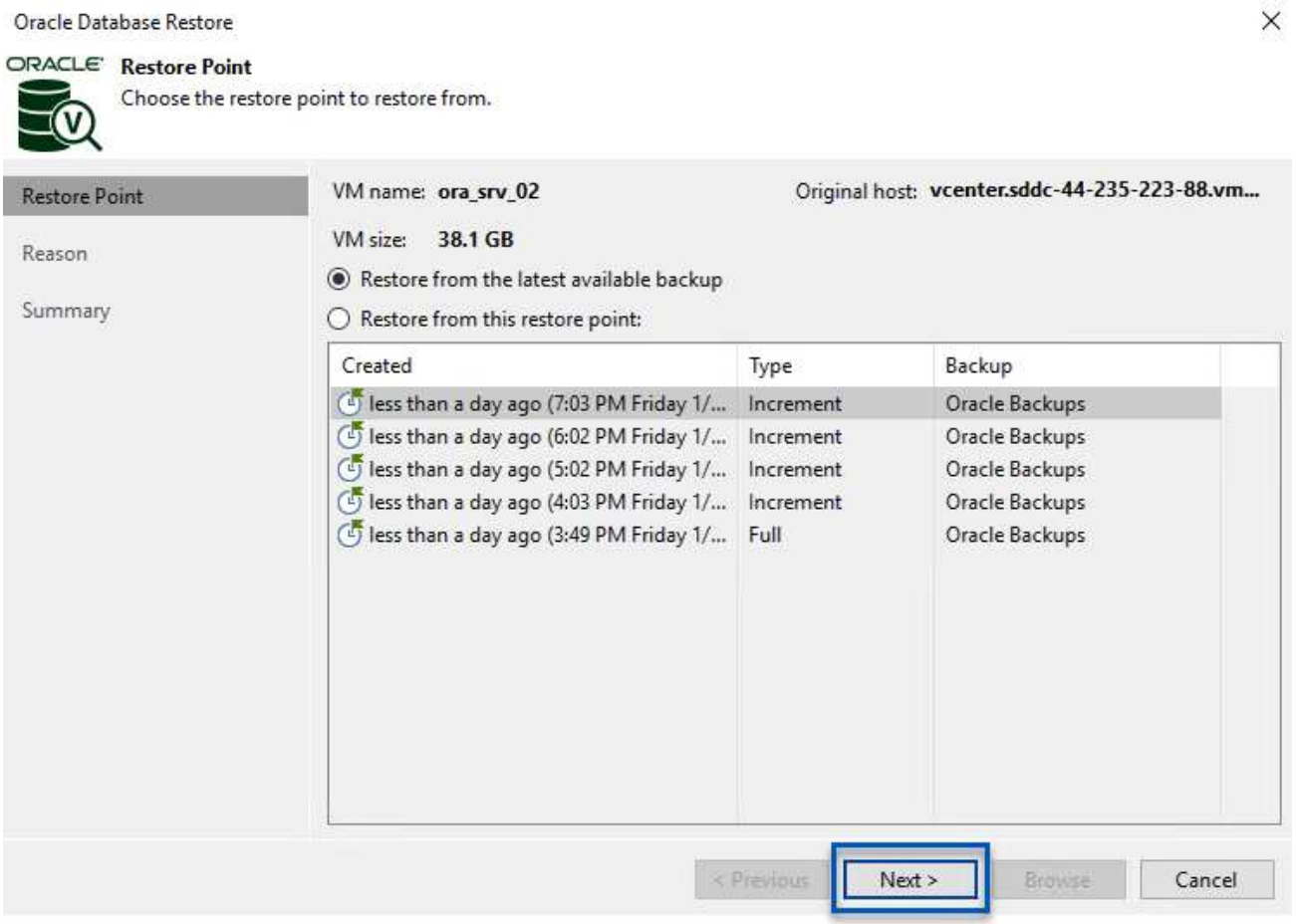
▼ **Publicar la base de datos Oracle en un servidor alternativo**

En esta sección se publica una base de datos en un servidor alternativo para 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 la aplicación** y luego **Bases de datos Oracle…**.

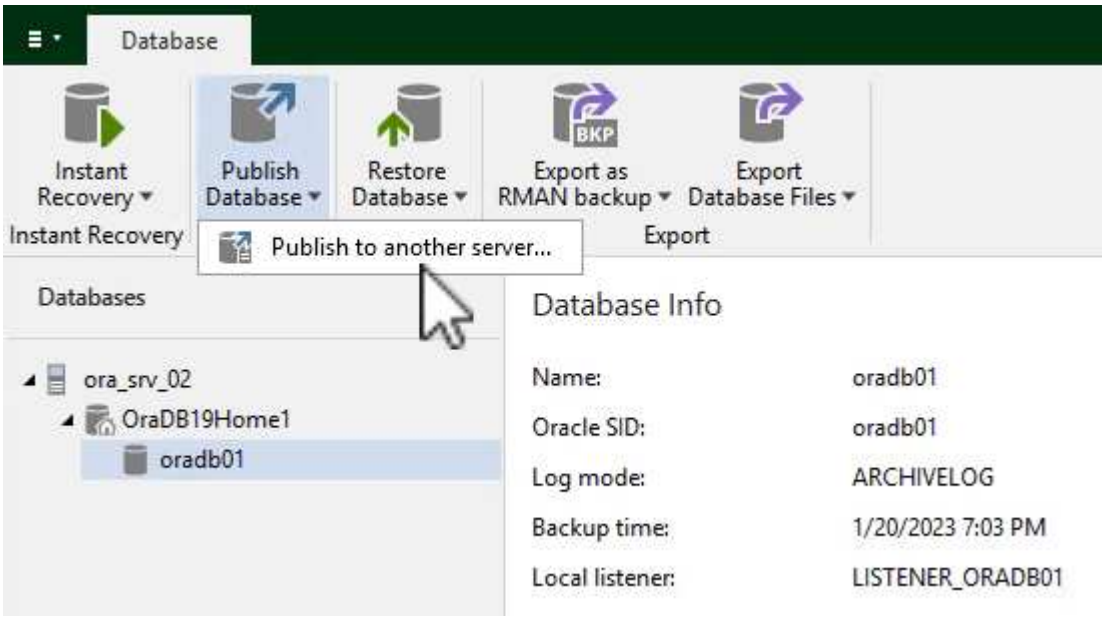


2. En el Asistente de restauración de base de datos de Oracle, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.

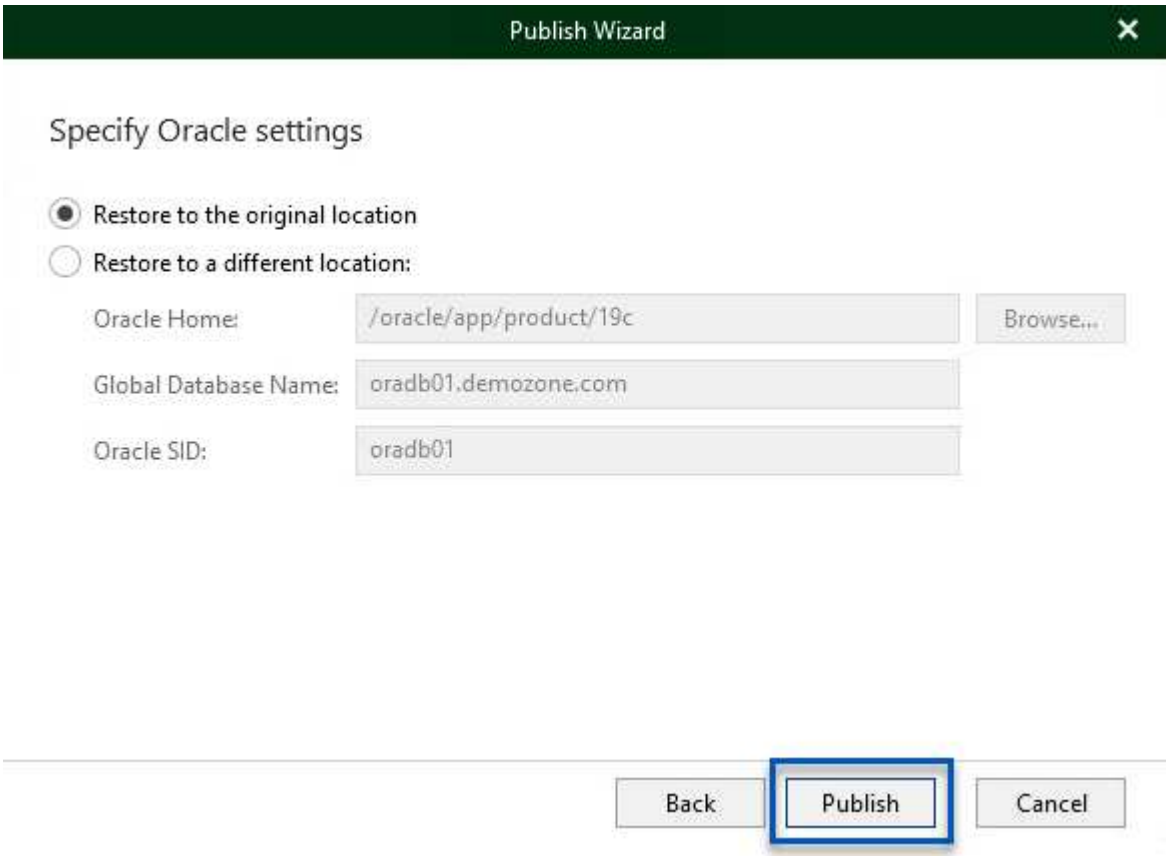


3. Ingrese un **Motivo de restauración** si lo desea y luego, en la página Resumen, haga clic en el botón **Explorar** para iniciar Veeam Explorer para Oracle.

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…**.



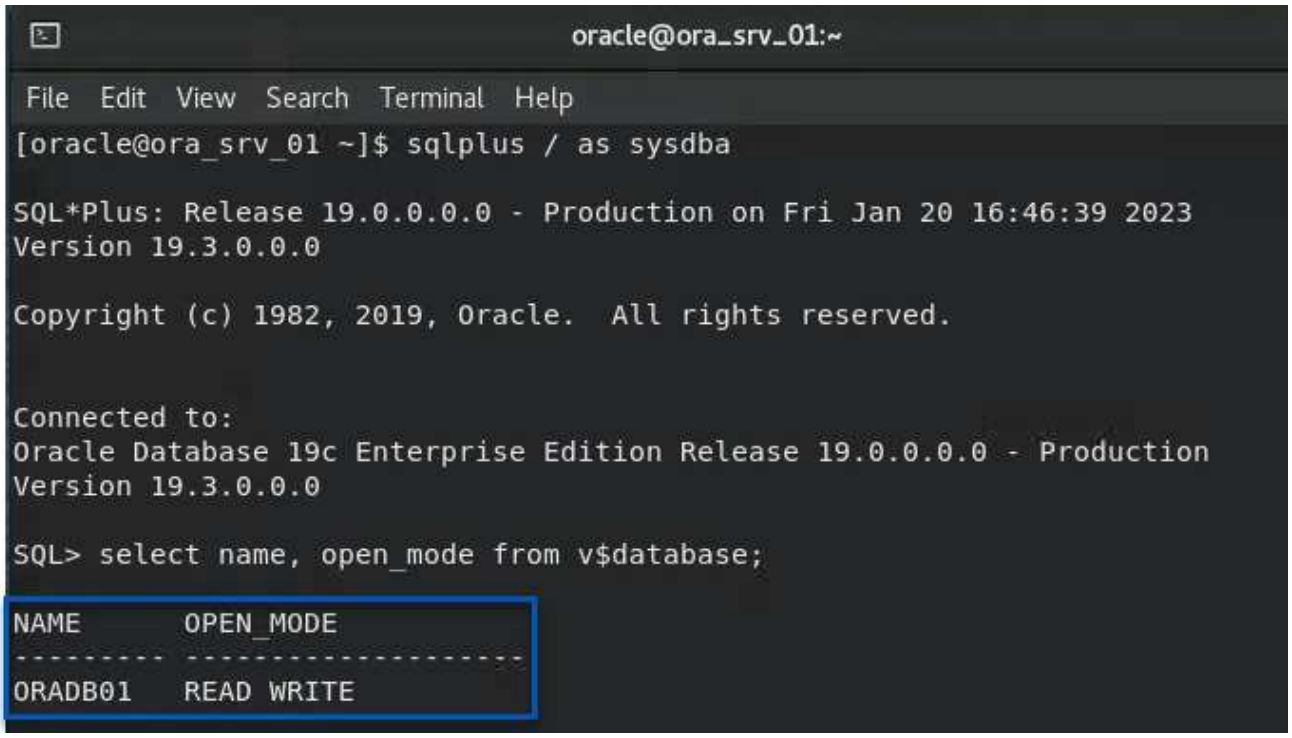
5. En el asistente de publicación, especifique el punto de restauración desde el cual desea publicar la base de datos y haga clic en **Siguiente**.
6. Por último, especifique la ubicación del sistema de archivos Linux de destino y haga clic en **Publicar** para comenzar el proceso de restauración.



7. Una vez completada la publicación, inicie sesión en el servidor de destino y ejecute los siguientes comandos para asegurarse de que la base de datos esté en ejecución:

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

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



Conclusión

VMware Cloud es una potente plataforma para ejecutar aplicaciones críticas 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 ayudar a protegerse contra las amenazas cibernéticas y la pérdida de datos. Al elegir una solución de protección de datos confiable y sólida, las empresas pueden estar seguras de que sus datos críticos están seguros y protegidos, pase lo que pase.

El caso de uso presentado en esta documentación se centra en tecnologías de protección de datos probadas que resaltan la integración entre NetApp, VMware y Veeam. FSx ONTAP se admite como almacén de datos NFS complementario para VMware Cloud en AWS y se utiliza para todos los datos de aplicaciones y máquinas virtuales. Veeam Backup & Replication es una solución integral de protección de datos diseñada para ayudar a las empresas a mejorar, automatizar y optimizar sus procesos de respaldo y recuperación. Veeam se utiliza junto con los volúmenes de destino de respaldo iSCSI, alojados en FSx ONTAP, para brindar una solución de protección de datos segura y fácil de administrar para los datos de aplicaciones que residen en VMware Cloud.

Información adicional

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

- "Guía del usuario de FSx 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 ONTAP y VMC (AWS VMware Cloud)

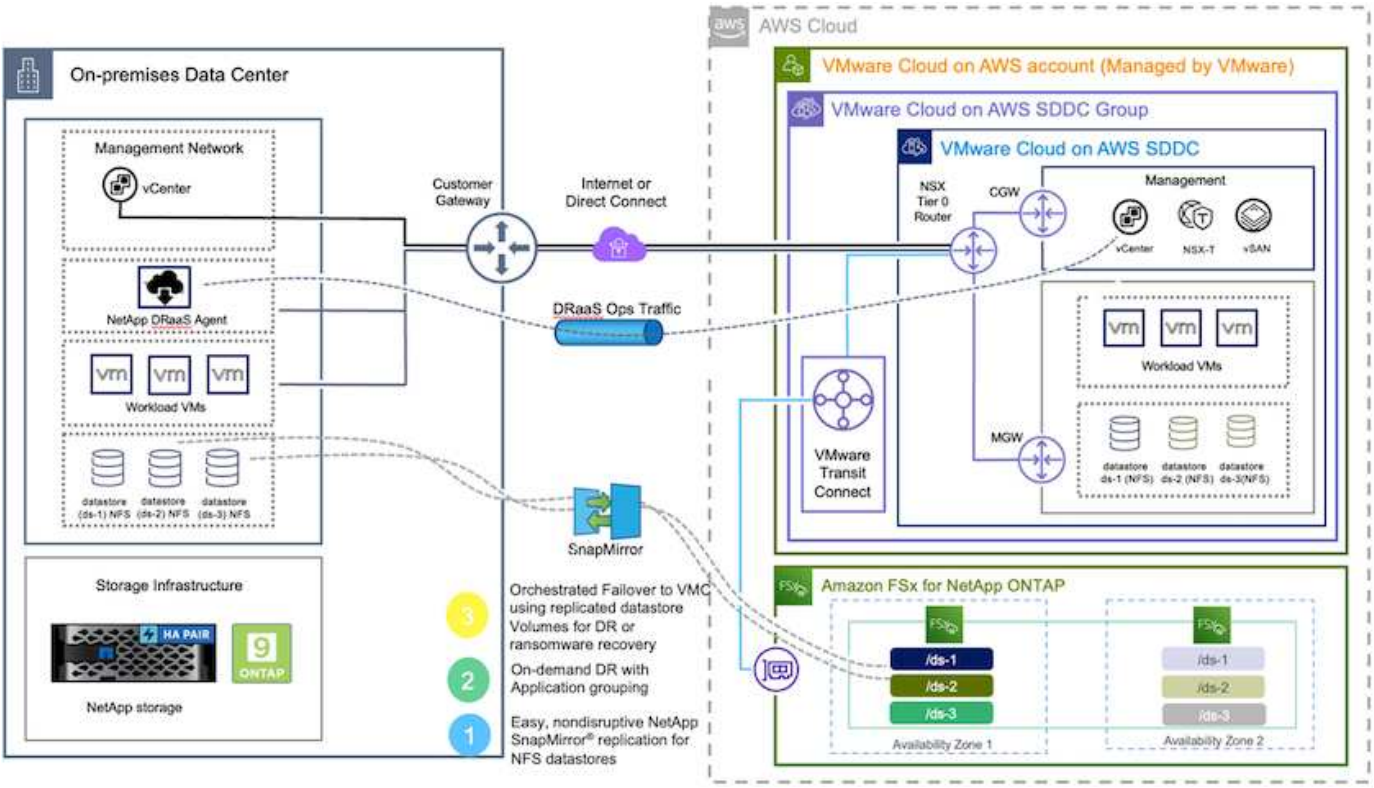
Disaster Recovery Orchestrator (DRO, una solución con script e interfaz de usuario) se puede utilizar para recuperar sin problemas cargas de trabajo replicadas desde las instalaciones locales a FSx ONTAP. DRO automatiza la recuperación desde el nivel de SnapMirror , mediante el registro de máquinas virtuales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

Niyaz Mohamed, NetApp

Descripción general

La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos (por ejemplo, ransomware). Con la tecnología NetApp SnapMirror , las cargas de trabajo locales de VMware se pueden replicar en FSx ONTAP que se ejecuta en AWS.

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



Implementar y configurar VMware Cloud en AWS

"VMware Cloud en AWS"Proporciona una experiencia nativa de la nube 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 una nube privada virtual (VPC) de Amazon y proporciona una pila VMware completa (incluido vCenter Server), redes definidas por software NSX-T, 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 los pasos a continuación"enlace" . También se puede utilizar un conjunto de luces piloto para fines de DR.

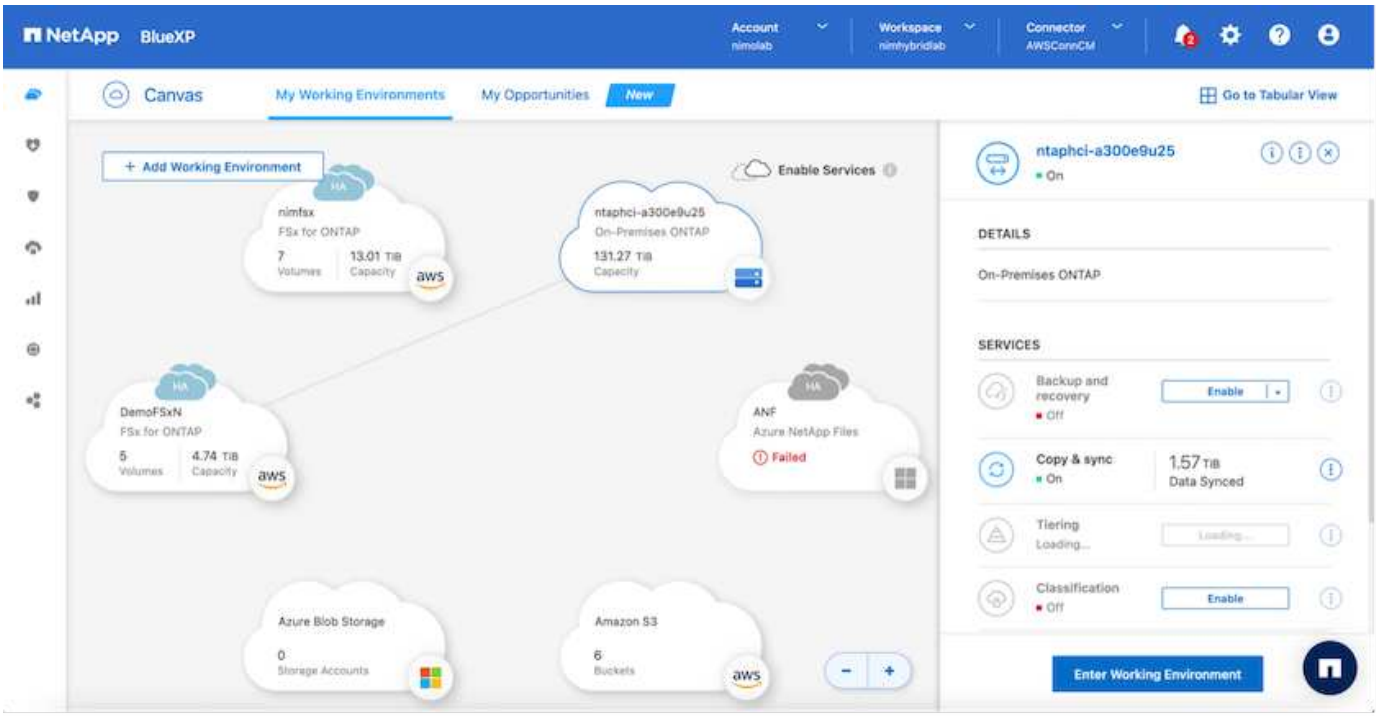
En la versión inicial, DRO admite un grupo de luces piloto existente. La creación de SDDC a pedido estará disponible en una próxima versión.

Aprovisionar y configurar FSx ONTAP

Amazon FSx ONTAP es un servicio completamente administrado que proporciona almacenamiento de archivos altamente confiable, escalable, de alto rendimiento y rico en funciones, creado sobre el popular sistema de archivos NetApp ONTAP . Siga los pasos a continuación"enlace" para aprovisionar y configurar FSx ONTAP.

Implementar y configurar SnapMirror en FSx ONTAP

El siguiente paso es usar NetApp Console y descubrir la instancia de FSx ONTAP en AWS aprovisionada, y replicar los volúmenes de datastore deseados desde un entorno local a FSx ONTAP con la frecuencia adecuada y la retención de copias Snapshot de NetApp correspondiente:



Sigue los pasos que se indican en este enlace para configurar DRO. También puedes utilizar la CLI de ONTAP de NetApp para programar la replicación siguiendo este enlace.

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

Instalación de DRO

Para comenzar a utilizar DRO, utilice el sistema operativo Ubuntu en una instancia EC2 o máquina virtual designada para asegurarse de cumplir con los requisitos previos. Luego instala el paquete.

Prerrequisitos

- Asegúrese de que exista conectividad con los sistemas de almacenamiento y vCenter de origen y destino.
- La resolución de DNS debe estar implementada si está utilizando nombres DNS. De lo contrario, debe utilizar direcciones IP para vCenter y los sistemas de almacenamiento.
- Crea un usuario con permisos de root. También puedes usar sudo con una instancia EC2.

Requisitos de OS

- Ubuntu 20.04 (LTS) con un mínimo de 2 GB y 4 vCPU
- Los siguientes paquetes deben instalarse en la máquina virtual del agente designado:
  - Docker
  - Docker-compose
  - Jq

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

El `deploy.sh` El script ejecuta todos los requisitos previos necesarios.

Instalar 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 una VPC de AWS.

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

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

3. Navegue hasta el directorio y ejecute el script de implementación de la siguiente manera:

```
sudo sh deploy.sh
```

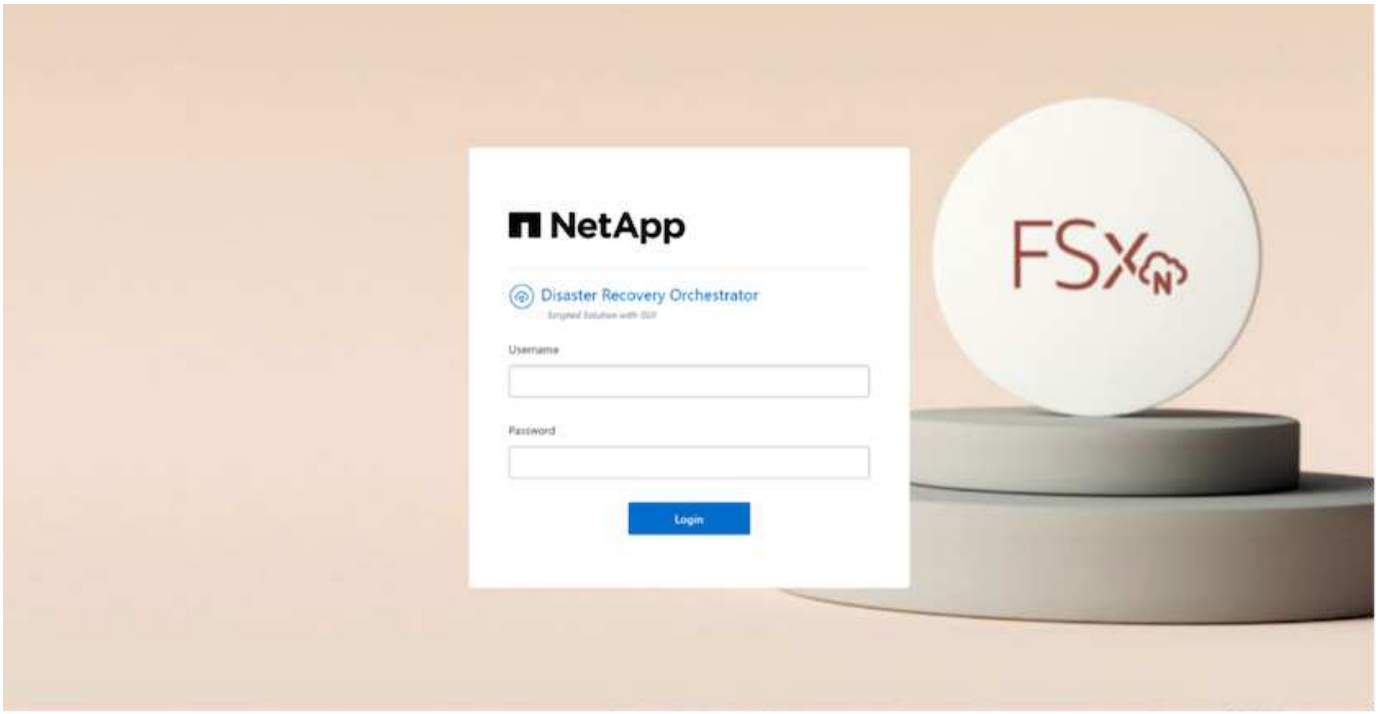
4. Acceda a la interfaz de usuario mediante:

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

con las siguientes credenciales predeterminadas:

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

La contraseña se puede cambiar utilizando la opción “Cambiar contraseña”.



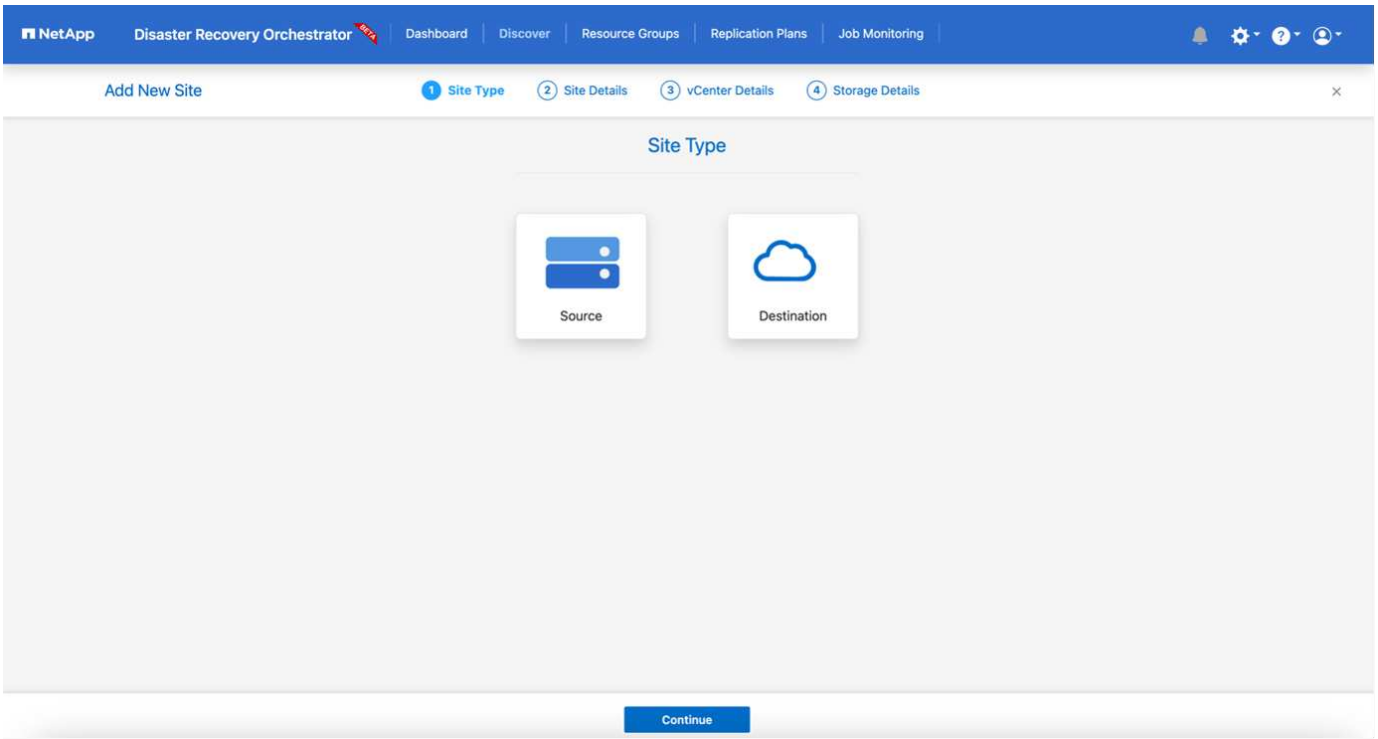
Configuración de DRO

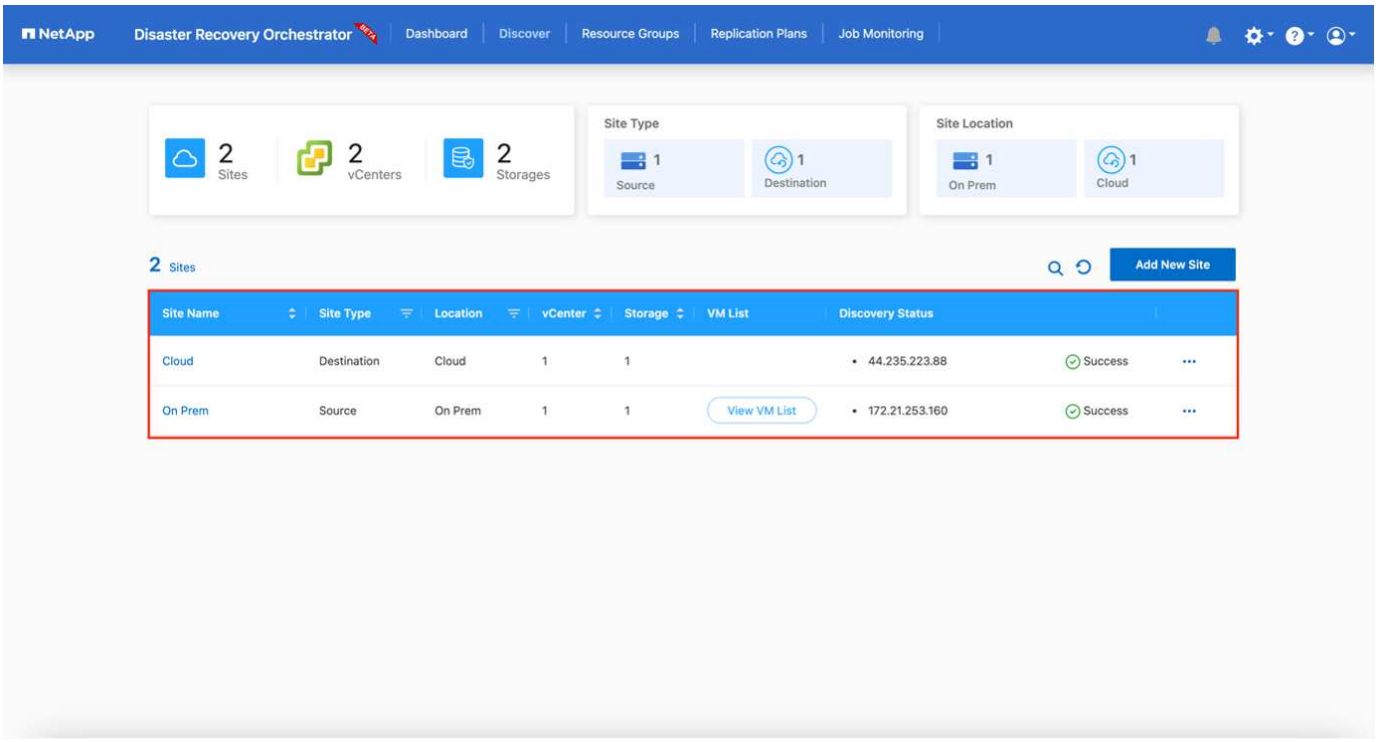
Una vez que FSx ONTAP y VMC se hayan configurado correctamente, puede comenzar a configurar DRO para automatizar la recuperación de cargas de trabajo locales en VMC mediante el uso de copias SnapMirror de solo lectura en FSx ONTAP.

NetApp recomienda implementar el agente DRO en AWS y también en la misma VPC donde se implementa FSx ONTAP (también se puede conectar entre pares), de modo que el agente DRO pueda comunicarse a través de la red con sus componentes locales, así como con los recursos FSx ONTAP y VMC.

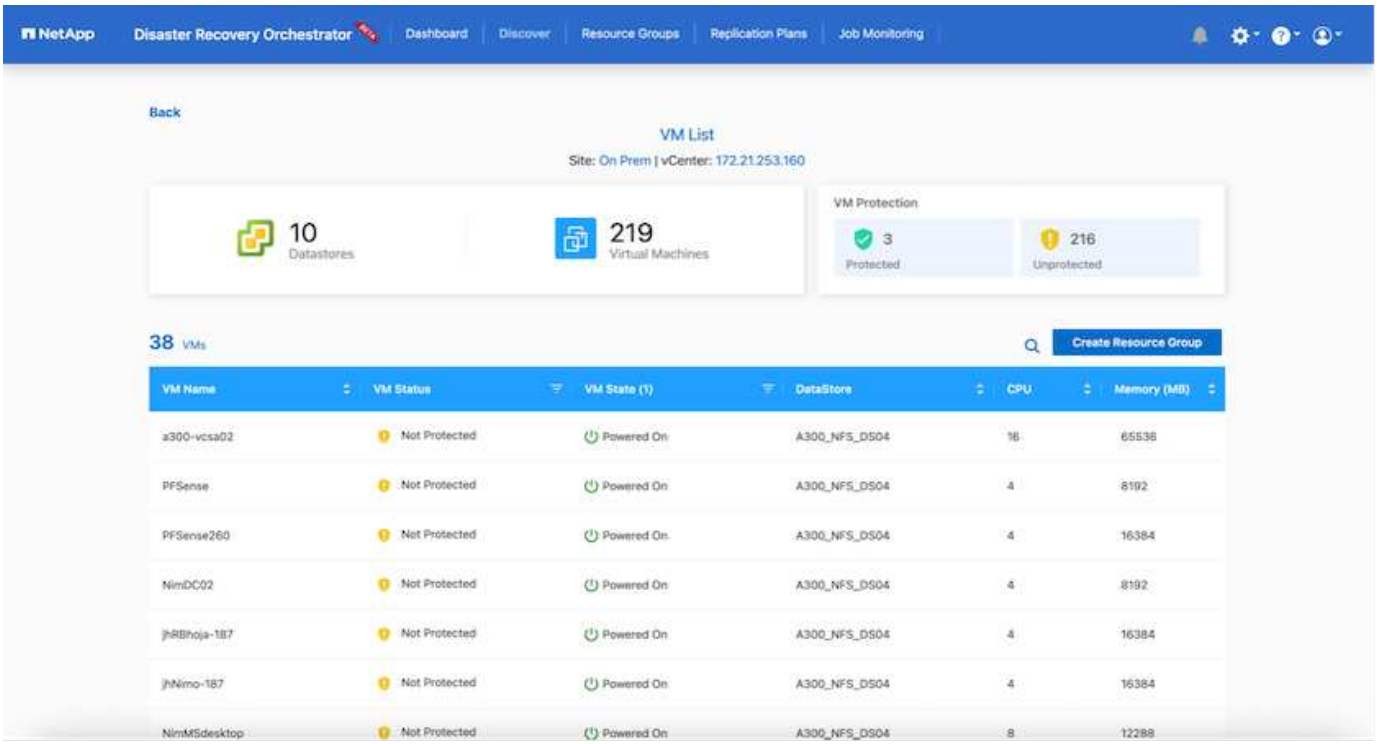
El primer paso es descubrir y agregar los recursos locales y en la nube (tanto vCenter como almacenamiento) a DRO. Abra DRO en un navegador compatible y use el nombre de usuario y la contraseña predeterminados (admin/admin) y agregue sitios. También se pueden agregar sitios usando la opción Descubrir. Agregue las siguientes plataformas:

- En las instalaciones
  - vCenter local
  - Sistema de almacenamiento ONTAP
- Nube
  - Centro de VMC
  - FSx ONTAP





Una vez agregado, DRO realiza un descubrimiento automático y muestra las máquinas virtuales que tienen réplicas SnapMirror correspondientes desde el almacenamiento de origen a FSx ONTAP. DRO detecta automáticamente las redes y los grupos de puertos utilizados por las máquinas virtuales y los completa.



El siguiente paso es agrupar las máquinas virtuales necesarias en grupos funcionales para que sirvan como grupos de recursos.

Agrupaciones de recursos

Una vez agregadas las plataformas, puedes agrupar las máquinas virtuales que deseas recuperar en grupos de recursos. Los grupos de recursos DRO le 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 durante la recuperación.

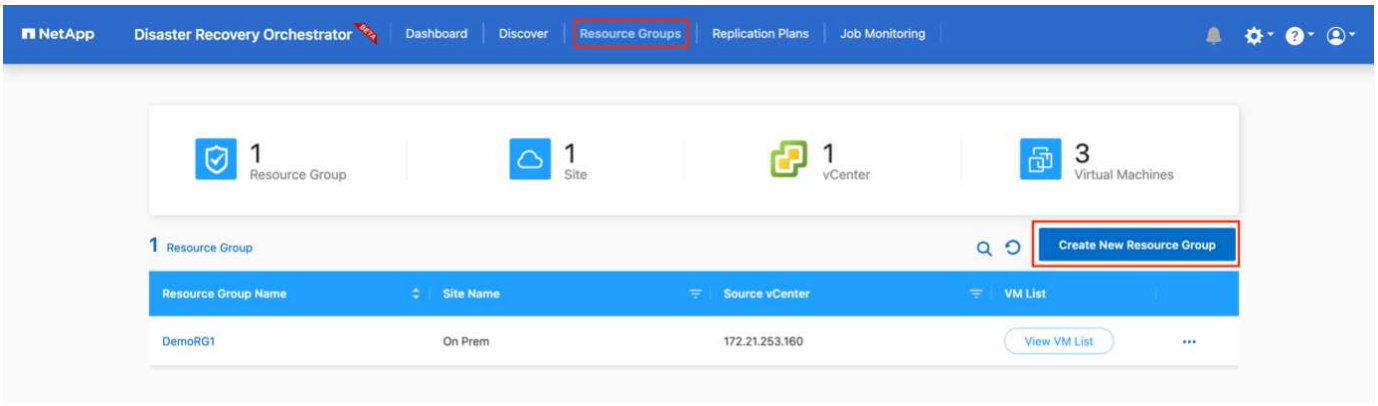
Para comenzar a crear grupos de recursos, complete los siguientes pasos:

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 el menú desplegable y haga clic en **Crear**.
3. Proporcione **Detalles del grupo de recursos** y haga clic en **Continuar**.
4. Seleccione las máquinas virtuales adecuadas mediante la opción de búsqueda.
5. Seleccione el orden de arranque y el retraso de arranque (segundos) para las máquinas virtuales seleccionadas. Establezca el orden de la secuencia de encendido seleccionando cada VM y configurando su prioridad. Tres es el valor predeterminado para todas las máquinas virtuales.

   Las opciones son las siguientes:

   1 – La primera máquina virtual en encenderse 3 – Predeterminado 5 – La última máquina virtual en encenderse

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

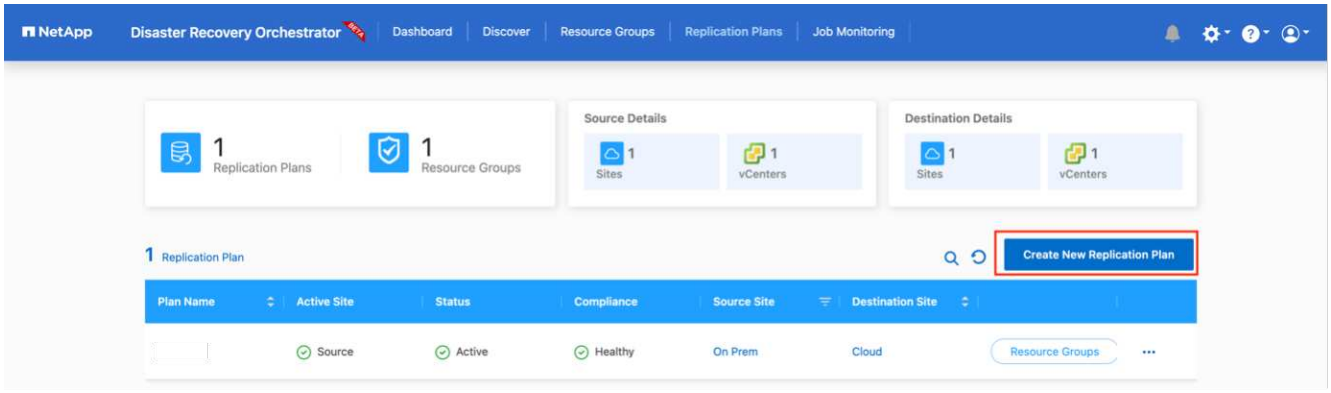


Planes de replicación

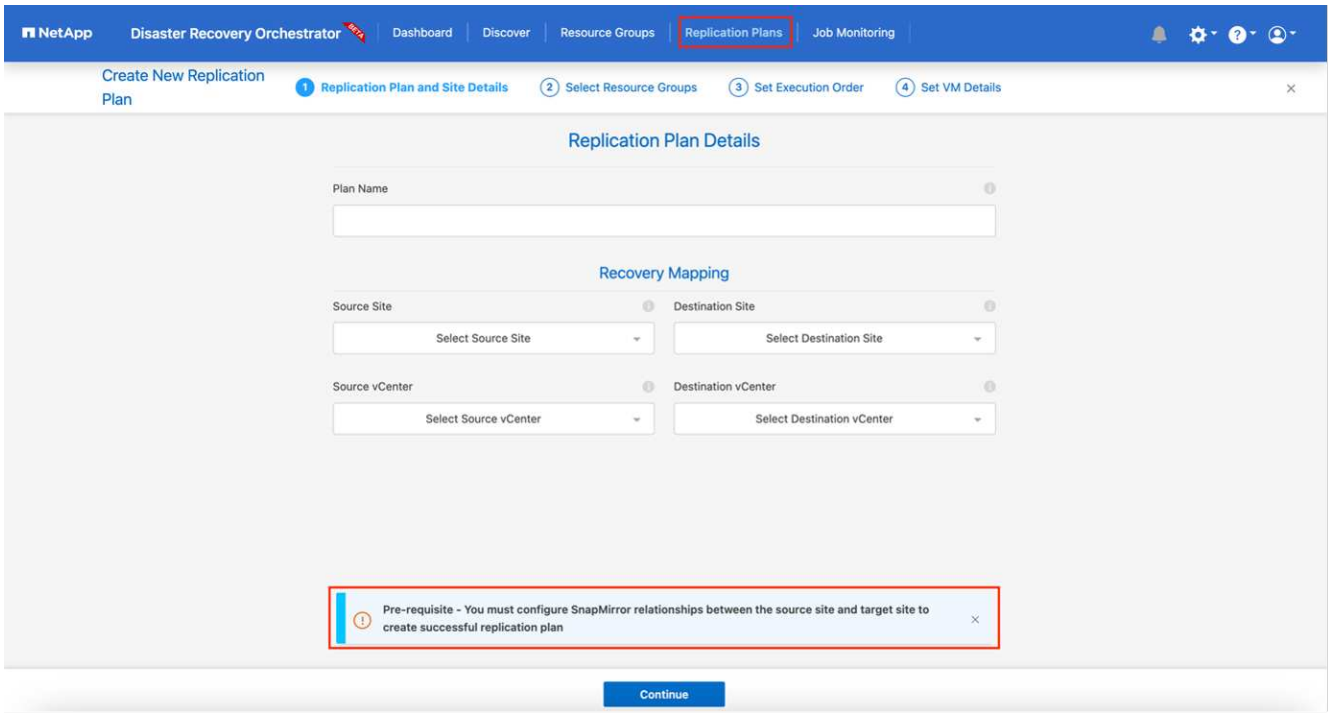
Necesita un plan para recuperar aplicaciones en caso de desastre. Seleccione las plataformas de vCenter de origen y destino del menú desplegable y elija los grupos de recursos que se incluirán en este plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones (por ejemplo, controladores de dominio, luego nivel 1, luego nivel 2, y así sucesivamente). A estos planes a veces también se les llama planos. Para definir el plan de recuperación, navegue a la pestaña **Plan de replicación** y haga clic en **Nuevo plan de replicación**.

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

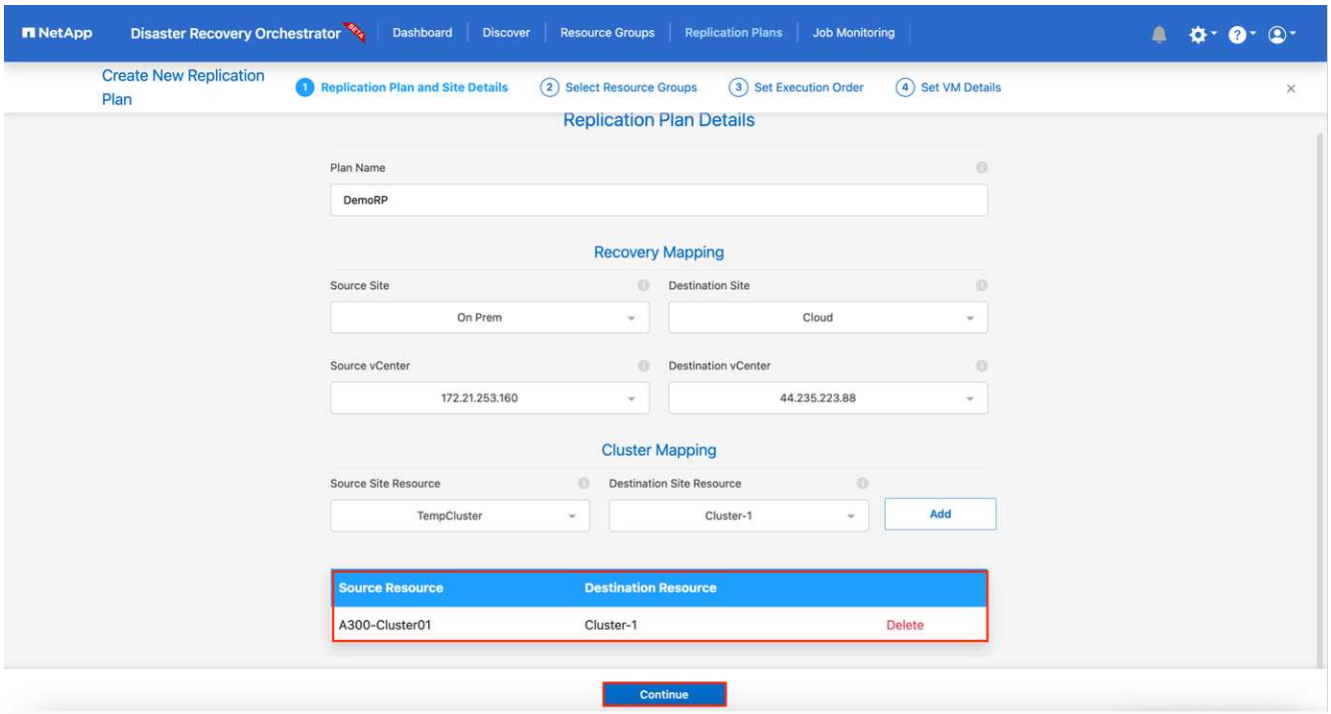
1. Acceda a **Planes de replicación** y haga clic en **Crear nuevo plan de replicación**.



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

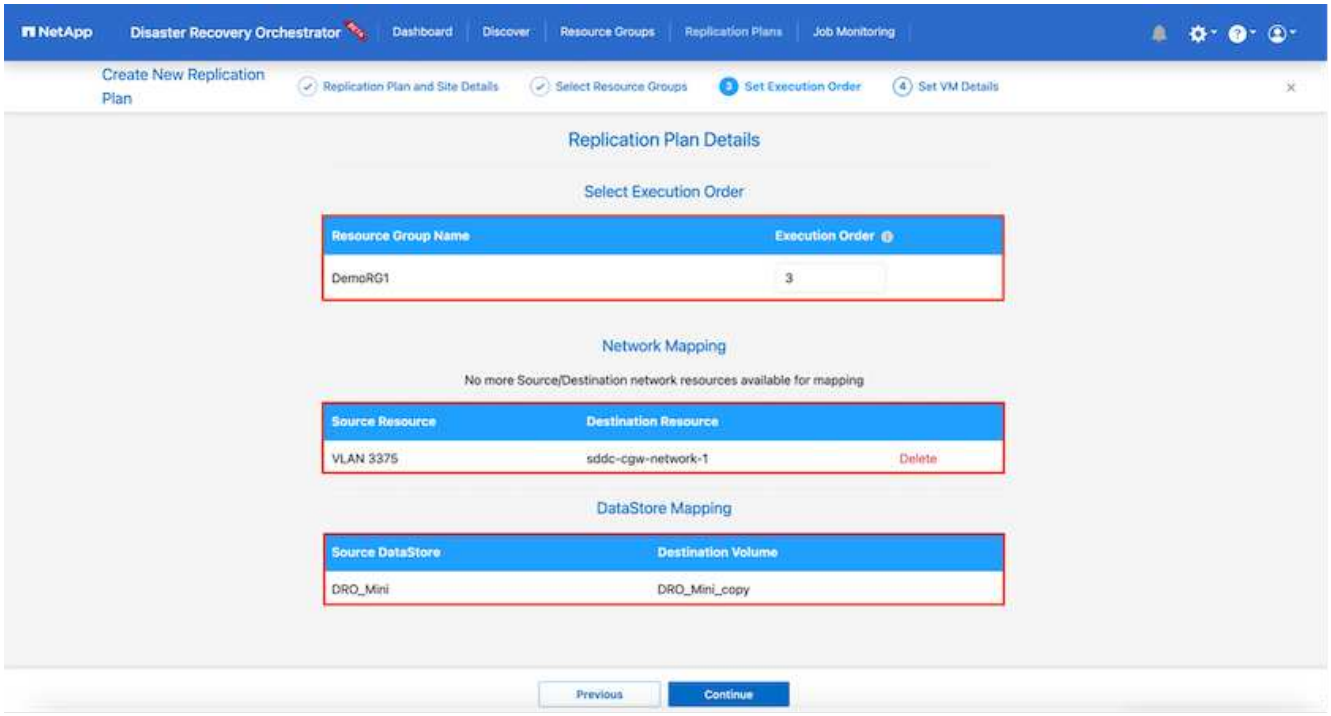


3. Una vez completado el mapeo de recuperación, seleccione el mapeo de clúster.

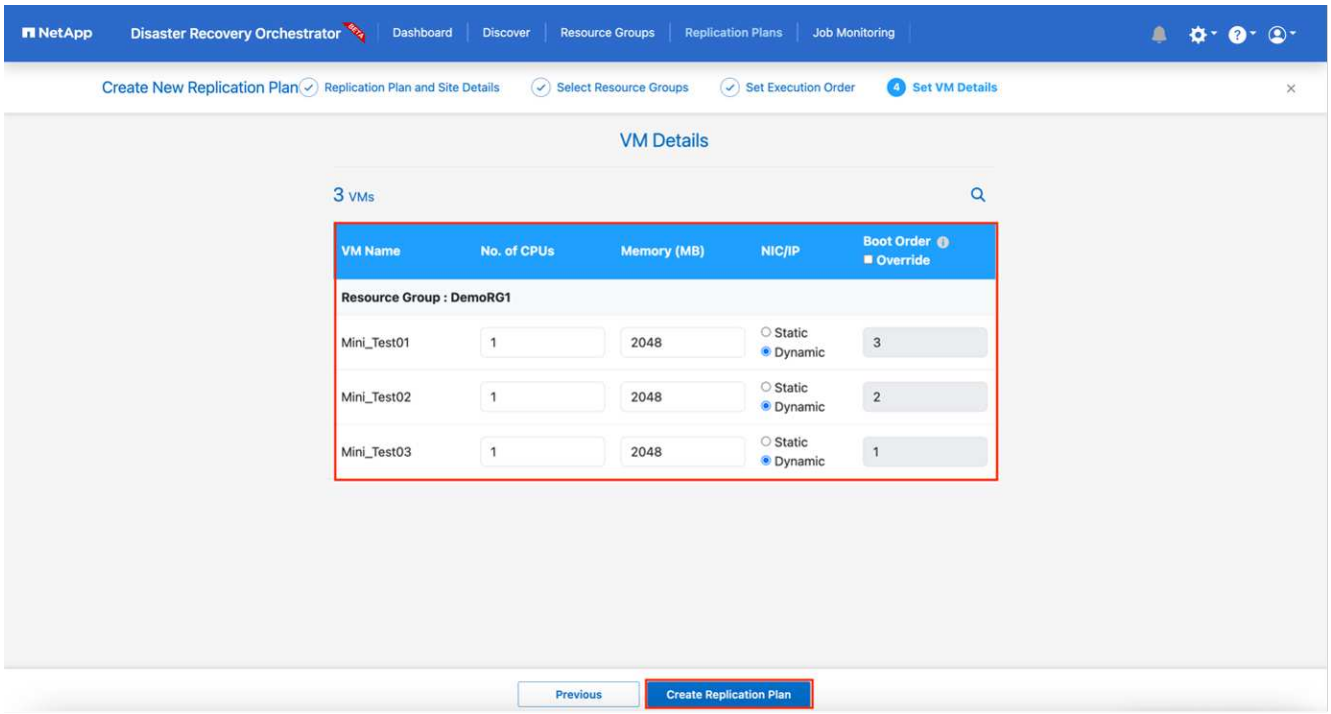


4. Seleccione **Detalles del grupo de recursos** y haga clic en **Continuar**.
5. Establecer el orden de ejecución para el grupo de recursos. Esta opción le permite seleccionar la secuencia de operaciones cuando existen múltiples grupos de recursos.
6. Una vez que haya terminado, seleccione la asignación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

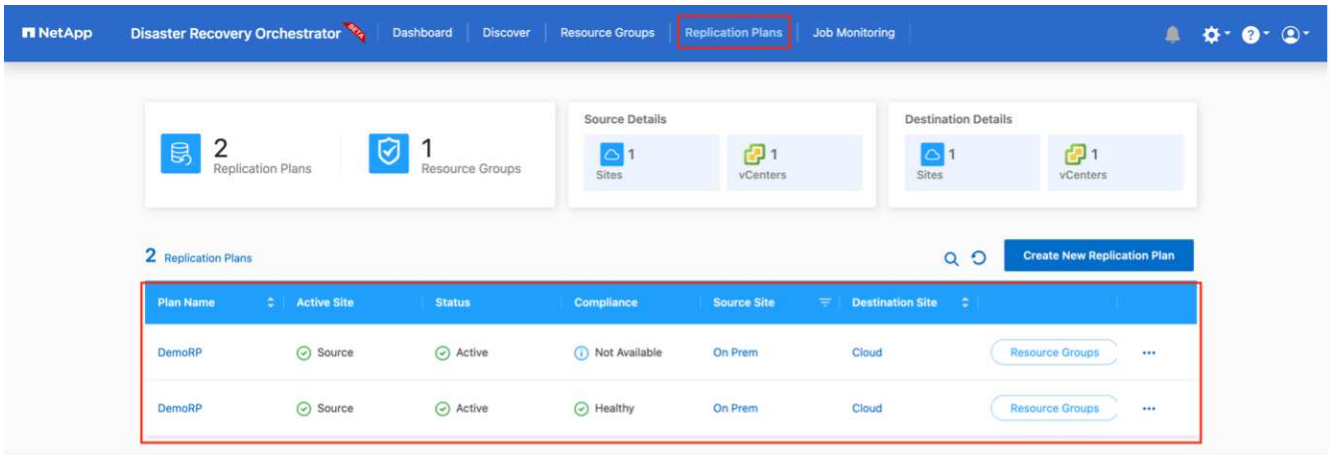
SnapMirror está en el nivel de volumen. Por lo tanto, todas las máquinas virtuales se replican en el destino de replicación. Asegúrese de seleccionar todas las máquinas virtuales que forman parte del almacén de datos. Si no se seleccionan, solo se procesan las máquinas virtuales que forman parte del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



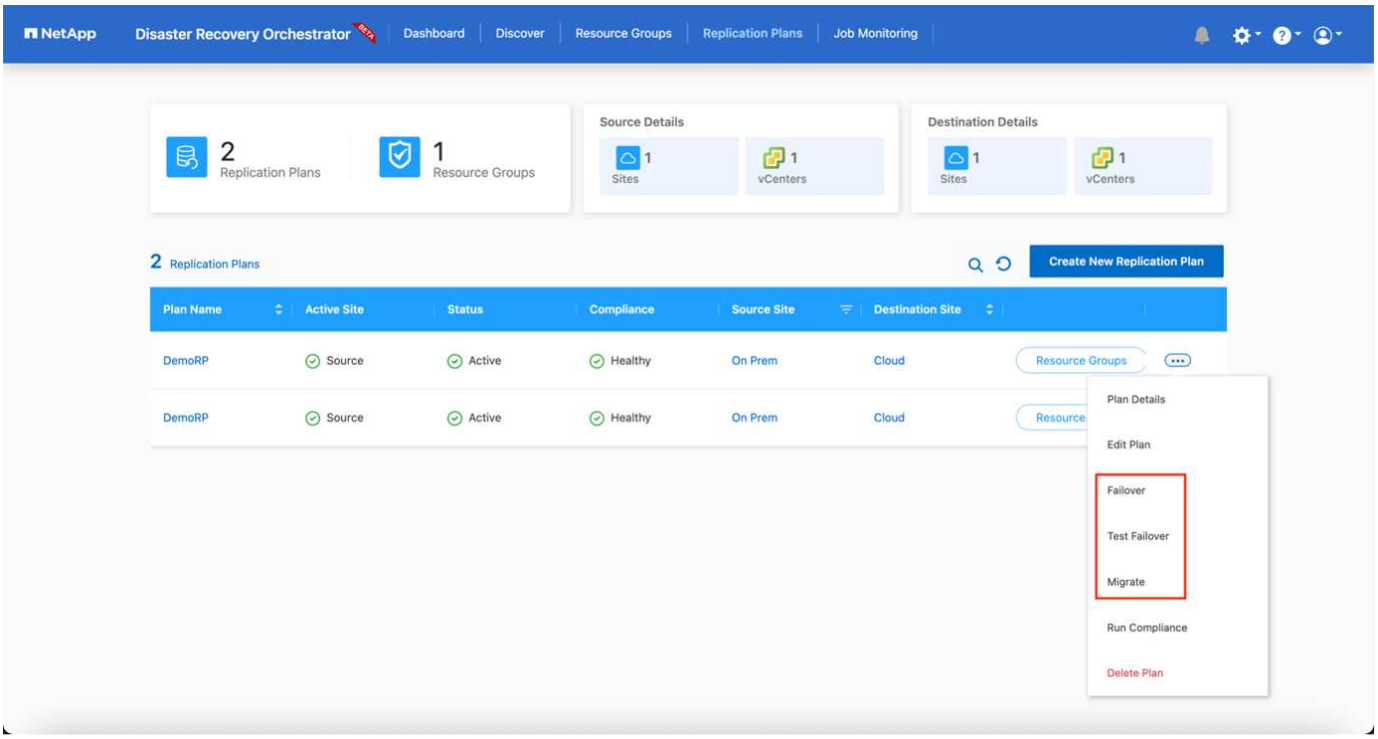
8. En los detalles de la máquina virtual, puede modificar opcionalmente el tamaño de los parámetros de CPU y RAM de la máquina virtual; esto puede ser muy útil al recuperar entornos grandes en clústeres de destino más pequeños o para realizar pruebas de recuperación ante desastres sin tener que aprovisionar una infraestructura VMware física uno a uno. Además, puede modificar el orden de arranque y el retraso de arranque (segundos) para todas las máquinas virtuales seleccionadas en los grupos de recursos. Hay una opción adicional para modificar el orden de arranque si se requieren cambios en los seleccionados durante la selección del orden de arranque del grupo de recursos. De forma predeterminada, se utiliza el orden de arranque seleccionado durante la selección del grupo de recursos; sin embargo, cualquier modificación se puede realizar en esta etapa.

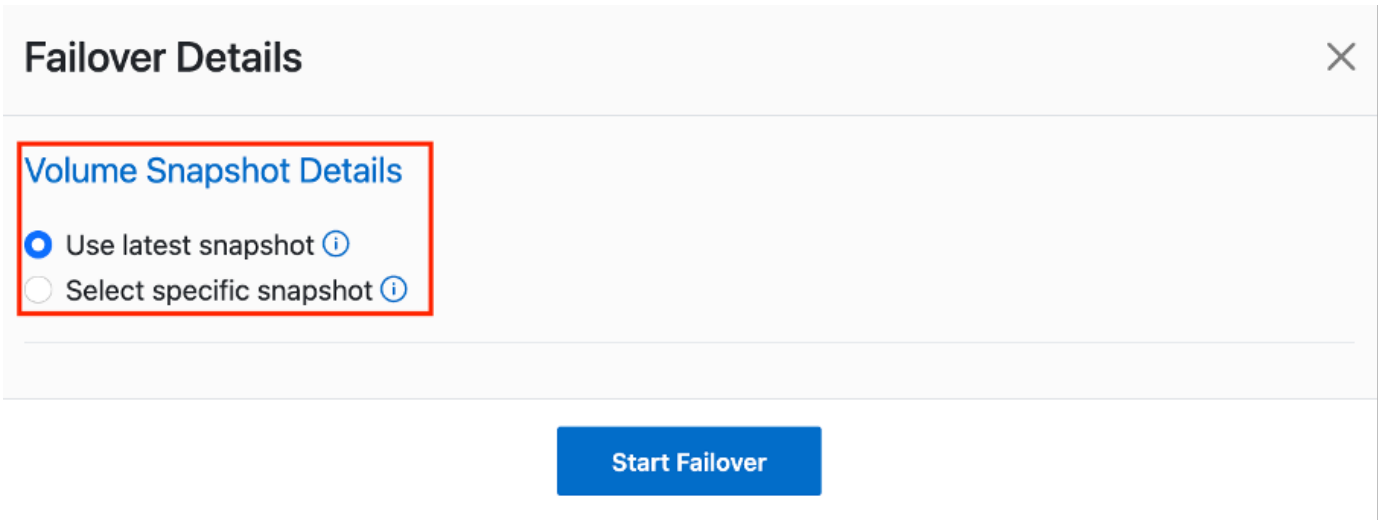


9. Haga clic en **Crear plan de replicación**.

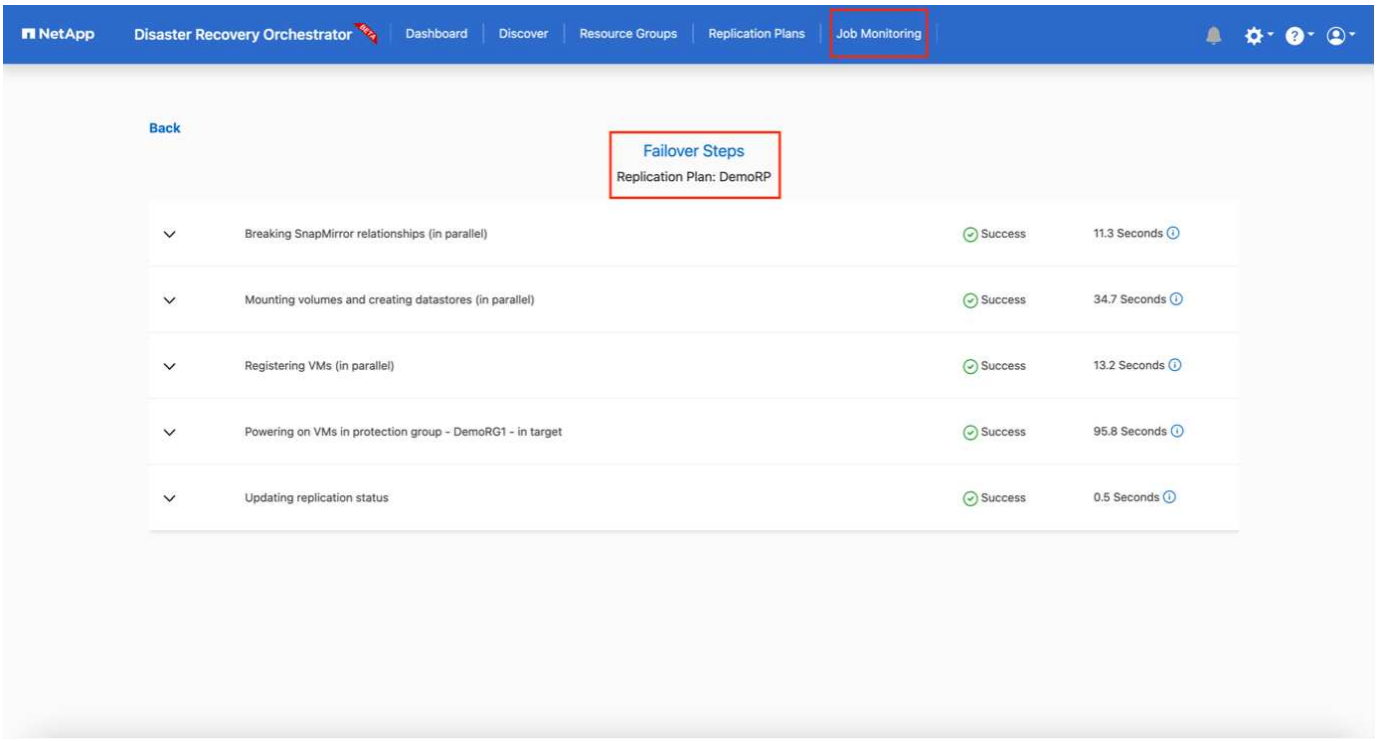


Una vez creado el plan de replicación, se pueden utilizar la opción de conmutación por error, la opción de conmutación por error de prueba o la opción de migración según los requisitos. Durante las opciones de conmutación por error y conmutación por error de prueba, se utiliza la copia de instantánea de SnapMirror más reciente o se puede seleccionar una copia de instantánea específica de una copia de instantánea de un punto en el tiempo (según la política de retención de SnapMirror). La opción de punto en el tiempo 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 o probar la conmutación por error con la configuración especificada en el plan de replicación, puede hacer clic en **Conmutación por error** o **Probar conmutación por error**.

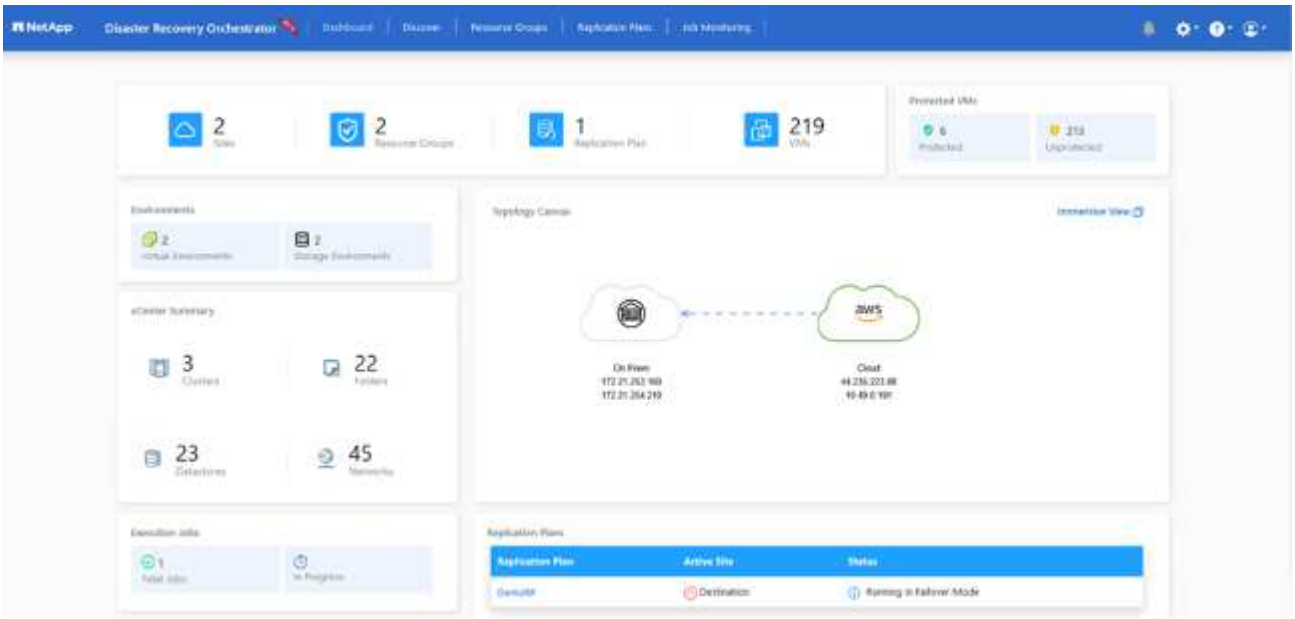




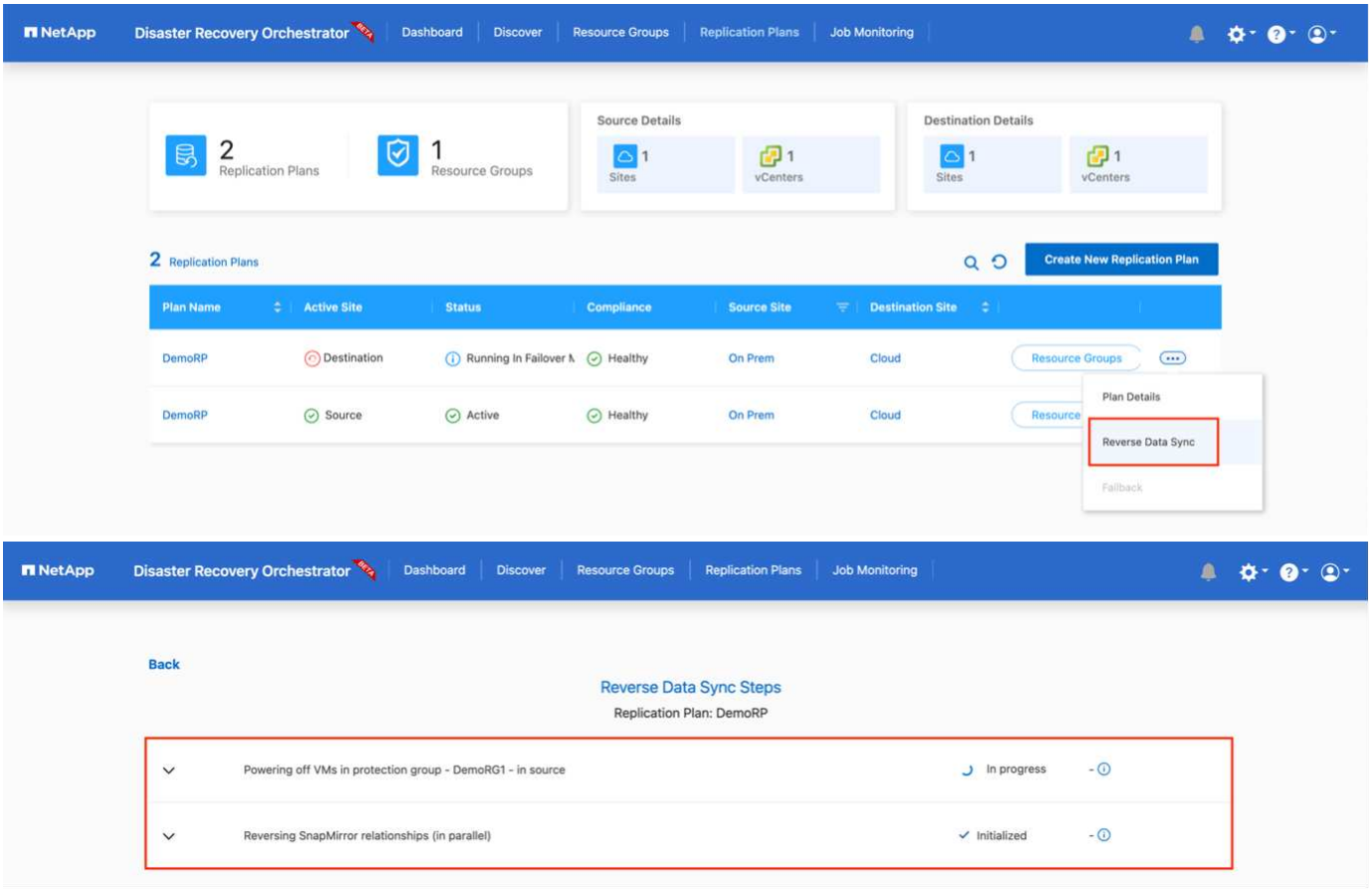
El plan de replicación se puede supervisar en el menú de tareas:



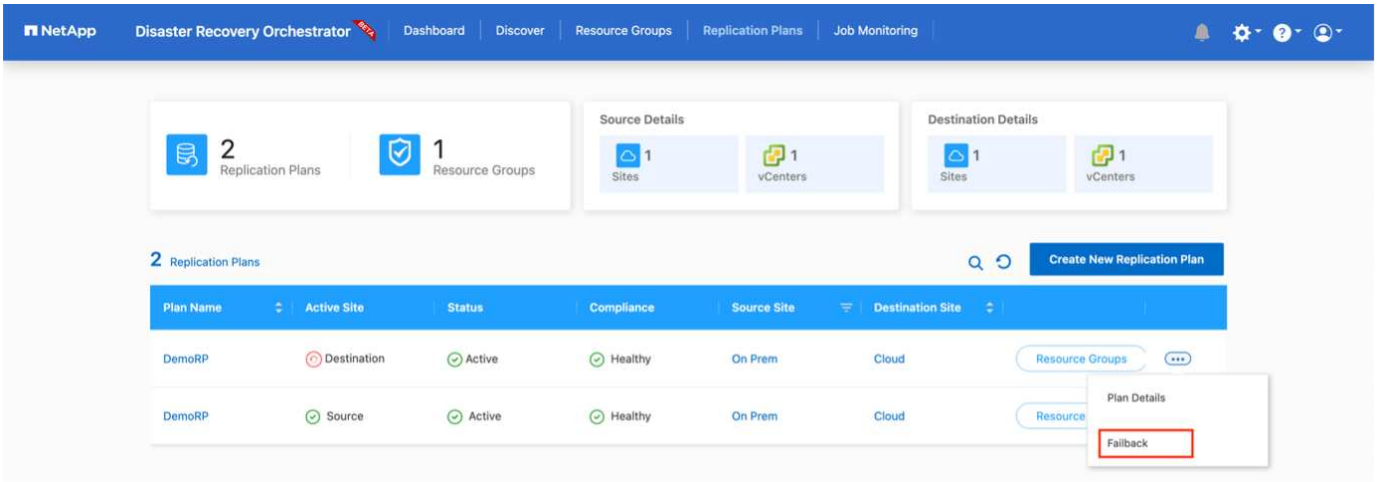
Una vez activada la conmutación por error, los elementos recuperados se pueden ver en el vCenter de VMC (máquinas virtuales, redes, almacenes de datos). De forma predeterminada, las máquinas virtuales se recuperan en la carpeta de carga de trabajo.

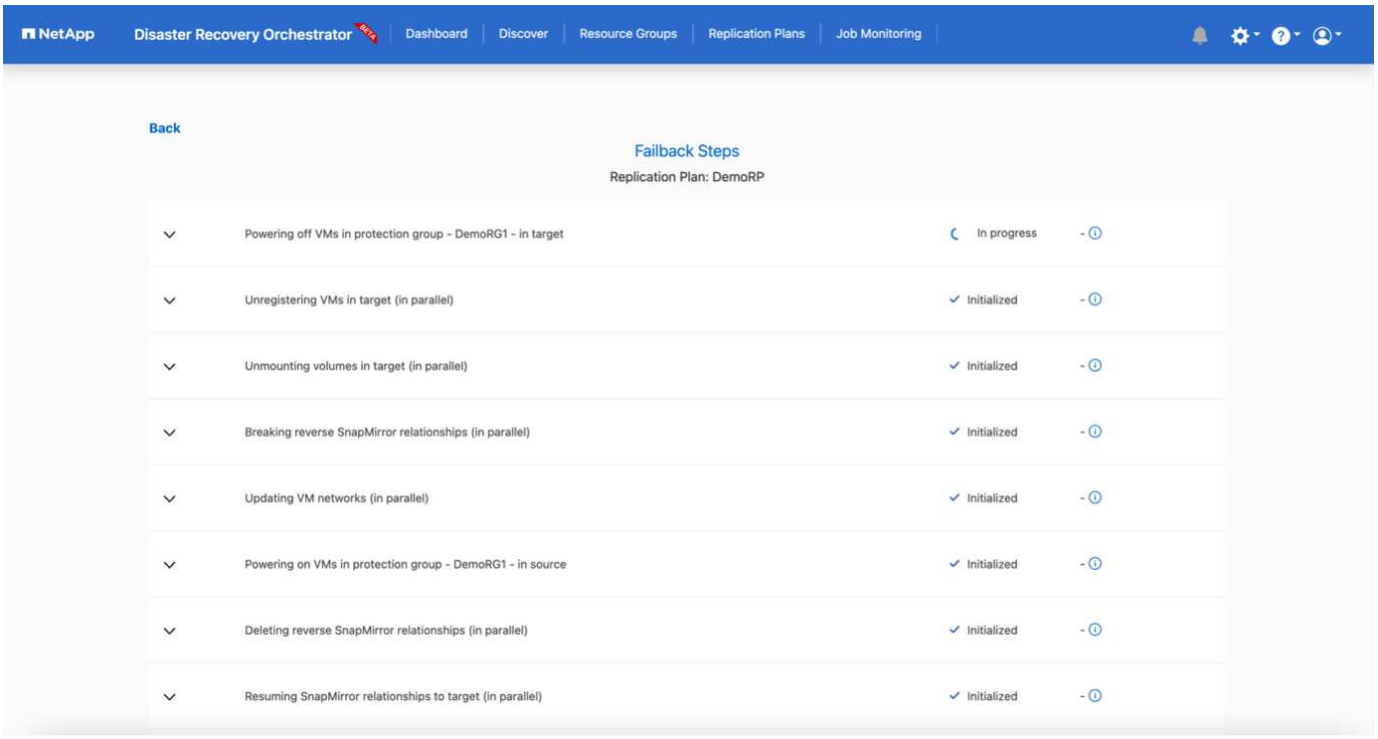


La conmutación por recuperación se puede activar en el nivel del plan de replicación. Para una conmutación por error de prueba, se puede utilizar la opción de desmantelamiento para revertir los cambios y eliminar la relación FlexClone . La recuperación relacionada con la conmutación por error es un proceso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

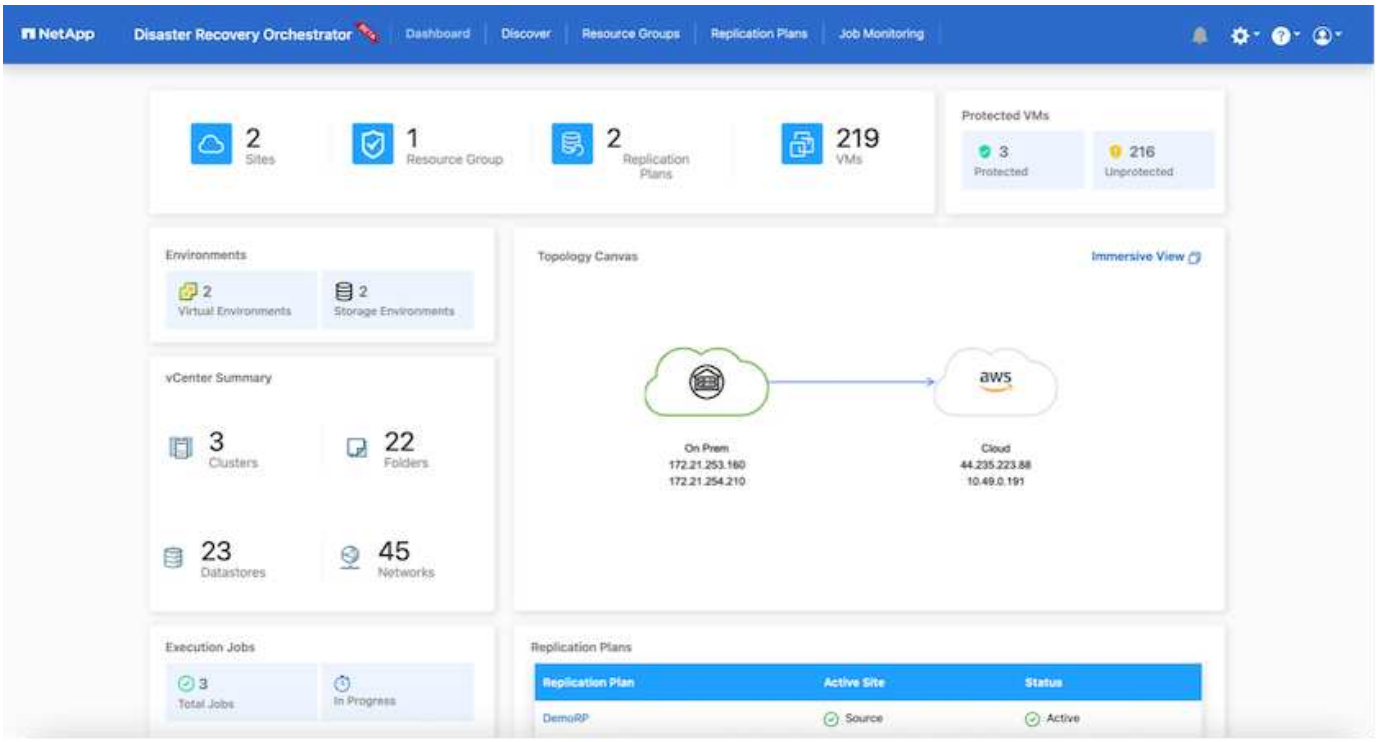


Una vez completado, puede activar la conmutación por error para regresar al sitio de producción original.





Desde NetApp Console, puedes ver que el estado de la replicación se ha interrumpido para los volúmenes correspondientes (aquellos que se mapearon a VMC como volúmenes de lectura y escritura). Durante la conmutación por error de prueba, DRO no mapea el volumen de destino o de réplica. En su lugar, crea una copia de FlexClone de la instancia requerida de SnapMirror (o Snapshot) y expone la instancia de FlexClone, que no consume capacidad física adicional para FSx ONTAP. Este proceso garantiza que el volumen no se modifique y que los trabajos de réplica puedan continuar incluso durante las pruebas de DR o los flujos de trabajo de evaluación de prioridades. Además, este proceso garantiza que, si se producen errores o se recuperan datos dañados, se pueda limpiar la recuperación sin riesgo de que se destruya la réplica.



Recuperación de ransomware

Recuperarse de un ransomware puede ser una tarea abrumadora. En concreto, puede resultar difícil para las organizaciones de TI determinar con precisión dónde está el punto de retorno seguro y, una vez determinado, proteger las cargas de trabajo recuperadas de ataques recurrentes, por ejemplo, de malware inactivo o aplicaciones vulnerables.

DRO aborda estos problemas permitiéndole recuperar su sistema desde cualquier momento disponible. También es posible recuperar cargas de trabajo en redes funcionales pero aisladas para que las aplicaciones puedan funcionar y comunicarse entre sí en una ubicación donde no estén expuestas al tráfico de norte a sur. Esto le brinda a su equipo de seguridad un lugar seguro para realizar análisis forenses y asegurarse de que no haya malware oculto o inactivo.

Beneficios

- Uso de la replicación eficiente y resistente SnapMirror .
- Recuperación a cualquier punto disponible en el tiempo con retención de copia instantánea.
- Automatización completa de todos los pasos necesarios para recuperar cientos a miles de máquinas virtuales de los pasos de almacenamiento, computación, red y validación de aplicaciones.
- Recuperación de carga de trabajo con tecnología ONTAP FlexClone utilizando un método que no cambia el volumen replicado.
  - Evita el riesgo de corrupción de datos en volúmenes o copias instantáneas.
  - Evita interrupciones de replicación durante los flujos de trabajo de prueba de DR.
  - Uso potencial de datos de DR con recursos de computación en la nube para flujos de trabajo más allá de DR, como DevTest, pruebas de seguridad, pruebas de parches o actualizaciones y pruebas de remediación.
- Optimización de CPU y RAM para ayudar a reducir los costos de la nube al permitir la recuperación a clústeres de cómputo más pequeños.

Uso de Veeam Replication y FSx ONTAP para la recuperación ante desastres en VMware Cloud en AWS

La integración de Amazon FSx ONTAP con VMware Cloud on AWS es un almacén de datos NFS externo administrado por AWS construido sobre el sistema de archivos ONTAP de NetApp que se puede conectar a un clúster en el SDDC. Proporciona a los clientes una infraestructura de almacenamiento virtualizada flexible y de alto rendimiento que escala independientemente de los recursos informáticos.

Descripción general

Para aquellos clientes que buscan utilizar VMware Cloud on AWS SDDC como destino de recuperación ante desastres, los almacenes de datos de FSx ONTAP se pueden usar para replicar datos desde las instalaciones locales mediante cualquier solución de terceros validada que proporcione capacidad de replicación de VM. Al agregar el almacén de datos FSx ONTAP , se permitirá una implementación con costos optimizados en comparación con la creación de VMware Cloud en AWS SDDC con una enorme cantidad de hosts ESXi solo para acomodar el almacenamiento.

Este enfoque también ayuda a los clientes a utilizar el clúster de luz piloto en VMC junto con los almacenes de datos de FSx ONTAP para alojar las réplicas de VM. El mismo proceso también se puede extender como una opción de migración a VMware Cloud on AWS al conmutar por error el plan de replicación.

Planteamiento del problema

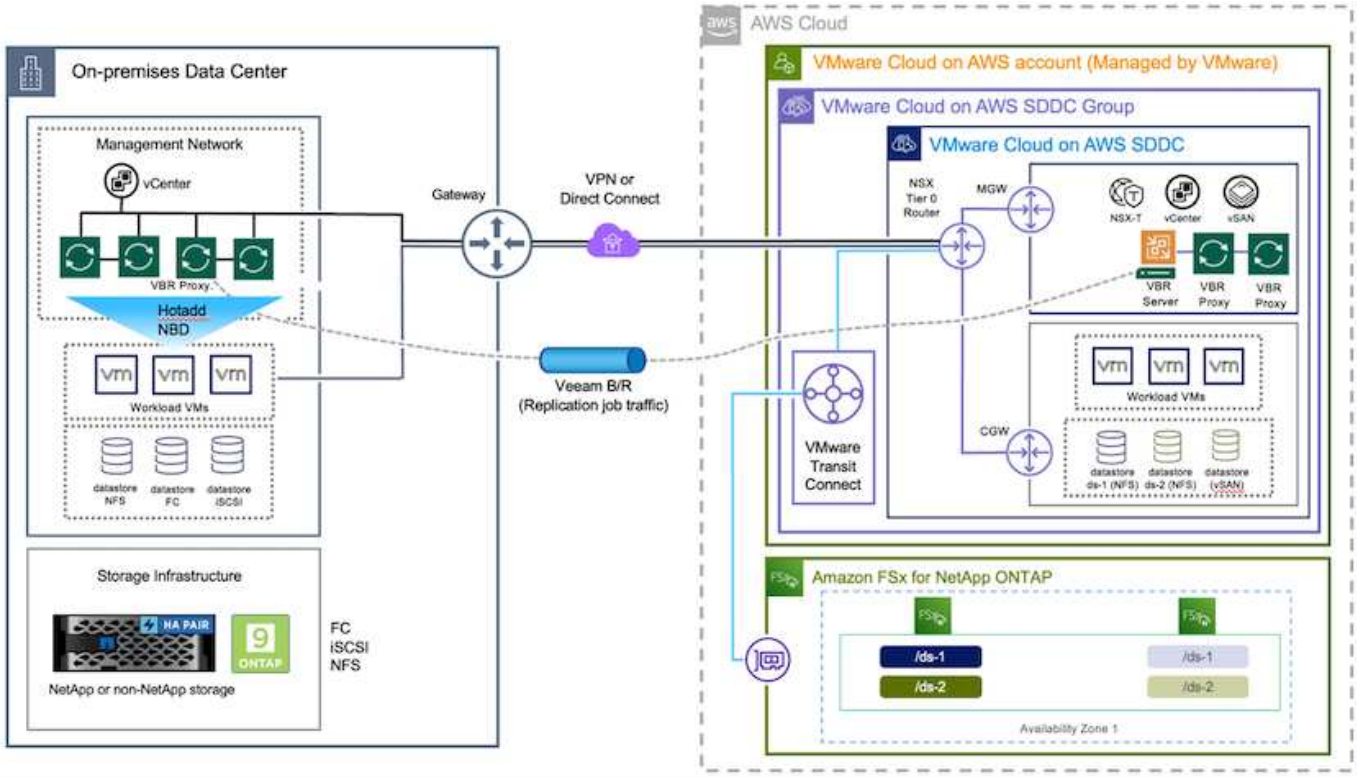
Este documento describe cómo usar el almacén de datos FSx ONTAP y Veeam Backup and Replication para configurar la recuperación ante desastres de máquinas virtuales VMware locales en VMware Cloud on AWS mediante la funcionalidad de replicación de máquinas virtuales.

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 una máquina virtual en estado listo para iniciarse. 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 de tráfico para la replicación a través de WAN y conexiones lentas. Además, también filtra bloques de datos duplicados, bloques de datos cero, archivos de intercambio y archivos del sistema operativo invitado de VM excluidos, y comprime el tráfico de réplica.

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

Cuando se realiza una conmutación por error, una VM replicada asume el rol de la VM original. La conmutación por error se puede realizar al último estado de una réplica o a cualquiera de sus puntos de restauración conocidos. Esto permite la recuperación de ransomware o pruebas aisladas según sea necesario. En Veeam Backup & Replication, la conmutación por error y la conmutación por recuperación son pasos intermedios temporales que deben finalizarse. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.



Pasos de alto nivel

1. El software Veeam Backup and Replication se ejecuta en un entorno local con conectividad de red adecuada.
2. Para configurar VMware Cloud on AWS, consulta el artículo de VMware Cloud Tech Zone "Guía de implementación de la integración de VMware Cloud on AWS con Amazon FSx ONTAP" para implementar y configurar VMware Cloud on AWS SDDC y FSx ONTAP como datastore NFS. (Se puede usar un entorno pilot-light configurado con una configuración mínima para fines de DR. Las VMs conmutarán por error a este clúster en caso de incidente y se pueden añadir nodos adicionales).
3. Configure trabajos de replicación para crear réplicas de máquinas virtuales mediante Veeam Backup and Replication.
4. Cree un plan de conmutación por error y realice la conmutación por error.
5. Vuelva a las máquinas virtuales de producción una vez que se complete el evento de desastre y el sitio principal esté activo.

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

1. Asegúrese de que la máquina virtual de respaldo de Veeam Backup & Replication esté conectada al vCenter de origen, así como a los clústeres VMware Cloud on AWS SDDC de destino.
2. El servidor de respaldo debe poder resolver nombres cortos y conectarse a los vCenter de origen y de destino.
3. El almacén de datos de destino de FSx ONTAP debe tener suficiente espacio libre para almacenar los VMDK de las máquinas virtuales replicadas

Para obtener información adicional, consulte el apartado "Consideraciones y limitaciones""aquí" .

Detalles de la implementación

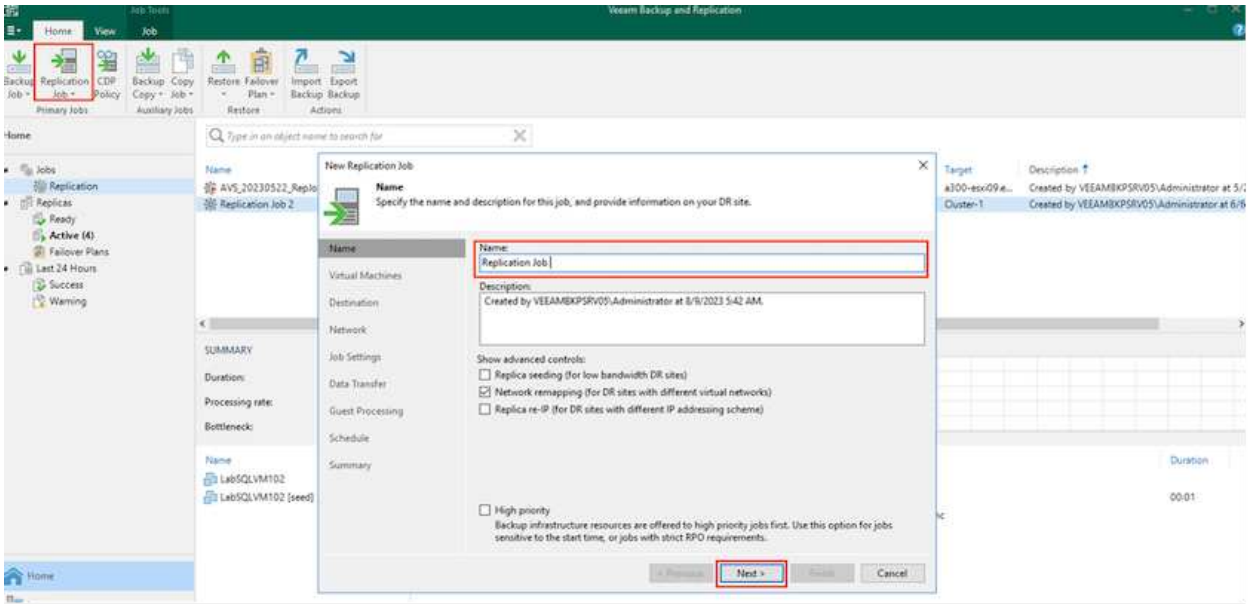
▼ Paso 1: replicar máquinas virtuales

Veeam Backup & Replication aprovecha las capacidades de instantáneas de VMware vSphere y, durante la replicación, Veeam Backup & Replication solicita a VMware vSphere que cree una instantánea de VM. La instantánea de VM es la copia puntual de una VM que incluye discos virtuales, estado del sistema, configuración, etc. Veeam Backup & Replication utiliza la instantánea como fuente de datos para la replicación.

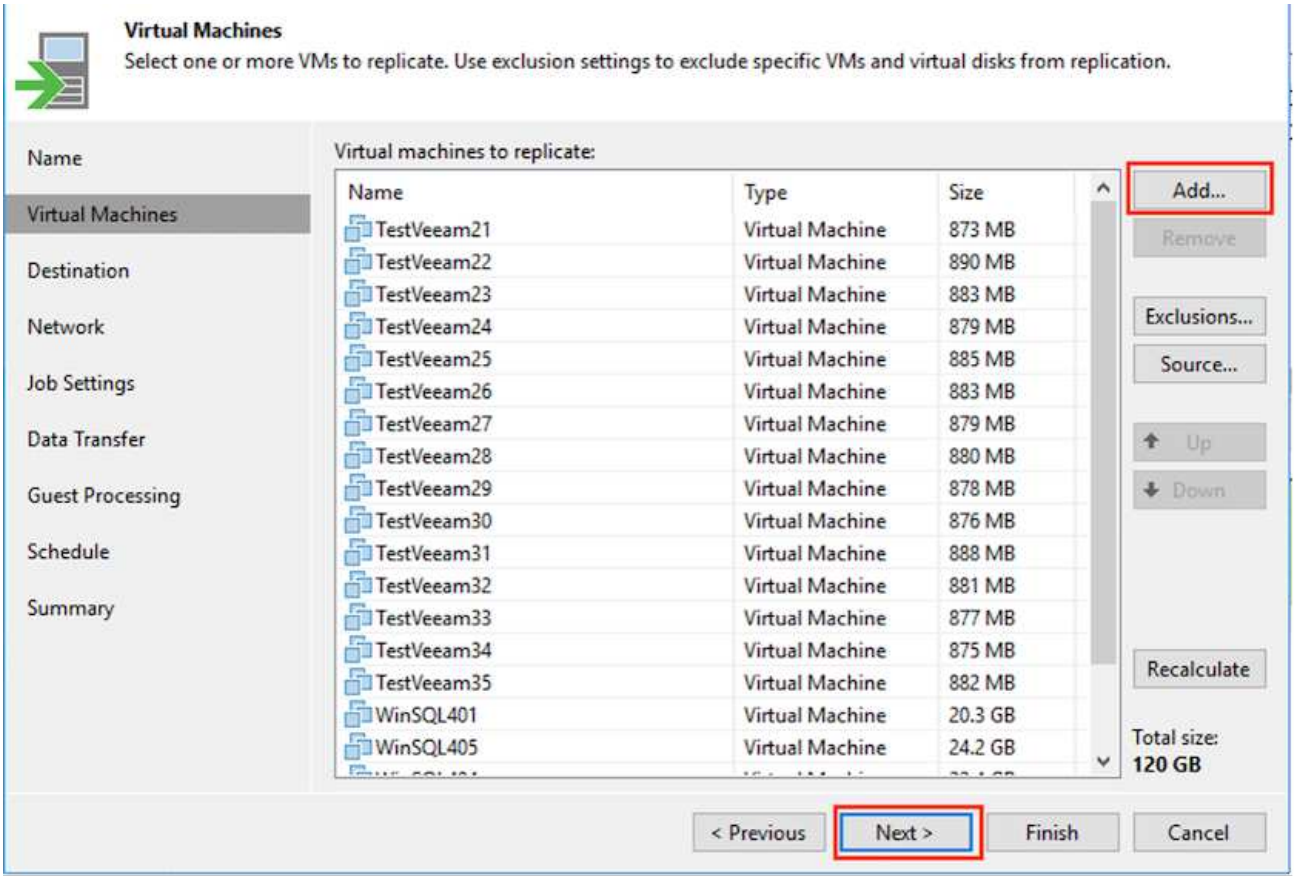
Para replicar máquinas virtuales, siga los pasos a continuación:

1. Abra la consola de Veeam Backup & Replication.
2. En la vista Inicio, seleccione Trabajo de replicación > Máquina virtual > VMware vSphere.
3. Especifique un nombre de trabajo y seleccione la casilla de verificación de control avanzado adecuada. Haga clic en Siguiente.
   - Seleccione la casilla de verificación Siembra de réplicas si la conectividad entre las instalaciones locales y AWS tiene un ancho de banda restringido.
   - Seleccione la casilla de verificación Reasignación de red (para sitios de AWS VMC con redes diferentes) si los segmentos en VMware Cloud on AWS SDDC no coinciden con los de las redes del sitio local.

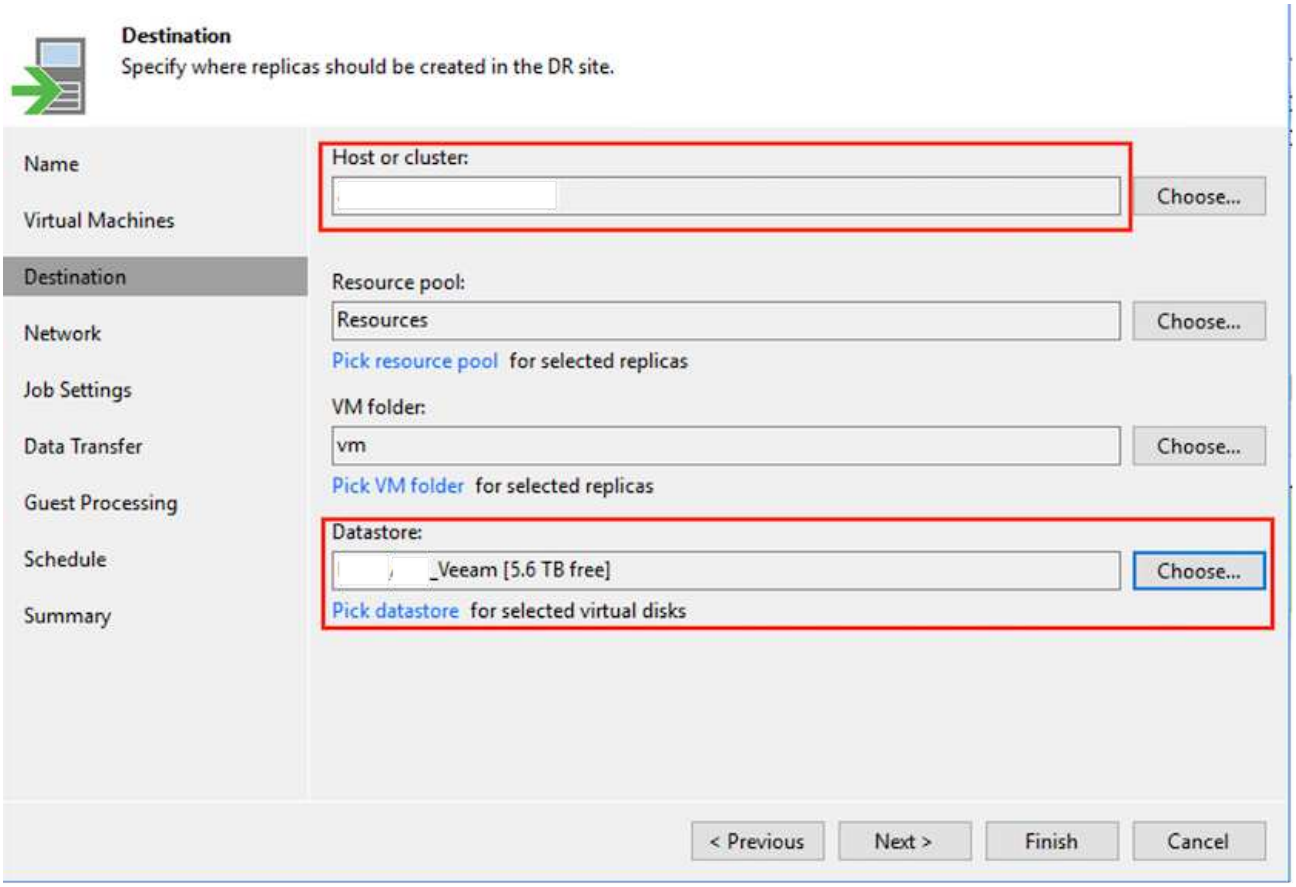
- Si el esquema de direccionamiento IP en el sitio de producción local difiere del esquema en el sitio de AWS VMC, seleccione la casilla de verificación Re-IP de réplica (para sitios de recuperación ante desastres con diferente esquema de direccionamiento IP).



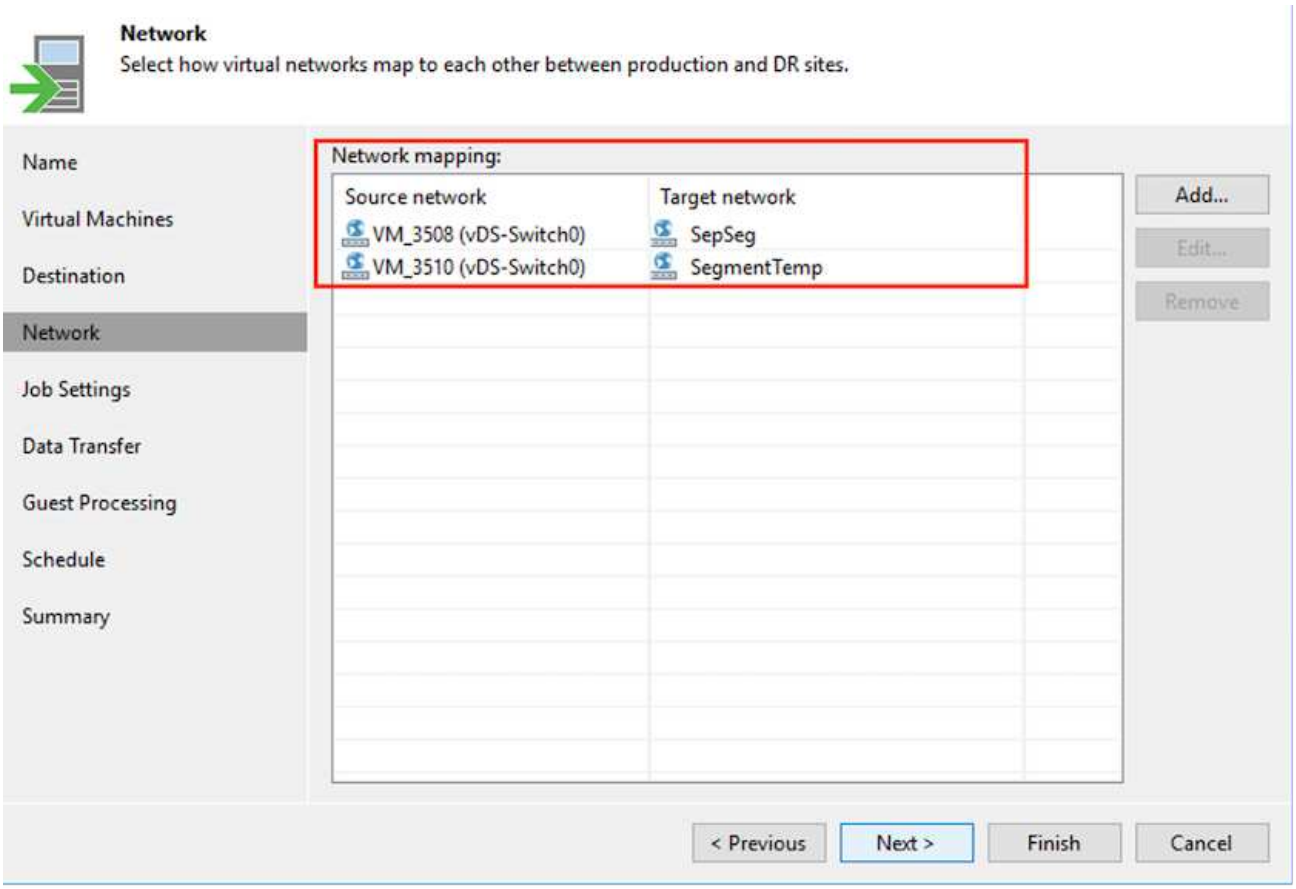
4. Seleccione las máquinas virtuales que deben replicarse en el almacén de datos de FSx ONTAP adjunto a VMware Cloud on AWS SDDC en el paso **Máquinas virtuales**. Las máquinas virtuales se pueden colocar en vSAN para llenar la capacidad del almacén de datos de vSAN disponible. En un clúster de luz piloto, la capacidad utilizable de un clúster de 3 nodos será limitada. El resto de los datos se pueden replicar en los almacenes de datos de FSx ONTAP . Haga clic en **Agregar**, luego en la ventana **Agregar objeto** seleccione las máquinas virtuales o los contenedores de máquinas virtuales necesarios y haga clic en **Agregar**. Haga clic en **Siguiente**.



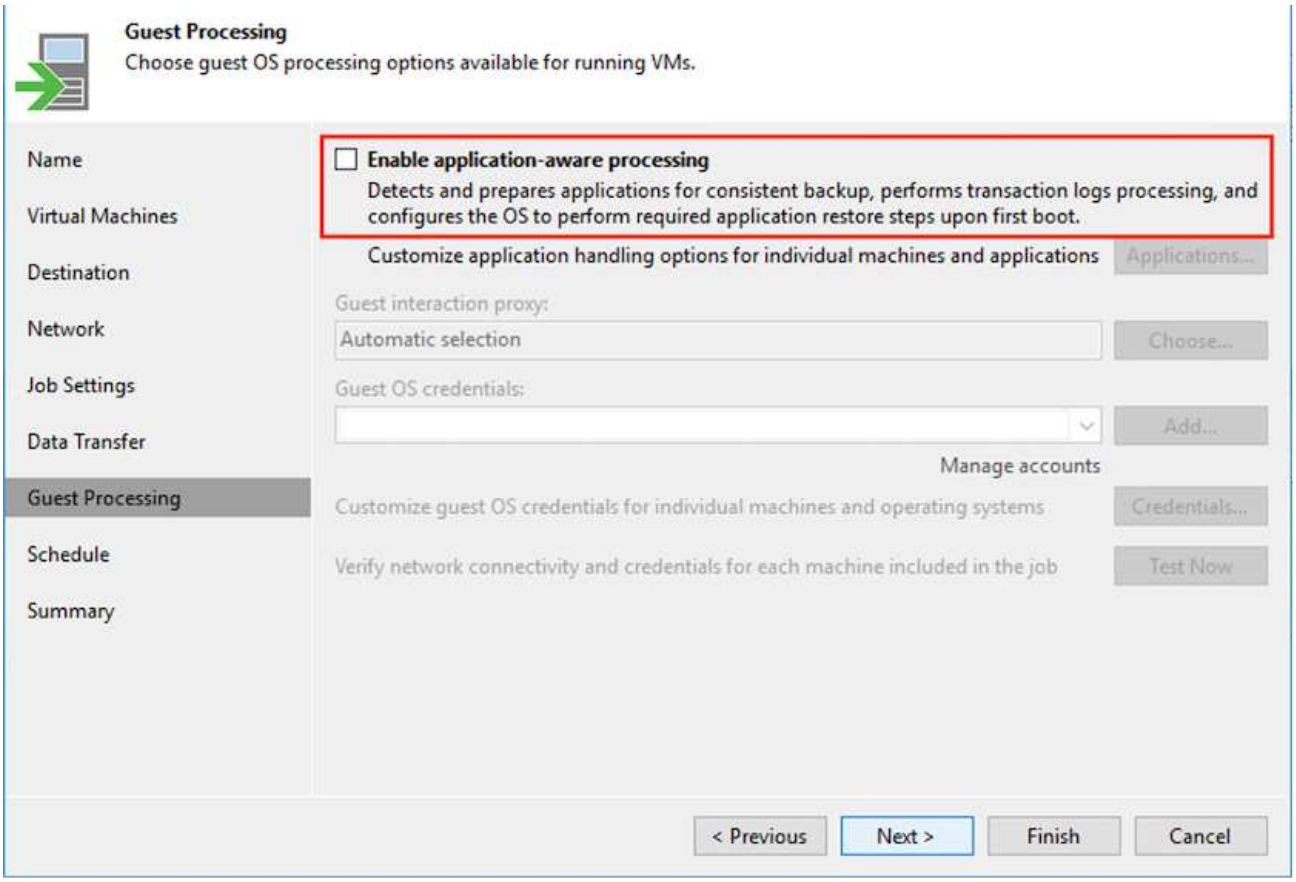
5. Después de eso, seleccione el destino como clúster/host SDDC de VMware Cloud on AWS y el grupo de recursos adecuado, la carpeta de VM y el almacén de datos de FSx ONTAP para las réplicas de VM. Luego haga clic en **Siguiente**.



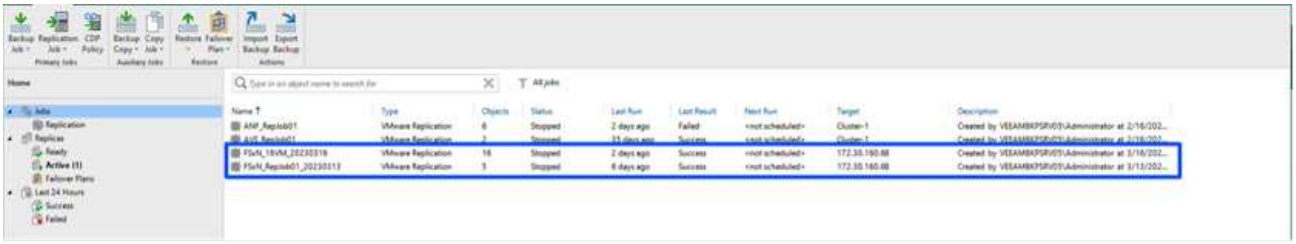
6. En el siguiente paso, cree la asignación entre la red virtual de origen y de destino según sea necesario.



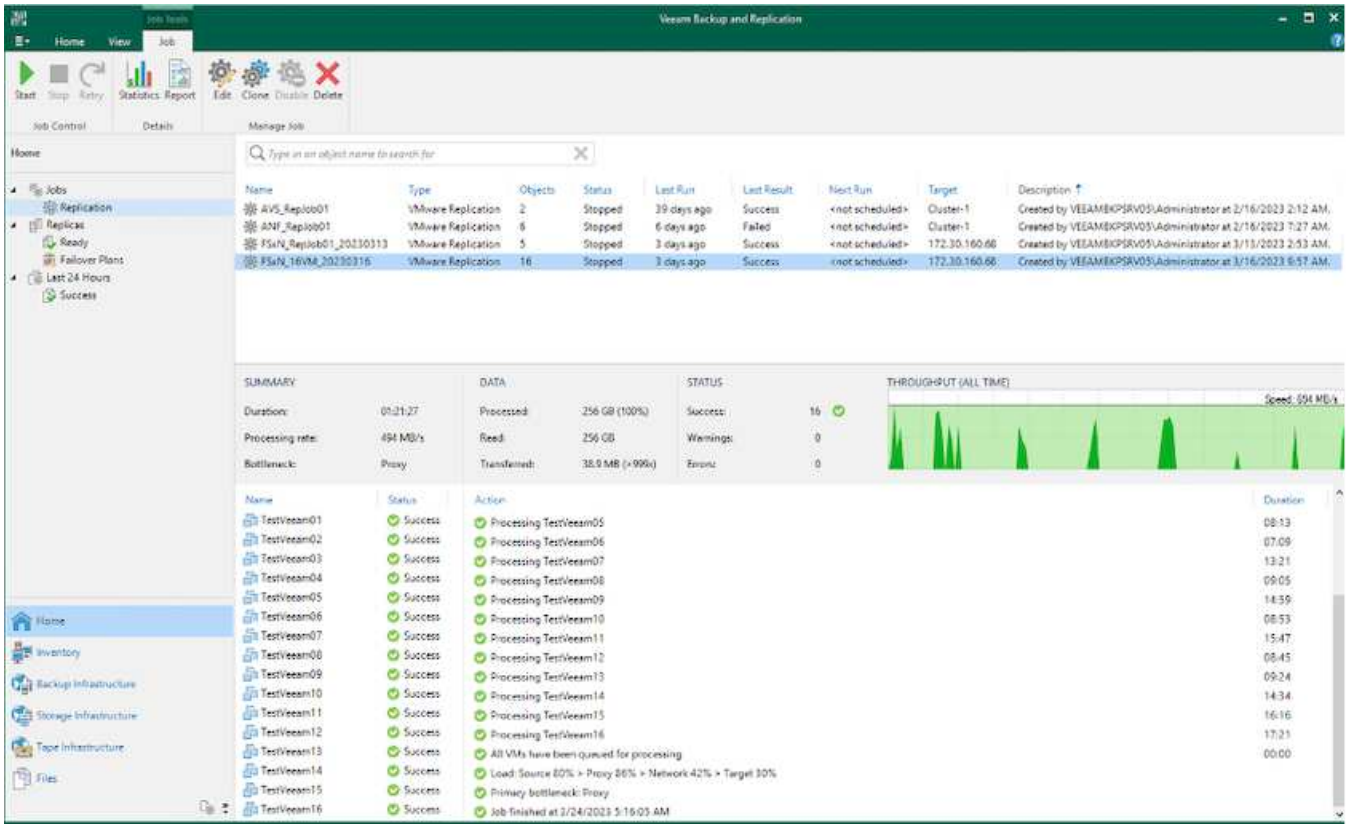
7. En el paso **Configuración del trabajo**, especifique el repositorio de respaldo que almacenará metadatos para las réplicas de VM, la política de retención, etc.
8. Actualice los servidores proxy **Origen** y **Destino** en el paso **Transferencia de datos** y deje la selección **Automática** (predeterminada) y mantenga seleccionada la opción **Directa** y haga clic en **Siguiente**.
9. En el paso **Procesamiento de invitado**, seleccione la opción **Habilitar procesamiento consciente de la aplicación** según sea necesario. Haga clic en **Siguiente**.



10. Seleccione la programación de replicación para ejecutar el trabajo de replicación de manera periódica.
11. En el paso **Resumen** del asistente, revise los detalles del trabajo de replicación. Para iniciar el trabajo inmediatamente después de cerrar el asistente, seleccione la casilla de verificación **Ejecutar el trabajo al hacer clic en Finalizar**; de lo contrario, deje la casilla de verificación sin seleccionar. Luego haga clic en **Finalizar** para cerrar el asistente.



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



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

▼ **Paso 2: Crear un plan de conmutación por error**

Cuando se complete la replicación o siembra inicial, cree el plan de conmutación por error. El plan de conmutación por error ayuda a realizar la conmutación por error de las máquinas virtuales dependientes una por una o como grupo de manera automática. El plan de conmutación por error es el modelo para el orden en que se procesan las máquinas virtuales, incluidos los retrasos en el arranque. El plan de conmutación por error también ayuda a garantizar que las máquinas virtuales dependientes críticas ya estén en ejecución.

Para crear el plan, navegue a la nueva subsección llamada Réplicas y seleccione Plan de conmutación por error. Seleccione las máquinas virtuales adecuadas. 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 se completa la replicación inicial y las réplicas de la máquina virtual están en estado Listo.

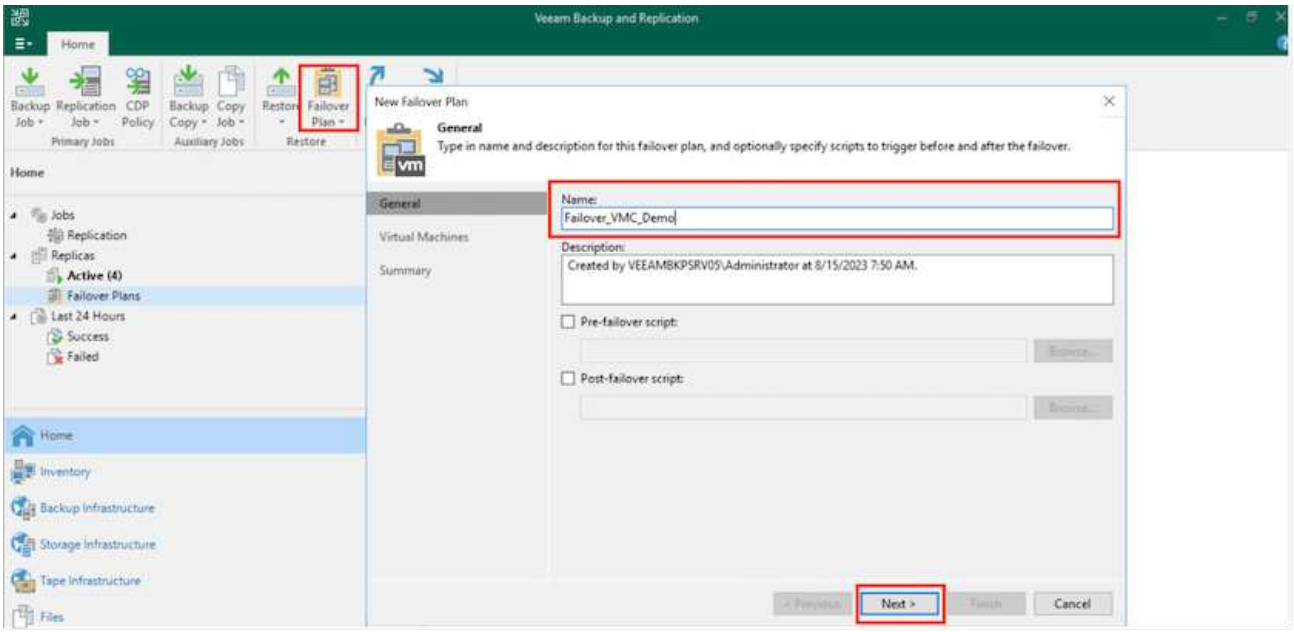
ⓘ La cantidad máxima de máquinas virtuales que se pueden iniciar simultáneamente cuando se ejecuta un plan de conmutación por error es 10.

ⓘ Durante el proceso de conmutación por error, las máquinas virtuales de origen no se apagarán.

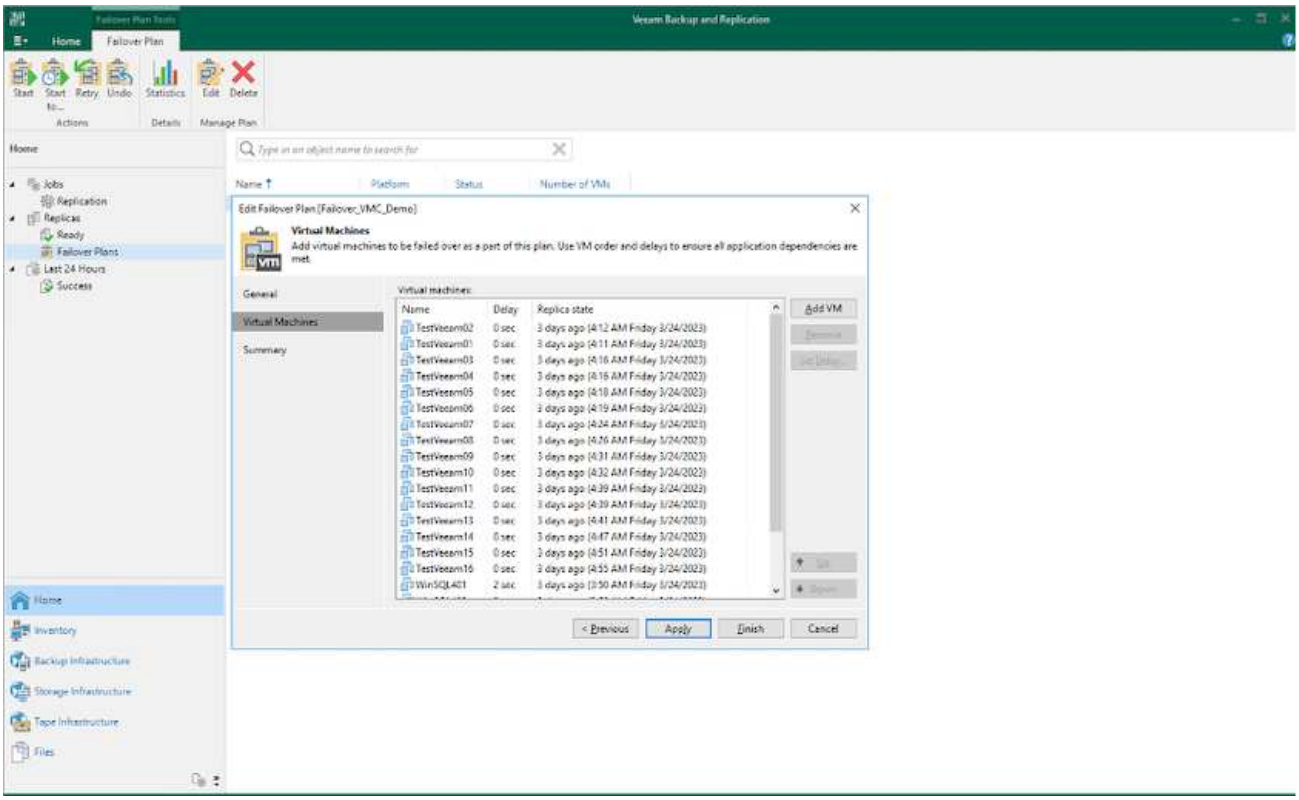
Para crear el **Plan de conmutación por error**, haga lo siguiente:

1. En la vista Inicio, seleccione **Plan de conmutación por error > VMware vSphere**.

2. A continuación, proporcione un nombre y una descripción al plan. Se pueden agregar scripts previos y posteriores a la conmutación por error según sea necesario. Por ejemplo, ejecute un script para apagar las máquinas virtuales antes de iniciar las máquinas virtuales replicadas.



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



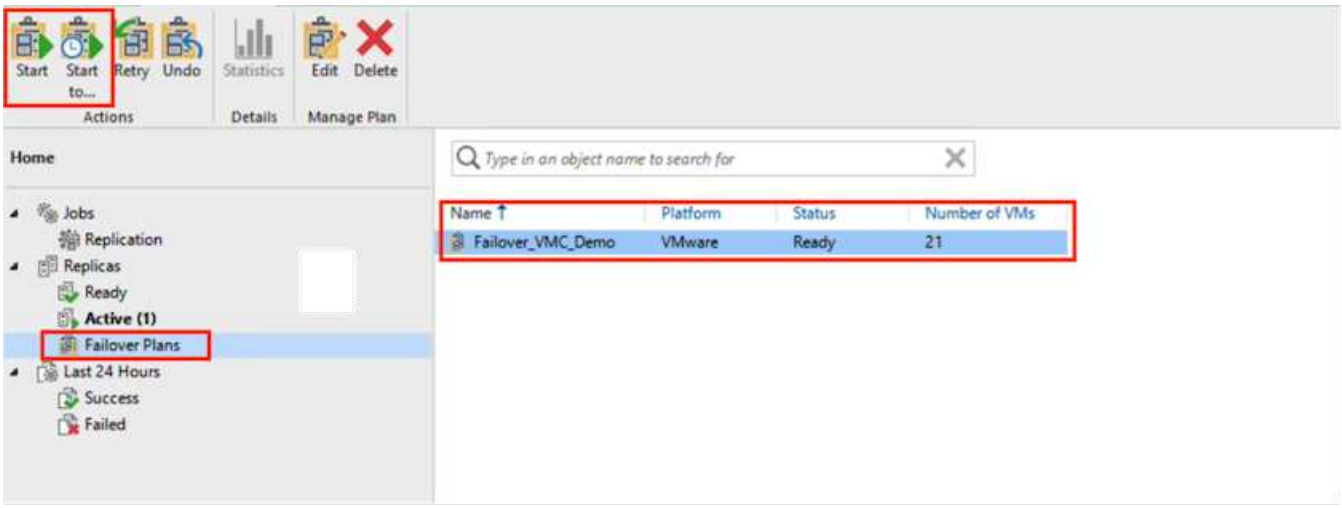
Para obtener información adicional sobre la creación de trabajos de replicación, consulte"Creación de trabajos de replicación" .

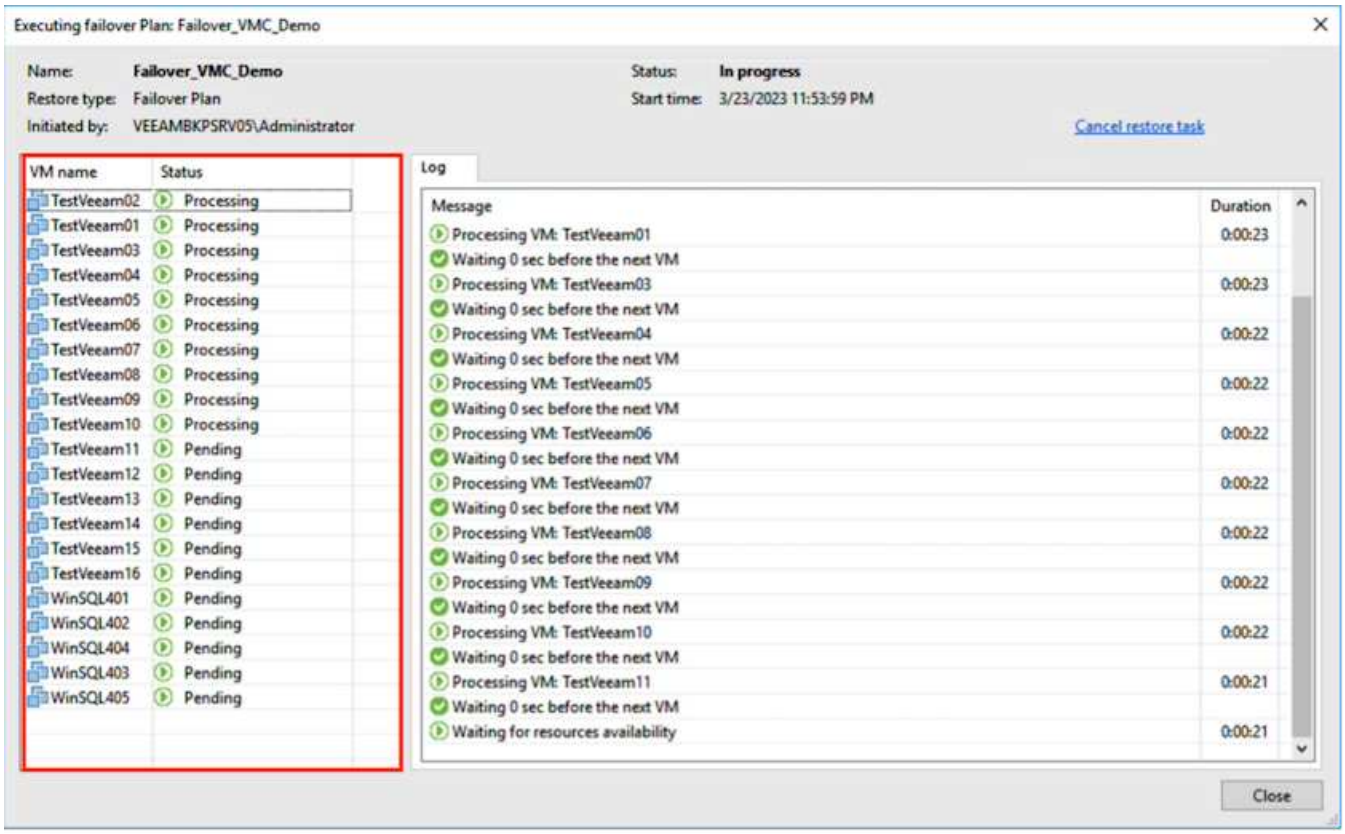
▼ Paso 3: Ejecutar el plan de conmutación por error

Durante la conmutación por error, la máquina virtual de origen en el sitio de producción se cambia a su réplica en el sitio de recuperación ante desastres. Como parte del proceso de conmutación por error, Veeam Backup & Replication restaura la réplica de la máquina virtual al punto de restauración requerido y mueve todas las actividades de E/S de la máquina virtual de origen a su réplica. Las réplicas se pueden utilizar no sólo en caso de desastre, sino también para simular simulacros de recuperación ante desastres. Durante la simulación de conmutación por error, la máquina virtual de origen permanece en ejecución. Una vez que se hayan realizado todas las pruebas necesarias, puede deshacer la conmutación por error y volver a las operaciones normales.

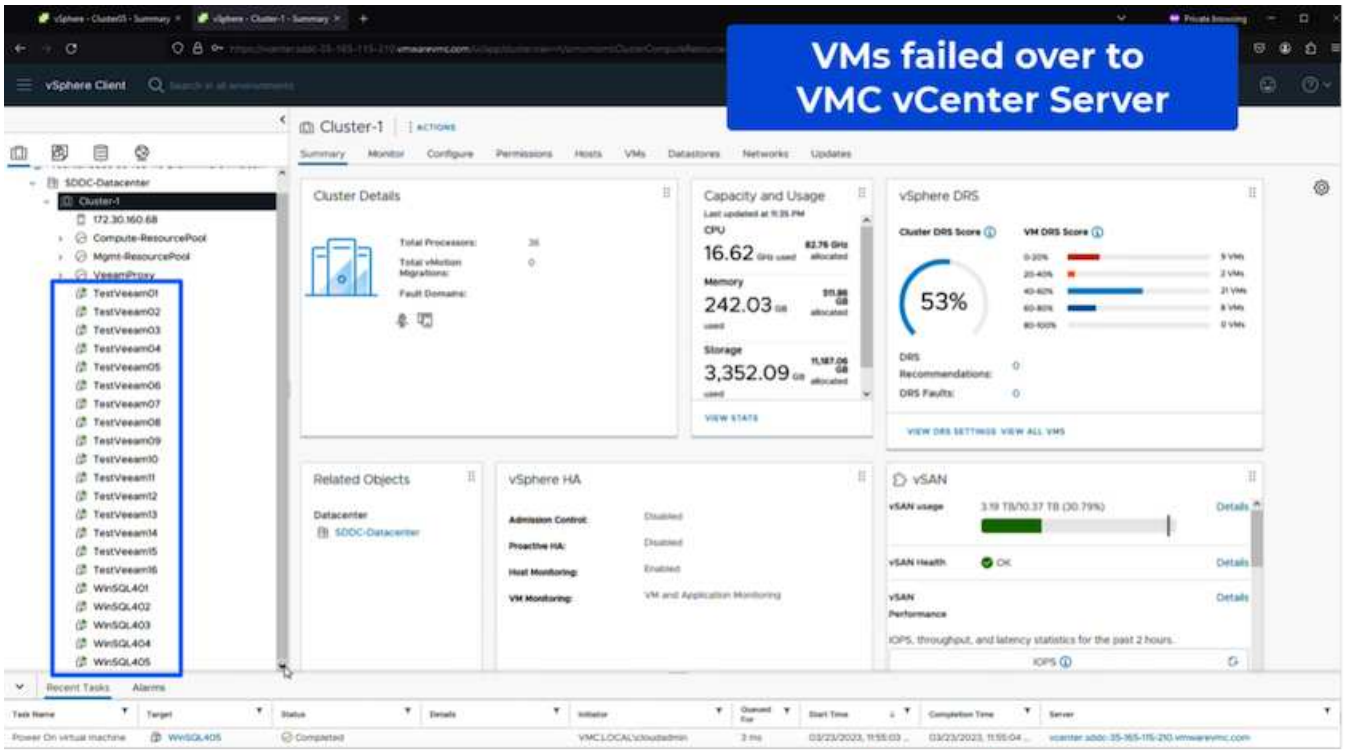
Asegúrese de que la segmentación de la red esté implementada para evitar conflictos de IP durante simulacros de recuperación ante desastres.

Para iniciar el plan de conmutación por error, simplemente haga clic en la pestaña **Planes de conmutación por error** y haga clic derecho en el plan de conmutación por error. Seleccione **Inicio**. Esto conmutará por error utilizando los últimos puntos de restauración de las réplicas de VM. Para conmutar por error a puntos de restauración específicos de réplicas de máquinas virtuales, seleccione **Iniciar en**.

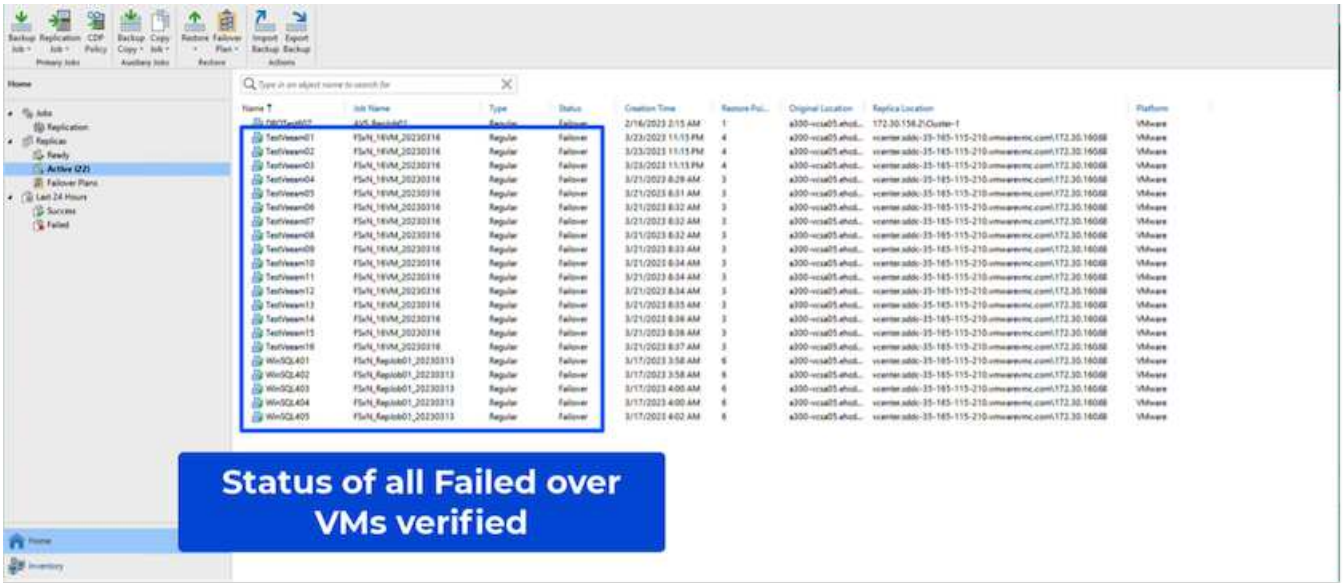




El estado de la réplica de la máquina virtual cambia de Listo a Conmutación por error y las máquinas virtuales se iniciarán en el clúster/host de VMware Cloud on AWS SDDC de destino.



Una vez completada la conmutación por error, el estado de las máquinas virtuales cambiará a "Conmutación por error".



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

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

▼ **Paso 4: Retorno al sitio de producción**

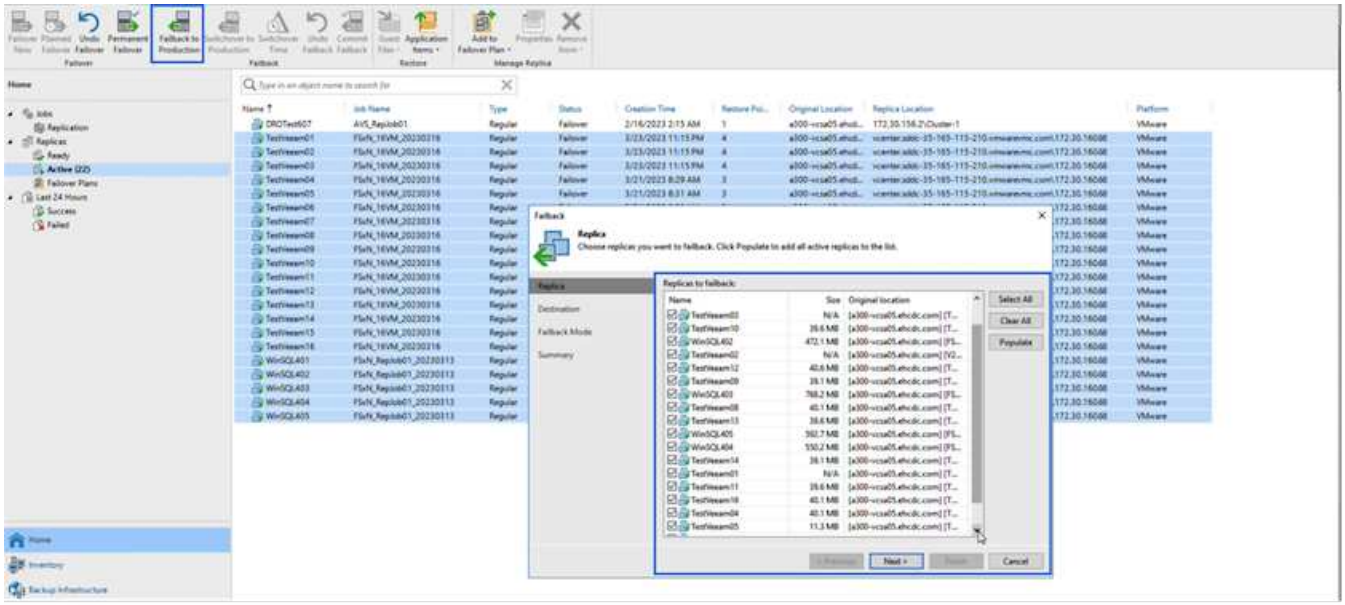
Cuando se ejecuta el plan de conmutación por error, se lo considera un paso intermedio y debe finalizarse según el requisito. Las opciones incluyen lo siguiente:

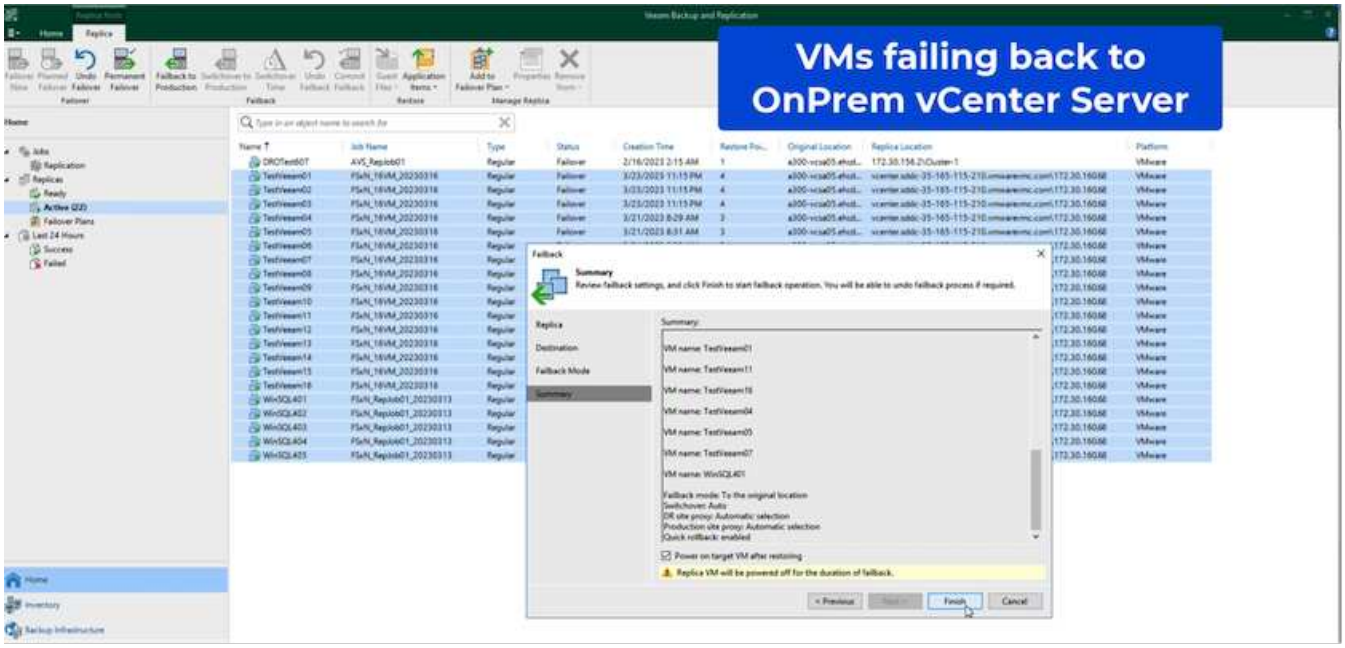
- **Retorno a producción**: vuelve a la máquina virtual original y transfiere todos los cambios que tuvieron lugar mientras la réplica de la máquina virtual estaba en ejecución a la máquina virtual original.

Al realizar una conmutación por error, los cambios solo se transfieren, pero no se publican. Seleccione **Confirmar conmutación por error** (una vez que se confirme que la VM original funciona como se espera) o **Deshacer conmutación por error** para volver a la réplica de la VM si la VM original no funciona como se espera.

- **Deshacer conmutación por error**: vuelve a la máquina virtual original y descarta todos los cambios realizados en la réplica de la máquina virtual mientras estaba en ejecución.
- **Conmutación por error permanente**: cambia de forma permanente de la máquina virtual original a una réplica de máquina virtual y utiliza esta réplica como la máquina virtual original.

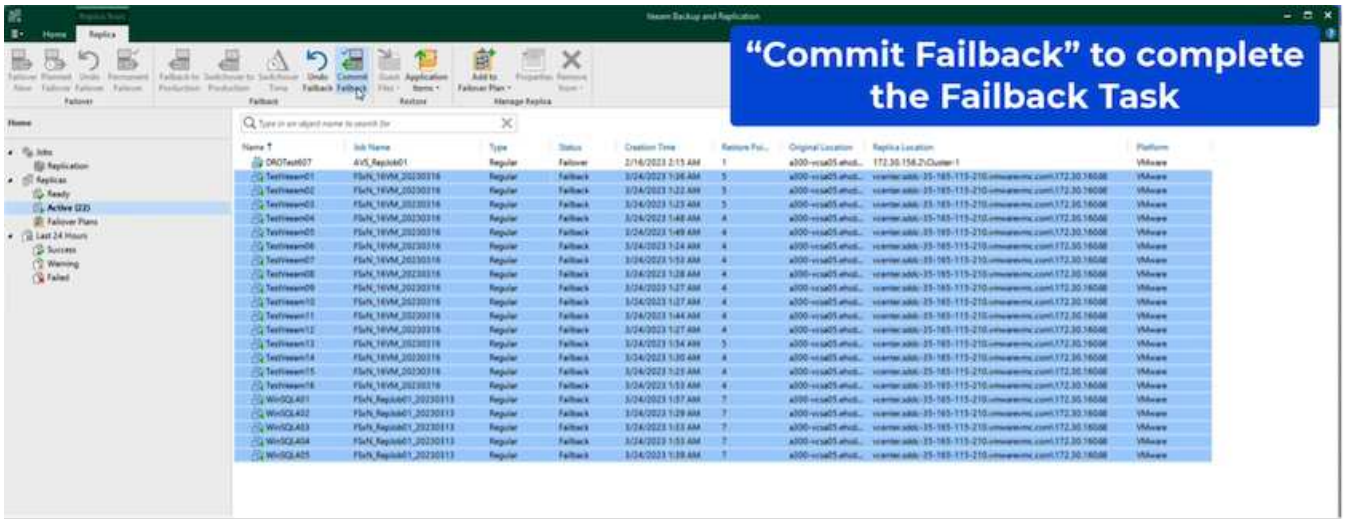
En esta demostración, se eligió Failback a producción. Se seleccionó la opción de retorno a la máquina virtual original durante el paso Destino del asistente y se habilitó la casilla de verificación "Encender la máquina virtual después de restaurar".

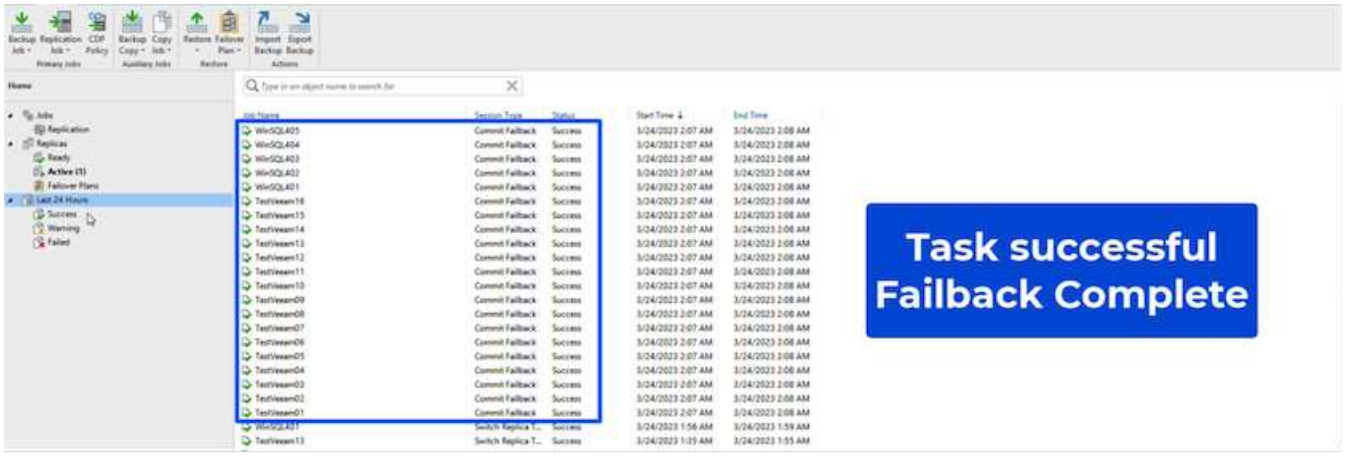




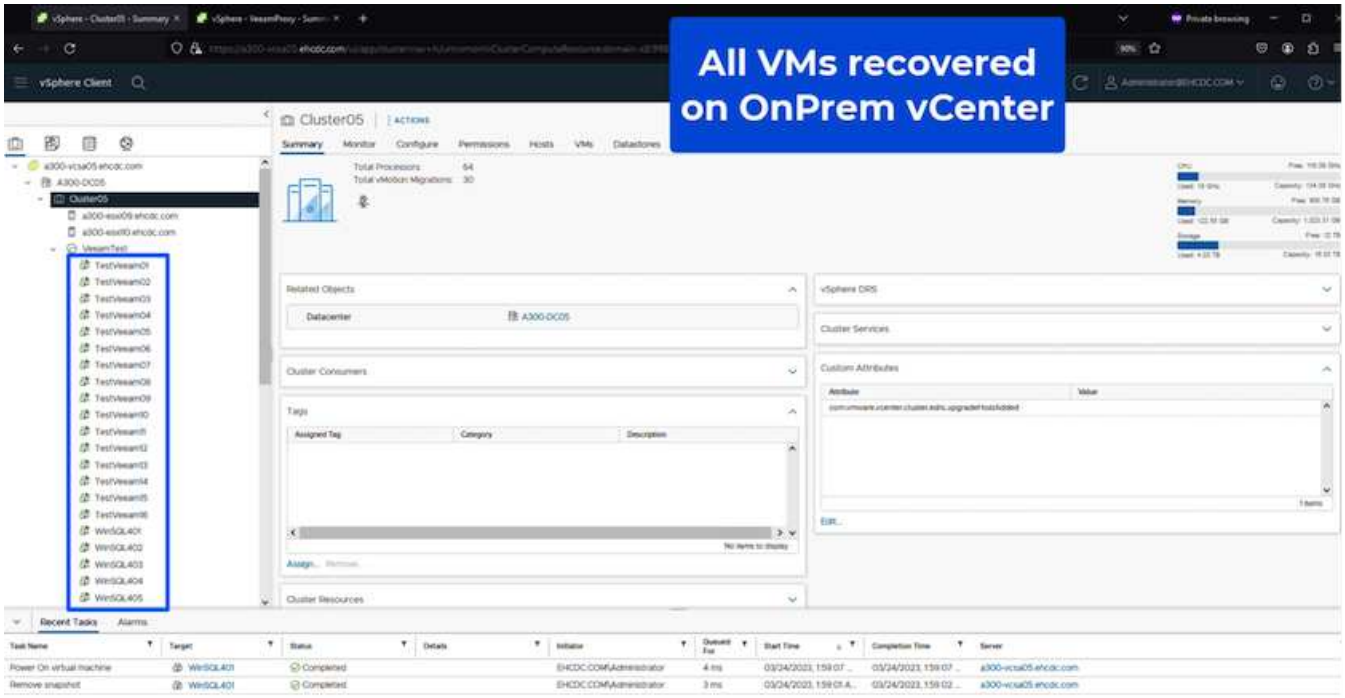
La confirmación de conmutación por error es una de las formas de finalizar la operación de conmutación por error. Cuando se confirma la conmutación por error, se confirma que los cambios enviados a la máquina virtual que se conmutó (la máquina virtual de producción) funcionan como se esperaba. Después de 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 error, consulte la documentación de Veeam."Conmutación por error y recuperación para replicación" .





Una vez que la conmutación a producción es exitosa, todas las máquinas virtuales se restauran al sitio de producción original.



Conclusión

La capacidad de almacenamiento de datos de FSx ONTAP permite que Veeam o cualquier herramienta de terceros validada proporcione una solución de recuperación ante desastres de bajo costo mediante un clúster Pilot Light y sin tener que instalar una gran cantidad de hosts en el clúster solo para acomodar la copia de réplica de la máquina virtual. Esto proporciona una solución poderosa para manejar un plan de recuperación ante desastres personalizado y a medida, y también permite reutilizar los productos de respaldo existentes internamente para satisfacer las necesidades de DR, habilitando así la recuperación ante desastres basada en la nube al salir de los centros de datos de DR en las instalaciones. La conmutación por error se puede realizar de forma planificada o con solo hacer clic en un botón cuando ocurre un desastre y se toma la decisión de activar el sitio de recuperación ante desastres.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado.

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

Migrar cargas de trabajo en AWS/VMC

TR 4942: Migración de cargas de trabajo al almacén de datos de FSx ONTAP mediante VMware HCX

Un caso de uso común de VMware Cloud (VMC) en Amazon Web Services (AWS), con su almacén de datos NFS complementario en Amazon FSx ONTAP, es la migración de cargas de trabajo de VMware. VMware HCX es una opción preferida y ofrece varios métodos de migración para mover máquinas virtuales (VM) locales y sus datos, que se ejecutan en cualquier almacén de datos compatible con VMware, a almacenes de datos VMC, que incluyen almacenes de datos NFS complementarios en FSx ONTAP.

Descripción general: Migración de máquinas virtuales con VMware HCX, almacenes de datos complementarios de FSx ONTAP y VMware Cloud

VMware HCX es principalmente una plataforma de movilidad diseñada para simplificar la migración de la carga de trabajo, el reequilibrio de la carga de trabajo y la continuidad del negocio en las nubes. Se incluye como parte de VMware Cloud on AWS y ofrece muchas formas de migrar cargas de trabajo y puede usarse para operaciones de recuperación ante desastres (DR).

Este documento proporciona una guía paso a paso para implementar y configurar VMware HCX, incluidos todos sus componentes principales, en las instalaciones y en el centro de datos de la nube, lo que permite varios mecanismos de migración de máquinas virtuales.

Para obtener más información, consulte "Guía del usuario de VMware HCX" y "Lista de verificación de instalación B - HCX con un entorno de destino SDDC de VMware Cloud on AWS" .

▼ **Pasos de alto nivel**

Esta lista proporciona los pasos de alto nivel para instalar y configurar VMware HCX:

1. Active HCX para el centro de datos definido por software (SDDC) de VMC a través de VMware Cloud Services Console.
2. Descargue e implemente el instalador OVA del conector HCX en el servidor vCenter local.
3. Activa HCX con una clave de licencia.
4. Empareje VMware HCX Connector local con VMC HCX Cloud Manager.
5. Configurar el perfil de red, el perfil de cómputo y la malla de servicio.

6. (Opcional) Realice la extensión de red para ampliar la red y evitar la re-IP.
7. Validar el estado del dispositivo y asegurarse de que la migración sea posible.
8. Migrar las cargas de trabajo de la máquina virtual.

▼ **Prerrequisitos**

Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte "Preparación para la instalación" . Una vez cumplidos los requisitos previos, incluida la conectividad, configure y active HCX generando una clave de licencia desde la consola VMware HCX en VMC. Una vez activado HCX, se implementa el complemento vCenter y se puede acceder a él mediante la consola vCenter para su administración.

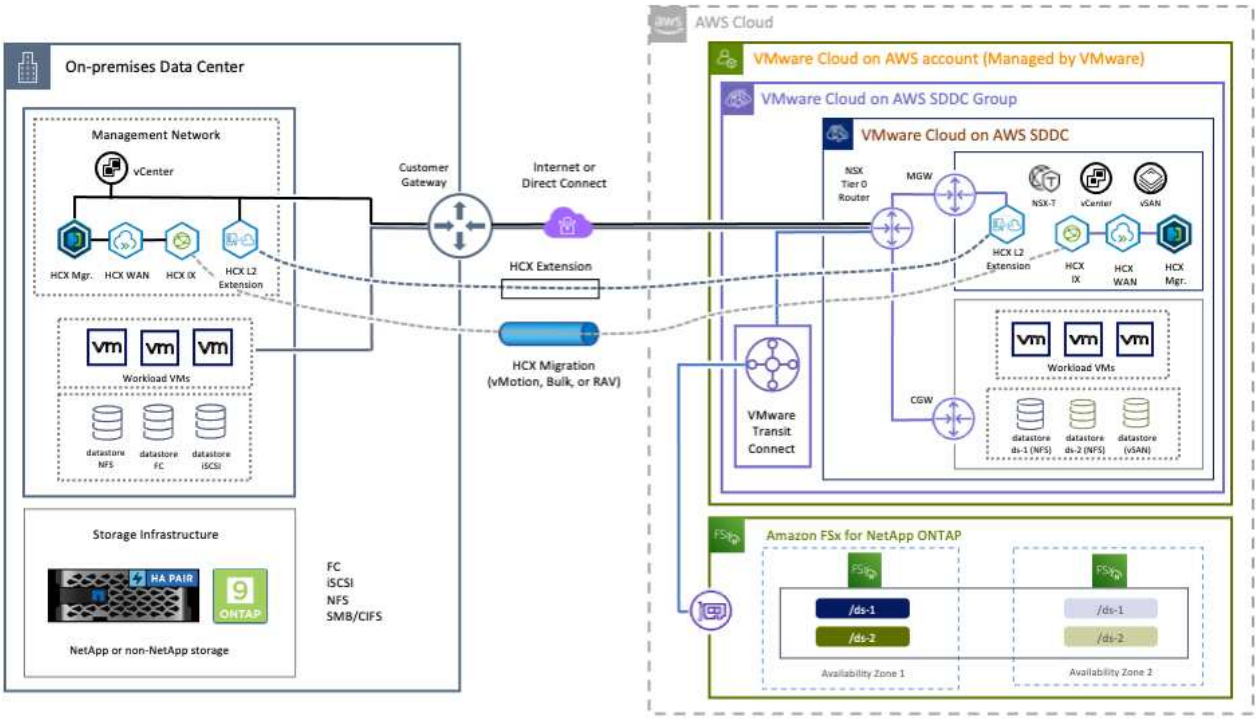
Los siguientes pasos de instalación deben completarse antes de continuar con la activación e implementación de HCX:

1. Utilice un SDDC de VMC existente o cree un nuevo SDDC siguiendo este procedimiento"Enlace de NetApp" o esto "Enlace de VMware" .
2. La ruta de red desde el entorno de vCenter local al SDDC de VMC debe admitir la migración de máquinas virtuales mediante vMotion.
3. Asegúrese de que se cumplan los requisitos "reglas y puertos de firewall" Se permiten para el tráfico de vMotion entre el servidor vCenter local y el vCenter del SDDC.
4. El volumen NFS de FSx ONTAP debe montarse como un almacén de datos complementario en el SDDC de VMC. Para conectar los almacenes de datos NFS al clúster apropiado, siga los pasos descritos en este"Enlace de NetApp" o esto "Enlace de VMware" .

▼ **Arquitectura de alto nivel**

Para fines de prueba, el entorno de laboratorio local utilizado para esta validación se conectó a través de una VPN de sitio a sitio a AWS VPC, lo que permitió la conectividad local a AWS y al SDDC de VMware Cloud a través de una puerta de enlace de tránsito externa. El tráfico de migración de HCX y extensión de red fluye a través de Internet entre el SDDC de destino local y el SDDC de nube de VMware. Esta arquitectura se puede modificar para utilizar interfaces virtuales privadas de Direct Connect.

La siguiente imagen muestra la arquitectura de alto nivel.



Implementación de la solución

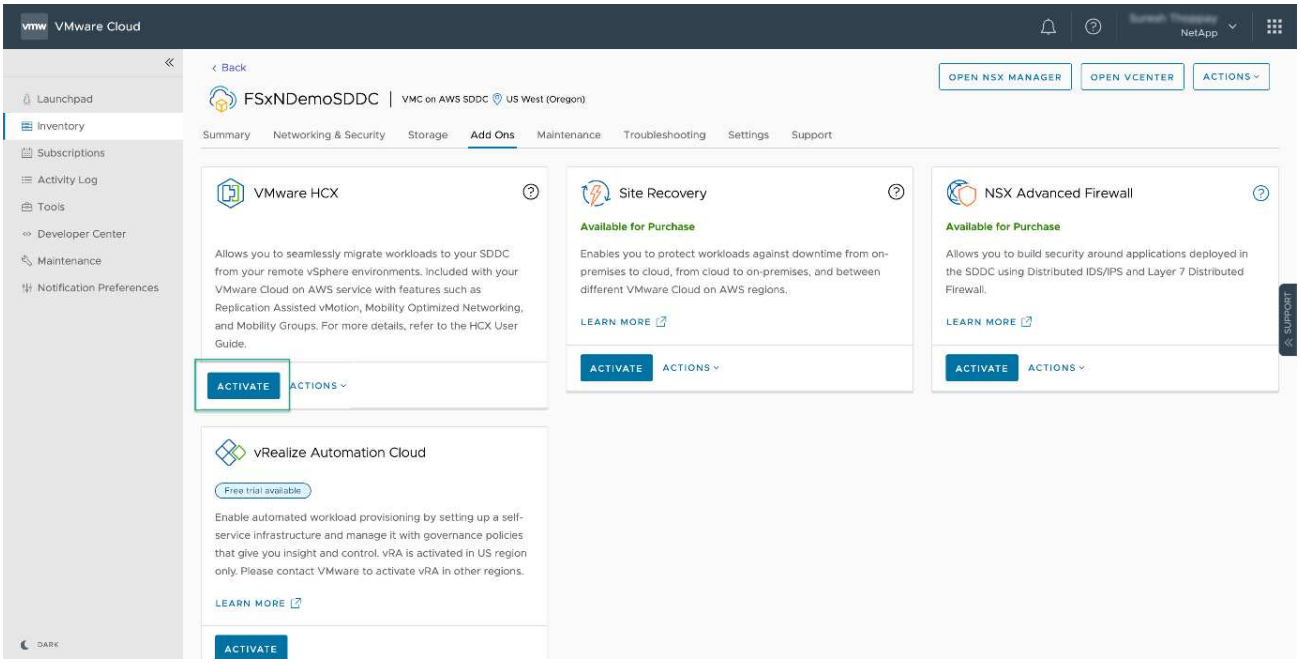
Siga la serie de pasos para completar la implementación de esta solución:

▼ **Paso 1: Activar HCX a través de VMC SDDC usando la opción Complementos**

Para realizar la instalación, complete los siguientes pasos:

1. Inicie sesión en la consola VMC en "vmc.vmware.com" y acceder al inventario.
2. Para seleccionar el SDDC apropiado y acceder a los complementos, haga clic en Ver detalles en SDDC y seleccione la pestaña Complementos.
3. Haga clic en Activar para VMware HCX.

Este paso tarda hasta 25 minutos en completarse.

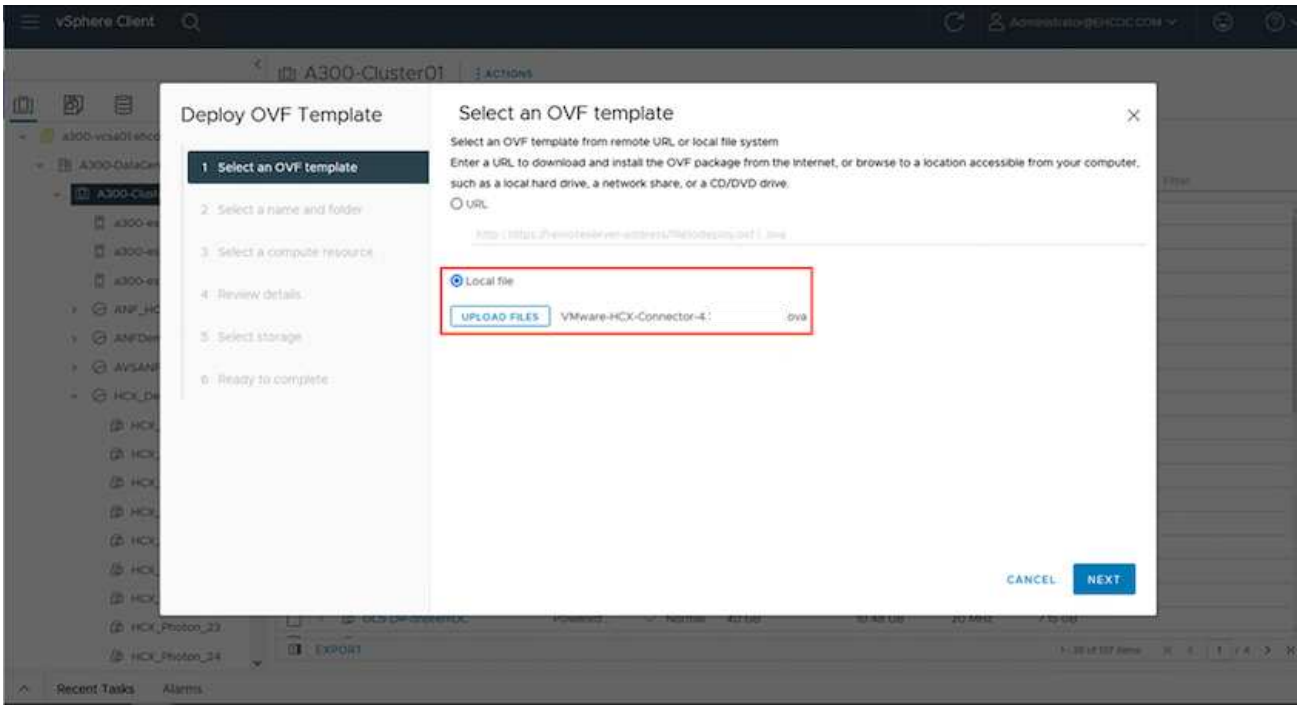


4. Una vez completada la implementación, valide la implementación confirmando que HCX Manager y sus complementos asociados estén disponibles en vCenter Console.
5. Cree los firewalls de Management Gateway adecuados para abrir los puertos necesarios para acceder a HCX Cloud Manager. HCX Cloud Manager ahora está listo para las operaciones de HCX.

▼ Paso 2: Implementar el instalador OVA en el servidor vCenter local

Para que el conector local se comunique con el administrador HCX en VMC, asegúrese de que los puertos de firewall adecuados estén abiertos en el entorno local.

1. Desde la consola VMC, navegue hasta el Panel de HCX, vaya a Administración y seleccione la pestaña Actualización de sistemas. Haga clic en Solicitar un enlace de descarga para la imagen OVA del conector HCX.
2. Con el conector HCX descargado, implemente el OVA en el servidor vCenter local. Haga clic con el botón derecho en vSphere Cluster y seleccione la opción Implementar plantilla OVF.

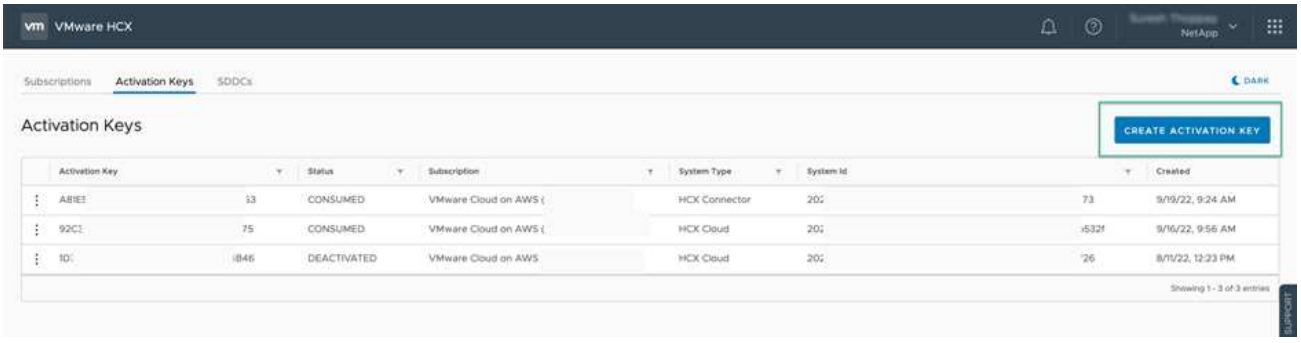


3. Ingrese la información requerida en el asistente Implementar plantilla OVF, haga clic en Siguiente y luego en Finalizar para implementar VMware HCX Connector OVA.
4. Encienda el dispositivo virtual manualmente. Para obtener instrucciones paso a paso, vaya a "Guía del usuario de VMware HCX" .

▼ Paso 3: Activar el conector HCX con la clave de licencia

Después de implementar VMware HCX Connector OVA en las instalaciones e iniciar el dispositivo, complete los siguientes pasos para activar HCX Connector. Genere la clave de licencia desde la consola VMware HCX en VMC e ingrese la licencia durante la configuración del conector VMware HCX.

1. Desde VMware Cloud Console, vaya a Inventario, seleccione el SDDC y haga clic en Ver detalles. Desde la pestaña Complementos, en el mosaico VMware HCX, haga clic en Abrir HCX.
2. Desde la pestaña Claves de activación, haga clic en Crear clave de activación. Seleccione el tipo de sistema como Conector HCX y haga clic en Confirmar para generar la clave. Copiar la clave de activación.



Se requiere una clave separada para cada conector HCX implementado localmente.

3. Inicie sesión en el conector VMware HCX local en "`https://hcxconnectorIP:9443`" utilizando credenciales de administrador.

Utilice la contraseña definida durante la implementación de OVA.

4. En la sección Licencias, ingrese la clave de activación copiada del paso 2 y haga clic en Activar.

El conector HCX local debe tener acceso a Internet para que la activación se complete correctamente.

5. En Ubicación del centro de datos, proporcione la ubicación deseada para instalar VMware HCX Manager en las instalaciones. Haga clic en Continuar.
6. En Nombre del sistema, actualice el nombre y haga clic en Continuar.
7. Seleccione Sí y luego Continuar.
8. En Conectar su vCenter, proporcione la dirección IP o el nombre de dominio completo (FQDN) y las credenciales para el vCenter Server y haga clic en Continuar.

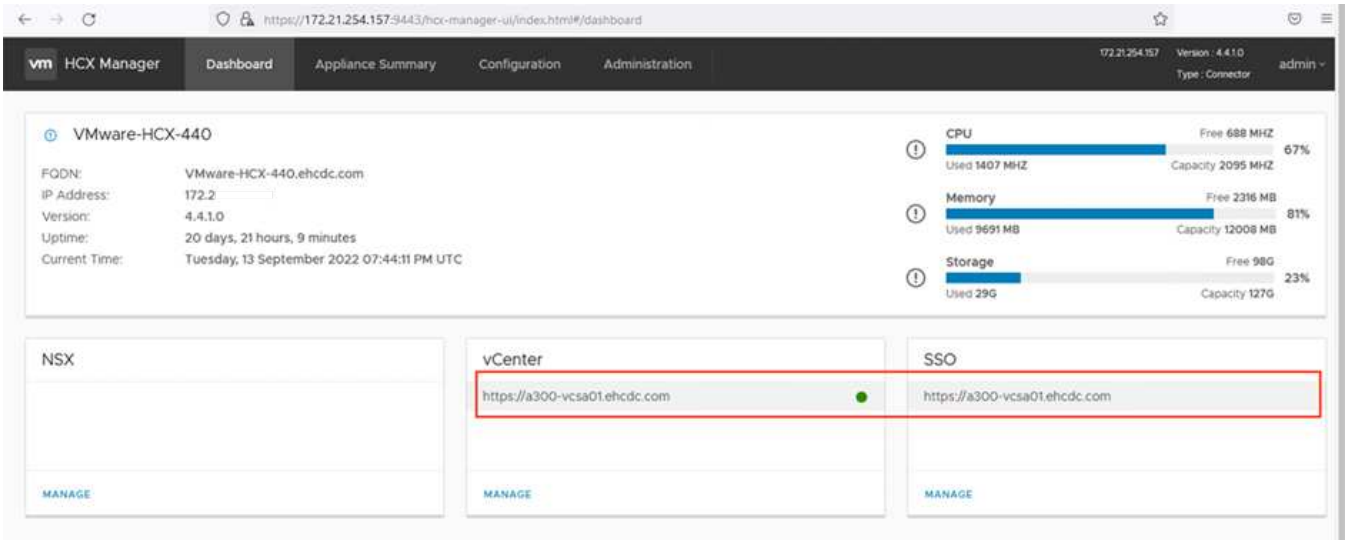
Utilice el FQDN para evitar problemas de comunicación más adelante.

9. En Configurar SSO/PSC, proporcione el FQDN o la dirección IP del controlador de servicios de plataforma y haga clic en Continuar.

Introduzca la dirección IP o el FQDN del vCenter Server.

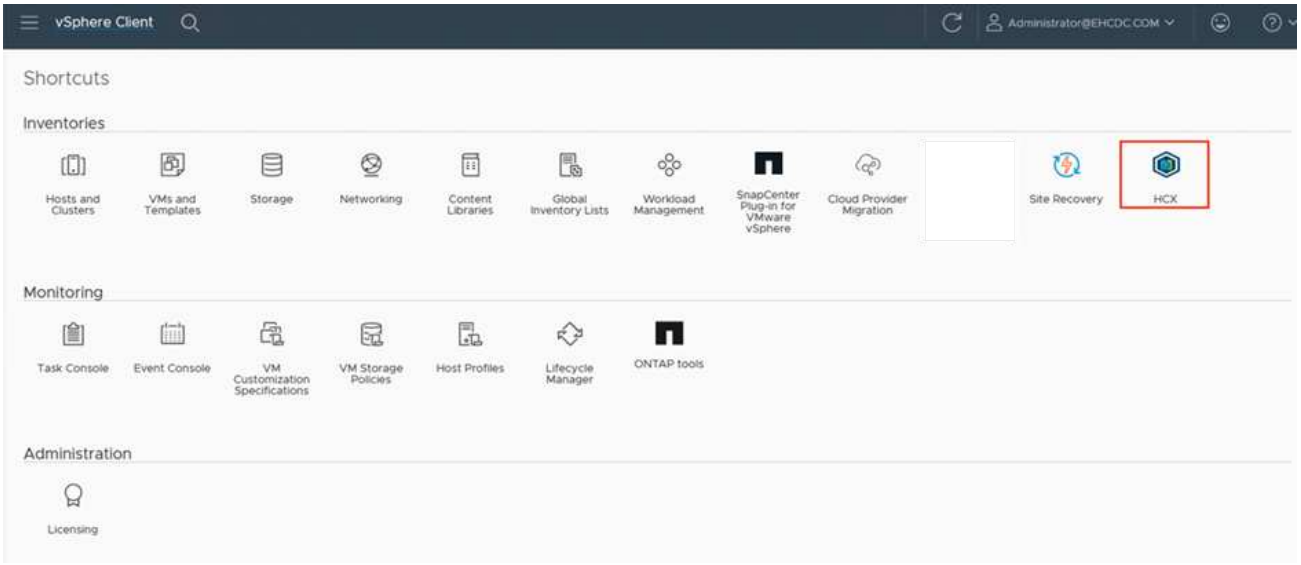
10. Verifique que la información esté ingresada correctamente y haga clic en Reiniciar.
11. Una vez completado, vCenter Server se muestra en verde. Tanto vCenter Server como SSO deben tener los parámetros de configuración correctos, que deben ser los mismos que en la página anterior.

Este proceso debería tardar aproximadamente entre 10 y 20 minutos para que el complemento se agregue al vCenter Server.

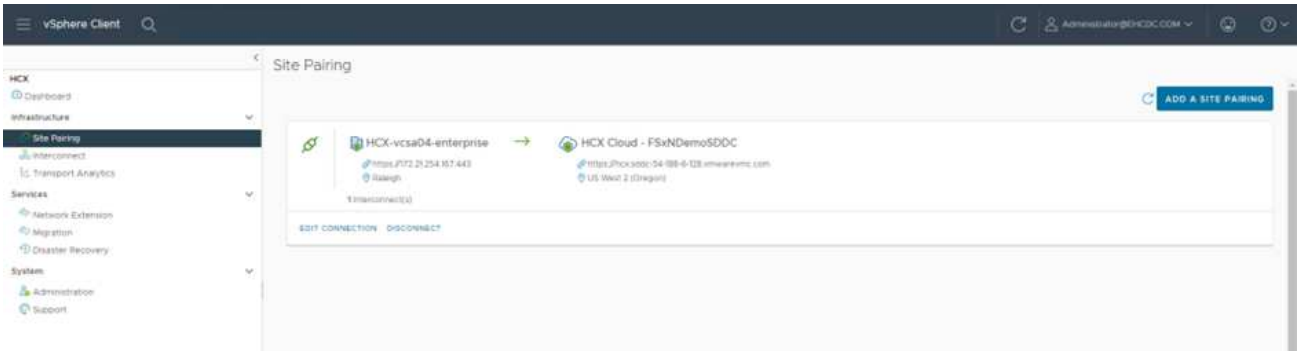


▼ Paso 4: Vincular el conector VMware HCX local con VMC HCX Cloud Manager

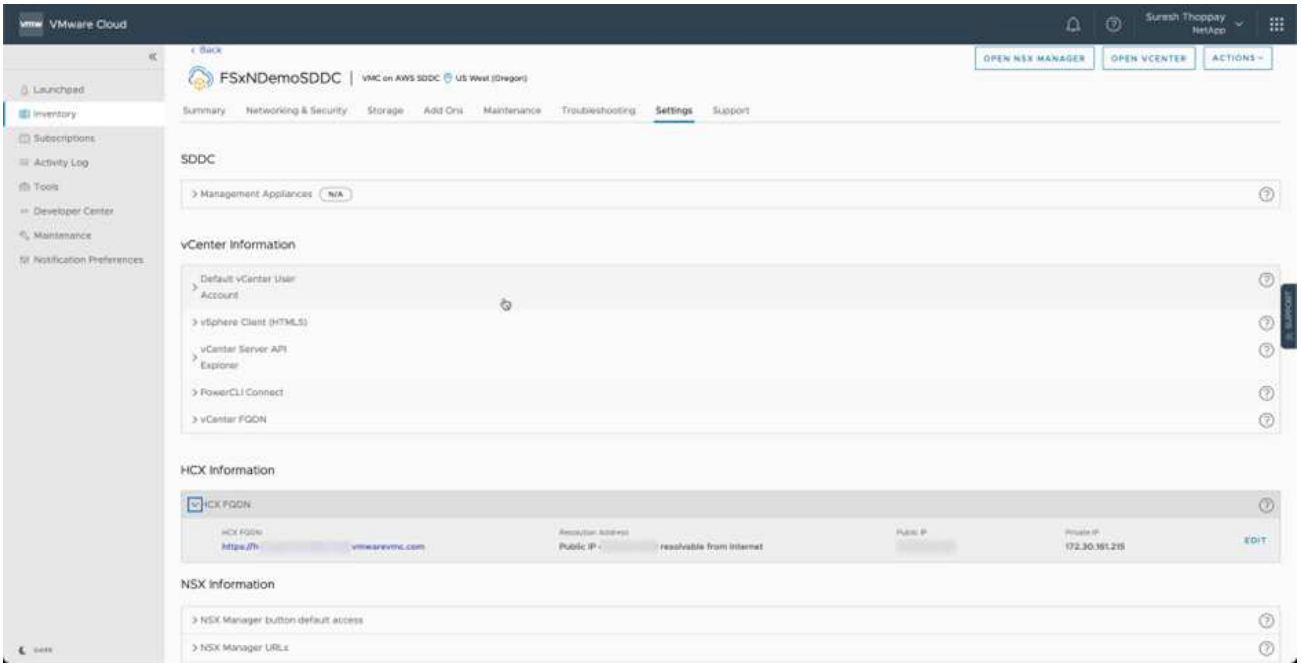
1. Para crear un par de sitios entre el vCenter Server local y el SDDC de VMC, inicie sesión en el vCenter Server local y acceda al complemento HCX vSphere Web Client.

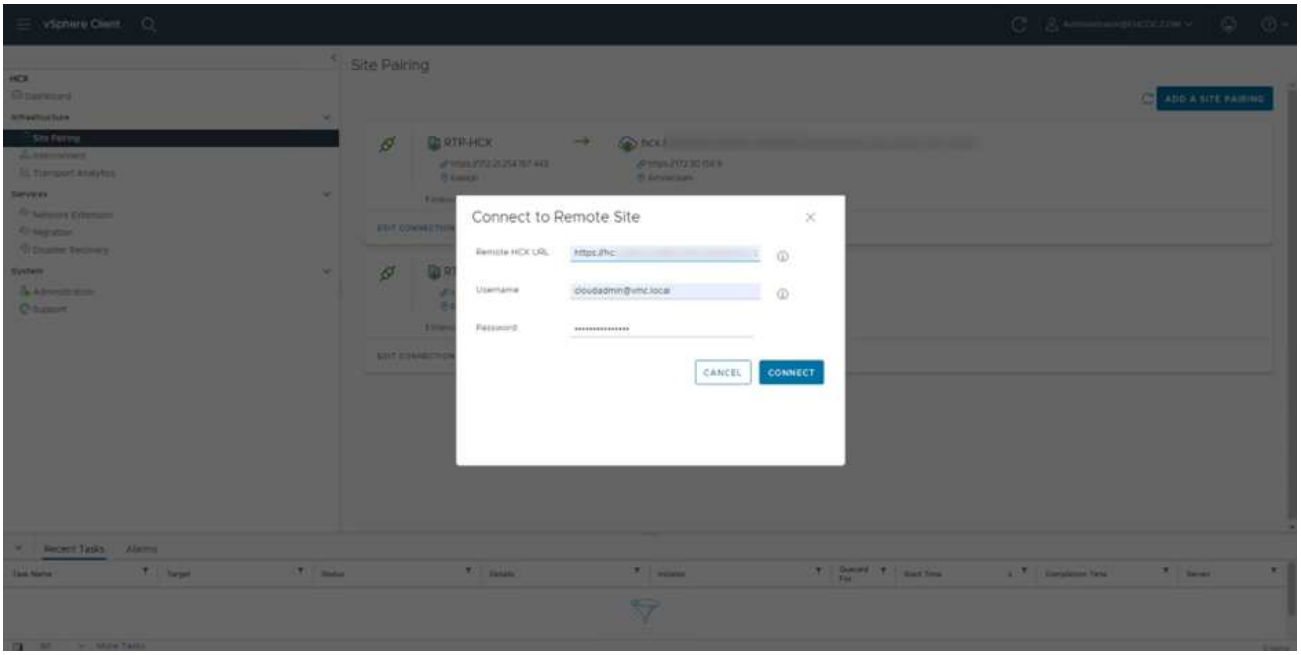


2. En Infraestructura, haga clic en Agregar un emparejamiento de sitios. Para autenticar el sitio remoto, ingrese la URL o la dirección IP de VMC HCX Cloud Manager y las credenciales para la función CloudAdmin.



La información de HCX se puede recuperar desde la página de configuración de SDDC.





3. Para iniciar el emparejamiento del sitio, haga clic en Conectar.

> VMware HCX Connector debe poder comunicarse con la IP de HCX Cloud Manager a través del puerto 443.

4. Una vez creado el emparejamiento, el emparejamiento del sitio recién configurado estará disponible en el Panel de HCX.

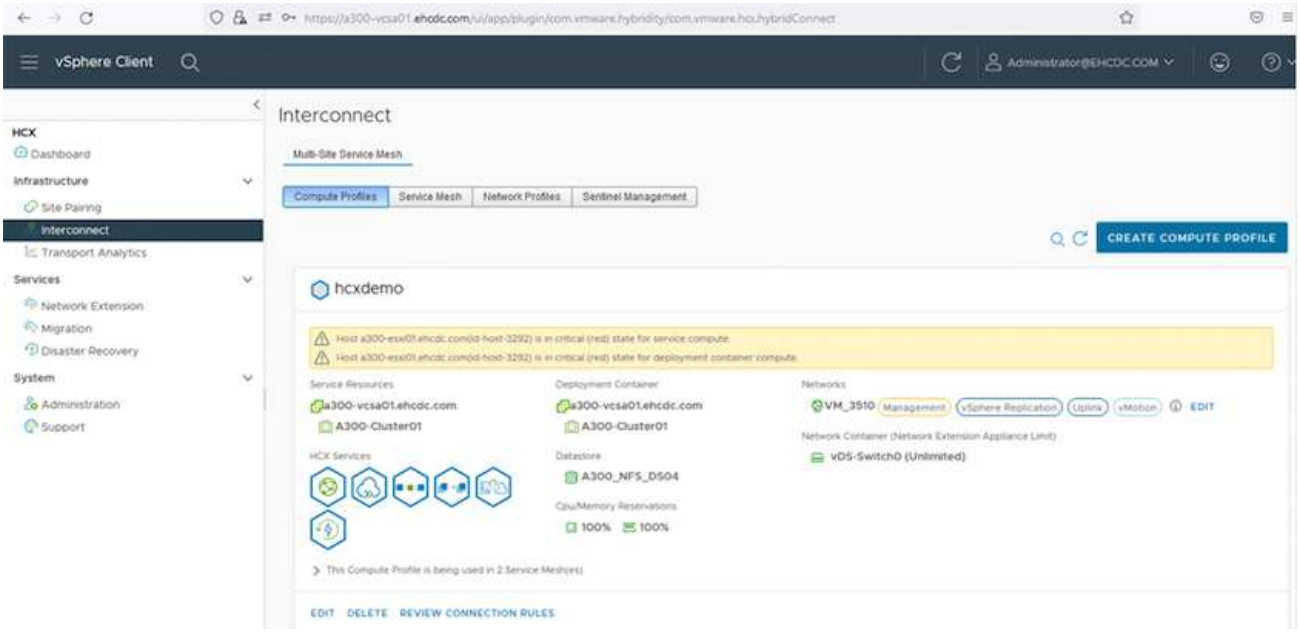
▼ **Paso 5: Configurar el perfil de red, el perfil de cómputo y la malla de servicio**

El dispositivo VMware HCX Interconnect (HCX-IX) proporciona capacidades de túnel seguro a través de Internet y conexiones privadas al sitio de destino que habilitan la replicación y las capacidades basadas en vMotion. La interconexión proporciona cifrado, ingeniería de tráfico y una SD-WAN. Para crear el dispositivo de interconexión HCI-IX, complete los siguientes pasos:

1. En Infraestructura, seleccione Interconexión > Malla de servicios multisitio > Perfiles de cómputo > Crear perfil de cómputo.

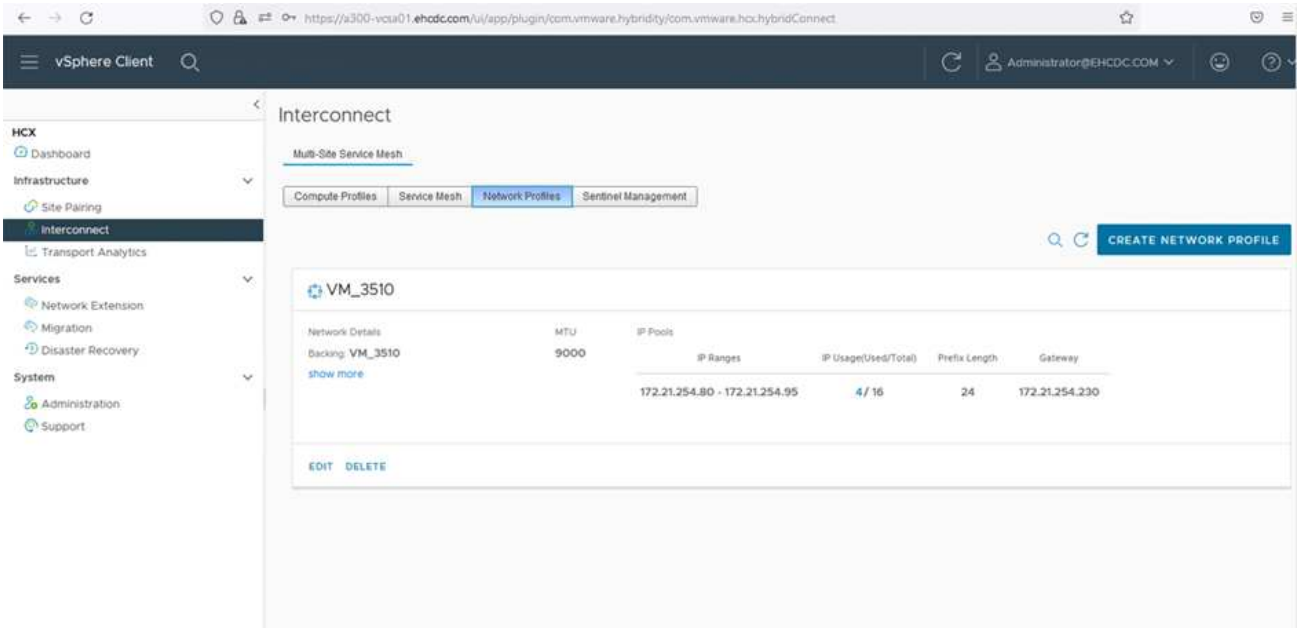
> Los perfiles de cómputo contienen los parámetros de implementación de red, almacenamiento y cómputo necesarios para implementar un dispositivo virtual de interconexión. También especifican qué parte del centro de datos de VMware será accesible para el servicio HCX.

Para obtener instrucciones detalladas, consulte "Creación de un perfil de cómputo" .



2. Una vez creado el perfil de cómputo, cree el perfil de red seleccionando Multi-Site Service Mesh > Perfiles de red > Crear perfil de red.
3. El perfil de red define un rango de direcciones IP y redes que HCX utilizará para sus dispositivos virtuales.

> Esto requerirá dos o más direcciones IP. Estas direcciones IP se asignarán desde la red de administración a los dispositivos virtuales.



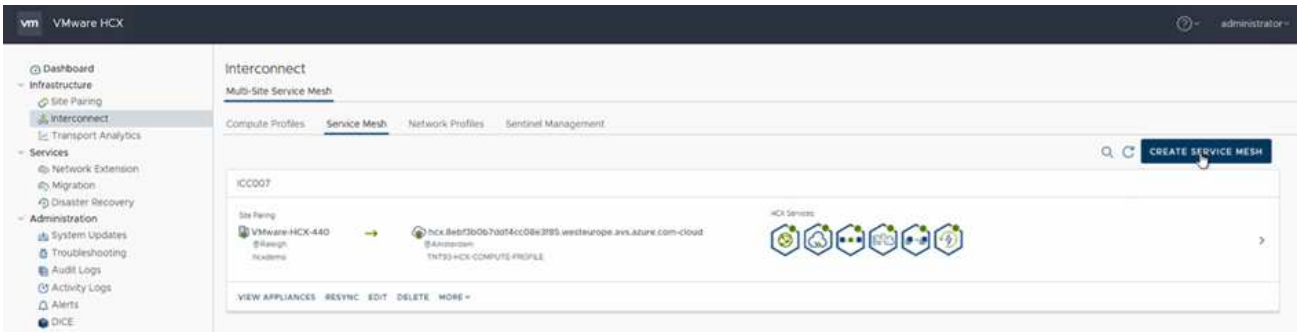
Para obtener instrucciones detalladas, consulte "Creación de un perfil de red" .

> Si se conecta a una SD-WAN a través de Internet, deberá reservar IP públicas en la sección Redes y seguridad.

4. Para crear una malla de servicio, seleccione la pestaña Malla de servicio dentro de la opción

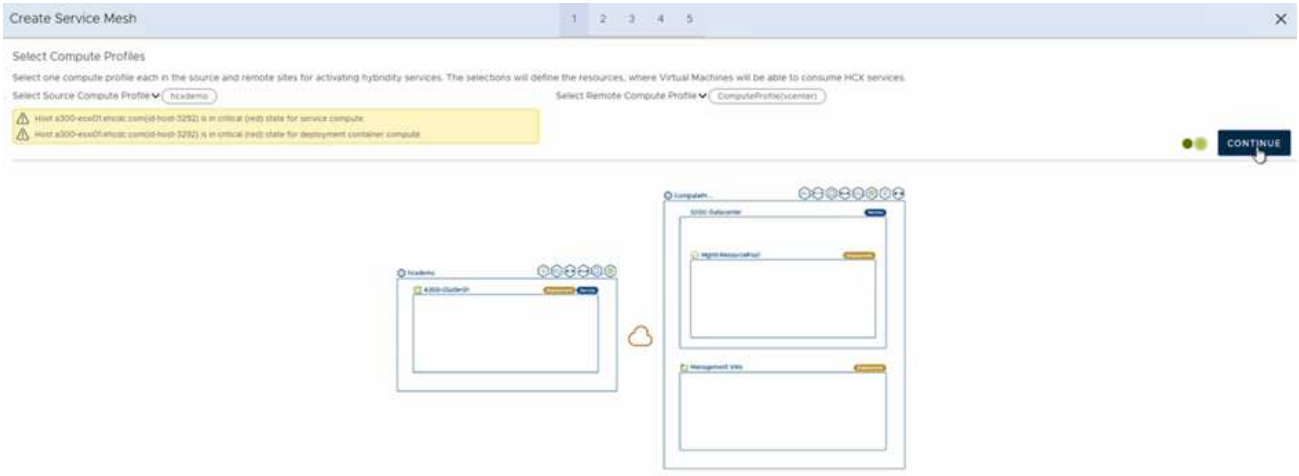
Interconexión y seleccione sitios locales y VMC SDDC.

La malla de servicio establece un par de perfiles de red y cómputo locales y remotos.

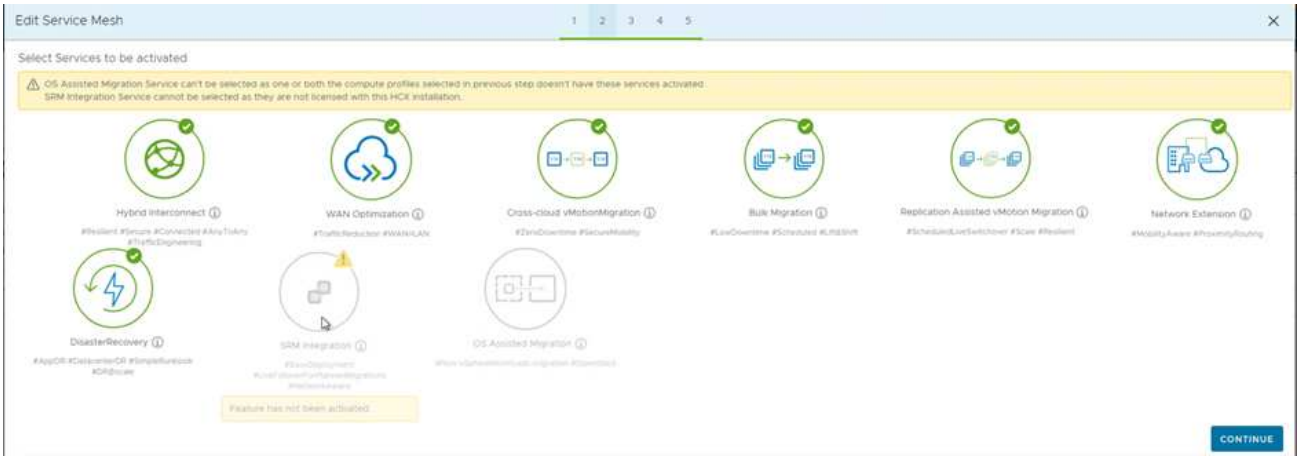


Parte de este proceso implica la implementación de dispositivos HCX que se configurarán automáticamente en los sitios de origen y de destino, creando una estructura de transporte segura.

5. Seleccione los perfiles de cómputo de origen y remoto y haga clic en Continuar.

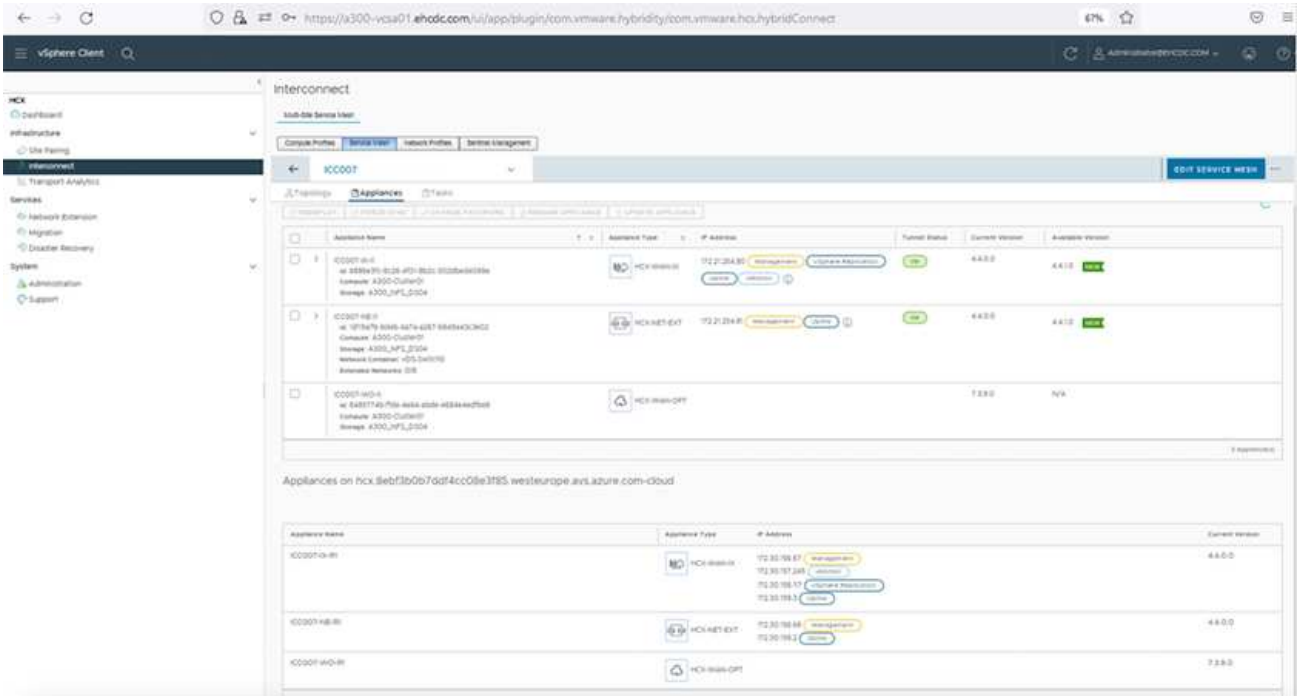


6. Seleccione el servicio que desea activar y haga clic en Continuar.



Se requiere una licencia HCX Enterprise para la migración vMotion asistida por replicación, la integración de SRM y la migración asistida por SO.

7. Cree un nombre para la malla de servicio y haga clic en Finalizar para comenzar el proceso de creación. La implementación debería tardar aproximadamente 30 minutos en completarse. Una vez configurada la malla de servicio, se ha creado la infraestructura virtual y la red necesarias para migrar las máquinas virtuales de carga de trabajo.



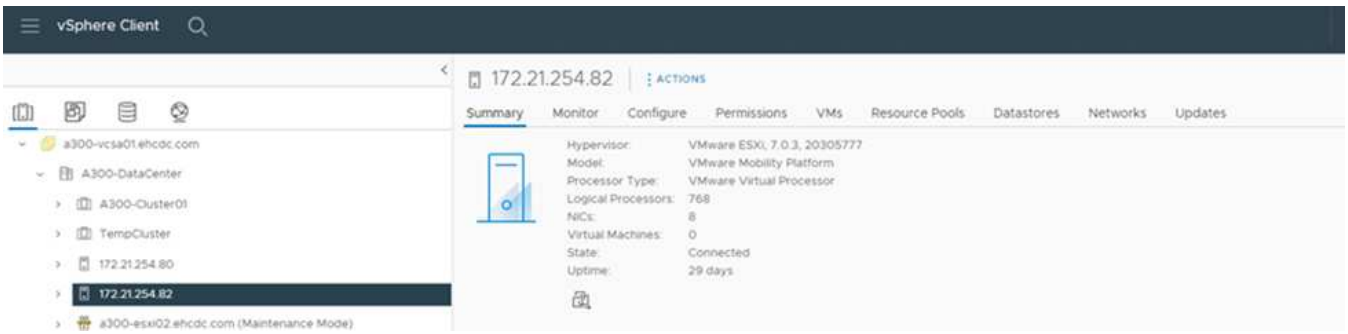
▼ Paso 6: Migración de cargas de trabajo

HCX proporciona servicios de migración bidireccional entre dos o más entornos distintos, como SDDC locales y VMC. Las cargas de trabajo de las aplicaciones se pueden migrar hacia y desde sitios activados por HCX mediante una variedad de tecnologías de migración, como migración masiva de HCX, HCX vMotion, migración en frío de HCX, HCX Replication Assisted vMotion (disponible con la edición HCX Enterprise) y HCX OS Assisted Migration (disponible con la edición HCX Enterprise).

Para obtener más información sobre las tecnologías de migración HCX disponibles, consulte "Tipos de migración de VMware HCX"

El dispositivo HCX-IX utiliza el servicio Mobility Agent para realizar migraciones de vMotion, Cold y Replication Assisted vMotion (RAV).

El dispositivo HCX-IX agrega el servicio Mobility Agent como un objeto host en vCenter Server. Los recursos de procesador, memoria, almacenamiento y red que se muestran en este objeto no representan el consumo real en el hipervisor físico que aloja el dispositivo IX.

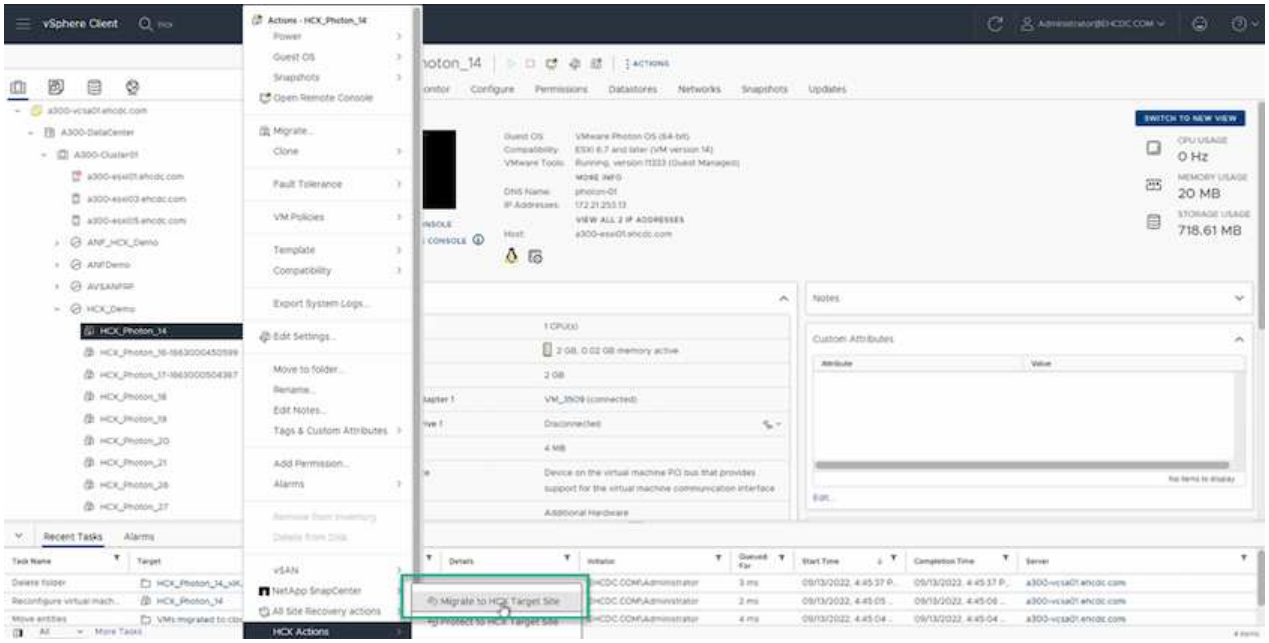


▼ VMware HCX vMotion

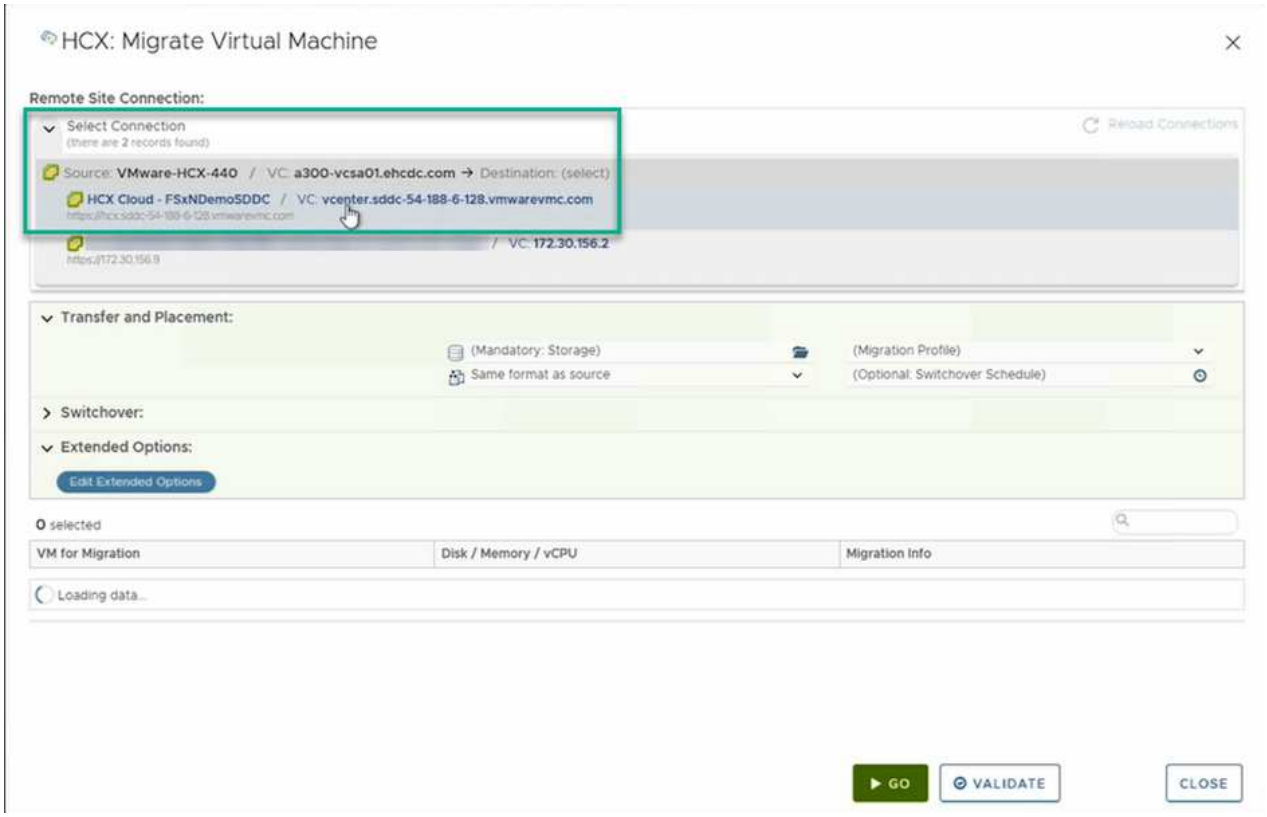
Esta sección describe el mecanismo HCX vMotion. Esta tecnología de migración utiliza el protocolo VMware vMotion para migrar una VM a VMC SDDC. La opción de migración de vMotion se utiliza para migrar el estado de una sola máquina virtual a la vez. No hay interrupción del servicio durante este método de migración.

> La extensión de red debe estar en su lugar (para el grupo de puertos en el que está conectada la VM) para poder migrar la VM sin la necesidad de realizar un cambio de dirección IP.

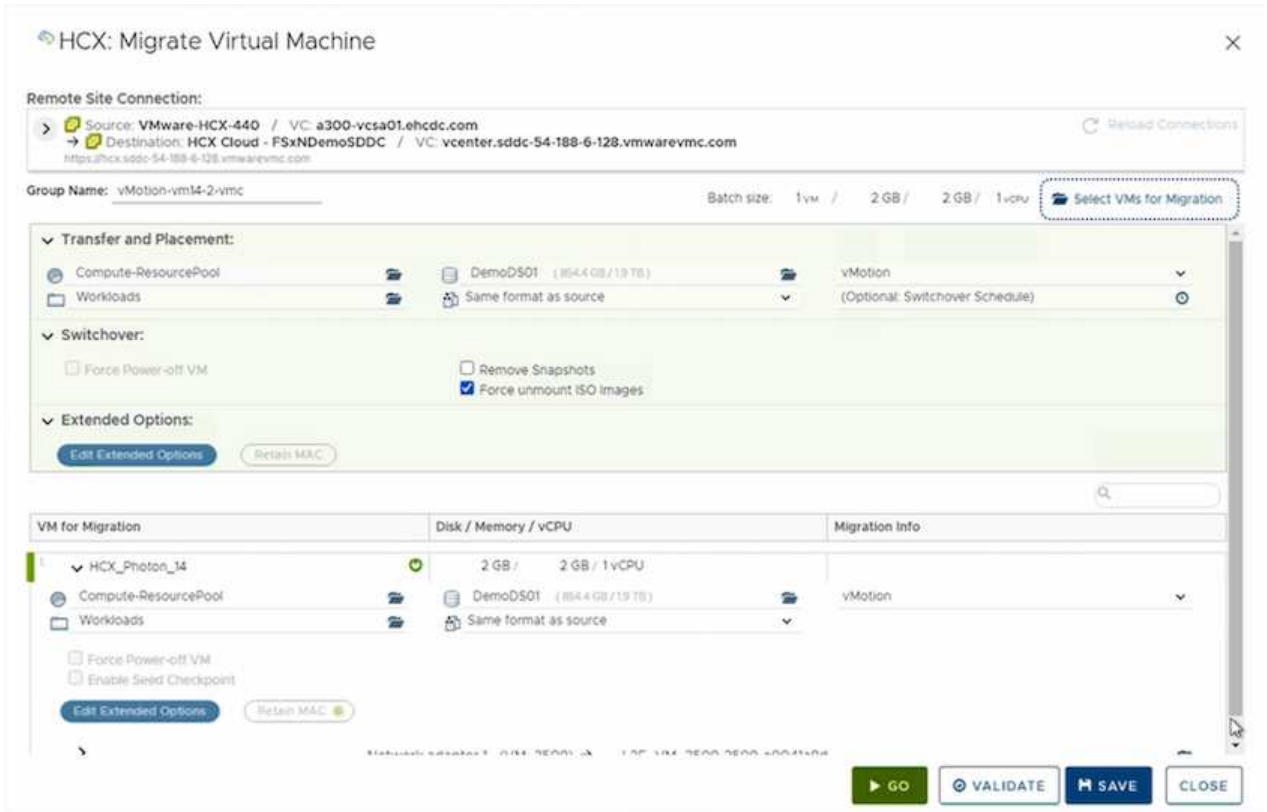
1. Desde el cliente vSphere local, vaya a Inventario, haga clic con el botón derecho en la VM que se migrará y seleccione Acciones HCX > Migrar al sitio de destino HCX.



2. En el asistente Migrar máquina virtual, seleccione la Conexión del sitio remoto (SDDC de VMC de destino).



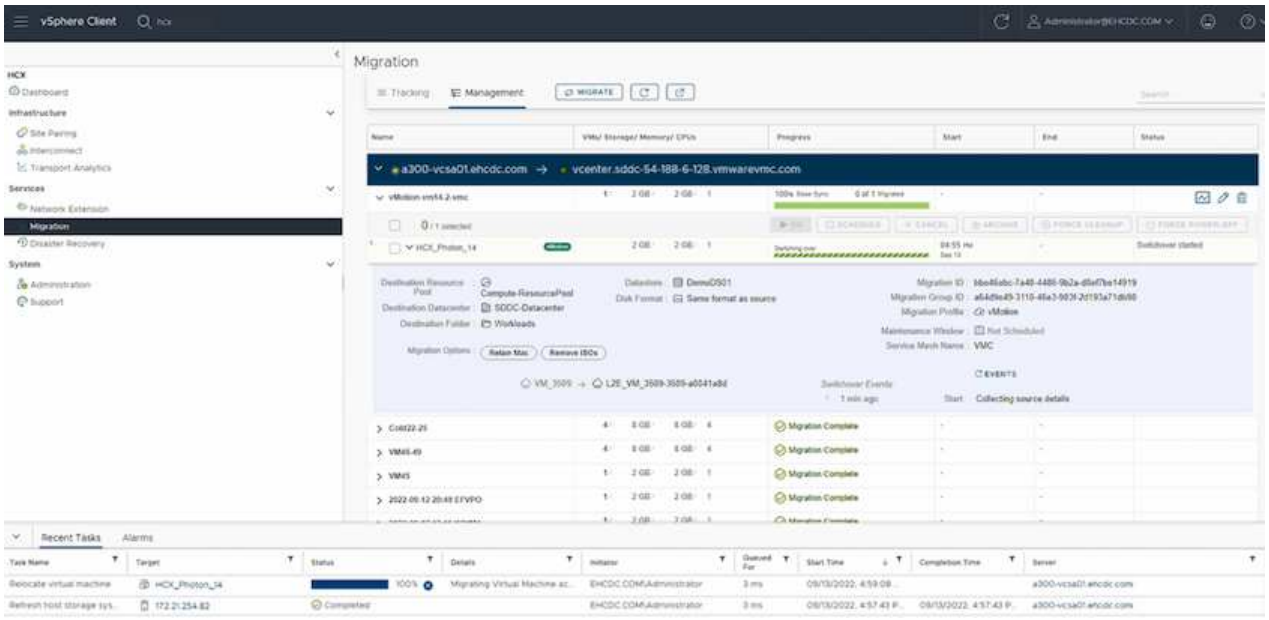
3. Agregue un nombre de grupo y, en Transferencia y ubicación, actualice los campos obligatorios (Clúster, Almacenamiento y Red de destino). Haga clic en Validar.



4. Una vez completadas las comprobaciones de validación, haga clic en Ir para iniciar la migración.

La transferencia de vMotion captura la memoria activa de la VM, su estado de ejecución, su dirección IP y su dirección MAC. Para obtener más información sobre los requisitos y limitaciones de HCX vMotion, consulte "Comprensión de VMware HCX vMotion y la migración en frío" .

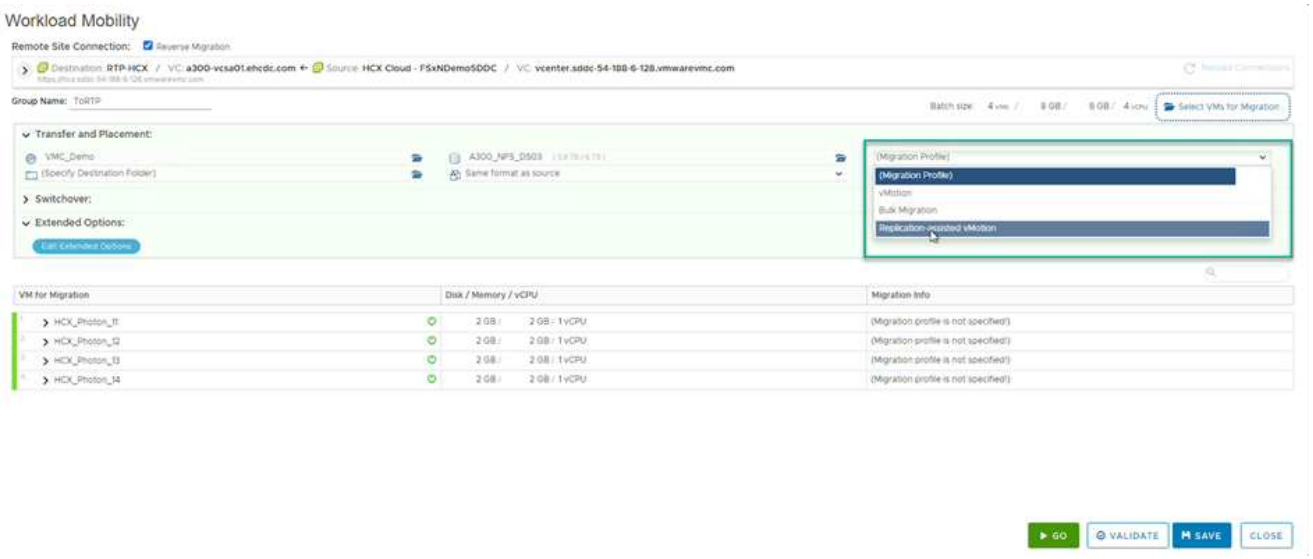
5. Puede supervisar el progreso y la finalización de vMotion desde el panel de HCX > Migración.



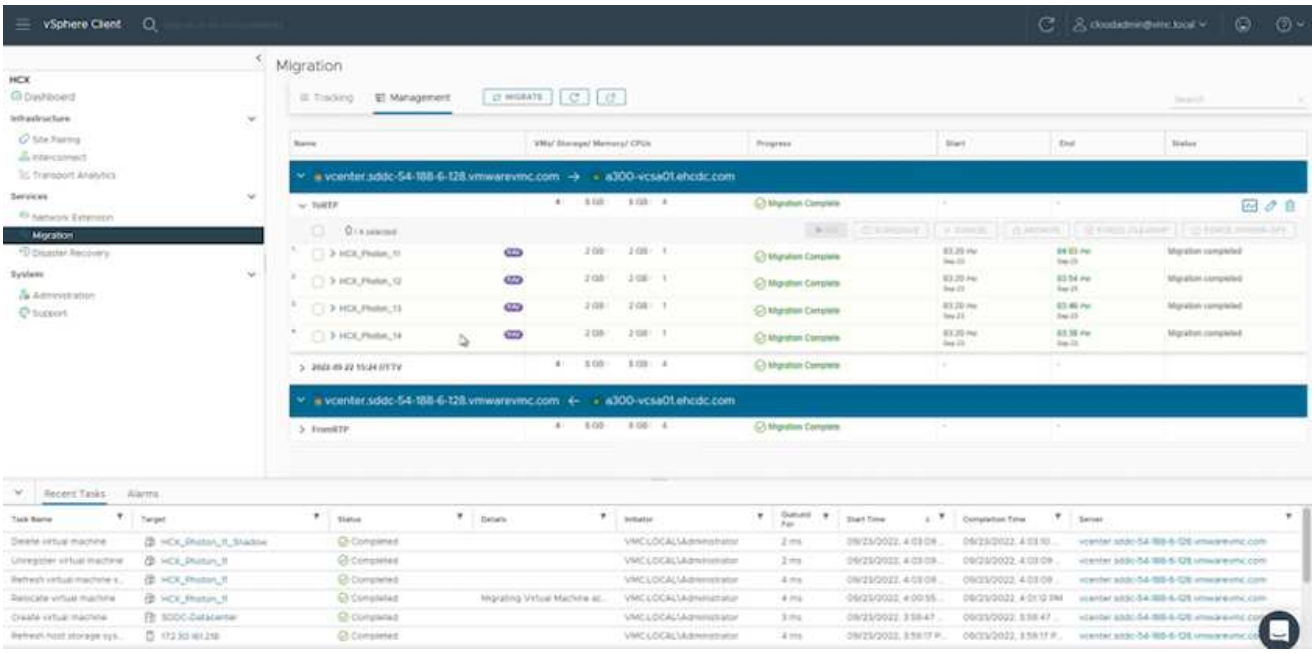
▼ **VMware Replication Assisted vMotion**

Como habrás notado en la documentación de VMware, VMware HCX Replication Assisted vMotion (RAV) combina los beneficios de la migración masiva y vMotion. La migración masiva utiliza vSphere Replication para migrar varias máquinas virtuales en paralelo: la máquina virtual se reinicia durante el cambio. HCX vMotion migra sin tiempo de inactividad, pero se realiza en serie, una máquina virtual a la vez en un grupo de replicación. RAV replica la VM en paralelo y la mantiene sincronizada hasta la ventana de cambio. Durante el proceso de cambio, se migra una máquina virtual a la vez sin tiempo de inactividad para la máquina virtual.

La siguiente captura de pantalla muestra el perfil de migración como Replication Assisted vMotion.



La duración de la replicación puede ser mayor en comparación con el vMotion de una pequeña cantidad de máquinas virtuales. Con RAV, solo sincroniza los deltas e incluye el contenido de la memoria. La siguiente es una captura de pantalla del estado de la migración: muestra cómo la hora de inicio de la migración es la misma y la hora de finalización es diferente para cada VM.



Para obtener información adicional sobre las opciones de migración de HCX y sobre cómo migrar cargas de trabajo desde las instalaciones locales a VMware Cloud on AWS mediante HCX, consulte "Guía del usuario de VMware HCX" .

VMware HCX vMotion requiere una capacidad de rendimiento de 100 Mbps o superior.

El almacén de datos de VMC FSx ONTAP de destino debe tener espacio suficiente para acomodar la migración.

Conclusión

Ya sea que su objetivo sea una nube completa o una nube híbrida y que los datos residan en cualquier tipo o proveedor de almacenamiento en las instalaciones, Amazon FSx ONTAP junto con HCX brindan excelentes opciones para implementar y migrar las cargas de trabajo al mismo tiempo que reducen el TCO al hacer que los requisitos de los datos se integren perfectamente con la capa de aplicación. Cualquiera que sea el caso de uso, elija VMC junto con el almacén de datos FSx ONTAP para obtener rápidamente los beneficios de la nube, una infraestructura consistente y operaciones en las instalaciones locales y en múltiples nubes, portabilidad bidireccional de cargas de trabajo y capacidad y rendimiento de nivel empresarial. Es el mismo proceso y procedimientos familiares que se utilizan para conectar el almacenamiento y migrar máquinas virtuales mediante la replicación de VMware vSphere, VMware vMotion o incluso la copia NFC.

Comida para llevar

Los puntos clave de este documento incluyen:

- Ahora puede utilizar Amazon FSx ONTAP como almacén de datos con VMC SDDC.
- Puede migrar fácilmente datos desde cualquier centro de datos local a VMC que se ejecuta con el almacén de datos FSx ONTAP

- Puede ampliar y reducir fácilmente el almacén de datos de FSx ONTAP para cumplir con los requisitos de capacidad y rendimiento durante la actividad de migración.

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes enlaces de sitios web:

- Documentación de VMware Cloud

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Documentación de Amazon FSx ONTAP

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  Guía del usuario de VMware HCX

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

NetApp para AWS/EVS

Montar FSx ONTAP como almacén de datos externo para EVS

Cómo montar Amazon FSx for NetApp ONTAP como un almacén de datos externo para Amazon Elastic VMware Service

Este documento presentará los pasos detallados para crear un sistema de archivos FSx para ONTAP y adjuntarlo para su uso como almacén de datos de Interfaz de sistemas de computadoras pequeñas de Internet (iSCSI) o Sistema de archivos de red (NFS) para su uso con Amazon EVS.

Introducción

Las organizaciones con inversiones existentes en VMware en sus instalaciones que buscan formas eficientes y rentables de modernizar sus implementaciones mediante la migración, la expansión, la extensión o la protección (copias de seguridad, recuperación ante desastres) de copias en AWS se han enfrentado a varios desafíos. Con el lanzamiento de Amazon Elastic VMware Service (Amazon EVS), ahora existe un servicio nativo de AWS que permite ejecutar VMware Cloud Foundation (VCF) directamente en una Amazon Virtual Private Cloud (VPC).

Amazon EVS permite ampliar las implementaciones de VCF existentes a AWS, integrarse en AWS para ampliar el rendimiento durante el uso pico y ejecutar completamente cargas de trabajo de VCF en AWS para facilitar modernizaciones, salidas de centros de datos, consolidaciones y otros casos de uso.

Si bien Amazon EVS ofrece importantes beneficios, la arquitectura hiperconvergente predeterminada combina computación y almacenamiento, lo que impide el escalamiento independiente de uno u otro según lo dicten las necesidades del negocio. En el mundo actual centrado en los datos, las demandas de almacenamiento en muchas organizaciones son mayores que las de computación. Sin embargo, con la arquitectura hiperconvergente de VMware, los recursos de almacenamiento se combinan con los recursos computacionales. Esto significa que el escalamiento del almacenamiento solo se puede realizar agregando hosts de cómputo que nunca se utilizarán. Es una situación que puede aumentar considerablemente los

costos, especialmente en cargas de trabajo con gran uso de almacenamiento.

Para resolver este problema, AWS y NetApp ofrecen Amazon FSx for NetApp ONTAP (FSx for ONTAP) como servicio de almacenamiento externo para Amazon EVS. FSx for ONTAP es un servicio de almacenamiento nativo de AWS que ofrece las características de alto rendimiento, resiliencia de datos y rentabilidad del software NetApp ONTAP . Al usar FSx para ONTAP como almacenamiento externo, los usuarios de Amazon EVS pueden escalar los recursos de cómputo y almacenamiento de forma independiente, lo que permite un costo total de propiedad (TCO) óptimo.

Descripción general

Este documento presentará los pasos detallados para crear un sistema de archivos FSx para ONTAP y adjuntarlo para su uso como almacén de datos de Interfaz de sistemas de computadoras pequeñas de Internet (iSCSI) o Sistema de archivos de red (NFS) para su uso con Amazon EVS.

Propósito de esta Guía

Esta guía proporciona instrucciones sobre cómo configurar un almacén de datos FSx para ONTAP para Amazon EVS, así como las mejores prácticas, los requisitos de compatibilidad, las consideraciones de tamaño y otra información para ayudarlo a planificar, diseñar e implementar la integración.

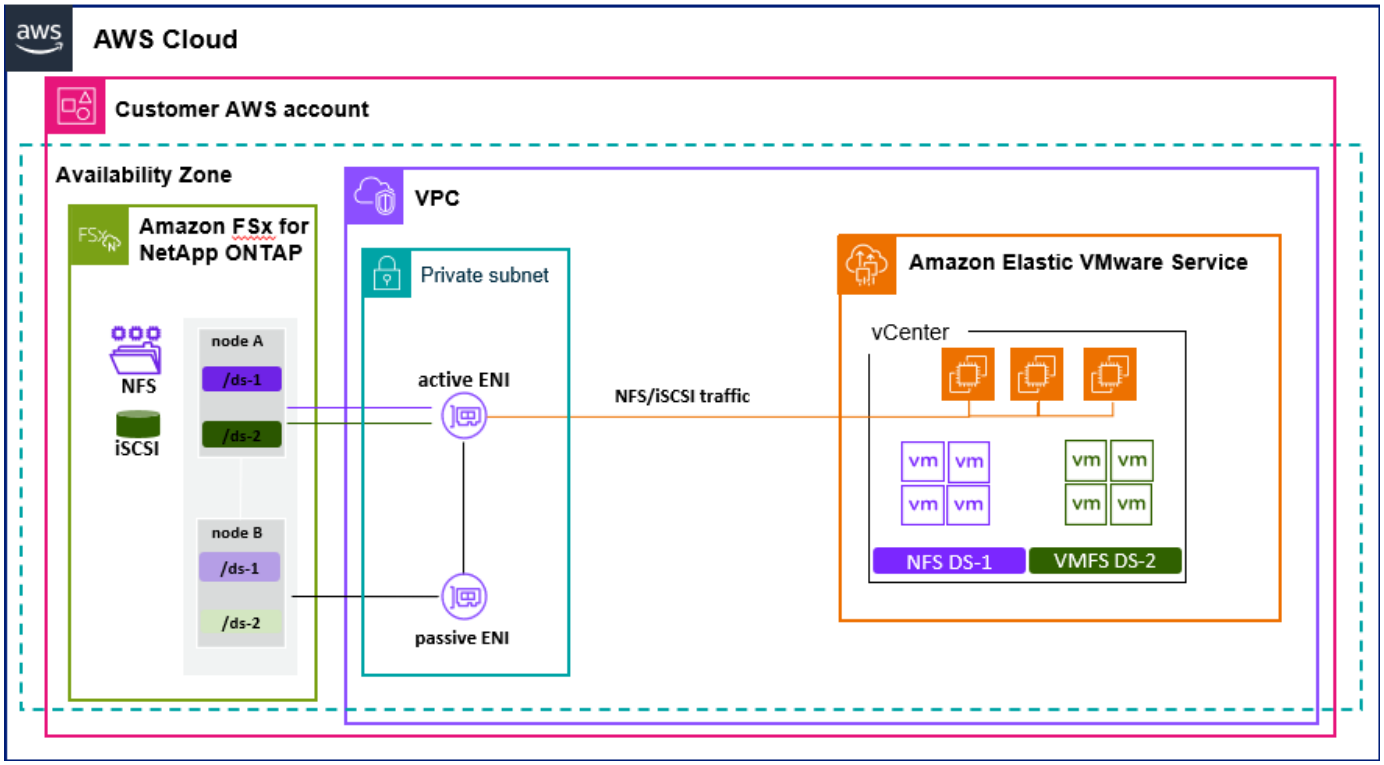
Audiencia

Este tutorial está destinado a arquitectos y administradores de la nube familiarizados con VMware vSphere, Amazon EVS, la consola de AWS y FSx para ONTAP.

Arquitectura de alto nivel

En esta sección, brindaremos una descripción general de la arquitectura de la solución para usar FSx para ONTAP como almacén de datos para Amazon EVS.

A continuación, puede ver una vista de alto nivel de la arquitectura del almacén de datos FSx para ONTAP con un entorno de Amazon EVS dentro de una VPC de AWS.



Procedimiento de implementación para usar FSx para ONTAP como almacén de datos NFS

Esta sección mostrará los pasos sobre cómo implementar FSx para ONTAP como un almacén de datos NFS. Los pasos para implementar un almacén de datos iSCSI se detallan en la siguiente sección.

Pasos de implementación de alto nivel

La implementación del sistema de archivos FSx para ONTAP para su uso como almacén de datos NFS para Amazon EVS y el establecimiento de la conectividad entre los dos servicios incluirán los siguientes pasos:

- Configuración de un sistema de archivos FSx para ONTAP en la misma VPC donde se encuentra el entorno VCF de Amazon EVS.
- Validar los grupos de seguridad y la tabla de enrutamiento.
- Adjuntar un volumen de almacenamiento FSx para ONTAP para usarlo como almacén de datos NFS para Amazon EVS.

Prerrequisitos

Los siguientes requisitos previos deben estar establecidos antes de comenzar el proceso para configurar un FSx para ONTAP como un almacén de datos NFS para Amazon EVS:

- Un entorno de virtualización de Amazon EVS. Para obtener más información sobre cómo hacerlo, consulte la documentación en"Guía de introducción a Amazon EVS" .
- Cree una zona de disponibilidad única (AZ) FSx para ONTAP con capacidad de almacenamiento SSD, IOPS aprovisionados y rendimiento adecuados.
- Para obtener un rendimiento óptimo, coloque el sistema de archivos FSx para ONTAP dentro de la misma VPC que la instancia de Amazon EVS. Tenga en cuenta que el intercambio de VPC también es compatible en el caso en que FSx para ONTAP se implementa en una VPC diferente.

- Según los requisitos de rendimiento, seleccione las IOPS y el rendimiento correctos necesarios para un sistema de archivos Single-AZ FSx para ONTAP . Ver"Detalles de la especificación de rendimiento de FSx para ONTAP" para comprender el rendimiento y las IOPS que ofrece cada opción disponible.

> Para esta guía, implementaremos el sistema de archivos FSx para ONTAP en la misma subred que la subred de acceso al servicio.

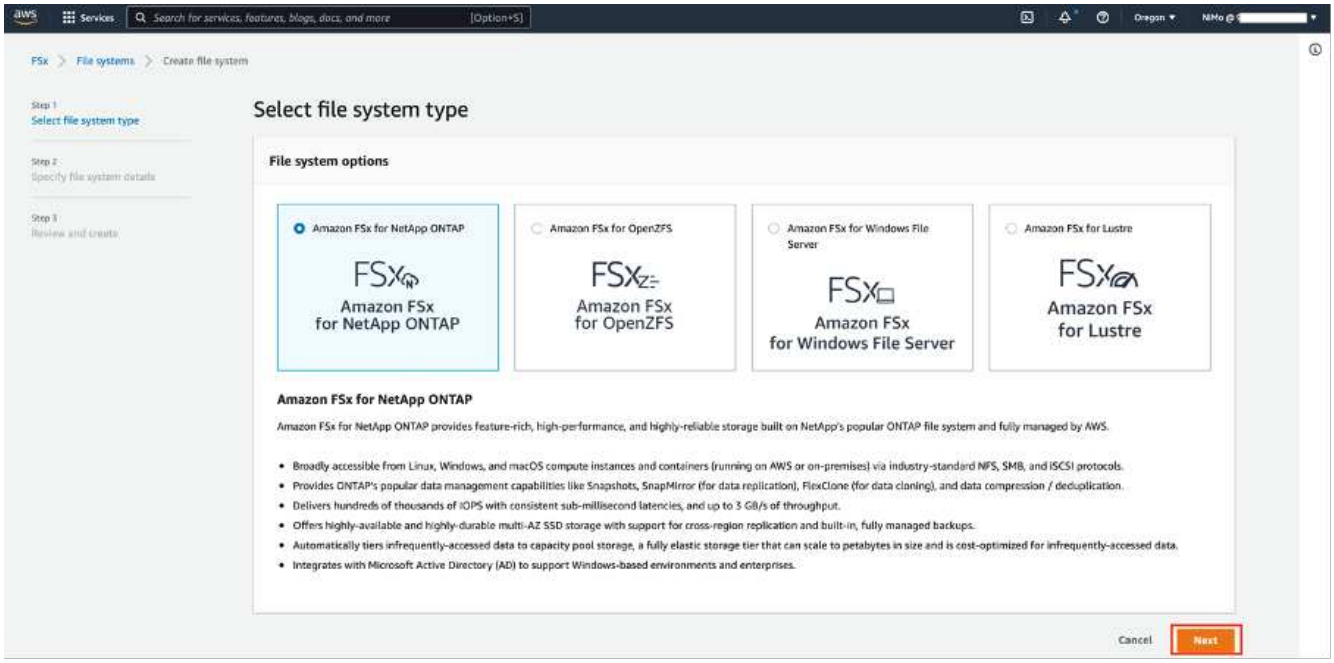
Una vez implementado el entorno de virtualización de Amazon EVS en la VPC, puede continuar con la configuración del sistema de archivos Single-AZ FSx para ONTAP que se utilizará como almacén de datos NFS.

> Su sistema de archivos FSx para ONTAP debe implementarse en la misma AZ que el SDDC de Amazon EVS.

Crear un sistema de archivos FSx para ONTAP

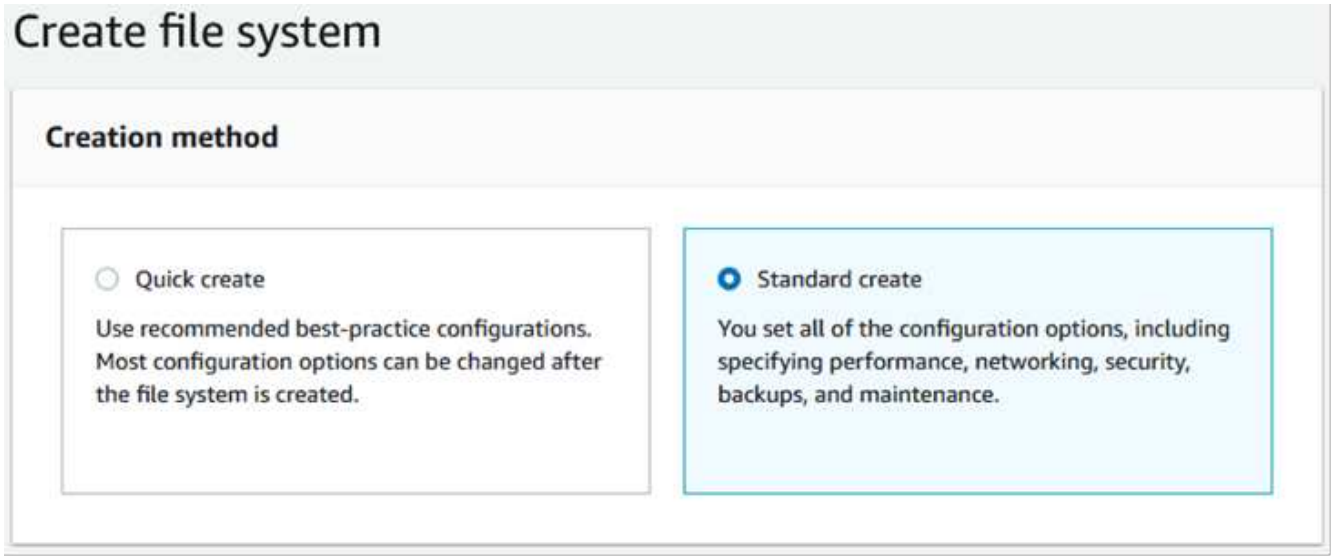
Los siguientes pasos le mostrarán cómo aprovisionar y montar un sistema de archivos FSx para ONTAP :

1. Vaya a la consola de Amazon FSx en `https://console.aws.amazon.com/fsx/` utilizando su navegador de internet e inicie sesión con sus credenciales.
2. En la consola, seleccione Crear sistema de archivos. Esto iniciará el asistente de configuración para crear un sistema de archivos FSx para ONTAP .
3. Primero, seleccione el tipo de sistema de archivos. De las opciones del sistema de archivos disponibles, seleccione “Amazon FSx for NetApp ONTAP” y continúe haciendo clic en el botón “Siguiente”.

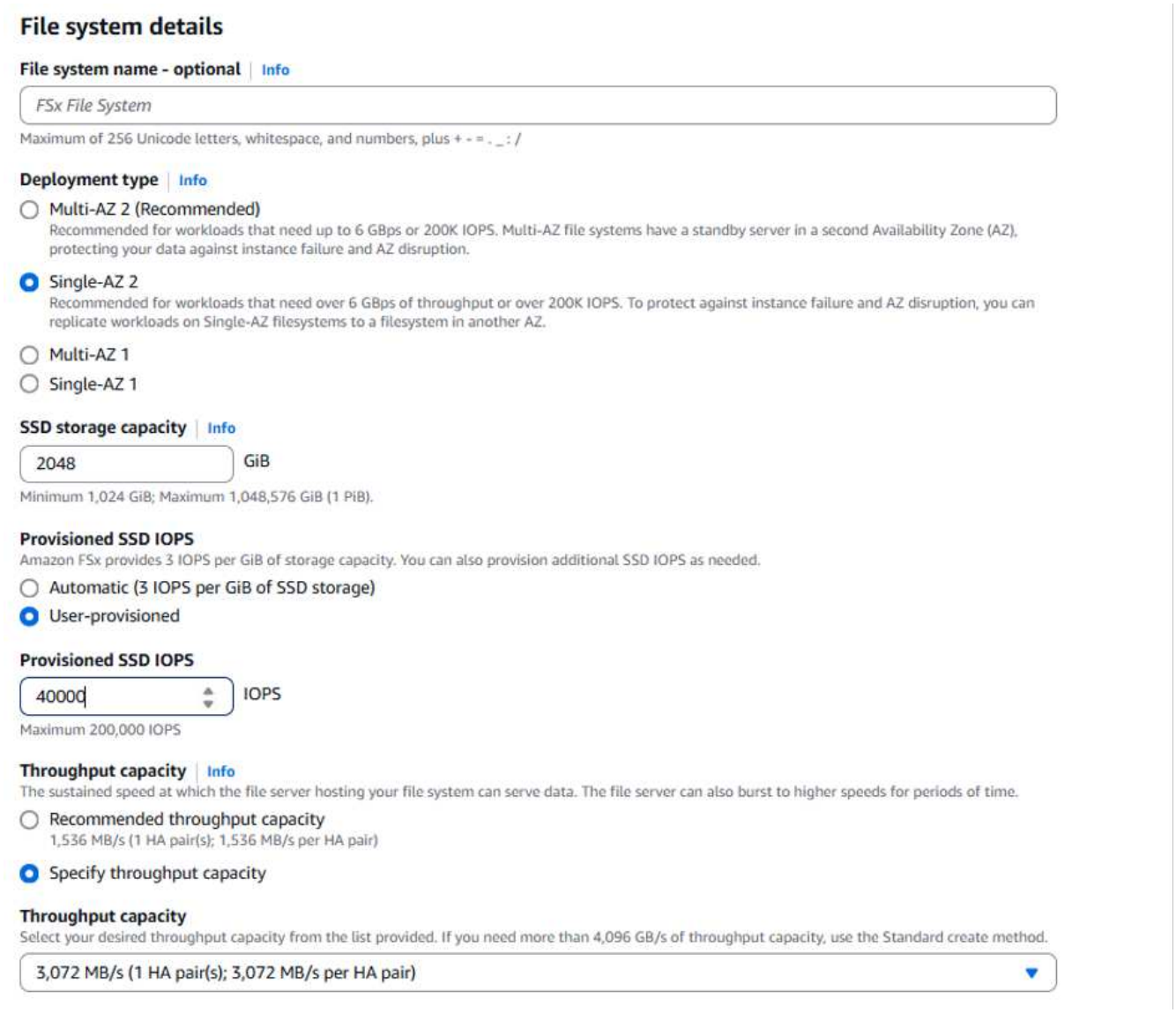


4. Se le presentará la opción de elegir entre las opciones de creación rápida y creación estándar. La creación rápida ofrece configuraciones predefinidas y la creación estándar le permite definir sus propias configuraciones.

   Seleccione la opción “Creación estándar”.

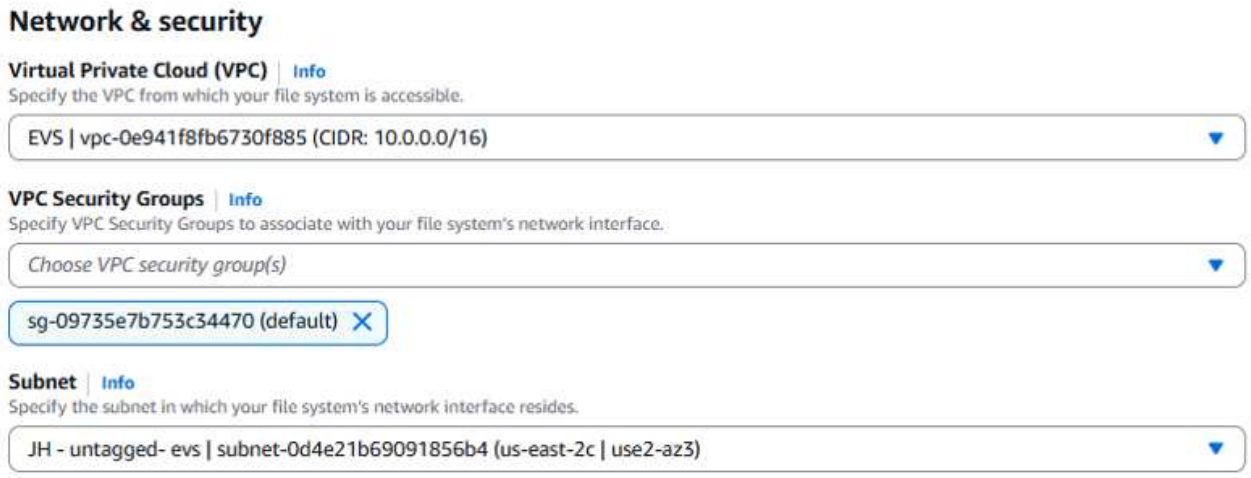


Ahora estará en el asistente de configuración de creación del sistema de archivos estándar. En la página de detalles del sistema de archivos, elija e ingrese la misma información que se muestra en la imagen a continuación:



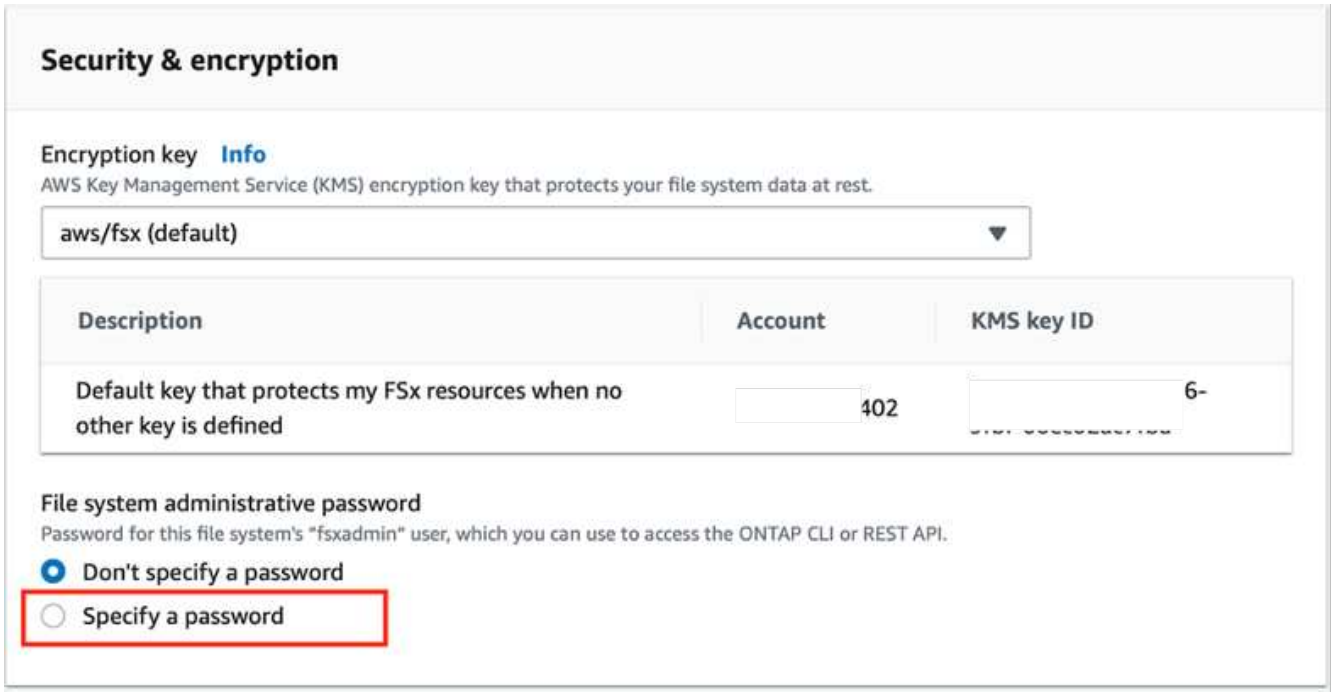
5. Desplácese hacia abajo hasta donde encontrará una sección denominada "Red y seguridad". En esta sección configurará los detalles de la subred y la VPC. Para los fines de esta guía, seleccionamos "EVS-VPC" del menú desplegable y seleccionamos la subred de acceso al servicio (VLAN sin etiquetar) como la subred para el entorno virtual EVS.

> La subred puede ser cualquier subred privada sin etiqueta en la VPC. También puede estar en una VPC/subred diferente conectada a través de VPC Peering, siempre que se haya configurado el enrutamiento adecuado.



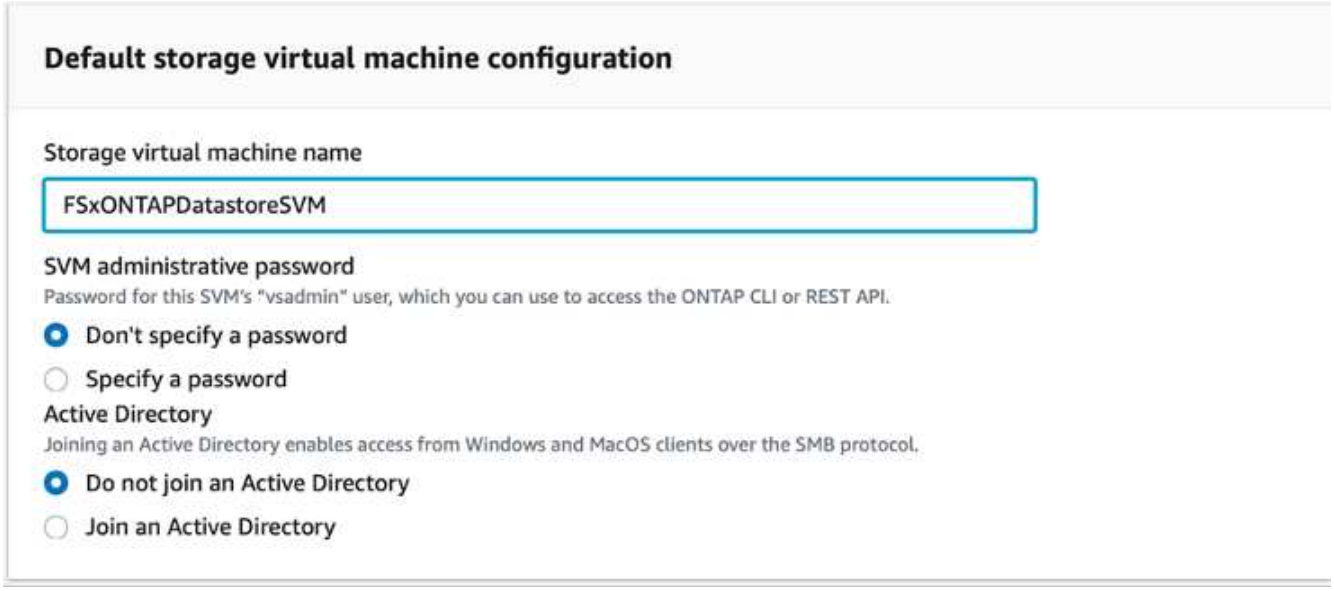
6. Desplazándose hacia abajo, encontrará la sección "Seguridad y cifrado". Aquí, seleccione la clave de cifrado en el menú desplegable. Estas claves son proporcionadas por AWS Key Management Service (AWS KMS) y protegerán los datos en reposo en su sistema de archivos FSx para ONTAP .

   A continuación, en la configuración “Contraseña administrativa del sistema de archivos”, especifique una contraseña única para el usuario fsxadmin que administrará el sistema de archivos.

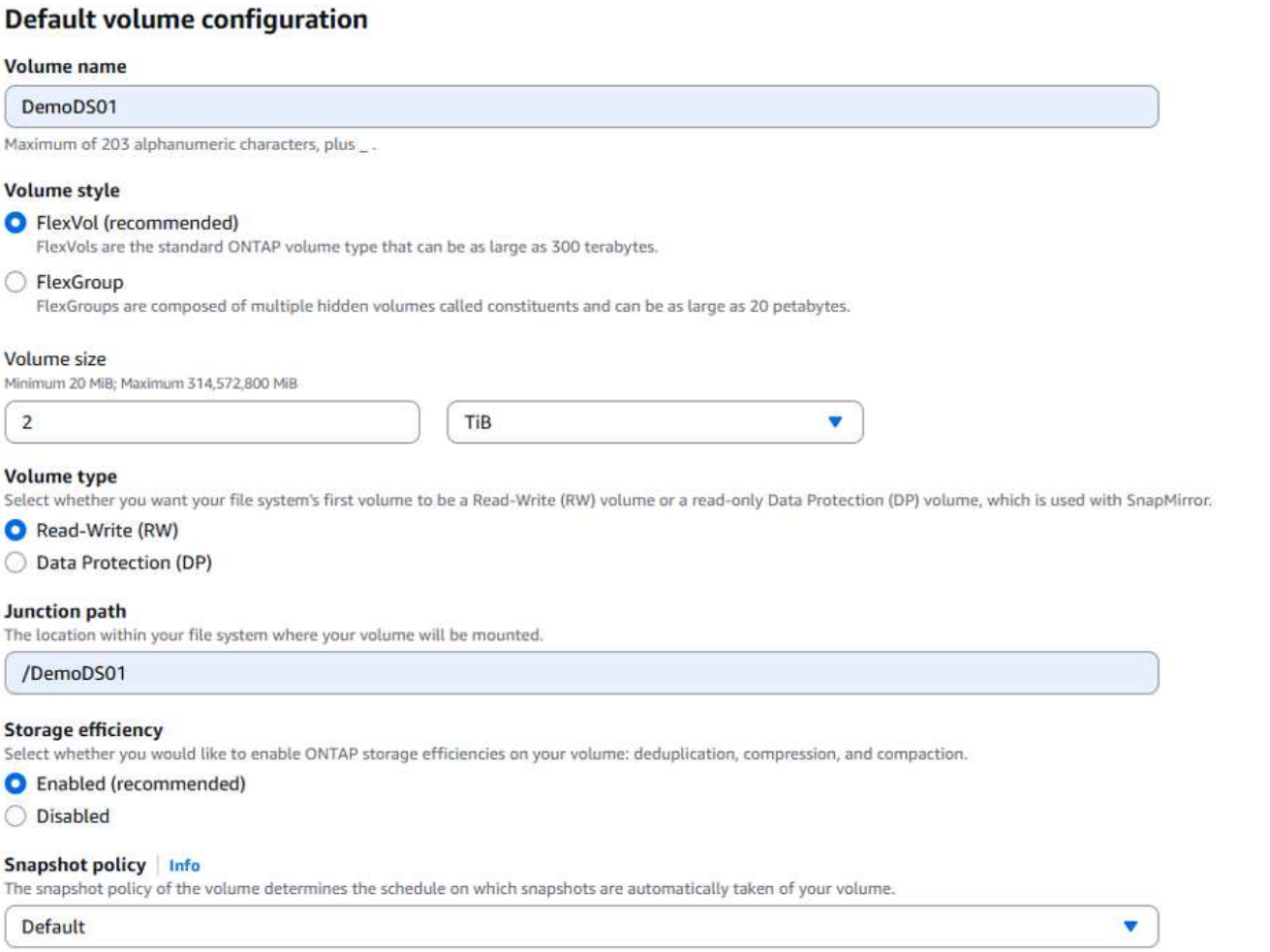


7. A continuación, desplácese hacia abajo hasta una sección titulada "Configuración de la máquina virtual de

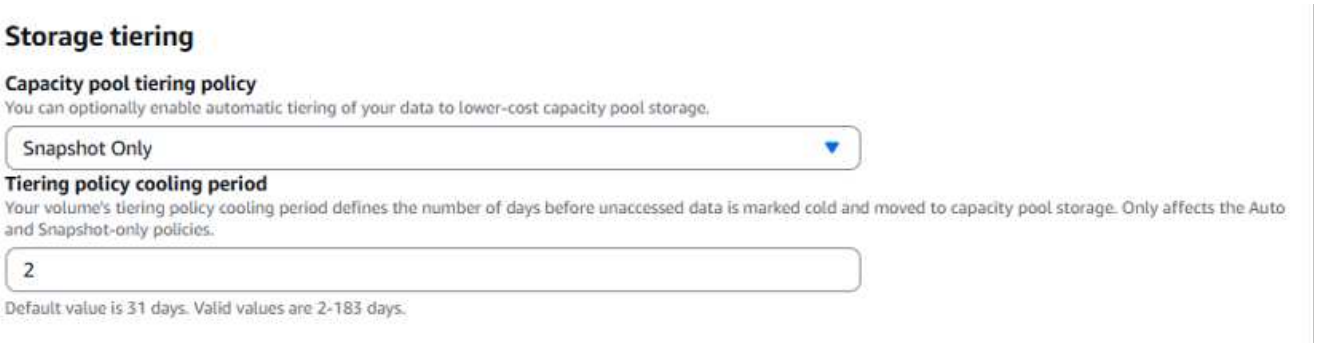
almacenamiento predeterminada". Aquí deberá proporcionar un nombre para la máquina virtual de almacenamiento (SVM).



8. A continuación, desplácese hacia abajo hasta la sección titulada "Configuración de volumen predeterminada". Aquí proporcionará un nombre para el volumen y establecerá el tamaño del volumen. El protocolo de volumen debe ser NFS v3 (habilitado de forma predeterminada). Haga clic en la opción para habilitar funciones de eficiencia de almacenamiento (compresión, deduplicación y compactación) para reducir el uso y los costos generales de almacenamiento.



9. Para la opción de niveles de almacenamiento, seleccione "Solo instantánea" en el menú desplegable y configure un período de enfriamiento de la política de niveles. El valor predeterminado es 31 días, pero para este ejemplo establecemos un período de enfriamiento de dos días.



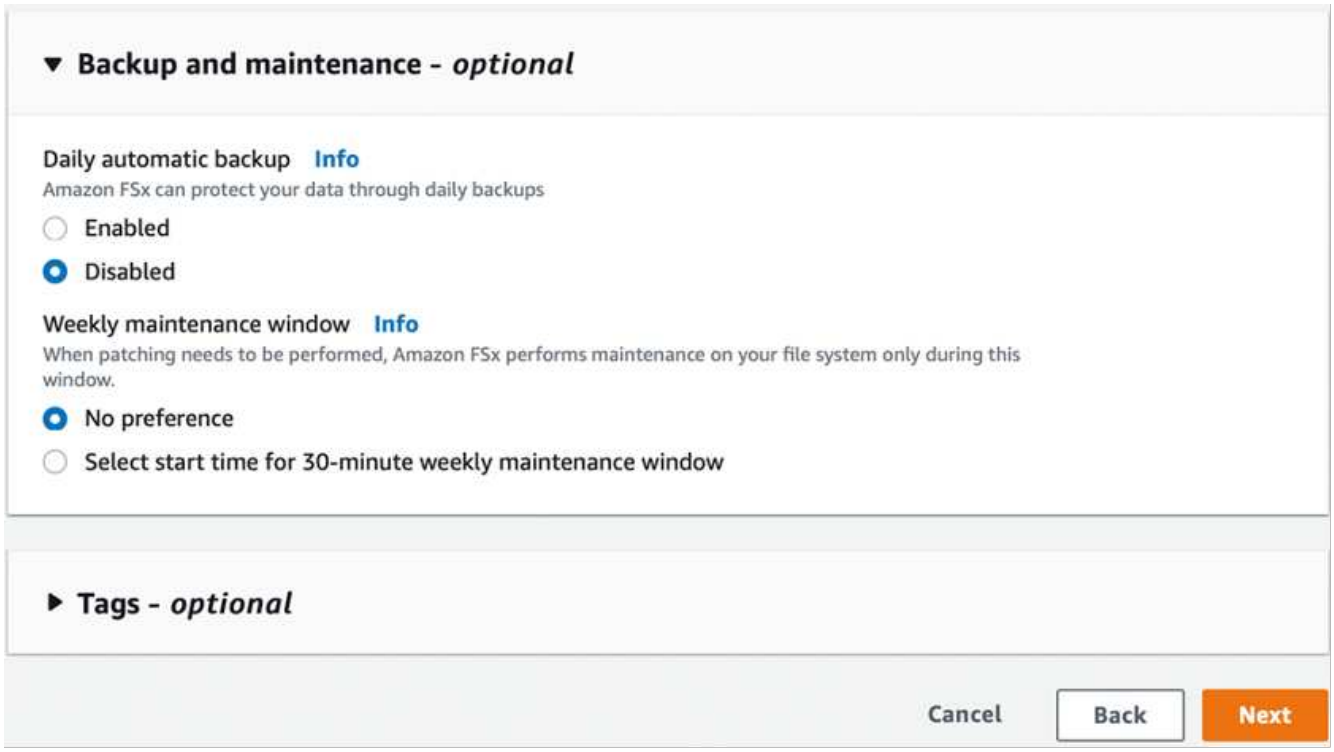
10. Una vez que haya creado el volumen, modifique los siguientes parámetros mediante la interfaz de línea de comandos de ONTAP (ONTAP CLI):

Configuración	Configuración
Garantía de volumen	Ninguno (aprovisionamiento fino)
reserva fraccionaria	0%
reserva instantánea	0%

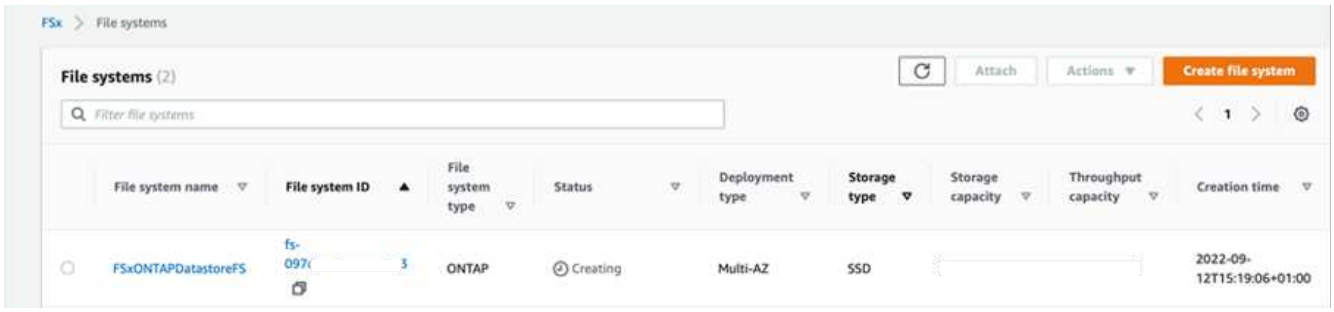
Configuración	Configuración
Tamaño automático	crecer_encoger
Eficiencia de almacenamiento	Habilitado
Política de niveles de volumen	Solo instantánea
Actualización del tiempo de acceso (-atime-update)	FALSO
Lectura anticipada mínima (-min-readahead)	FALSO
Política de instantáneas	Ninguno

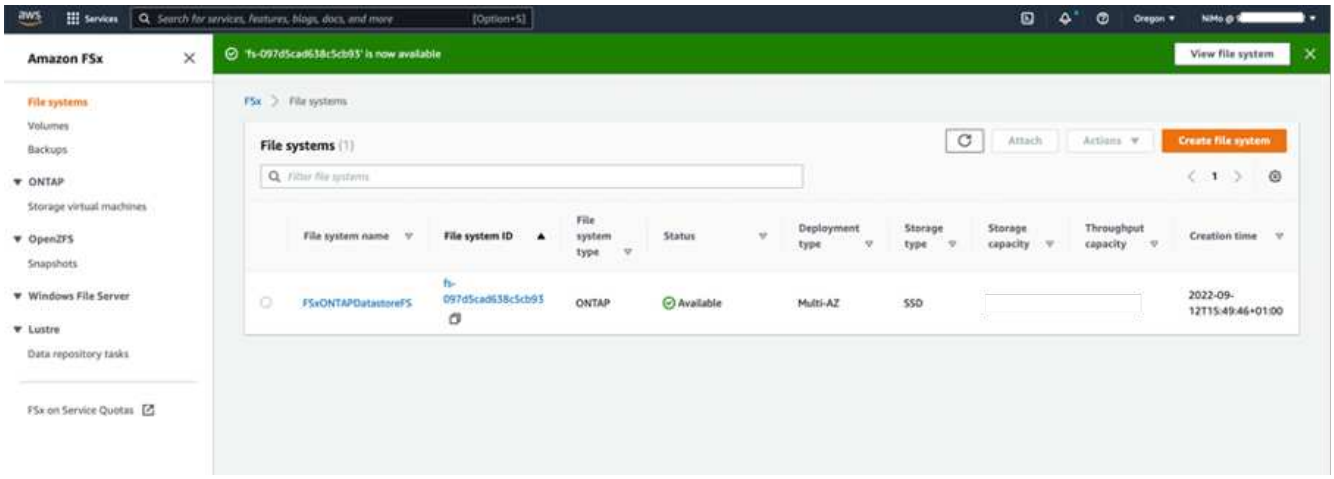
11. En el paso opcional "Copia de seguridad y mantenimiento", desactive las copias de seguridad automáticas diarias y seleccione "Sin preferencia" para la ventana de mantenimiento semanal.

    Haga clic en "Siguiente" cuando haya terminado.



12. Ahora se le proporcionará una revisión de toda la configuración del sistema de archivos que configuró siguiendo los pasos anteriores. Verifique que todos los parámetros sean correctos, luego haga clic en el botón "Crear sistema de archivos" para completar la configuración.



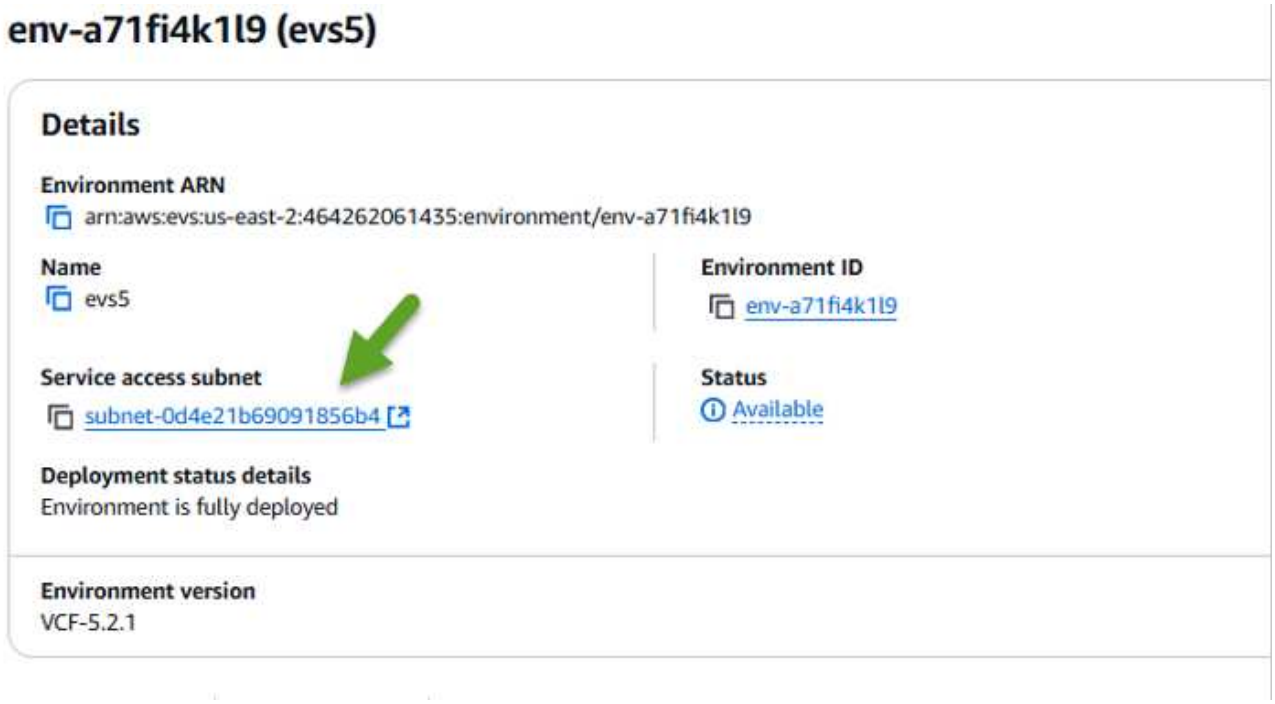


Para crear sistemas de archivos FSx adicionales para ONTAP , puede seguir los pasos detallados anteriormente y ajustar los valores que afectan el rendimiento y la capacidad del disco según sea necesario. Para obtener más información sobre las opciones de rendimiento de FSx para ONTAP, consulte"esta página de documentación" .

Validación de grupos de seguridad y enrutamiento de entornos de virtualización y VPC

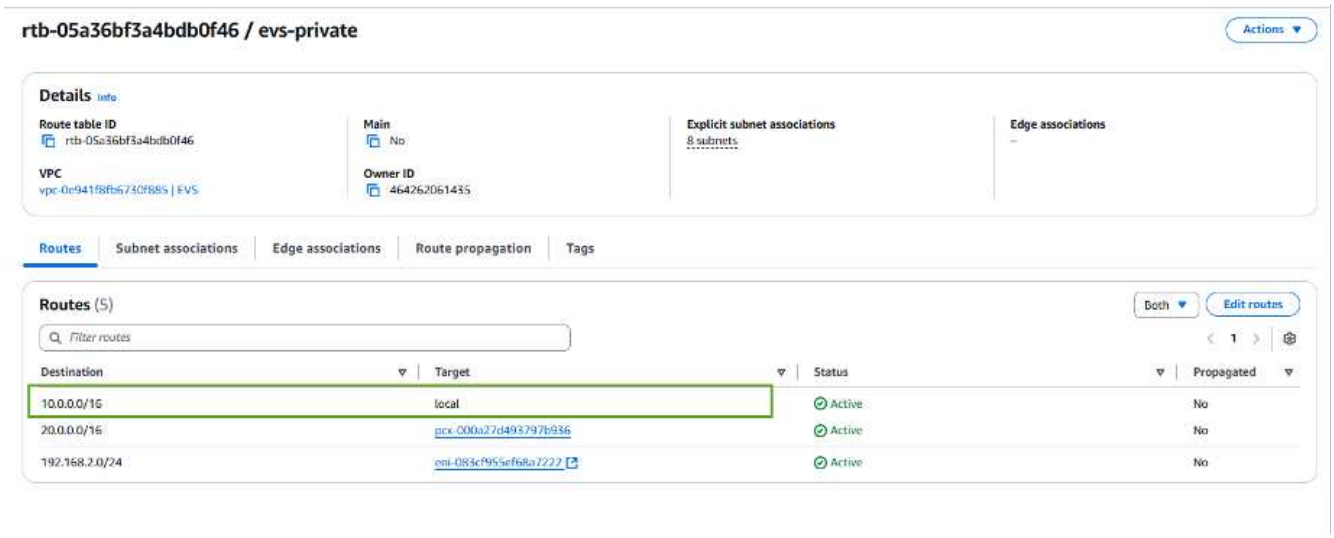
Validar los grupos de enrutamiento y seguridad de VPC y SDDC es importante para garantizar que el entorno de virtualización de Amazon EVS y los componentes del sistema de archivos de FSx for ONTAP puedan funcionar juntos correctamente.

1. Vaya a Elastic VMware Service > Entornos de virtualización > [su entorno de Amazon EVS] y seleccione la subred de acceso al servicio, como lo indica la flecha verde a continuación:

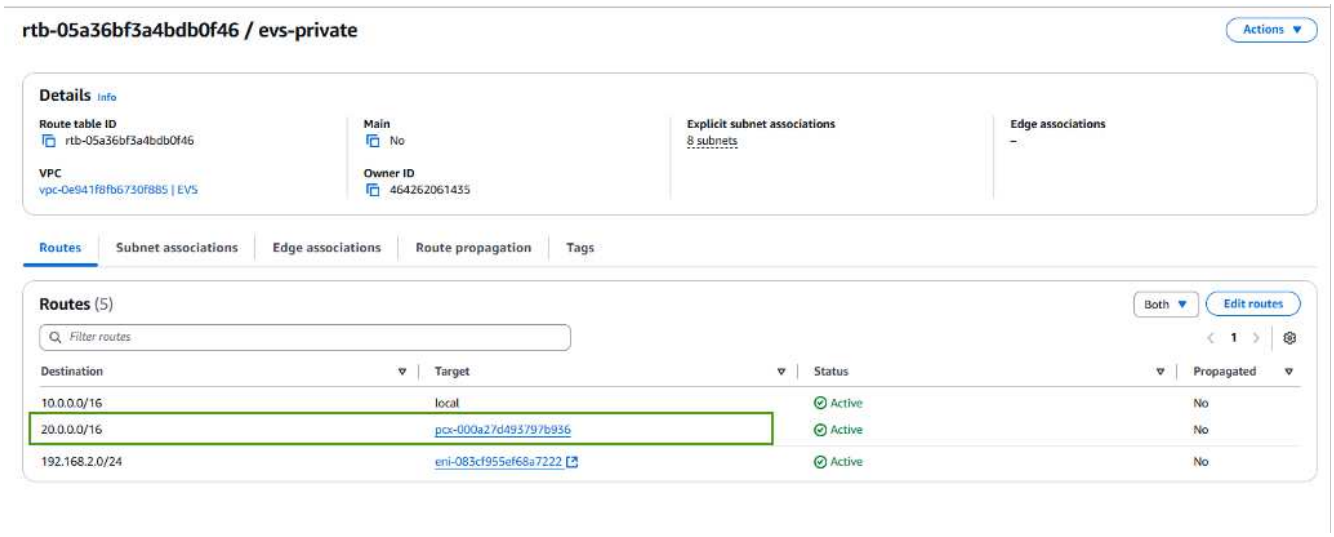


2. Esto abrirá el panel de subred. Busque la tabla Rutas en este panel y haga clic en ella.

   En este ejemplo, el sistema de archivos FSxN ONTAP está en la misma VPC que el entorno VCF de Amazon EVS, por lo que las rutas predeterminadas son suficientes.



Si el sistema de archivos FSx para ONTAP está en una VPC diferente, verifique que se hayan agregado las rutas a esa VPC. En este ejemplo, se agregaron rutas para el intercambio de VPC con la VPC donde reside el sistema FSx para ONTAP .

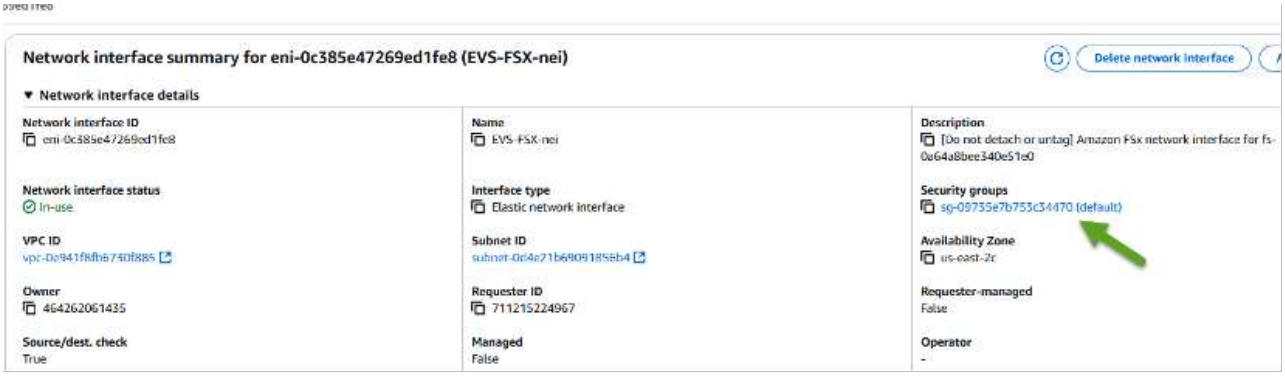


3. A continuación, deberá verificar que el grupo de seguridad conectado al sistema de archivos FSx para ONTAP (es decir, el que está conectado a la interfaz de red elástica (ENI) permite el acceso a los puertos NFS).

   Para obtener una lista completa de los puertos de protocolo NFS e iSCSI, consulte el enlace: https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]Documentación de control de acceso al sistema de archivos con Amazon VPC].

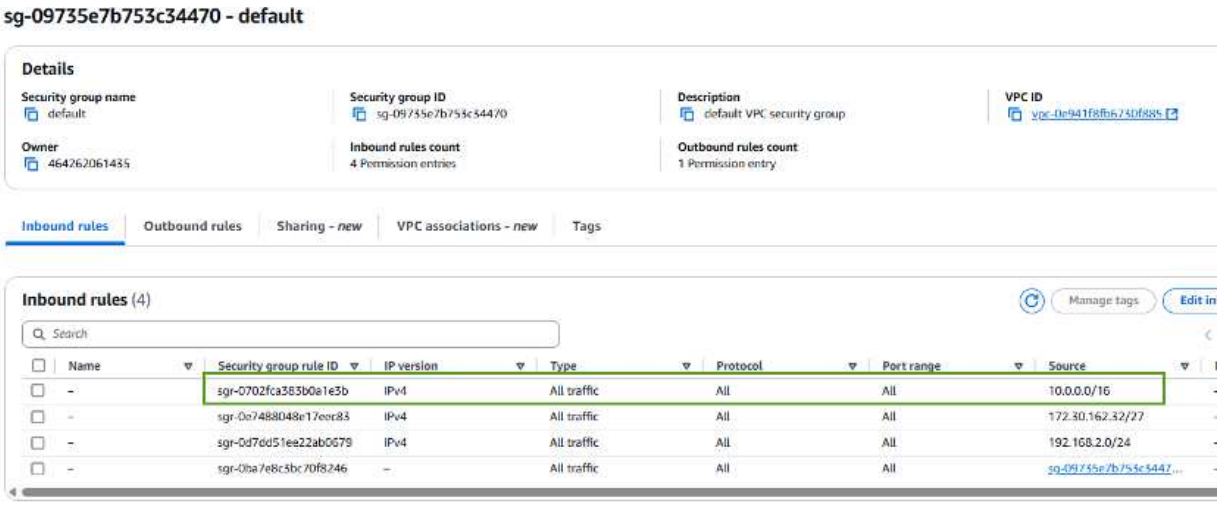
   Para verificar que su sistema de archivos FSx para ONTAP esté asociado con el grupo de seguridad:

   a. En la consola de AWS, navegue a FSx > Sistemas de archivos > [su sistema de archivos FSx para ONTAP].
   b. En la pestaña Red y seguridad, haga clic en ENI.
   c. Busque el grupo de seguridad que aparece en los detalles de la interfaz de red asociado con la ENI (indicado por la flecha verde en la imagen a continuación).



d. Validar los puertos. En este ejemplo que se muestra en la siguiente pantalla, se permite todo el tráfico. Sin embargo, puedes limitarlos a puertos NFS únicamente. Aquí está la lista de los puertos:

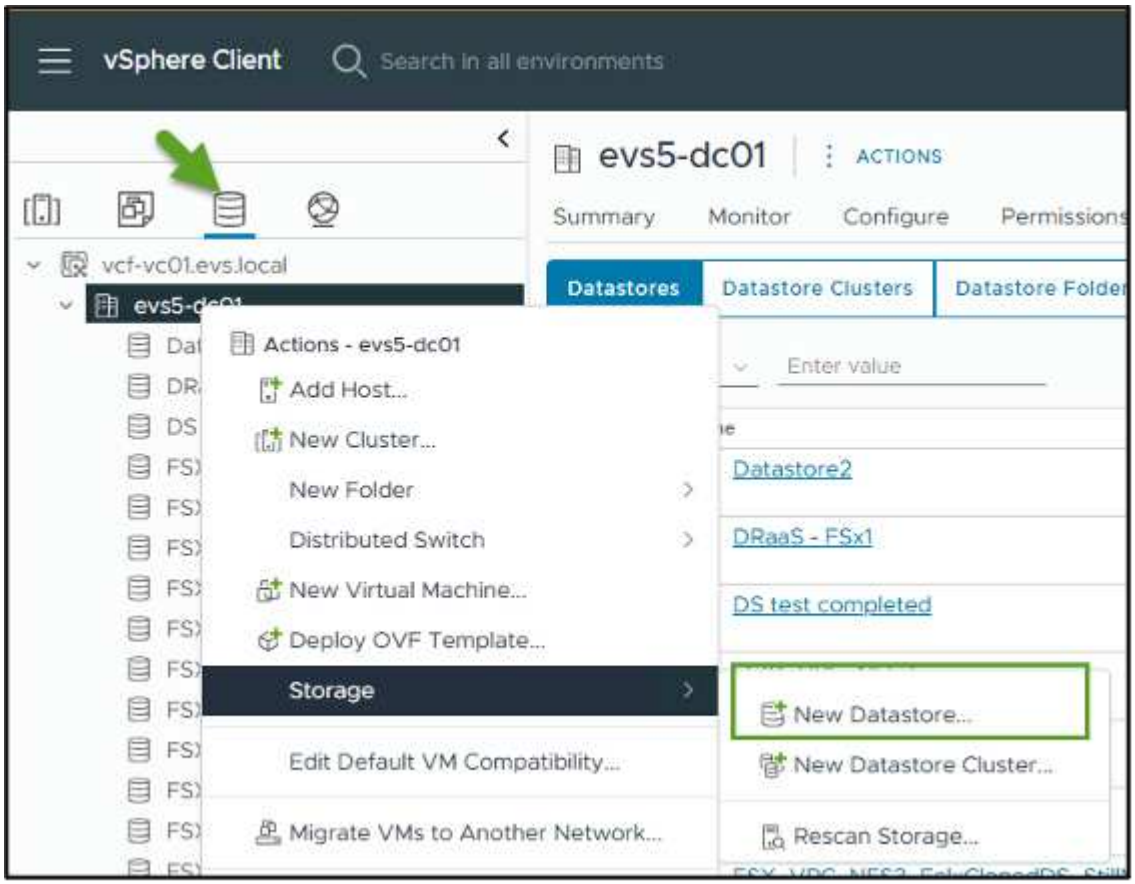
- Puerto 111 TCP: Portmapper, se utiliza para negociar qué puertos se utilizan en las solicitudes NFS.
- Puerto 635 TCP: Mountd, que sirve para recibir solicitudes de montaje entrantes.
- Puerto 2049 TCP: NFS, que maneja el tráfico NFS.
- Puerto 4045 TCP: Administrador de bloqueo de red (NLM), que se ocupa de las solicitudes de bloqueo.
- Puerto 4046 TCP: Monitor de estado de red (NSM), que envía notificaciones a los clientes NFS cuando el servidor se reinicia para la administración de bloqueos.



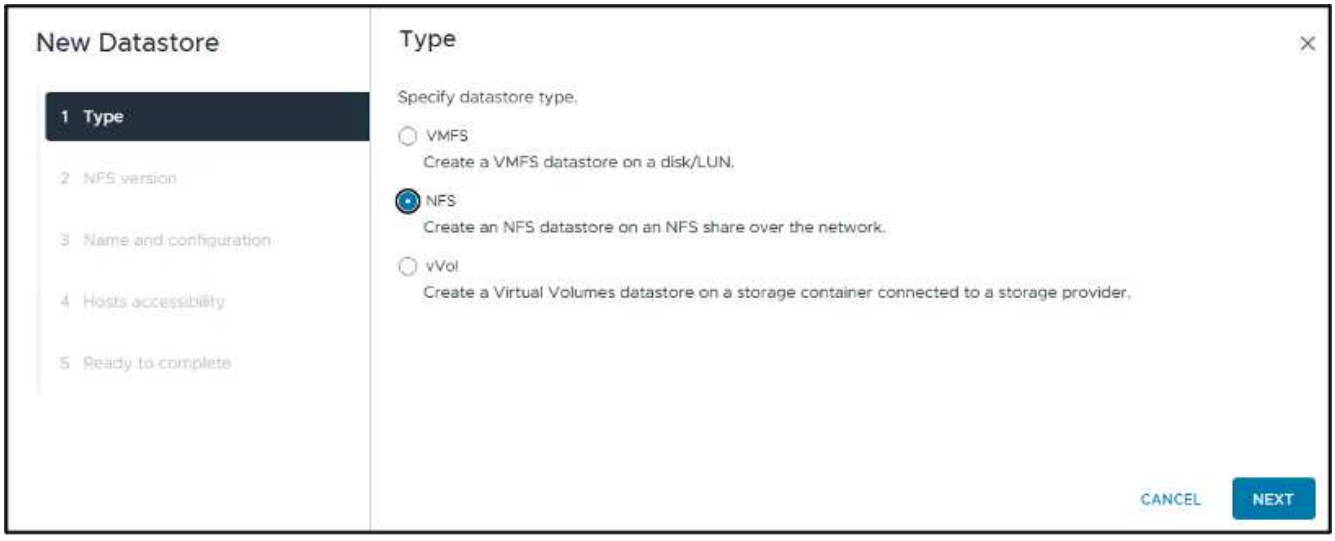
Cómo conectar un volumen NFS de FSx para ONTAP a Amazon EVS para usarlo como almacén de datos

Ahora que su sistema de archivos FSx para ONTAP ha sido aprovisionado y se han validado todos los parámetros de conectividad adecuados, es momento de conectar un volumen de almacenamiento FSx para ONTAP a Amazon EVS. Los siguientes pasos mostrarán cómo acceder a vCenter y montar el volumen FSx para ONTAP como un almacén de datos NFS:

1. En el cliente vSphere, vaya a la pestaña "Almacén de datos". Busque el centro de datos y navegue hasta Almacenamiento > Nuevo almacén de datos, como se muestra a continuación:

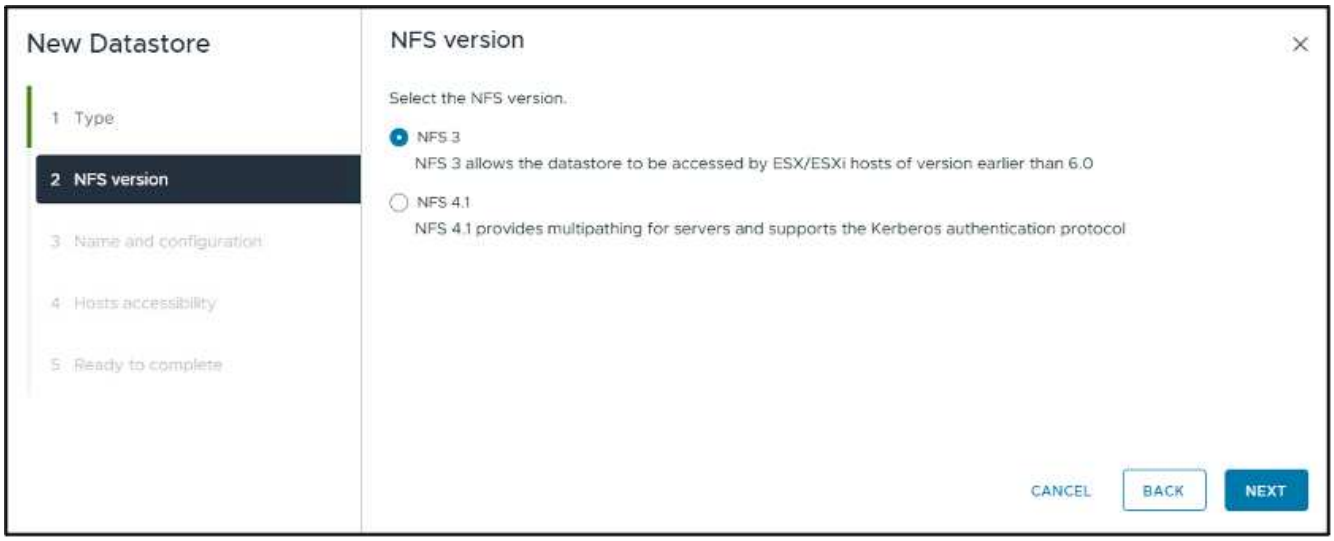


2. Ahora estará en el asistente Nuevo almacén de datos. En el paso "Tipo", elegirá un tipo de almacén de datos. Seleccione “NFS” y haga clic en “SIGUIENTE” para continuar.



3. En el paso "Versión NFS", seleccionará una versión NFS.

   Para los fines de este ejemplo, elegiremos "NFS 3", pero tenga en cuenta que también se puede utilizar NFS v4.1.



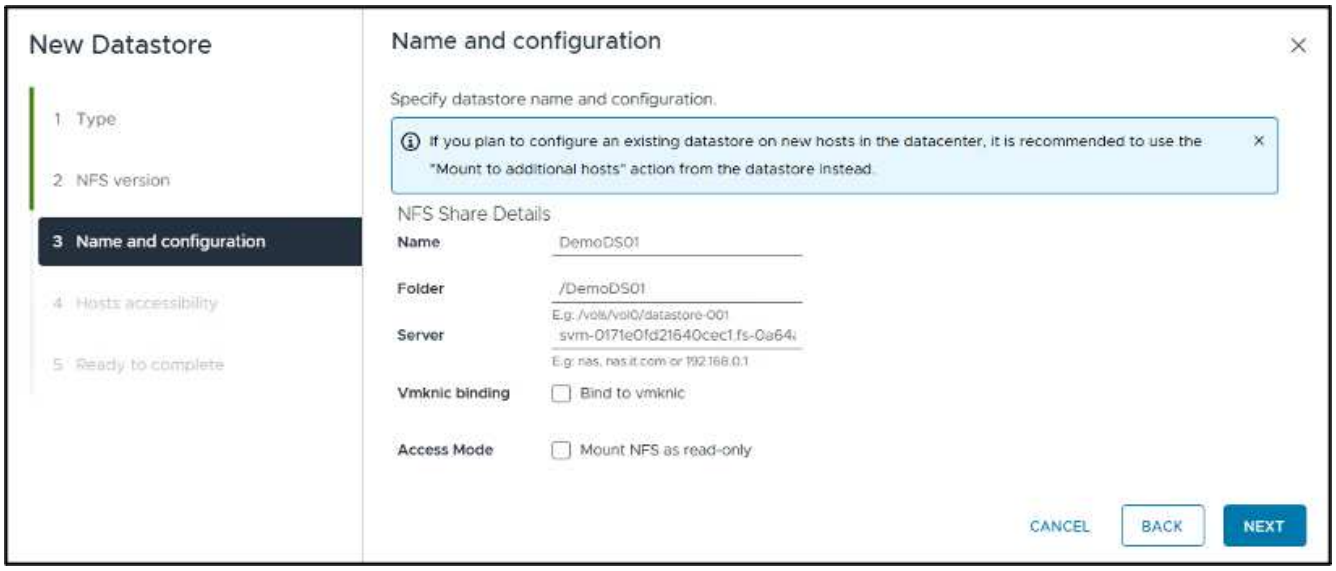
4. En el paso "Nombre y configuración", deberás:

   a. Nombra el almacén de datos.

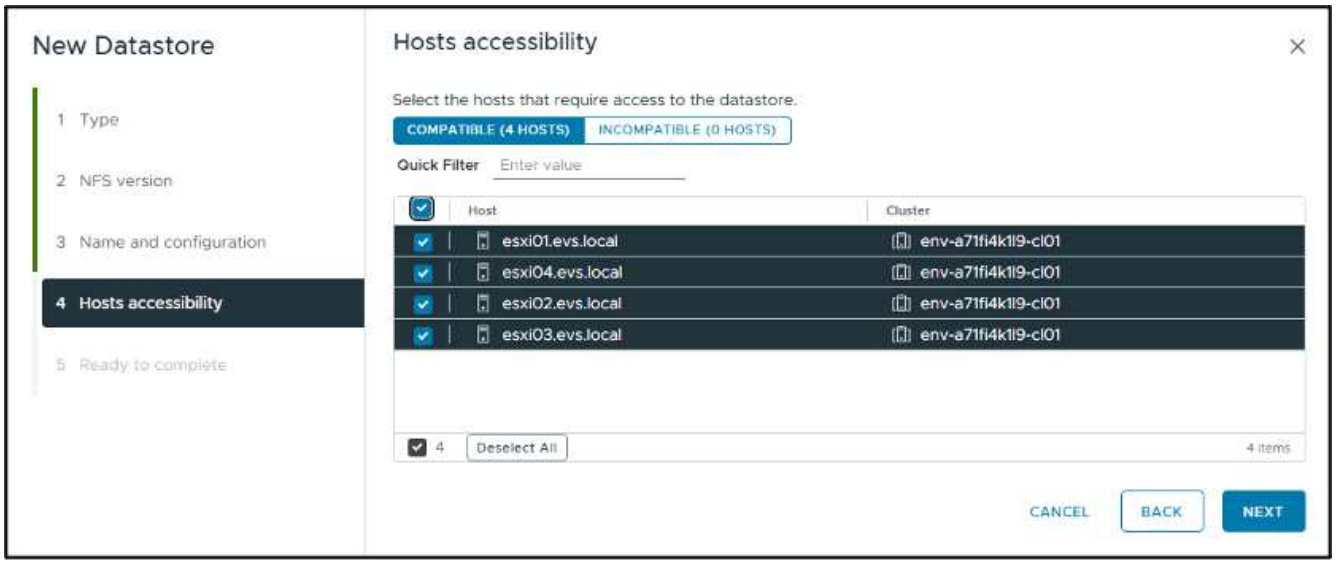
   b. Nombra la carpeta. Utilice la ruta de unión a su volumen NFS.

   c. Nombra el servidor. Utilice el nombre DNS NFS de su SVM o la dirección IP del NFS.

   Haga clic en “SIGUIENTE” para continuar.



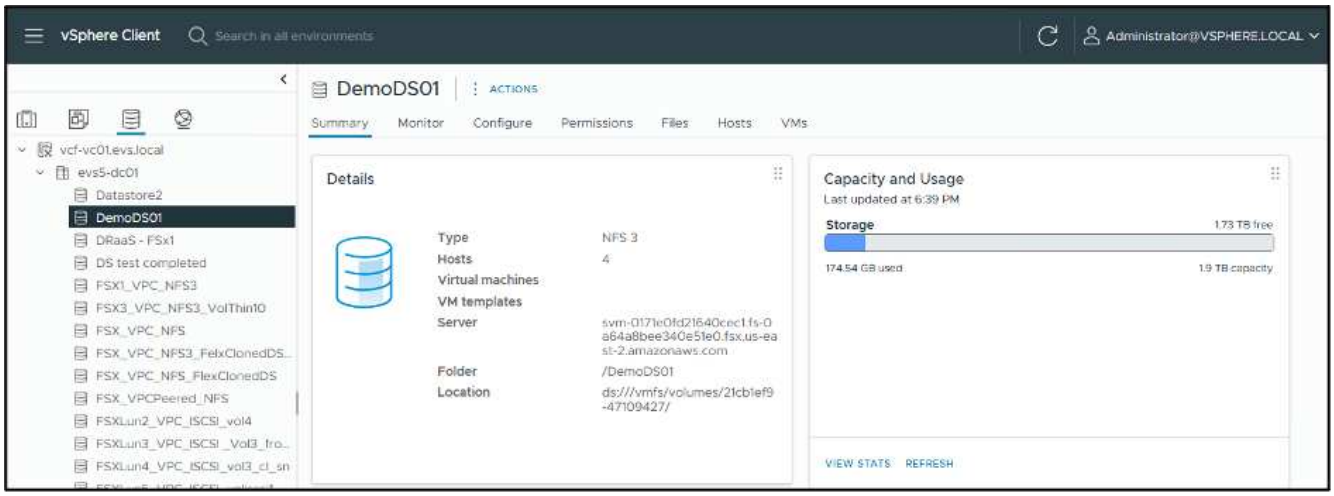
5. En el paso "Accesibilidad del host", seleccione todos los hosts que requieren acceso al almacén de datos, luego haga clic en "SIGUIENTE" para continuar.



6. En el paso "Listo para completar", revise los datos y haga clic en "FINALIZAR" para completar la configuración.



7. Valide que el almacén de datos NFS se haya conectado accediendo a vCenter, como se muestra a continuación:



Procedimiento de implementación para usar FSx para ONTAP como almacén de datos iSCSI

Esta sección cubre los pasos para configurar un almacén de datos iSCSI utilizando FSx para ONTAP.

Prerrequisitos

Antes de aprovisionar y conectar FSx para ONTAP como un almacén de datos iSCSI, primero debe implementar un entorno de virtualización de Amazon EVS. Para obtener más información, consulte la documentación en la guía Introducción a Amazon EVS. Esta sección también asume que ha implementado un sistema de archivos FSx para ONTAP ; consulte la sección Enfoque detallado más arriba para conocer los pasos adecuados.

Pasos de implementación de alto nivel

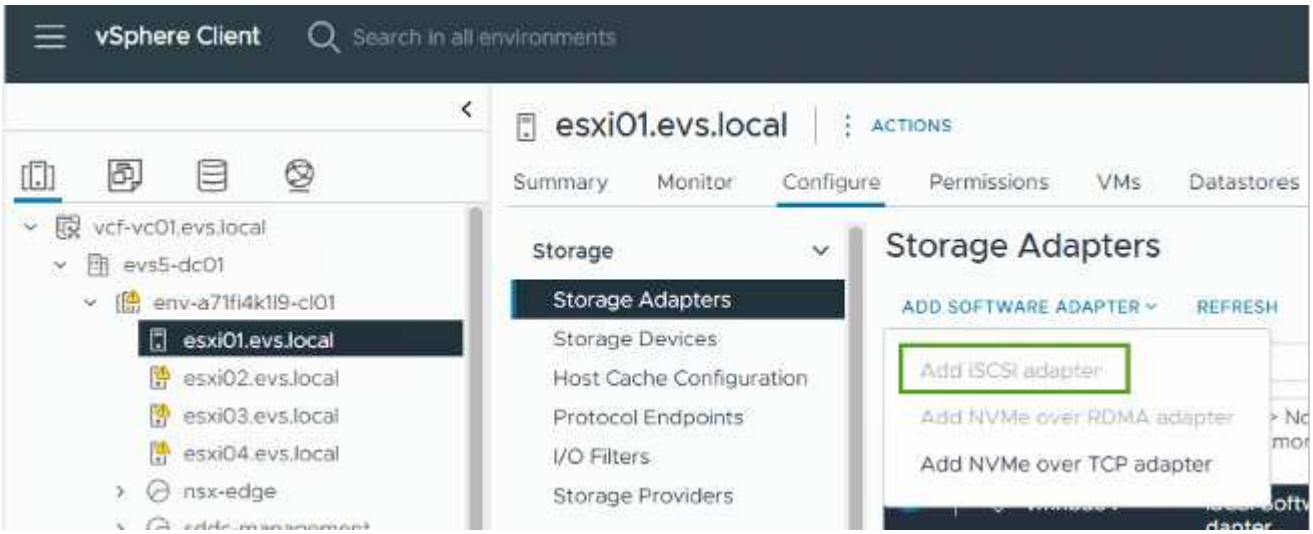
La implementación del sistema de archivos FSx para ONTAP para su uso como almacén de datos iSCSI para Amazon EVS y el establecimiento de la conectividad entre los dos servicios incluirán los siguientes pasos:

- Configuración de un adaptador de red iSCSI para cada host ESXi.
- Creación y configuración del FSx para el sistema de archivos ONTAP , volumen, LUN, etc.
- Conexión de los hosts ESXi al servidor del sistema de archivos FSx para ONTAP .
- Creación de un sistema de archivos de máquina virtual (VMFS) de almacén de datos iSCSI.

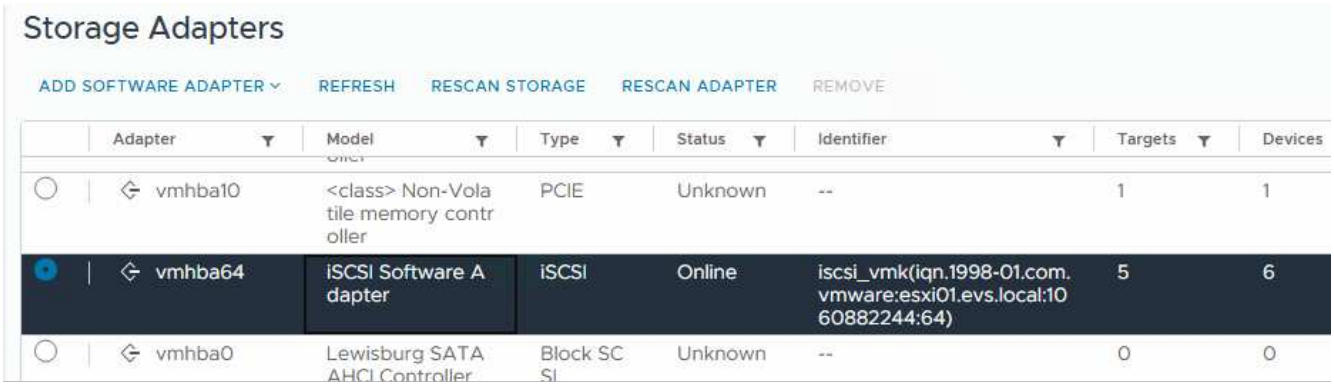
Agregar adaptador de red iSCSI

Los siguientes pasos deben realizarse en cada host ESXi de su entorno.

1. Ingrese al cliente vSphere y seleccione el host ESXi. En la pestaña Configurar, elija "Agregar adaptador de software" y luego seleccione "Agregar adaptador iSCSI" en el menú desplegable, como se muestra aquí:

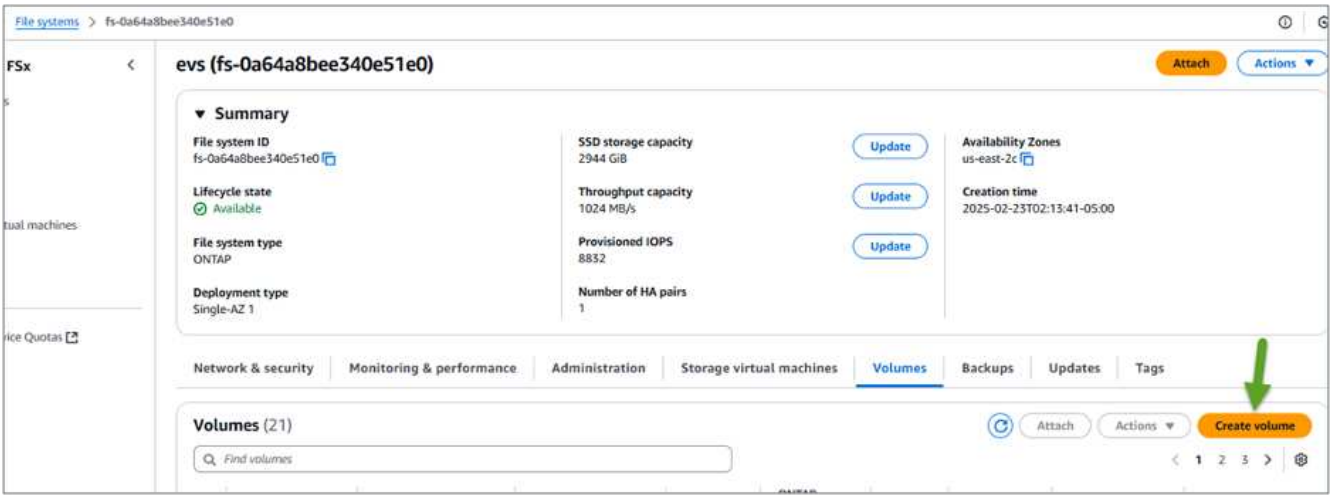


2. Una vez completada la instalación, estará en la pantalla Adaptadores de almacenamiento. Seleccione “Volver a escanear adaptador” en la barra de menú. Registre el IQN del adaptador iSCSI: iqn.xxxx. Este valor se utilizará en el paso de mapeo de LUN más adelante.



Crear un FSx para el volumen ONTAP

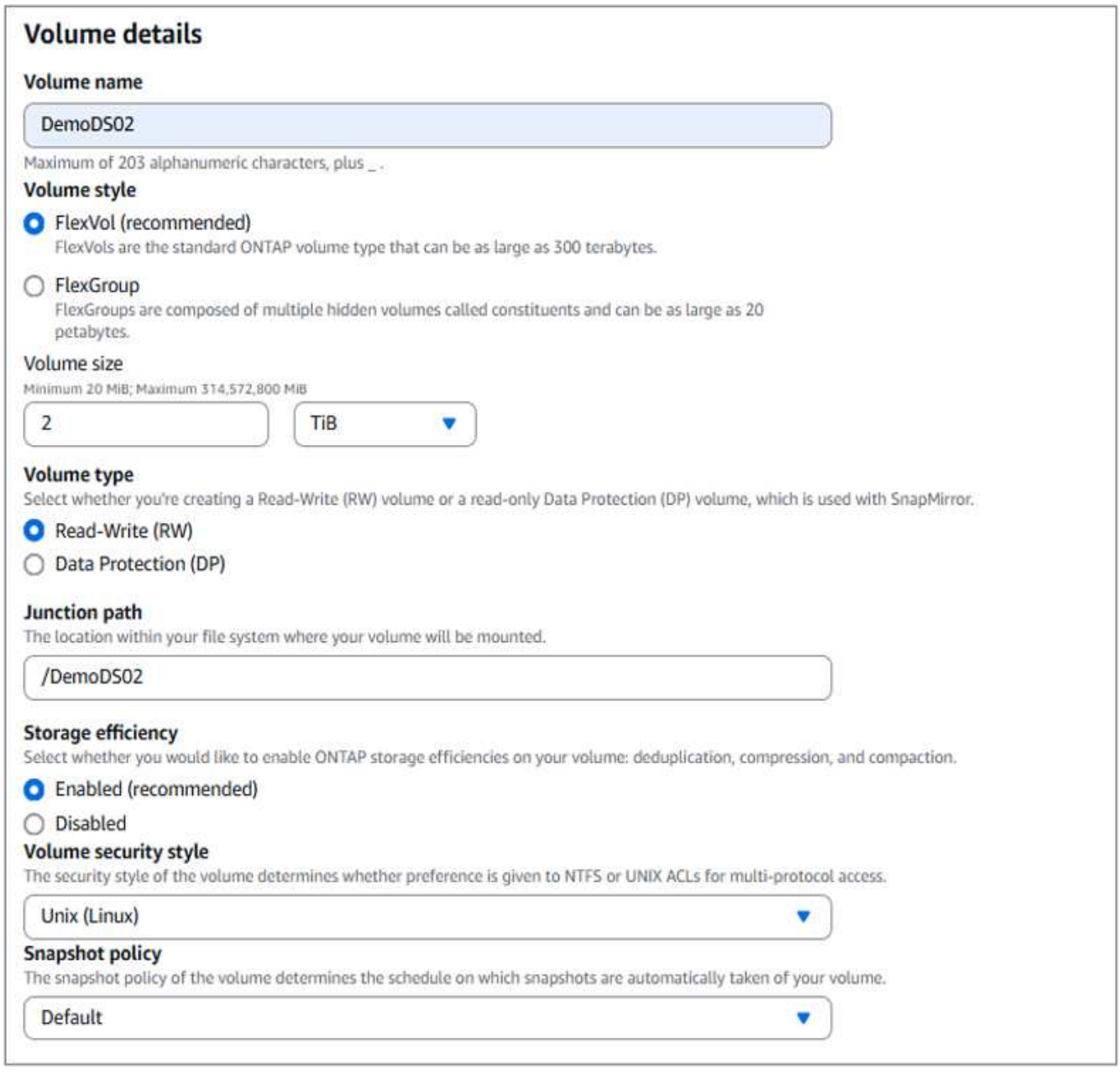
1. Vaya a la consola de AWS e ingrese a la página de su sistema de archivos FSx para ONTAP y haga clic en "Crear volumen".



2. Seleccione la SVM donde desea crear el volumen.



3. En la página "Detalles del volumen", ingrese los detalles como se muestra en la captura de pantalla a continuación. Cuando haya terminado, haga clic en "Crear" para configurar el volumen. Elija "Habilitado" para activar las funciones de eficiencia de almacenamiento de ONTAP (compresión, deduplicación y compactación).



4. Para la opción de niveles de almacenamiento, seleccione "Solo instantánea" en el menú desplegable y configure un período de enfriamiento de la política de niveles. El valor predeterminado es 31 días, pero para este ejemplo establecemos un período de enfriamiento de dos días.



5. Una vez creado el volumen, utilice la CLI de ONTAP para establecer los siguientes valores:

Configuración	Configuración
Garantía de volumen	Ninguno (aprovisionamiento fino)
reserva fraccionaria	0%
reserva instantánea	0%
Tamaño automático	crecer_encoger
Eficiencia de almacenamiento	Habilitado
Política de niveles de volumen	Solo instantánea
Actualización del tiempo de acceso (-atime-update)	FALSO
Lectura anticipada mínima (-min-readahead)	FALSO
Política de instantáneas	Ninguno
Reserva de espacio LUN	Desactivado
Asignación de espacio LUN	Habilitado

Crear un LUN, un igroup y asignar el LUN

En esta sección mostramos cómo crear el LUN que aparecerá como un disco en vSphere. También mostraremos cómo crear un grupo de iniciadores (igroup), que es la lista de los iniciadores que tienen acceso al LUN. El igroup permitirá el acceso al LUN desde los hosts vSphere ESXi. Finalmente, mostraremos cómo mapear el igroup al LUN.

1. Para acceder a la CLI de ONTAP , establezca una sesión SSH en el puerto de administración del sistema de archivos FSx para ONTAP o SVM ejecutando el siguiente comando:

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. Crear el LUN. Asegúrese de configurar la asignación de espacio y la reserva de espacio como habilitadas. El tamaño debe ser hasta el 90% del tamaño del volumen:

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. Cree el igroup y agregue el IQN de todos los hosts ESXi dentro del clúster.

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. Asigne el LUN con el siguiente código:

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. Revise la asignación de LUN y verifique que el estado se haya cambiado a "asignado". Esta es una verificación doble necesaria para asegurarse de que el LUN esté en un estado asignado:

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

Obtener información de configuración de iSCSI de la SVM

1. Ejecute iSCSI show y registre el nombre del destino. Esto se utilizará en el descubrimiento de vSphere de los discos FSx para ONTAP (Nota: este nombre de destino es exclusivo de su SVM):

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. Registre las direcciones IP iSCSI:

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

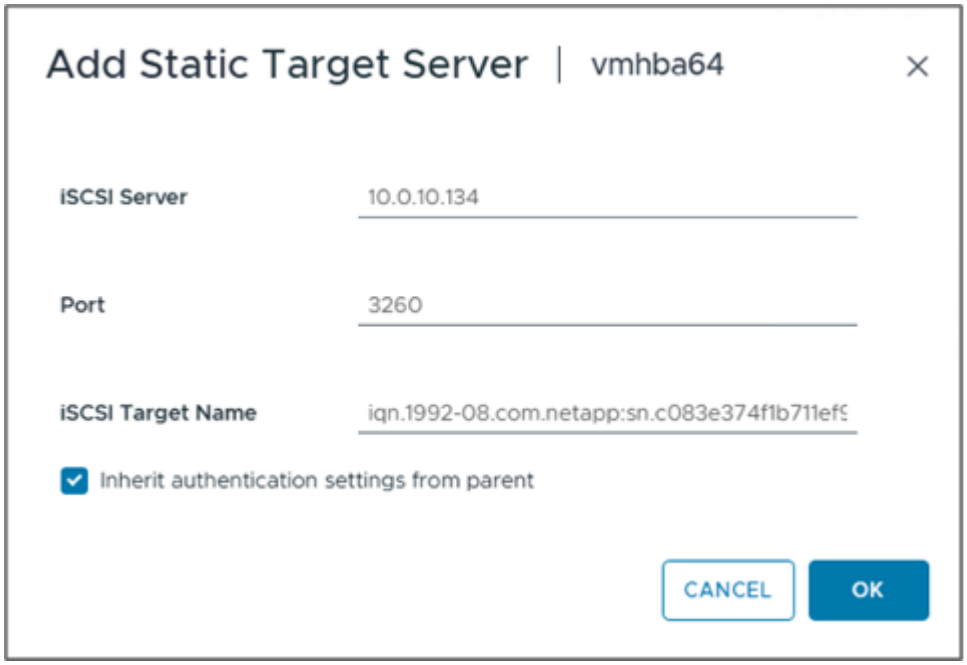
Descubra el servidor iSCSI FSx para ONTAP

Ahora que tenemos el LUN asignado, podemos descubrir el servidor iSCSI FSx for ONTAP para el SVM. Tenga en cuenta que para cada host ESXi que exista en su SDDC deberá repetir los pasos que se enumeran aquí.

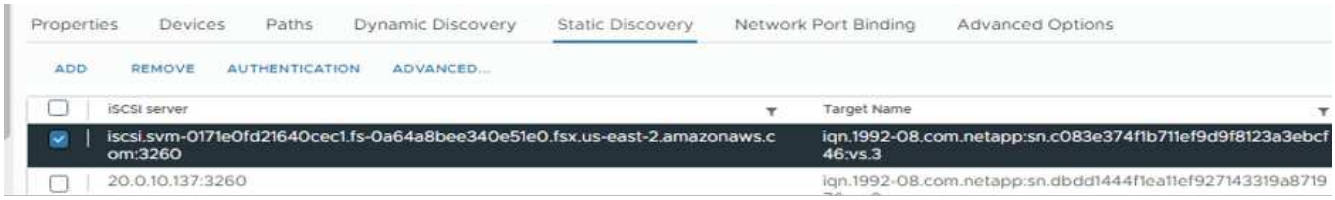
1. Primero, asegúrese de que el grupo de seguridad vinculado al sistema de archivos FSx para ONTAP (es decir, el conectado a ENI) permita puertos iSCSI.

   Para obtener una lista completa de los puertos del protocolo iSCSI y cómo aplicarlos, consulte"Control de acceso al sistema de archivos con Amazon VPC" .

2. En vSphere Client, vaya a Host ESXi > Adaptadores de almacenamiento > Detección estática y haga clic en "Agregar".
3. Ingrese la dirección IP del servidor iSCSI de arriba (el puerto es 3260). El nombre del objetivo iSCSI es el IQN del comando show iSCSI. Haga clic en "Aceptar" para continuar.



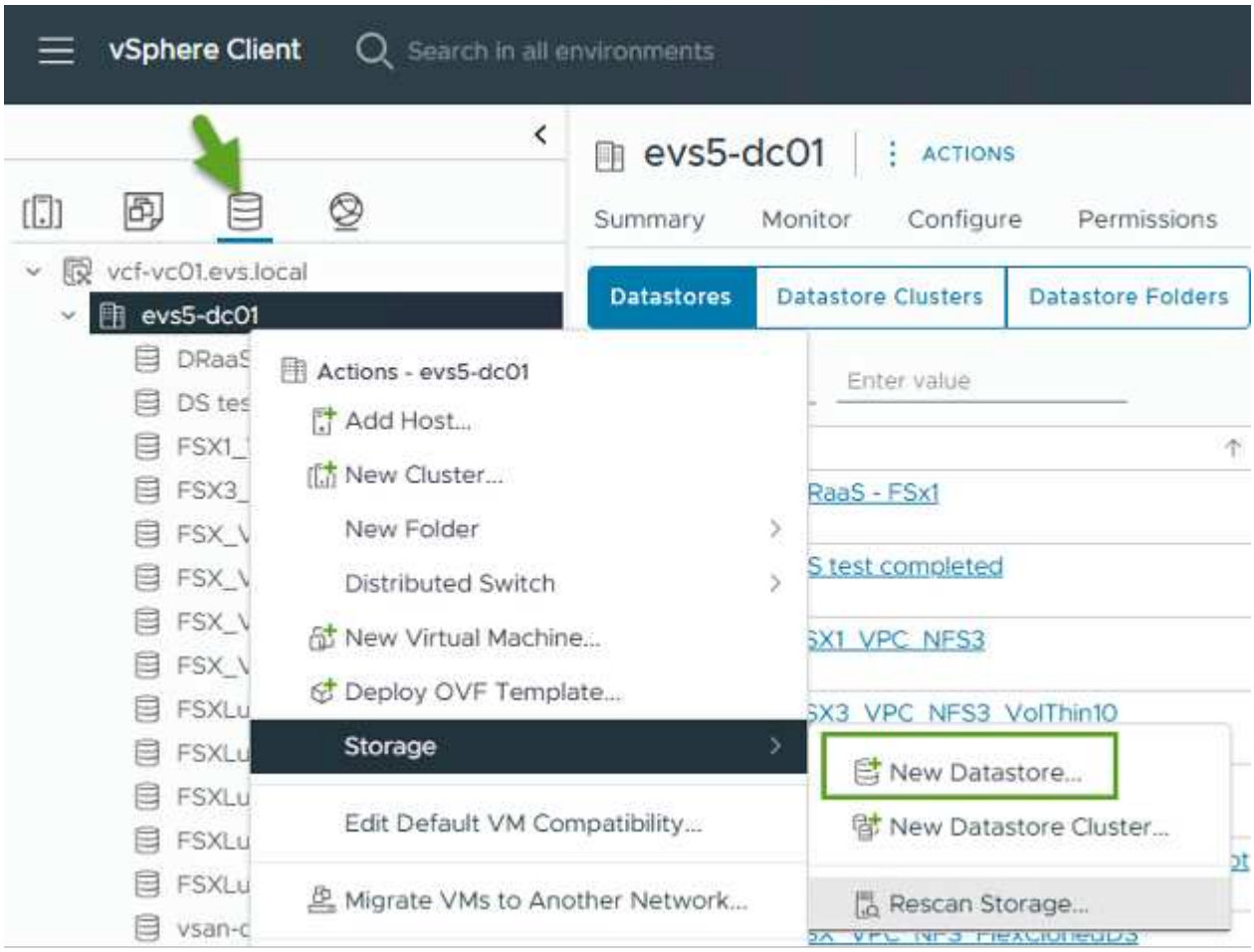
4. El asistente se cerrará y estará en la pantalla Descubrimiento estático del almacén de datos. En la tabla de esta página podrás verificar que el objetivo ha sido descubierto.



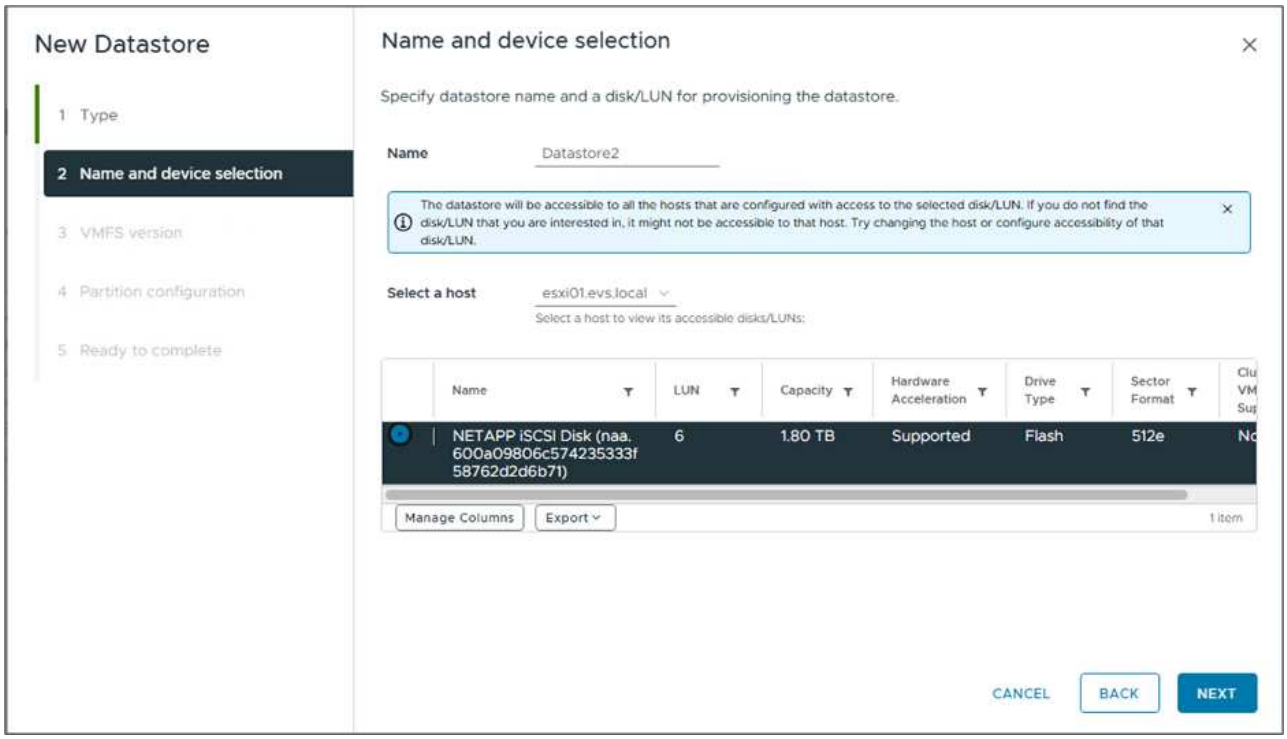
Crear un almacén de datos iSCSI

Ahora que hemos descubierto el servidor iSCSI, podemos crear un almacén de datos iSCSI.

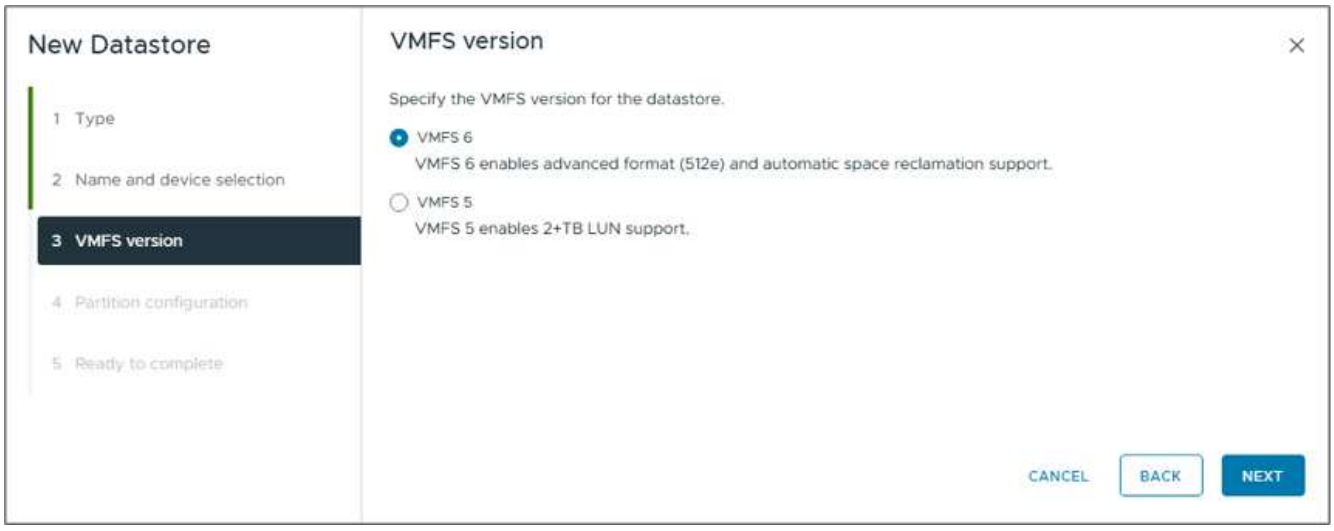
1. En el cliente vSphere, vaya a la pestaña Almacén de datos y seleccione el SDDC donde desea implementar el almacén de datos. Haga clic derecho y seleccione el ícono de Almacenamiento (indicado por la flecha verde en la captura de pantalla a continuación), luego seleccione "Nuevo almacén de datos" en el menú desplegable:



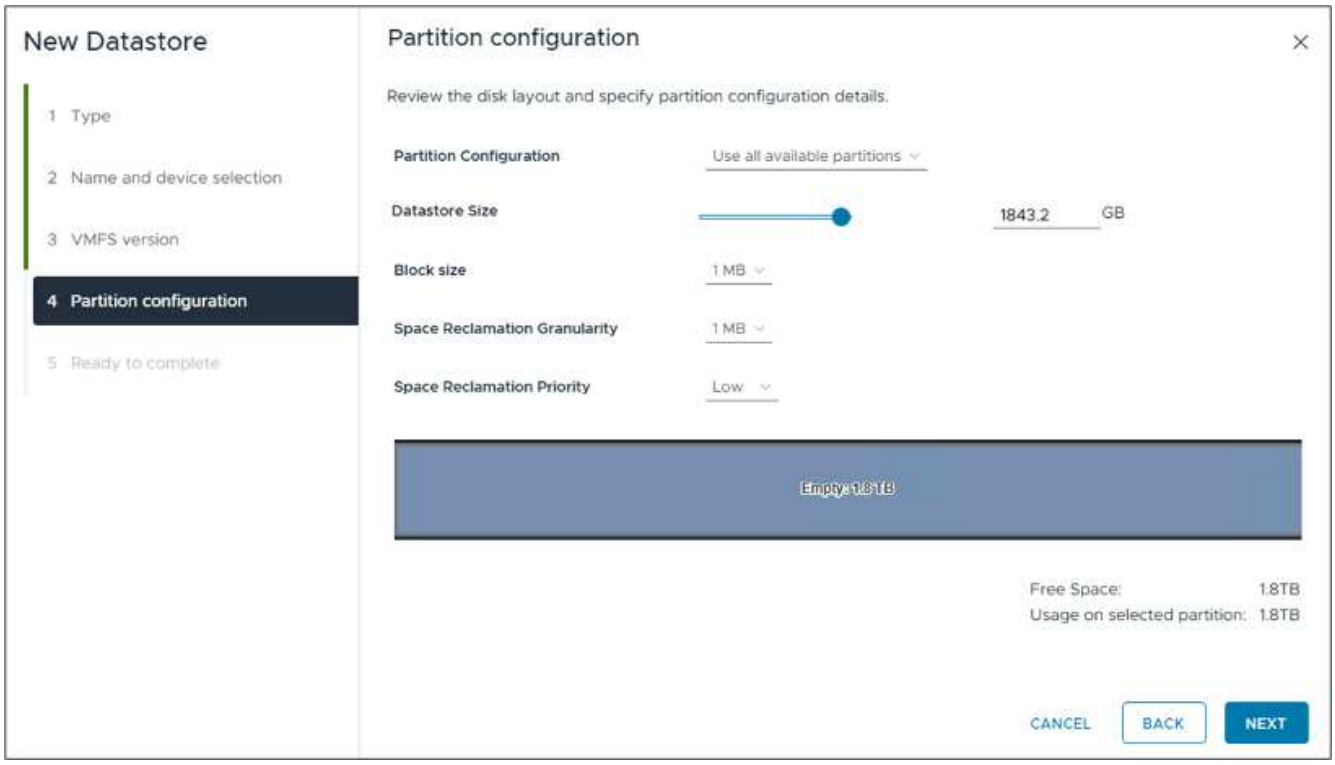
2. Ahora estará en el asistente Nuevo almacén de datos. En el paso "Tipo", seleccione la opción VMFS.
3. En el paso "Selección de nombre y dispositivo":
   a. Proporcione un nombre para su almacén de datos.
   b. Seleccione el host ESXi que desea conectar al almacén de datos.
   c. Seleccione el disco descubierto (LUN) y haga clic en "Siguiente".



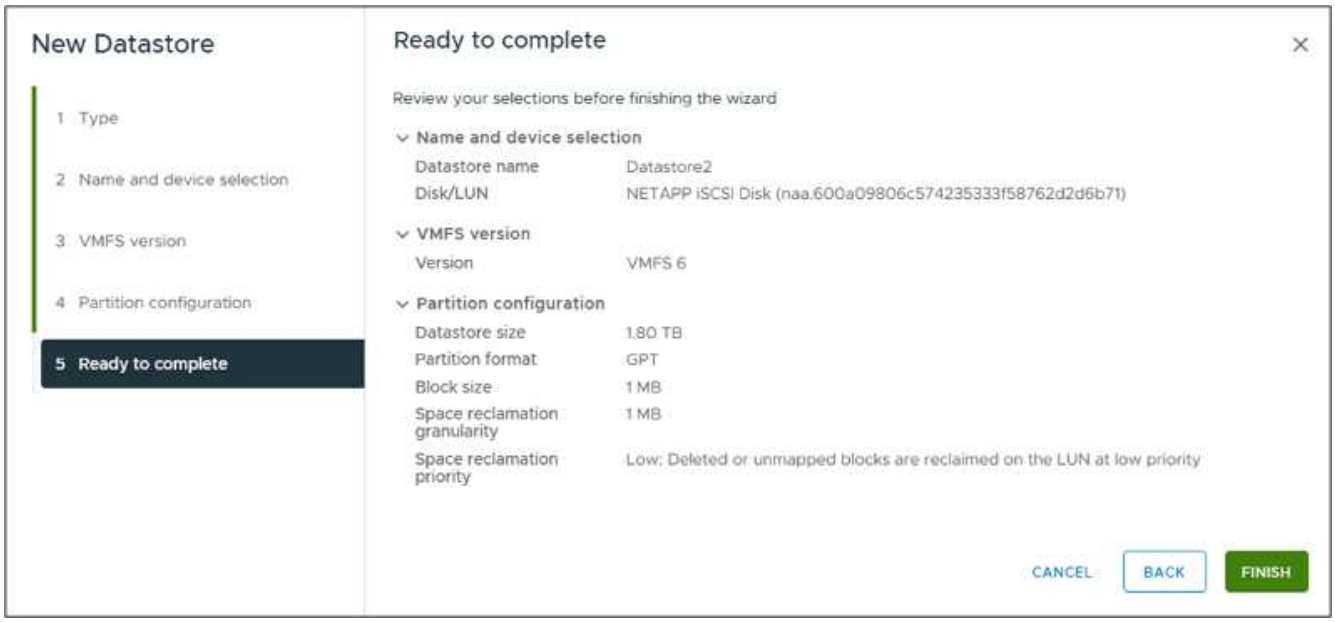
4. En el paso "Versión VMFS", seleccione "VMFS 6".



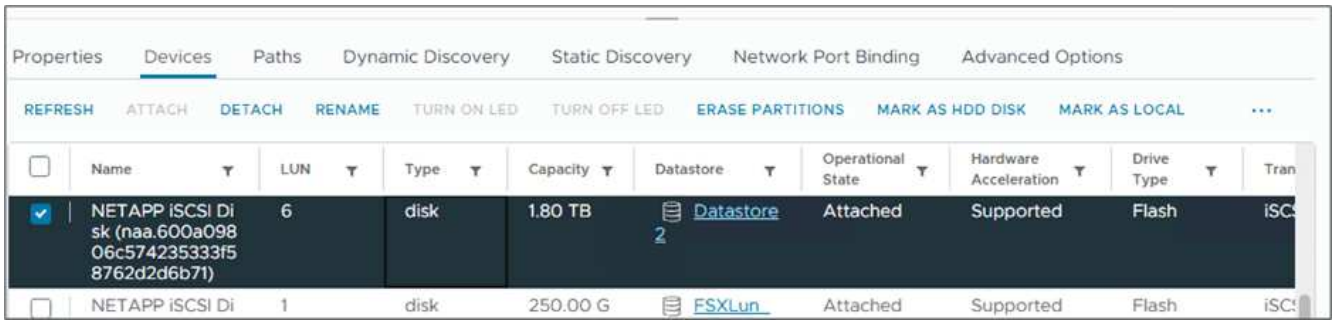
5. En el paso "Configuración de partición", deje la configuración predeterminada como está, incluida la opción "Usar todas las particiones disponibles". Haga clic en "Siguiente" para continuar.



6. En el paso "Listo para completar", asegúrese de que la configuración sea correcta. Cuando haya terminado, haga clic en "FINALIZAR" para completar la configuración.



7. Regrese a la página Dispositivos y verifique que se haya adjuntado el almacén de datos.



Conclusión

Este documento ha proporcionado instrucciones sobre cómo configurar FSx para ONTAP como almacenamiento externo para Amazon EVS para su uso con los protocolos NFS e iSCSI.

El uso de FSx para ONTAP como almacenamiento externo para Amazon EVS proporciona valores comerciales y operativos claros. Proporciona mayor resiliencia de datos, protección, replicación y rentabilidad a través de la tecnología ONTAP , y mantiene el TCO optimizado gracias al desacoplamiento de la arquitectura hiperconvergente de VMware. Con FSx para ONTAP, los usuarios de Amazon EVS pueden escalar el almacenamiento sin agregar recursos informáticos y sin inflar los costos. Esto abre todo el potencial de elasticidad y escalabilidad que ofrece la nube de AWS.

Para obtener más información, lea el anuncio de novedades de Amazon:"Amazon EVS ahora se integra con FSx para ONTAP" , y el blog de NetApp :"Amazon EVS anuncia compatibilidad con FSx para ONTAP" .

Proteger datastore FSx ONTAP para EVS

Cómo proteger los datastores de Amazon FSx for NetApp ONTAP con Amazon Elastic VMware Service usando el NetApp SnapCenter Plug-in for VMware

Esta guía te va a mostrar un enfoque sencillo de implementación para proteger los datastores de Amazon FSx for ONTAP Network File System (NFS) e iSCSI EVS y las máquinas virtuales asociadas usando la solución de backup y recuperación NetApp SnapCenter® Plug-in for VMware vSphere (SCV) para VMs.

Introducción

Los almacenes de datos suplementarios basados en Amazon FSx for NetApp ONTAP (FSx for ONTAP) para Amazon Elastic VMware Service (Amazon EVS) ofrecen una solución excelente para ejecutar tanto cargas de trabajo exigentes en cuanto a rendimiento—como aprovechar nConnect, el peering de Amazon Virtual Private Cloud (Amazon VPC) y el uso de varias conexiones de red por montaje de almacén de datos—como cargas de trabajo intensivas en almacenamiento.

Esta capacidad permite a los clientes superar las limitaciones del almacenamiento de instancia local proporcionado por una red de área de almacenamiento virtual (vSAN), escalar el almacenamiento independientemente del cómputo y reducir el coste total de propiedad. Más allá de los beneficios del coste total de propiedad (TCO), FSx for ONTAP ofrece Amazon EVS con características de clase empresarial familiares para los clientes de ONTAP® on-premises, ayudando a optimizar y agilizar las implementaciones. Usar FSx for ONTAP proporciona acceso a las tecnologías NetApp® Snapshot™, SnapMirror® y SnapVault® que admiten operaciones de backup y restauración para máquinas virtuales (VM), almacenes de datos y discos de máquinas virtuales (VMDK). Una función clave es la protección basada en Snapshot.

Descripción general

A medida que las organizaciones escalan y consolidan entornos, la necesidad de proteger esas cargas de trabajo y el almacenamiento subyacente se vuelve cada vez más importante. SCV puede usarse para hacer copias de seguridad de datastores y máquinas virtuales directamente desde el cliente de Amazon EVS vSphere.

Propósito de esta Guía

Esta guía proporciona instrucciones sobre cómo proteger un datastore FSx for ONTAP para Amazon EVS usando SCV. Se proporcionan ejemplos de escenarios para proteger VMs y bases de datos, así como de restauración.

Audiencia

Este tutorial está destinado a arquitectos y administradores de la nube familiarizados con VMware vSphere, Amazon EVS, la consola de AWS y FSx para ONTAP.

Pasos a grandes rasgos para el despliegue y la configuración

A continuación se indican los pasos a grandes rasgos para implementar y configurar SCV para proteger tus máquinas virtuales y almacenes de datos en Amazon EVS:

1. Descarga el SCV Open Virtual Appliance (OVA).
2. Inicia sesión con las credenciales del vSphere Client en Amazon EVS.
3. Despliega una plantilla de Open Virtualization Format (OVF) para iniciar el asistente de despliegue de VMware.
4. Para acceder al plug-in, selecciona SnapCenter Plug-in for VMware en el menú.
5. Agrega almacenamiento.
6. Crea políticas de backup.
7. Crea grupos de recursos.
8. Grupos de backup.
9. Restaura toda la máquina virtual o un disco virtual o archivos de invitado concretos.

Procedimiento de configuración para SnapCenter Plug-in for VMware

Esta sección cubre los pasos para configurar SnapCenter Plug-in for VMware.

Prerrequisitos

Se requieren los siguientes requisitos previos antes de que empieces:

1. Para registrar el servidor vCenter mientras despliegas el OVA, especifica el nombre de dominio completo (FQDN) o la dirección IP de vCenter.
2. Para las credenciales de vCenter, usa una cuenta con los privilegios mínimos requeridos
3. Abre los puertos del cortafuegos para el acceso a vCenter Server.
4. Actualiza el grupo de seguridad de la VPC de Amazon donde se está ejecutando FSx para ONTAP para permitir que SCV acceda a FSx para ONTAP.

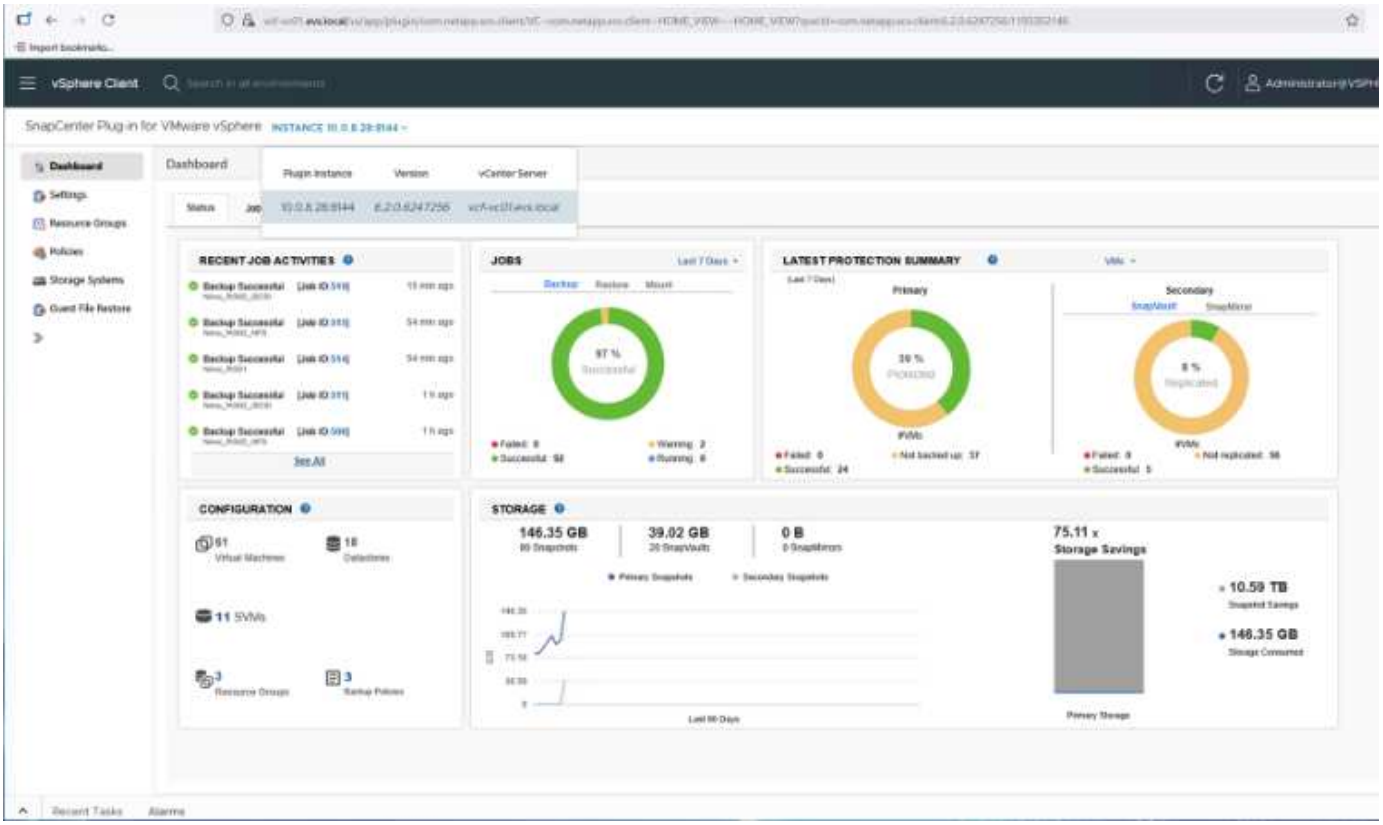
SCV está disponible de forma gratuita.

Configurando el complemento de SnapCenter para VMware

Para proteger las máquinas virtuales y los almacenes de datos basados en NFS/iSCSI que las alojan, SCV debe ser desplegado. Es una simple importación de OVF.

Los pasos para desplegar son los siguientes:

1. Descarga el OVA de "Sitio de soporte de NetApp".
2. Inicia sesión en el Amazon EVS vCenter.
3. Dentro de vCenter, haz clic derecho en cualquier objeto del inventario, como un centro de datos, una carpeta, un clúster o un host, y selecciona "Desplegar plantilla OVF".
4. Selecciona la configuración correcta, incluyendo el almacenamiento, el segmento y personaliza la plantilla para actualizar el vCenter y sus credenciales, crear credenciales SCV y detalles de dirección IP. Una vez revisado, selecciona "Finalizar".
5. Espera a que finalicen las tareas de importación y despliegue de OVF.
6. Una vez que SCV se haya desplegado correctamente, se registrará dentro de vCenter.
7. Para acceder al complemento, navega a la barra lateral izquierda de la página del cliente web de vCenter y selecciona "SnapCenter Plug-in for VMware".



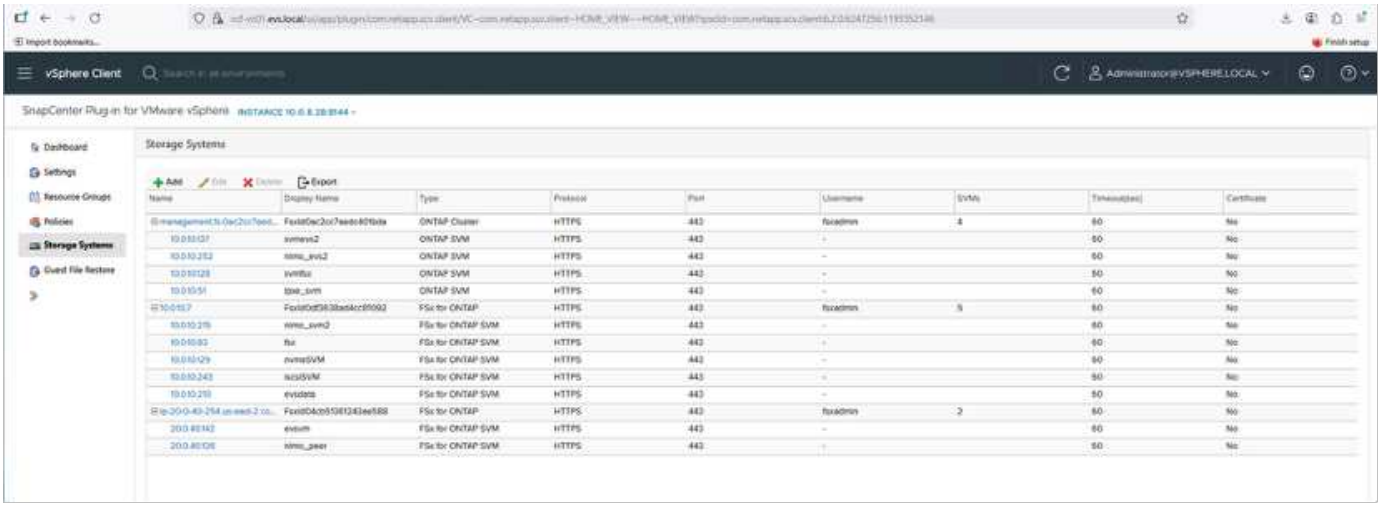
Procedimiento de configuración para SnapCenter Plug-in for VMware

Esta sección cubre los pasos para configurar SnapCenter Plug-in for VMware. Las siguientes secciones detallarán cómo añadir almacenamiento, crear una política de backup y cómo crear grupos de recursos.

Agregar el sistema de almacenamiento

El siguiente paso para proteger las cargas de trabajo con SVC es añadir el "sistema de almacenamiento". Añadir almacenamiento permite que SCV detecte y gestione las operaciones de backup y restauración dentro de vCenter. Incluye el endpoint de gestión de FSx for NetApp ONTAP o la IP del endpoint de administración de la máquina virtual de almacenamiento (SVM) como sistema de almacenamiento para habilitar el backup y la restauración de máquinas virtuales.

1. Desde el menú de navegación izquierdo de EVS vCenter, selecciona "SnapCenter Plug-in for VMware".
2. Selecciona "Storage System".
3. Selecciona "Add" para añadir los detalles de FSx para ONTAP.
4. Usa el método "Credentials as the Authentication" e ingresa FSxadmin como nombre de usuario y contraseña. Luego selecciona "Add" para guardar la configuración.



Todas las SVM se añaden automáticamente cuando se añade el sistema de archivos.

Si la versión de SCV es 6.2, ve a "la página de soporte de SCV" y descarga la versión SCV 6.2P1.

Crea una política de backup

Una estrategia de backup sólida debe definir factores clave como la programación del backup, los datos que se van a respaldar y el periodo de retención de los backups. Las copias snapshot se pueden programar cada hora o cada día para proteger almacenes de datos completos. Programar los backups de esta manera no solo protege los almacenes de datos, sino que también permite realizar operaciones de backup y restauración para las VMs y VMDKs que están dentro de esos almacenes de datos.

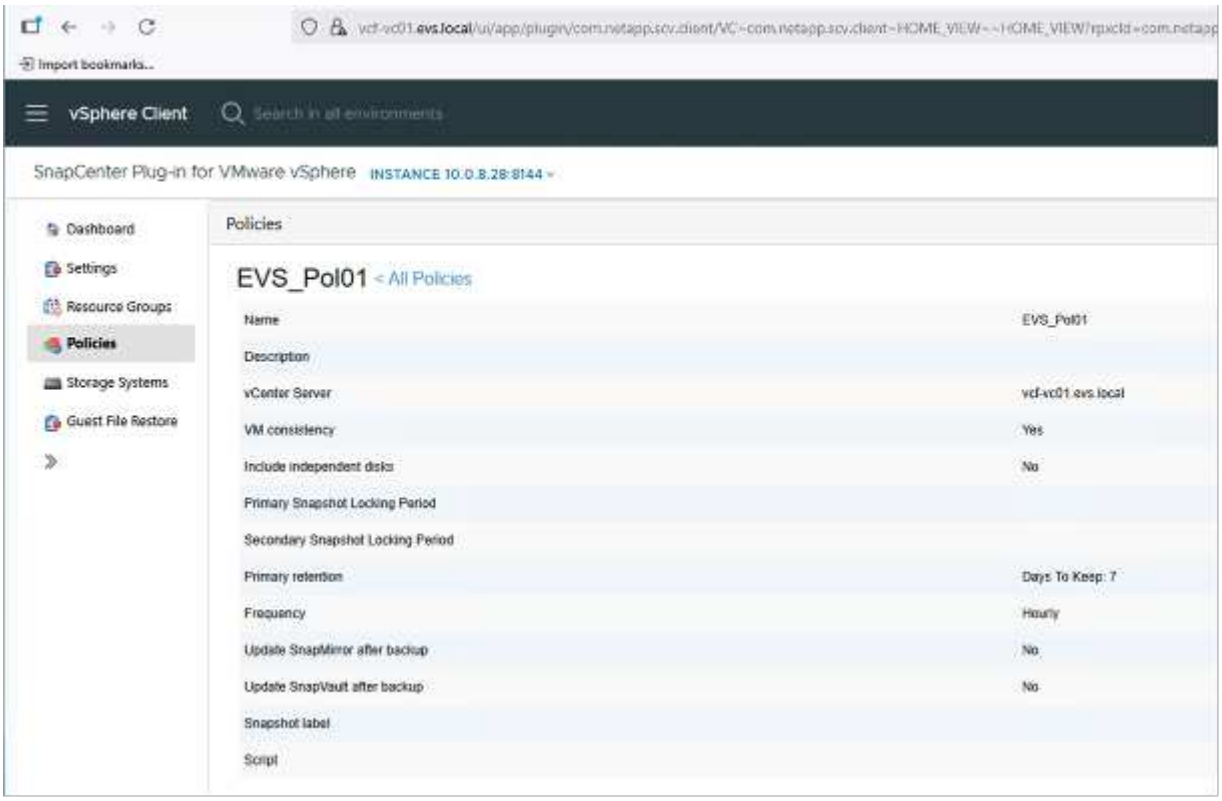
Antes de iniciar copias de seguridad para VMs y datastores, crea un "política de backup" y un grupo de recursos. La política de backup especifica parámetros como la programación de backup y la configuración de retención.

Aquí tienes los pasos para crear una política de backup:

1. Ve al menú de navegación de la izquierda en SCV y selecciona "Policies".
2. En la página Políticas, selecciona "Crear" para iniciar el asistente.
3. En la página "Nueva política de backup", ingresa un nombre para la política.
4. Especifica el periodo de retención, la frecuencia de backup y los ajustes de replicación.

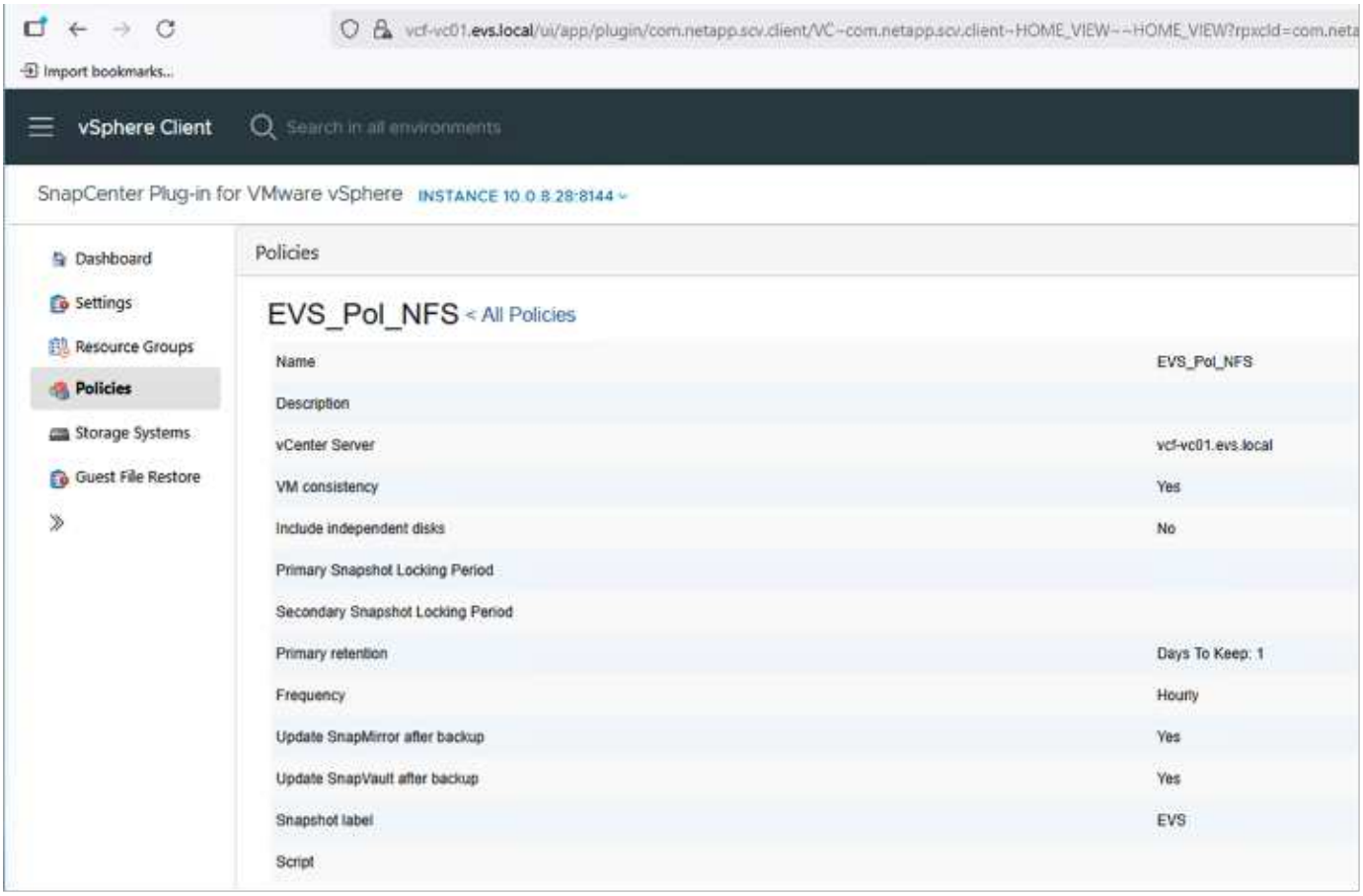
5. Selecciona la casilla de verificación "Locking Period" para activar el bloqueo de Snapshot. Puedes seleccionar los periodos de bloqueo de Snapshot primario y secundario como días/meses/años.

Independientemente del valor de retención definido en la política de SnapMirror, la copia Snapshot secundaria permanece intacta hasta que expira el periodo de bloqueo de la instantánea secundaria especificado.



Para habilitar las copias de seguridad consistentes con VM, VMware tools debe estar instalado y en ejecución. Cuando la casilla de consistencia de VM está marcada, primero las VMs se ponen en reposo, luego VMware realiza una instantánea consistente con VM (excluyendo la memoria), después SCV realiza su operación de backup y luego se reanudan las operaciones de VM.

Para replicar copias Snapshot a un sistema de archivos mirror o vault secundario, las relaciones deben estar configuradas de antemano.



Una vez creada la política, el siguiente paso es crear el grupo de recursos que definirá los datastores NFS o iSCSI apropiados y las VMs que se deben respaldar.

Crear un grupo de recursos

Un grupo de recursos sirve como contenedor para máquinas virtuales y almacenes de datos que requieren protección. Los recursos pueden añadirse o eliminarse de un grupo de recursos en cualquier momento, proporcionando flexibilidad al gestionar las configuraciones de backup.

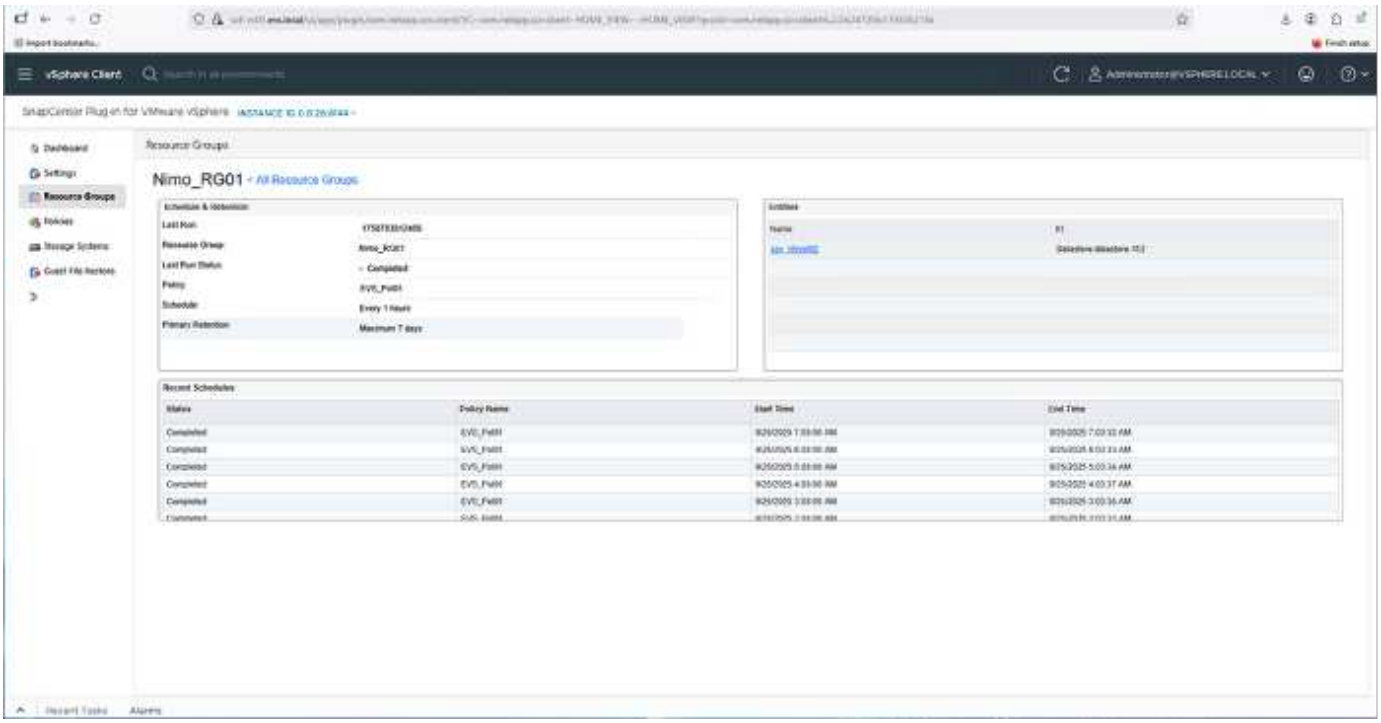
Puedes crear un "grupo de recursos" usando los siguientes pasos:

1. Ve al panel de navegación de la izquierda en SCV y selecciona "Resource Groups".
2. En la página Grupos de recursos, selecciona "Crear" para iniciar el asistente de creación de grupos de recursos.

> Otra opción para crear grupos de recursos es seleccionar una máquina virtual o un almacén de datos individual y crear un grupo de recursos que contenga solo ese recurso.

3. En la página "Recursos", selecciona el ámbito (VMs o almacenes de datos) y el data center.
4. En la página "Spanning disks", selecciona la opción "Virtual Machines with multiple VMDKs across multiple datastores".
5. A continuación, asocia una política de backup. Selecciona una política existente o crea una nueva política de backup.
6. En la página "Programaciones", configura la programación de backup para cada política seleccionada.

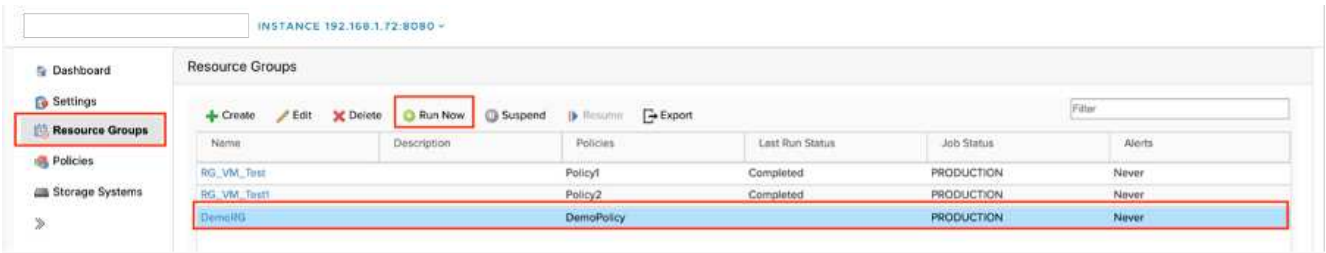
7. Una vez que hagas las selecciones apropiadas, selecciona "Finish". Esto creará un nuevo grupo de recursos y lo añadirá a la lista de grupos de recursos.



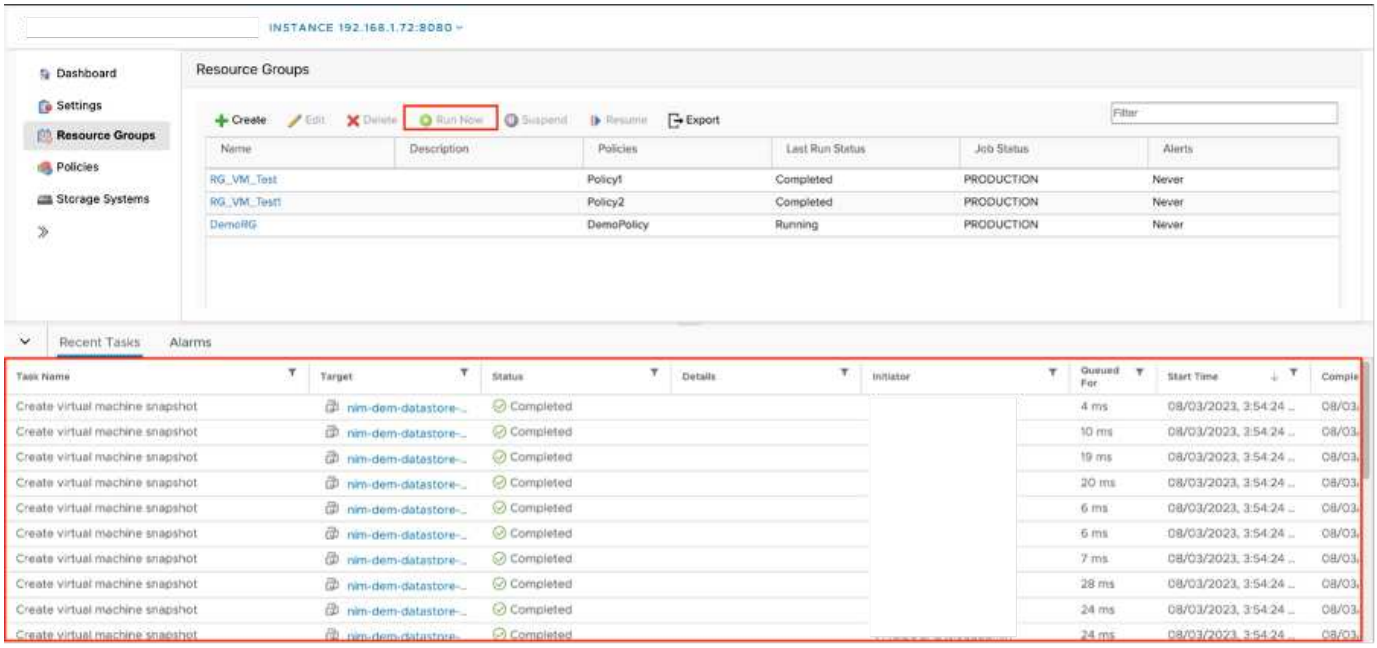
Backup de grupos de recursos

Las operaciones de backup se ejecutan en todos los recursos definidos dentro de un grupo de recursos. Si un grupo de recursos tiene una política adjunta y una programación configurada, los backups ocurren automáticamente según la programación.

1. En el panel de navegación izquierdo de la página del cliente web de vCenter, selecciona "SnapCenter Plug-in for VMware" y luego "Resource Groups".
2. En la página Resource Groups, encuentra el grupo de recursos designado y selecciona "Run Now" para iniciar el backup manual.



3. Si el grupo de recursos tiene varias políticas configuradas, selecciona la política para la operación de backup en el cuadro de diálogo "Backup Now".
4. Selecciona "OK" para iniciar el backup.

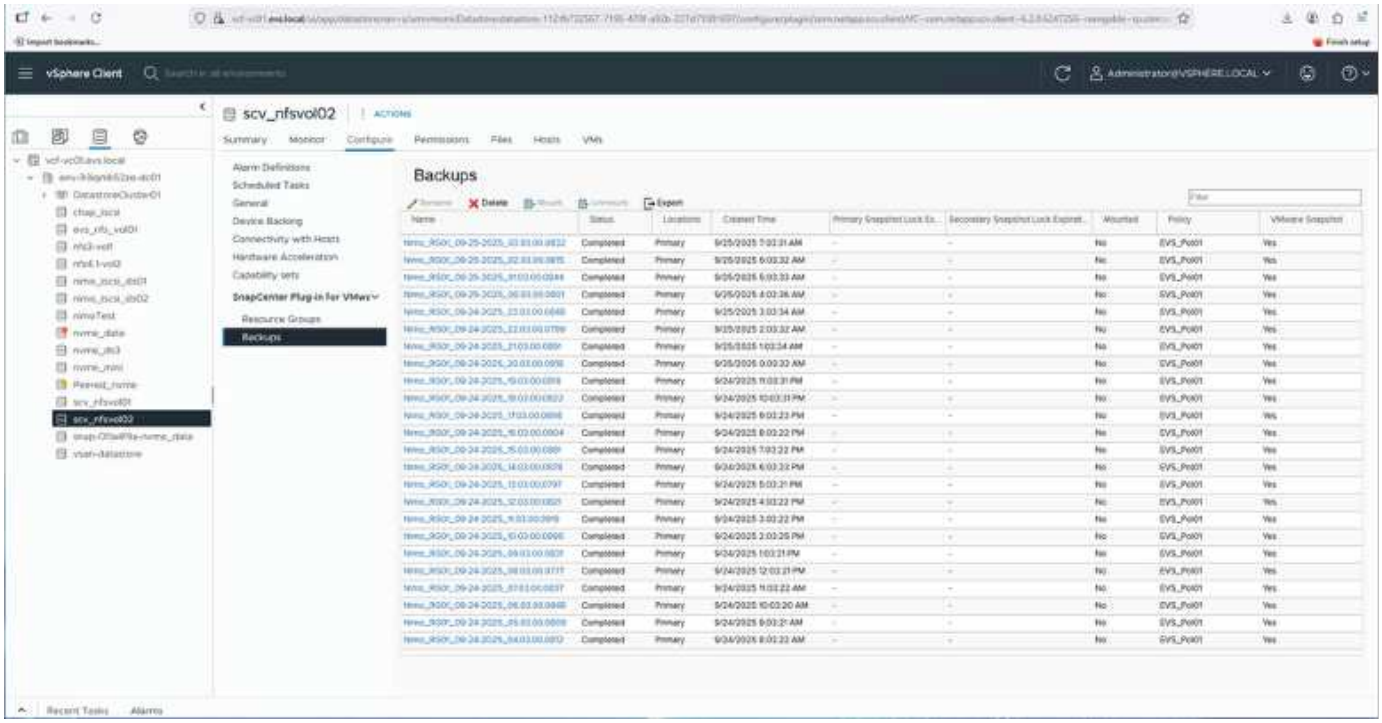


Supervisa el progreso de la operación seleccionando "Tareas recientes" en la parte inferior de la ventana o, para más detalles, selecciona "Monitor de trabajos" en el panel de control.

El proceso para crear políticas de backup, configurar grupos de recursos y realizar operaciones de backup es coherente en los diferentes protocolos de almacenamiento, incluidos NFS e iSCSI.

Los backups se realizan según el calendario definido en la política.

Después de que se complete el backup, puedes verlo a nivel de datastore o para máquinas virtuales individuales seleccionando "SnapCenter Plug-in for VMware vSphere" en la lista desplegable y luego eligiendo "Restore".



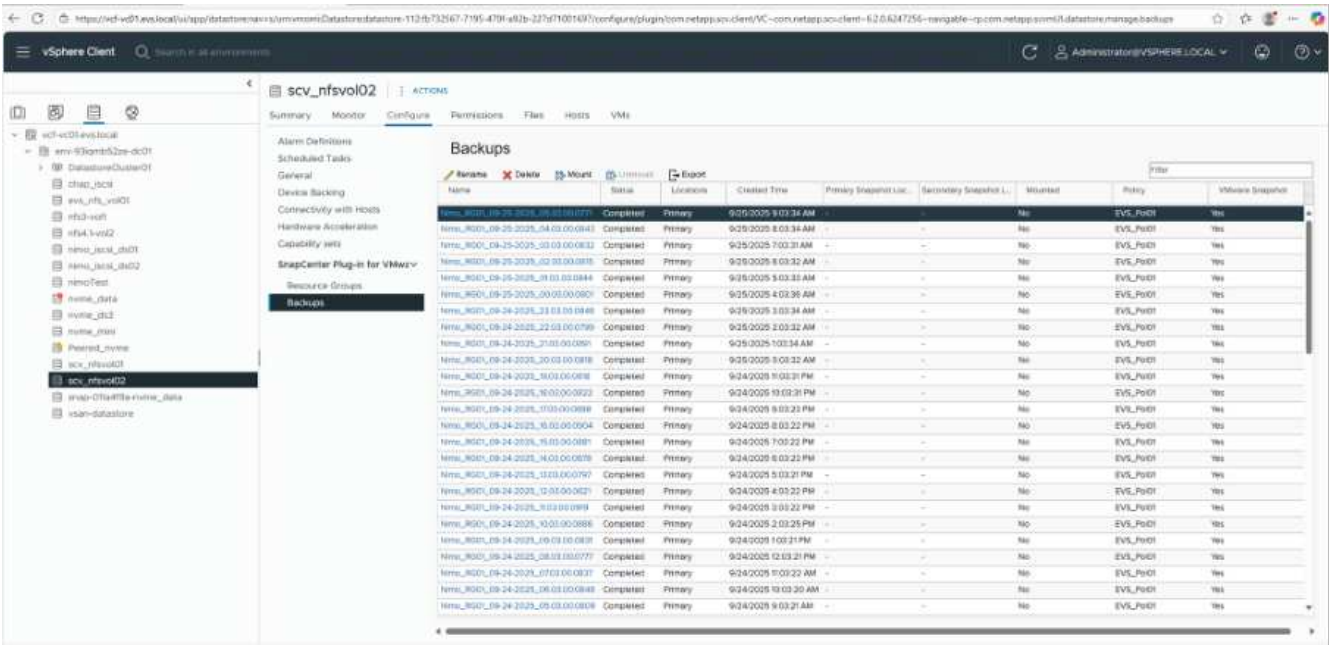
Procedimiento de restauración para VMs protegidas por SnapCenter Plug-in for VMware

Esta sección cubre los pasos para restaurar VMs desde backups. SCV se puede usar para restaurar VMs dentro de vCenter, permitiendo recuperarlas en el datastore original en el host ESXi original (sobrescribiendo el contenido existente), restaurar VMs eliminadas o renombradas desde una copia de backup, en un datastore diferente en el host ESXi original, en el datastore original en un host ESXi diferente gestionado por el mismo vCenter, o en un datastore diferente en otro host ESXi dentro del mismo entorno vCenter.

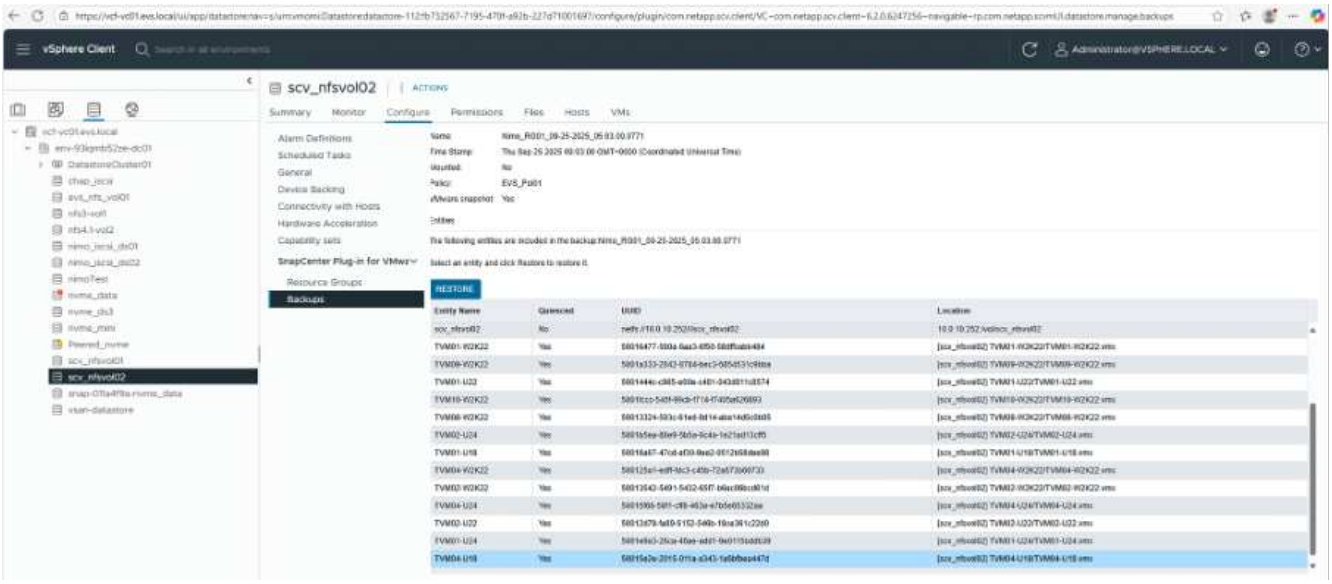
Pasos para realizar la operación de restauración

Para realizar la operación de restauración, sigue estos pasos:

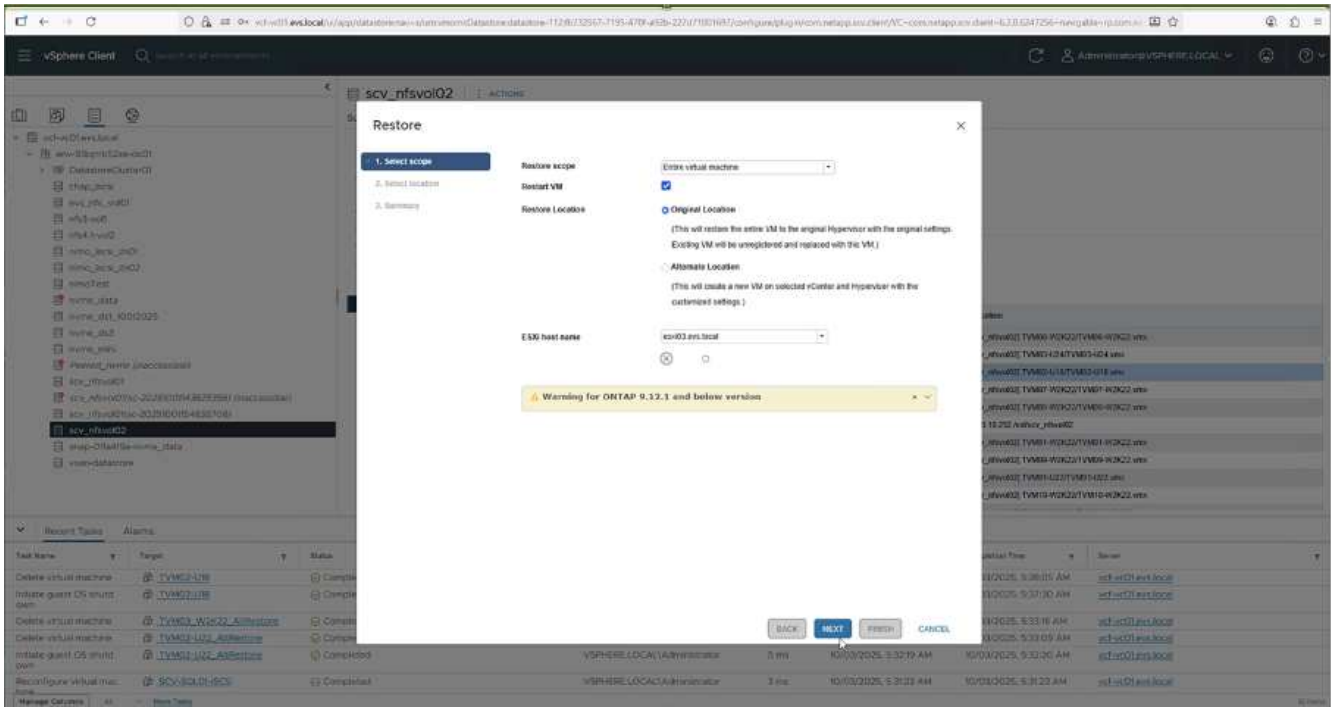
1. En la interfaz gráfica de usuario del cliente web de EVS vSphere, ve a **Inventory › Datastores** y selecciona el datastore que quieras. Luego navega a **Configure › Backups** en la sección "SnapCenter Plug-in for VMware vSphere".



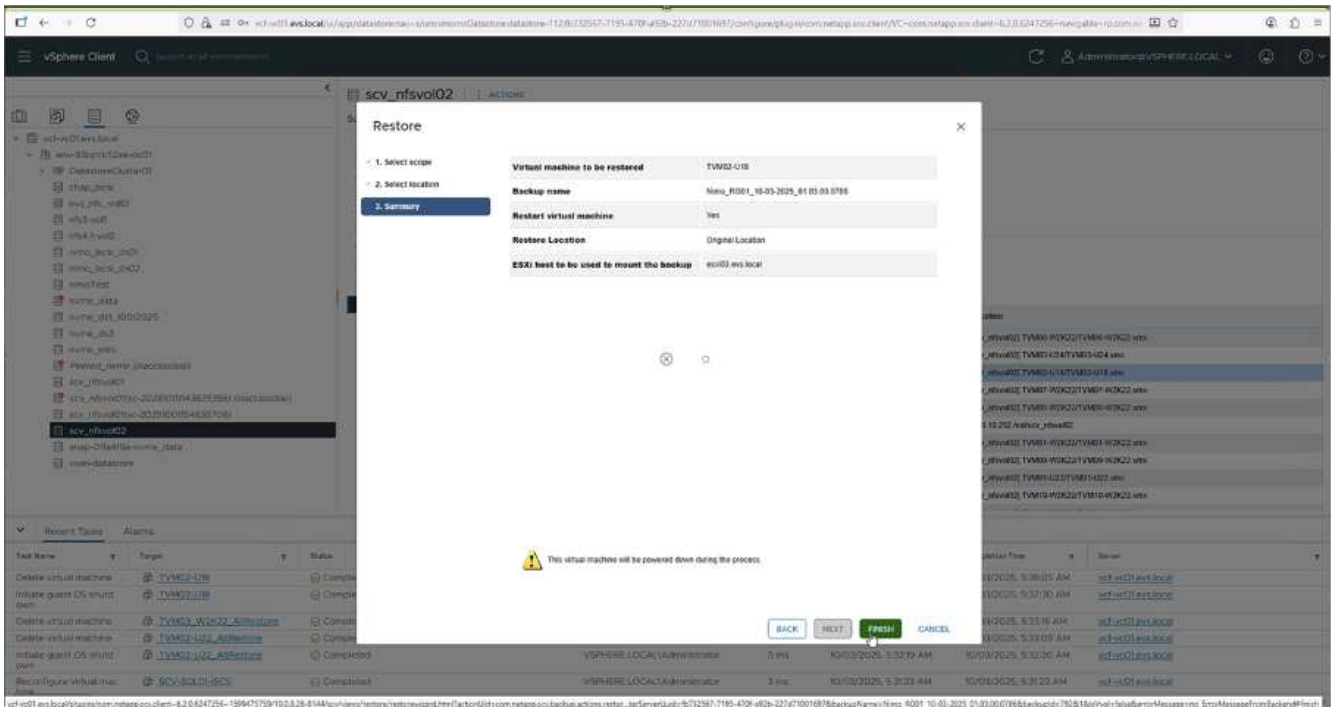
2. Haz doble clic en una copia de seguridad para ver todas las máquinas virtuales incluidas en esa copia de seguridad. Busca la máquina virtual que quieres restaurar en la lista y selecciona "Restaurar".



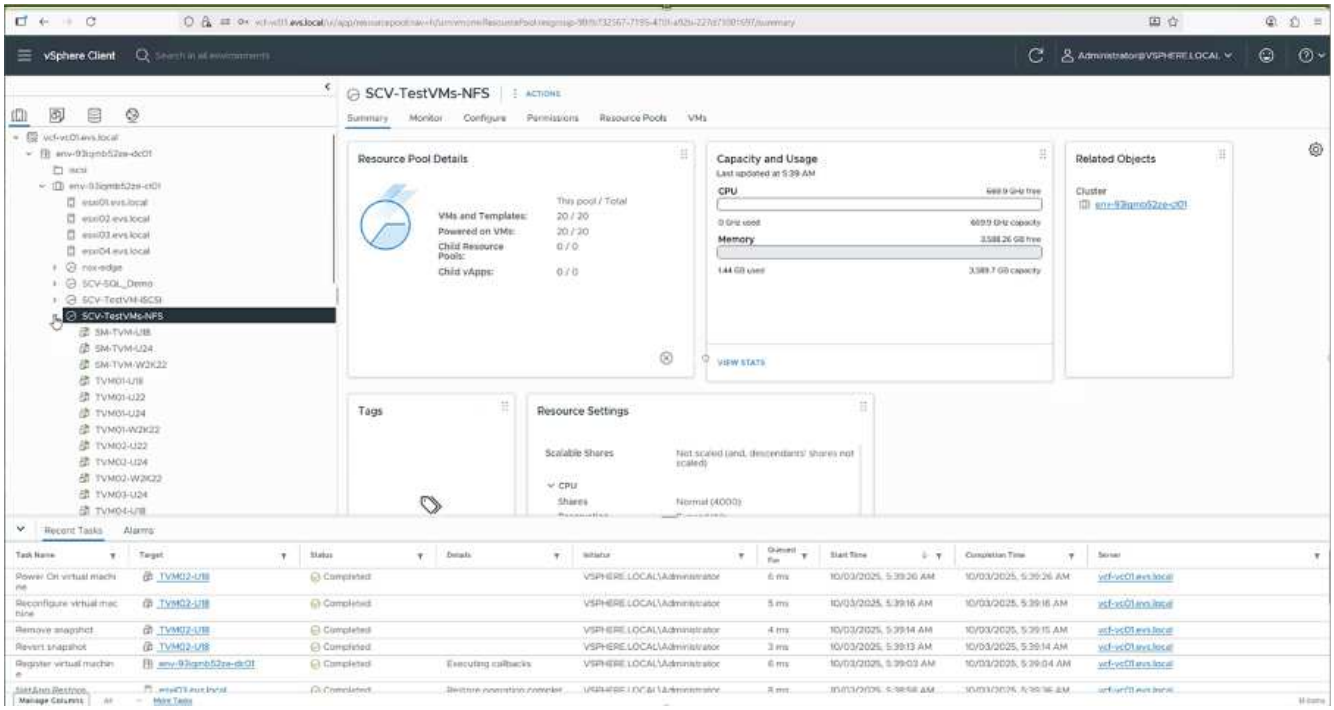
3. En la página "Seleccionar ámbito", selecciona "Máquina virtual completa" en el campo "Ámbito de restauración", luego selecciona "Ubicación de restauración" e ingresa la información del ESXi de destino donde se debe montar el backup.
4. Activa la casilla "Reiniciar VM" si la VM necesita encenderse después de la operación de restauración.
5. En la página "Seleccionar ubicación", selecciona una ubicación principal.



6. Revisa la página "Resumen" y luego selecciona "Finalizar".



7. Supervisa el progreso de la operación seleccionando "Tareas recientes" en la parte inferior de la pantalla.



Aunque las máquinas virtuales se restauran, no se añaden automáticamente a sus antiguos grupos de recursos. Si quieres proteger esas máquinas virtuales, añádelas manualmente a los grupos de recursos adecuados.

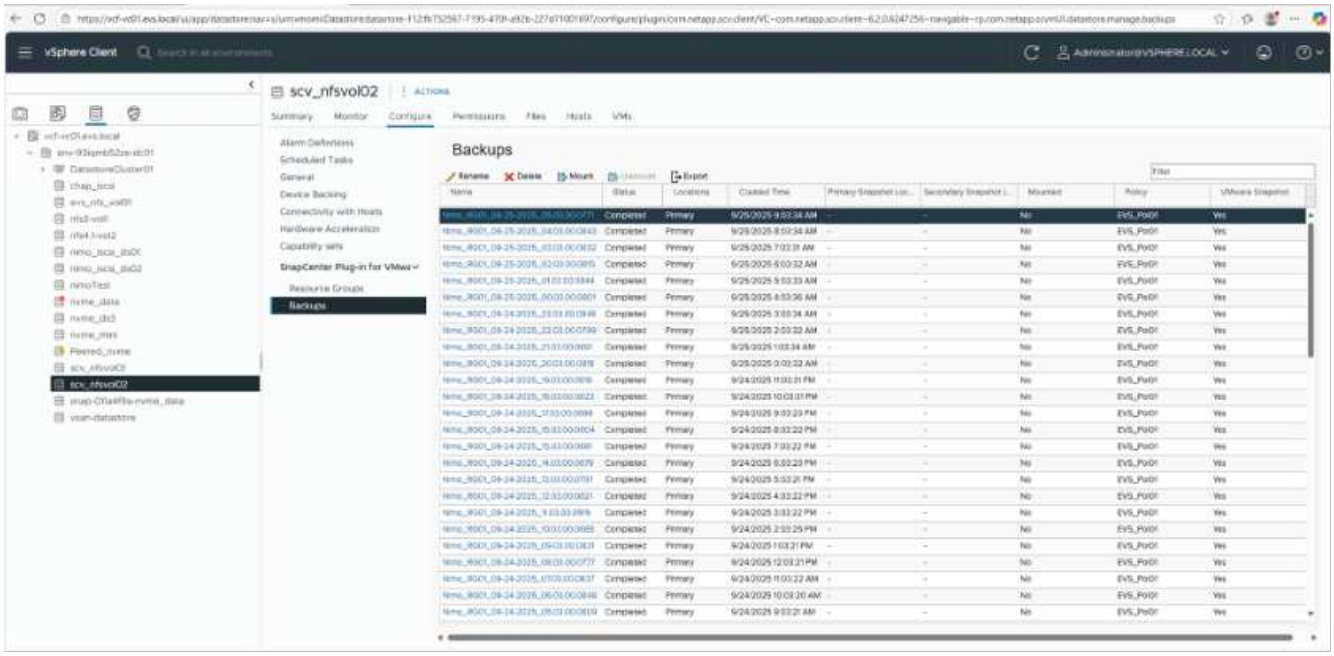
La operación de restauración también puede activarse desde el nivel individual de la VM.

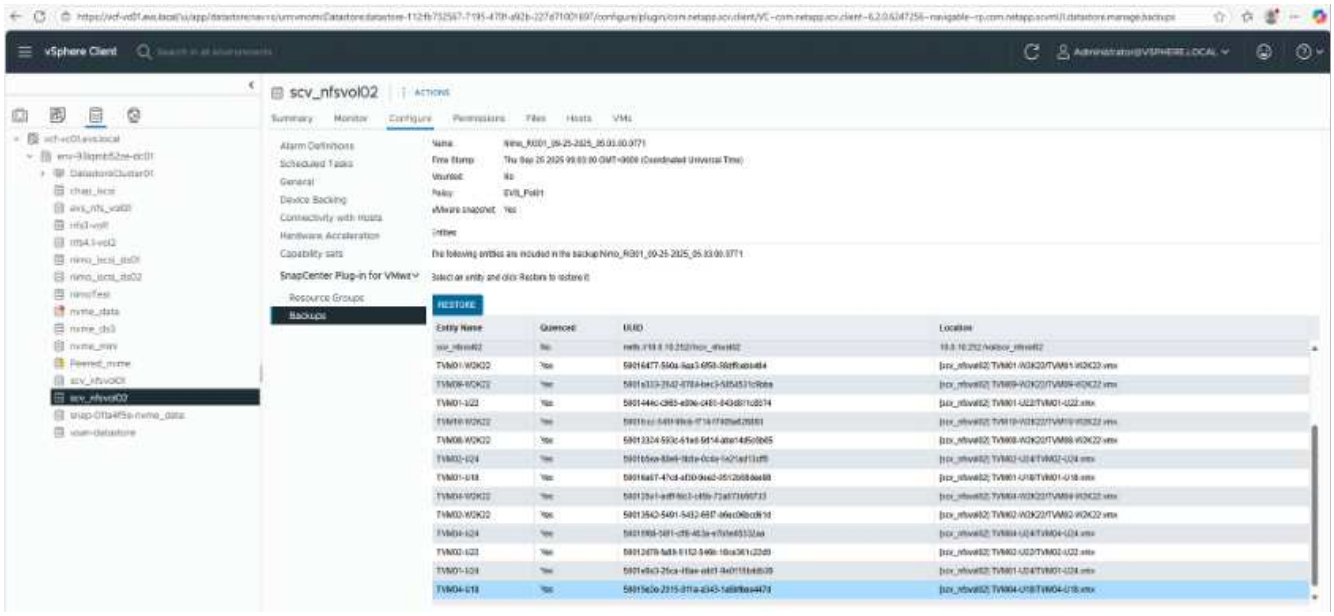
Pasos para restaurar una VM eliminada

Restaurar una VM eliminada es un proceso sencillo con SCV.

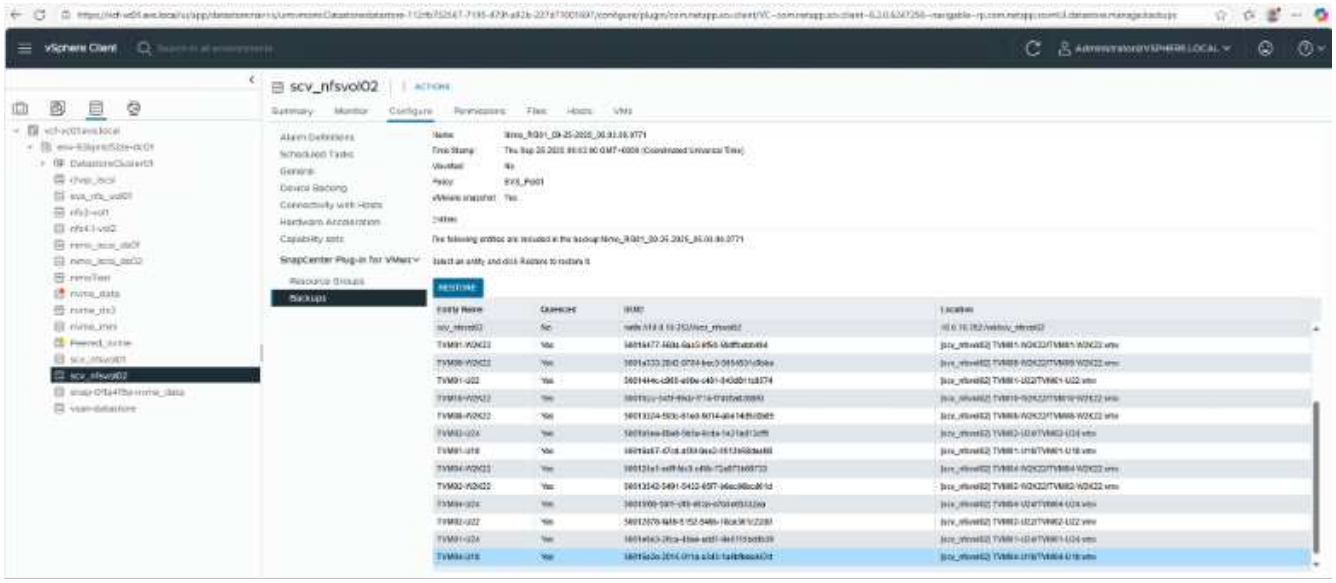
La operación de restauración de una máquina virtual eliminada se puede realizar desde el nivel del almacén de datos.

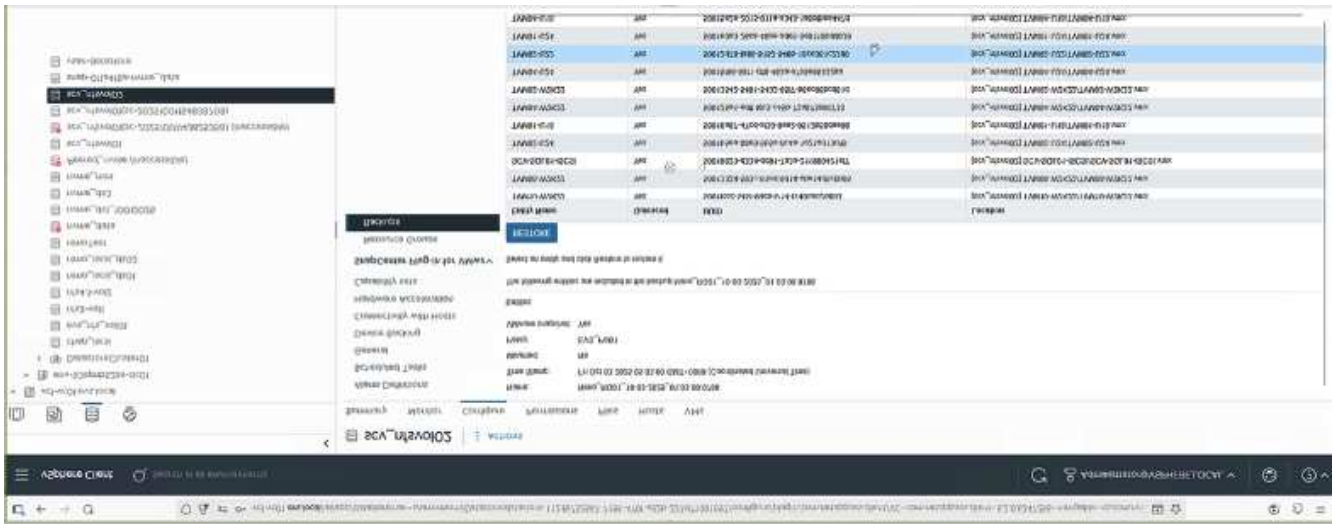
1. Ve al Datastore respectivo > Configure > Backups. Ahí, selecciona la VM eliminada y selecciona "Restore".

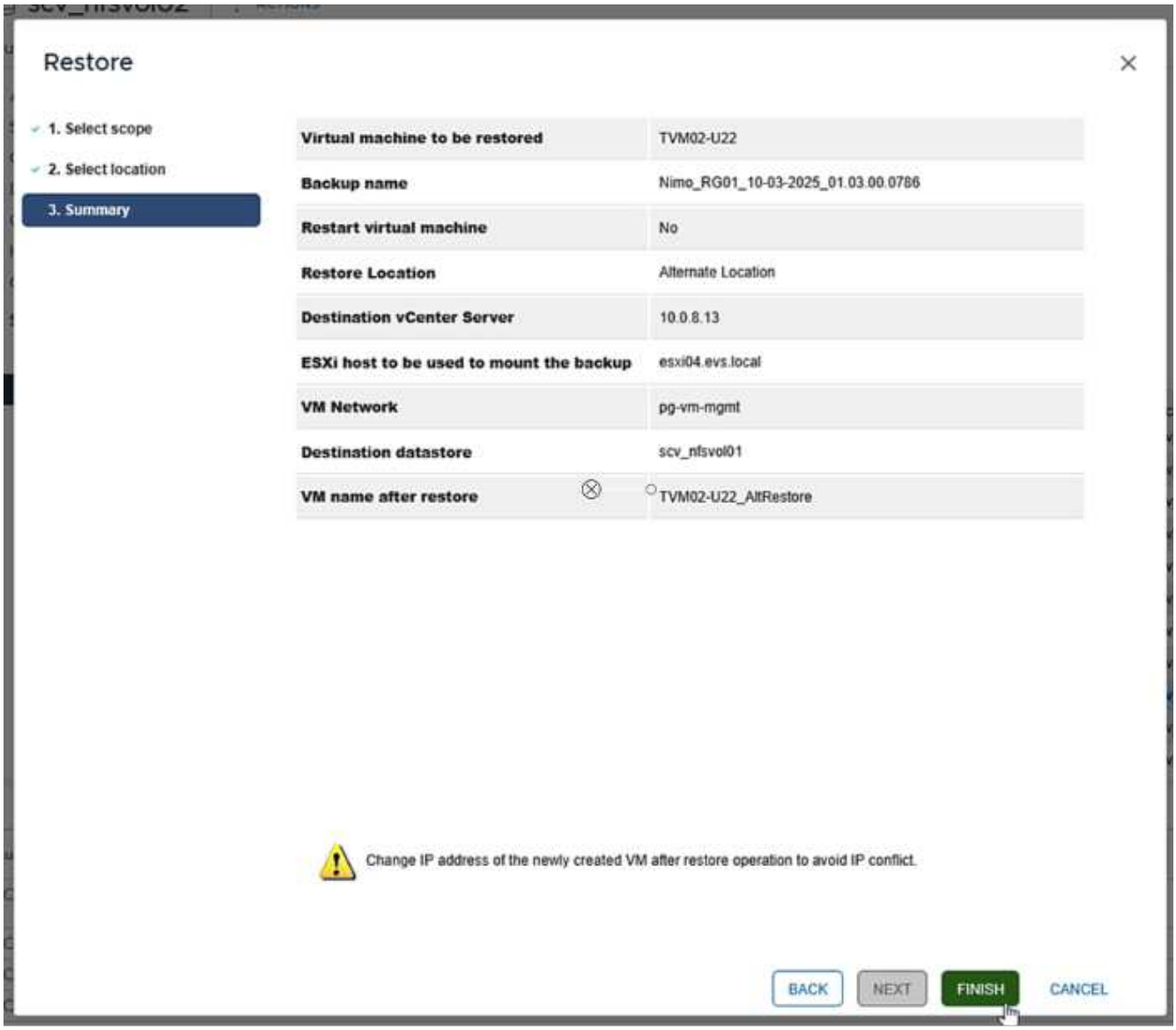


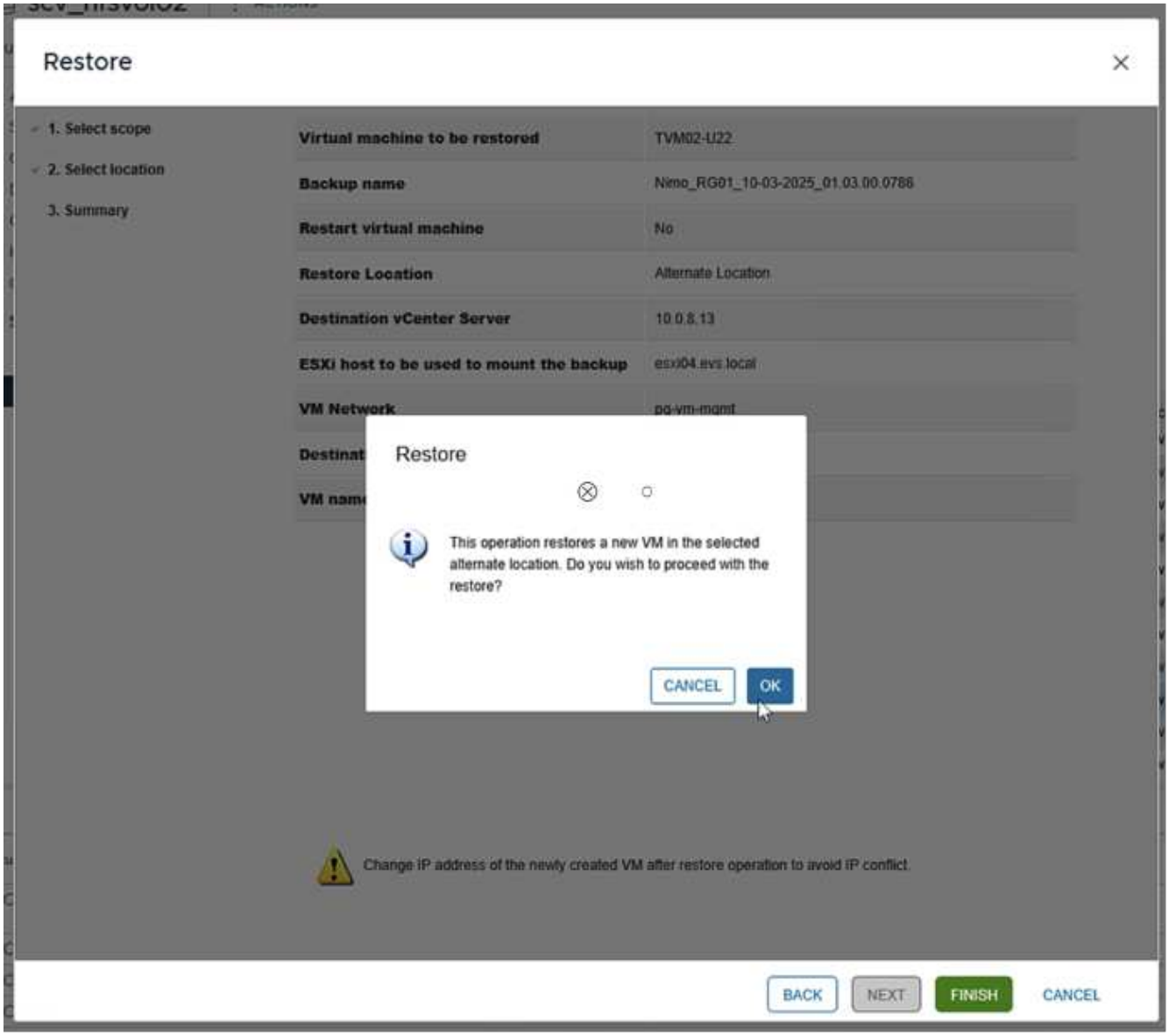


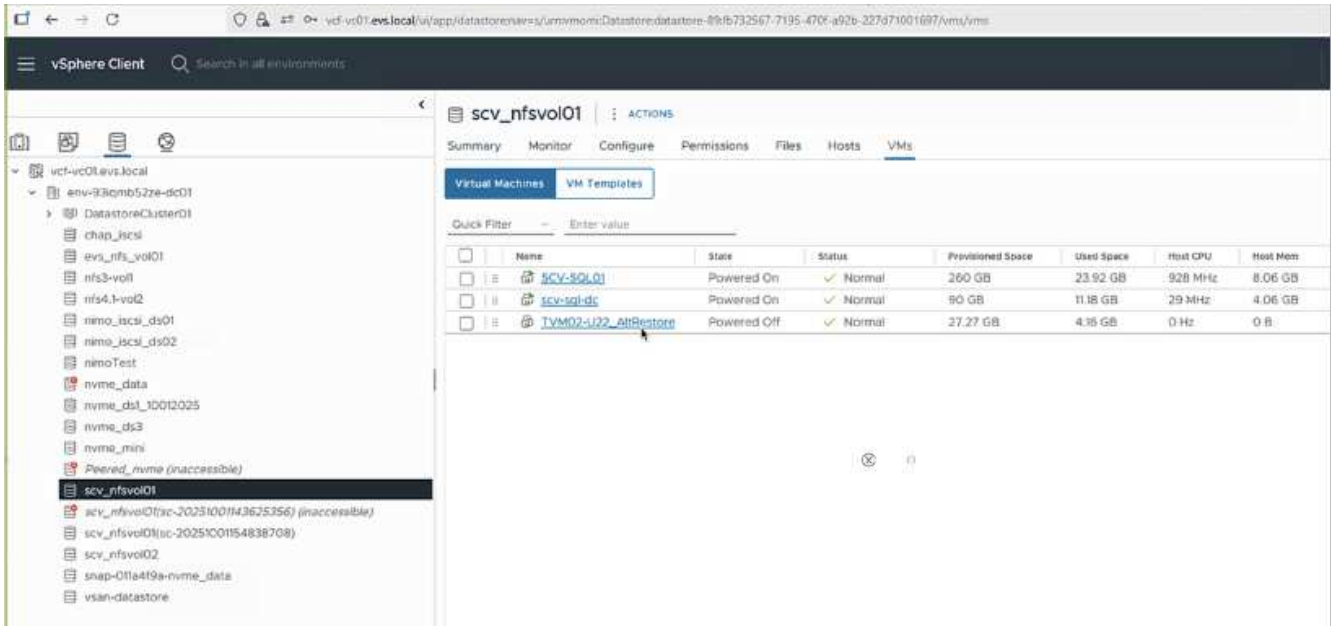
2. El flujo de capturas de pantalla que se muestra a continuación cubre la restauración de una VM en un host ESXi alternativo y en un datastore diferente.


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE




Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

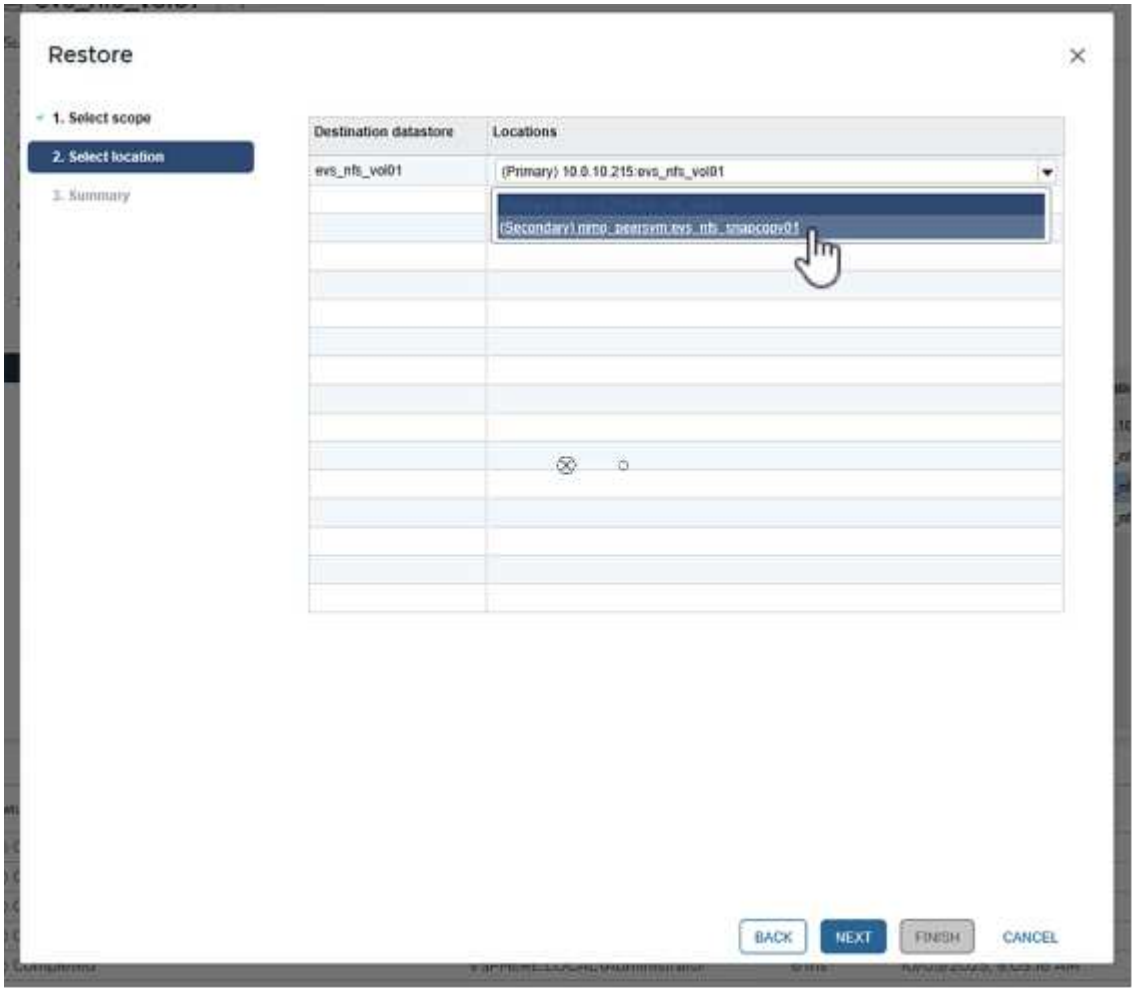

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001143625356) (inaccessible)
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

El almacén de datos de destino debe tener espacio libre suficiente y el vCenter especificado en el campo "Restaurar en ubicación alternativa" debe poder resolverse mediante DNS.

Para mejorar la eficiencia de la restauración en entornos NFS, activa la API de VMware vStorage para la integración de matrices (VAAI).

Las restauraciones también pueden realizarse desde ubicaciones secundarias, como un SnapMirror destino.



+

Procedimiento de restauración para archivos y carpetas de invitados protegidos por SnapCenter Plug-in for VMware

La siguiente sección muestra cómo restaurar archivos y carpetas de invitados desde VMDKs.

SnapCenter admite la restauración de archivos y carpetas desde VMDK solo cuando el sistema operativo invitado es Windows.

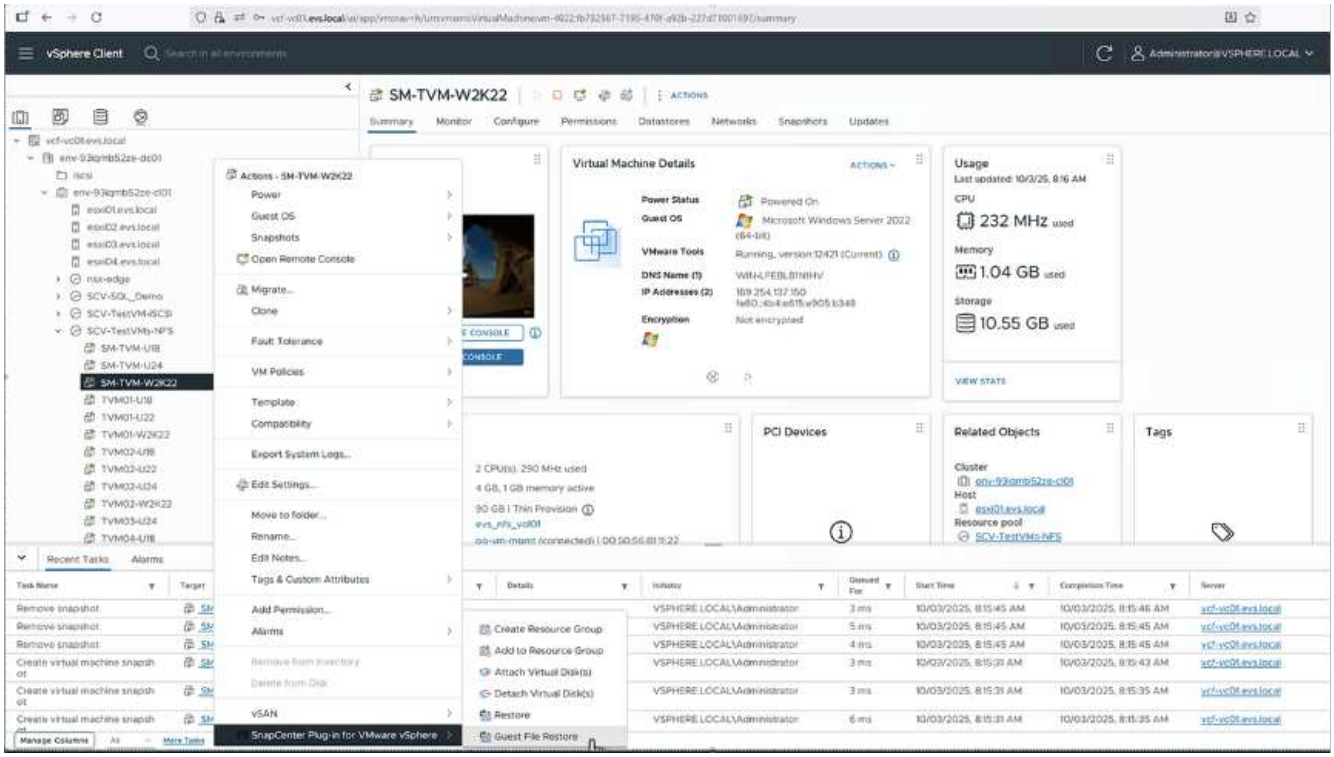
Consideraciones para la restauración de archivos y carpetas de invitados con SCV:

- VMware tools debe estar ejecutándose en la máquina virtual.

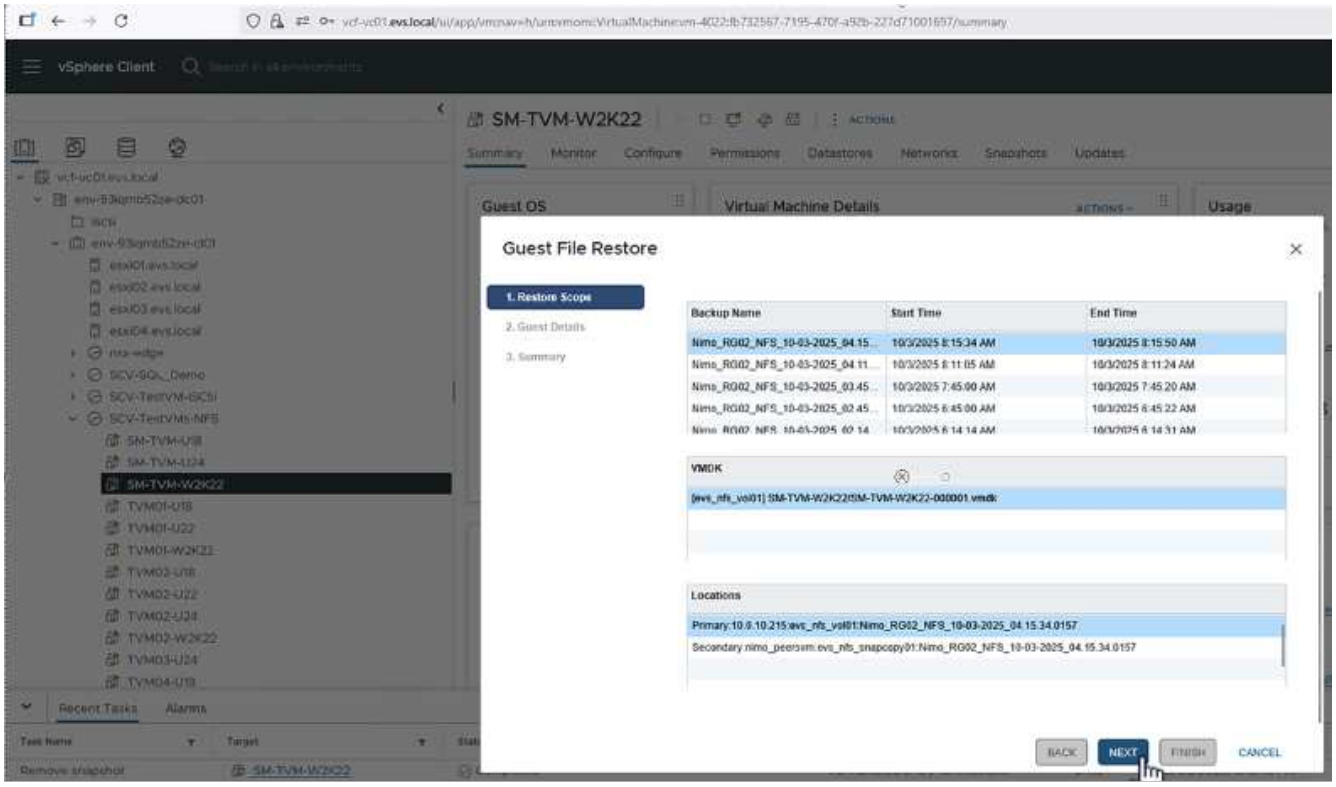
- El VMDK adjunto es accesible por 24 horas por defecto.
- Solo se puede realizar una operación de restauración o conexión en una máquina virtual a la vez.
- Los archivos de sistema, ocultos y cifrados pueden restaurarse; sin embargo, sus atributos originales no se conservarán.
- Evita restaurar archivos encriptados en carpetas encriptadas o sobrescribir archivos del sistema.

Pasos para la restauración de archivos y carpetas de invitados:

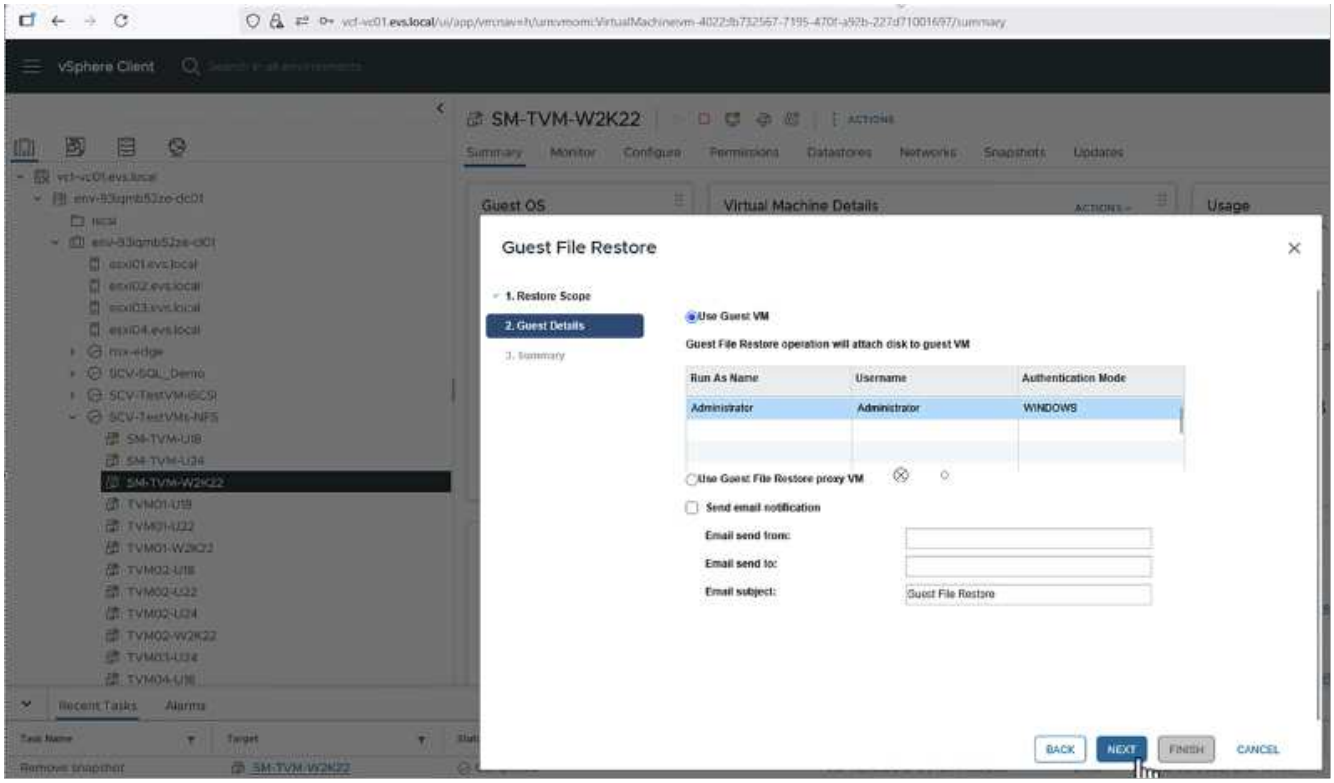
1. Haz clic derecho en la VM de destino y selecciona **NetApp SnapCenter › Guest File Restore**.



2. Elige la copia de seguridad que contiene el VMDK necesario. Especifica el VMDK y su ubicación (primaria o secundaria).



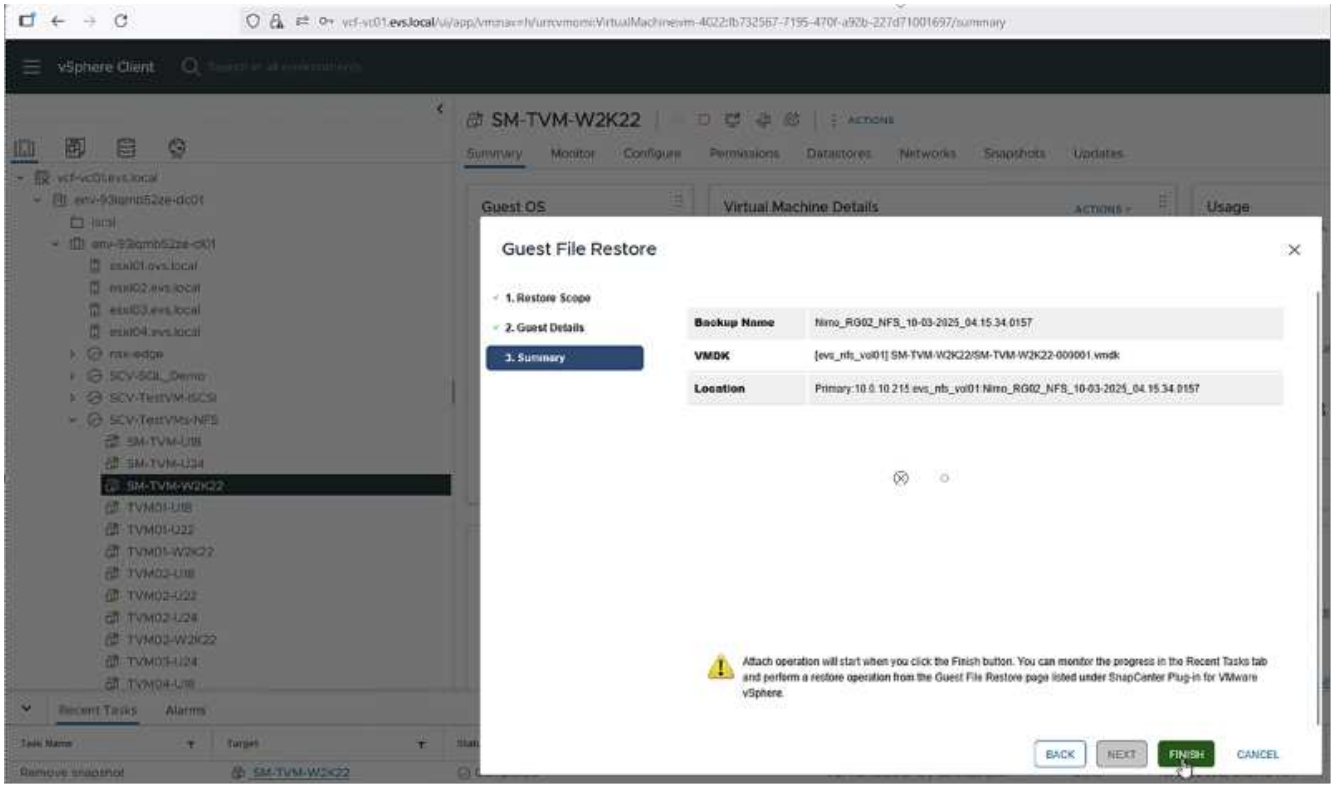
3. Elige "Disk Attachment Method".

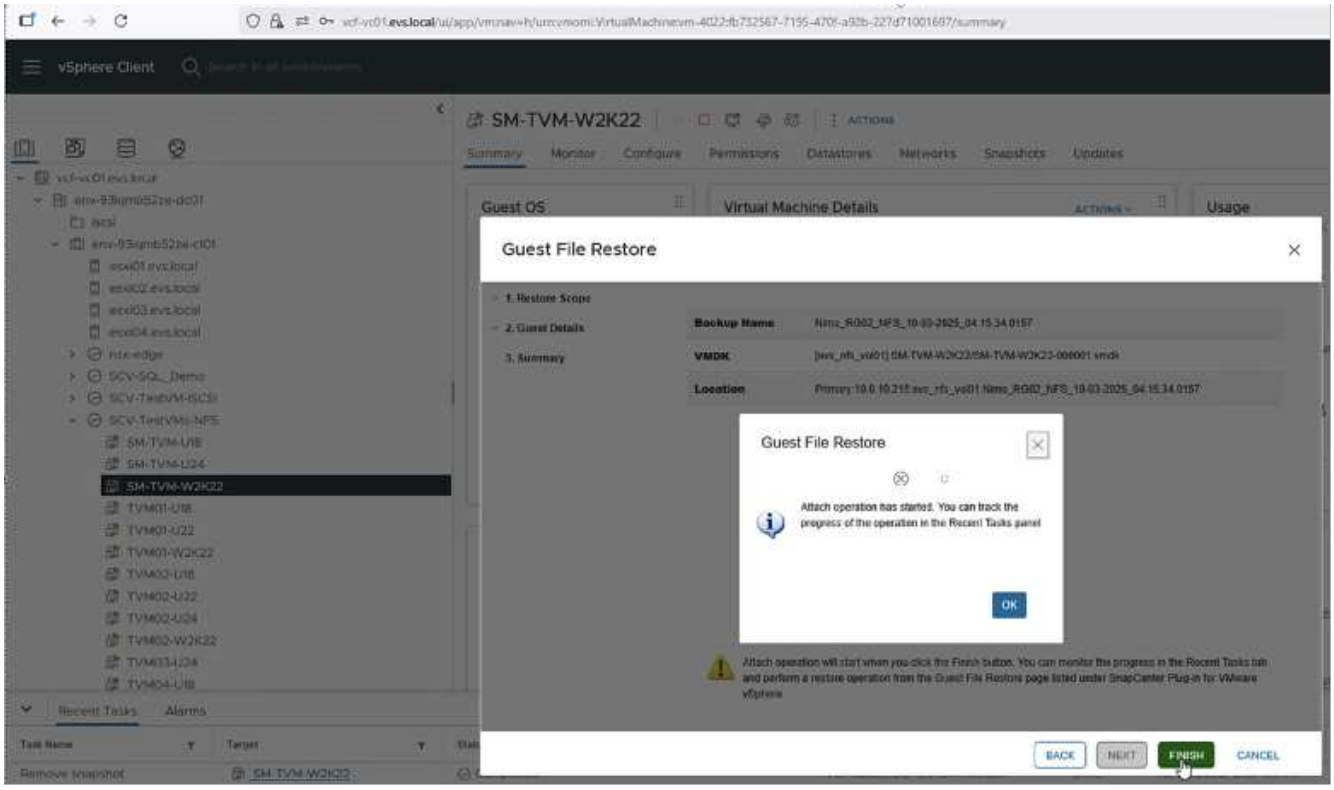


- Opción de VM huésped: adjunta el disco a la VM original (requiere credenciales preconfiguradas). Esta es la opción que se usa en esta demostración.
- Opción de VM proxy: adjunta el disco a una VM proxy designada (debe configurarse previamente).

4. Espera a que termine la operación de adjuntar antes de explorar y restaurar archivos. Una vez que la

operación se complete, SnapCenter crea automáticamente una sesión de restauración de archivos de invitado.





5. Ve al VMDK en la sesión de Guest File Restore, selecciona los archivos o carpetas que necesites y restáuralos en la ubicación especificada.

Procedimientos de protección para bases de datos que se ejecutan en VMware VMDKs con SnapCenter for SQL (SCSQL)

La siguiente sección muestra cómo proteger las bases de datos que se ejecutan en VMware VMDKs con SnapCenter for SQL (SCSQL).

Configurar SCSQL

La configuración para usar SCSQL para proteger bases de datos en VMDKs es la siguiente:

1. "Instala y configura" Servidor SnapCenter.
2. Inicia sesión en SnapCenter.
3. Configura el entorno de SnapCenter:
   - "Agregar o asignar" conexiones de sistemas de almacenamiento.
   - "Crear" credenciales.
4. Para bases de datos Microsoft SQL Server en VMware VMDKs:
   - "Implementa SCV" (ya cubierto en la sección de configuración).
   - Registra el plug-in en SnapCenter.
5. Agrega "Hosts de SQL Server e instalación de plug-ins":
   - "Configura los plug-ins SQL".
   - "Configura el plan de protección y los horarios para la base de datos y los registros".

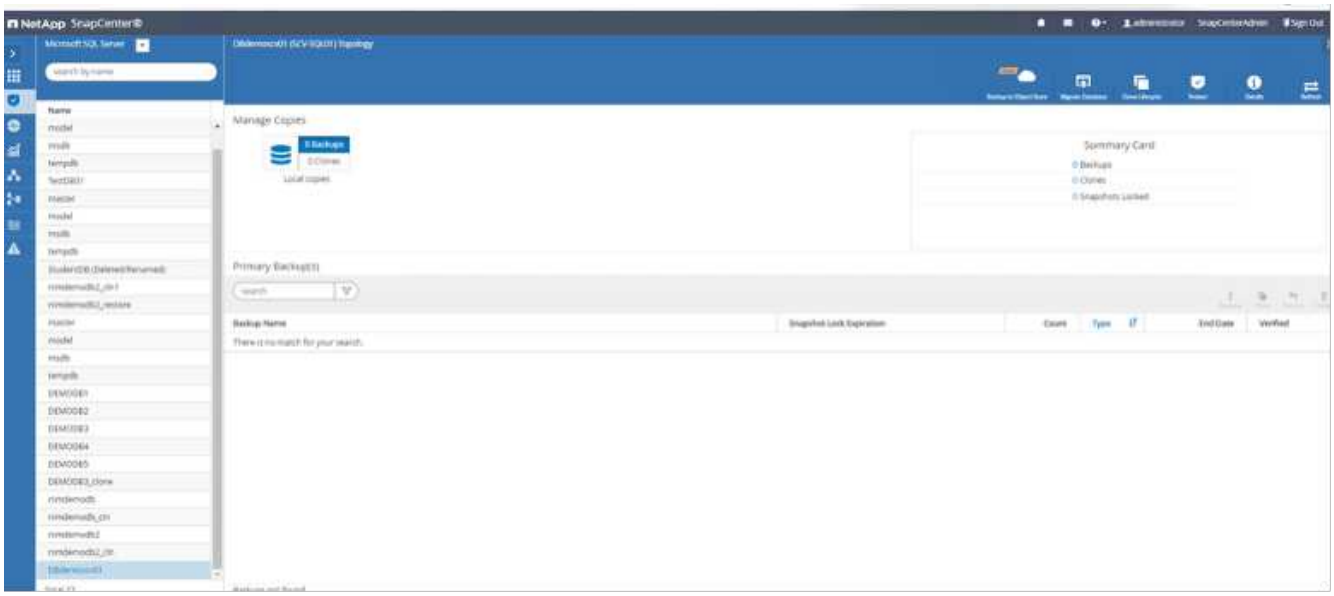


Configurar una política de backup

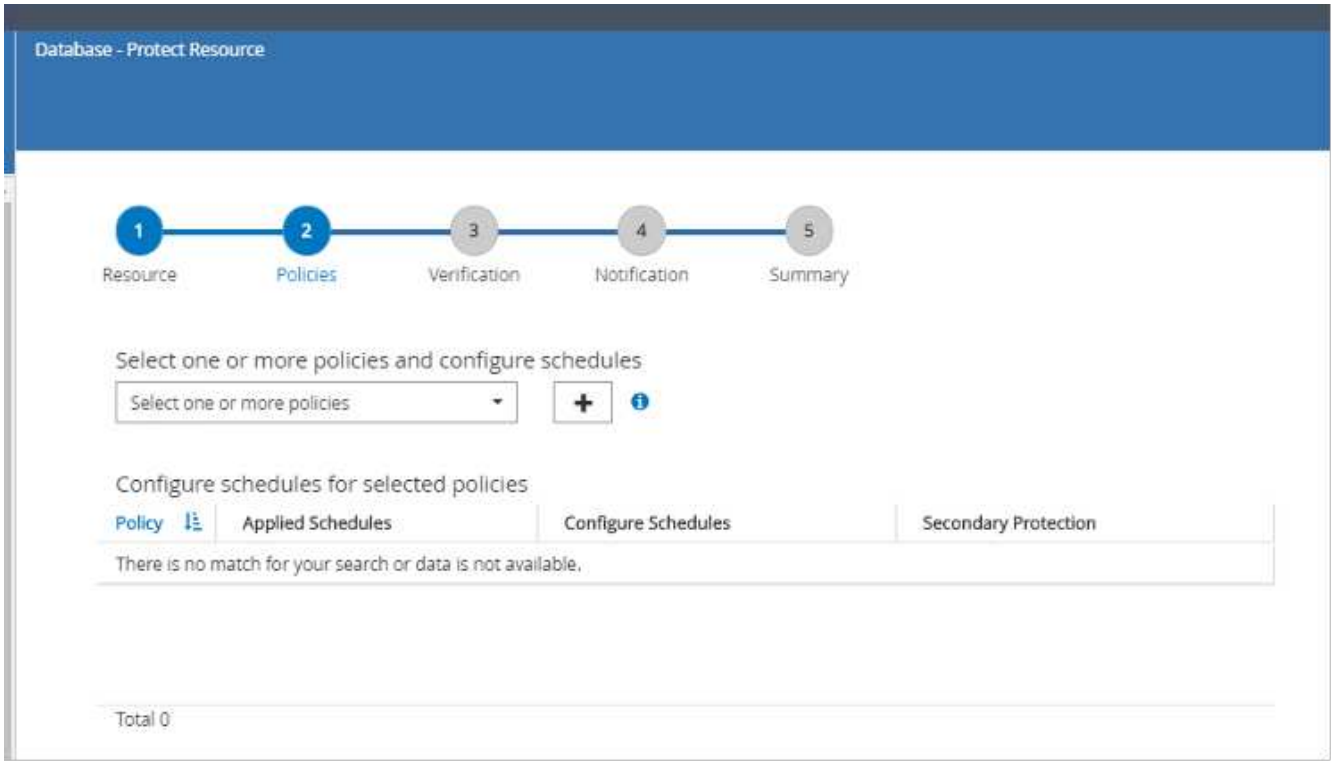
Los siguientes pasos te mostrarán cómo configurar una política de backup.

1. Selecciona la base de datos en la pestaña de recursos y elige "Proteger" en la esquina superior derecha.

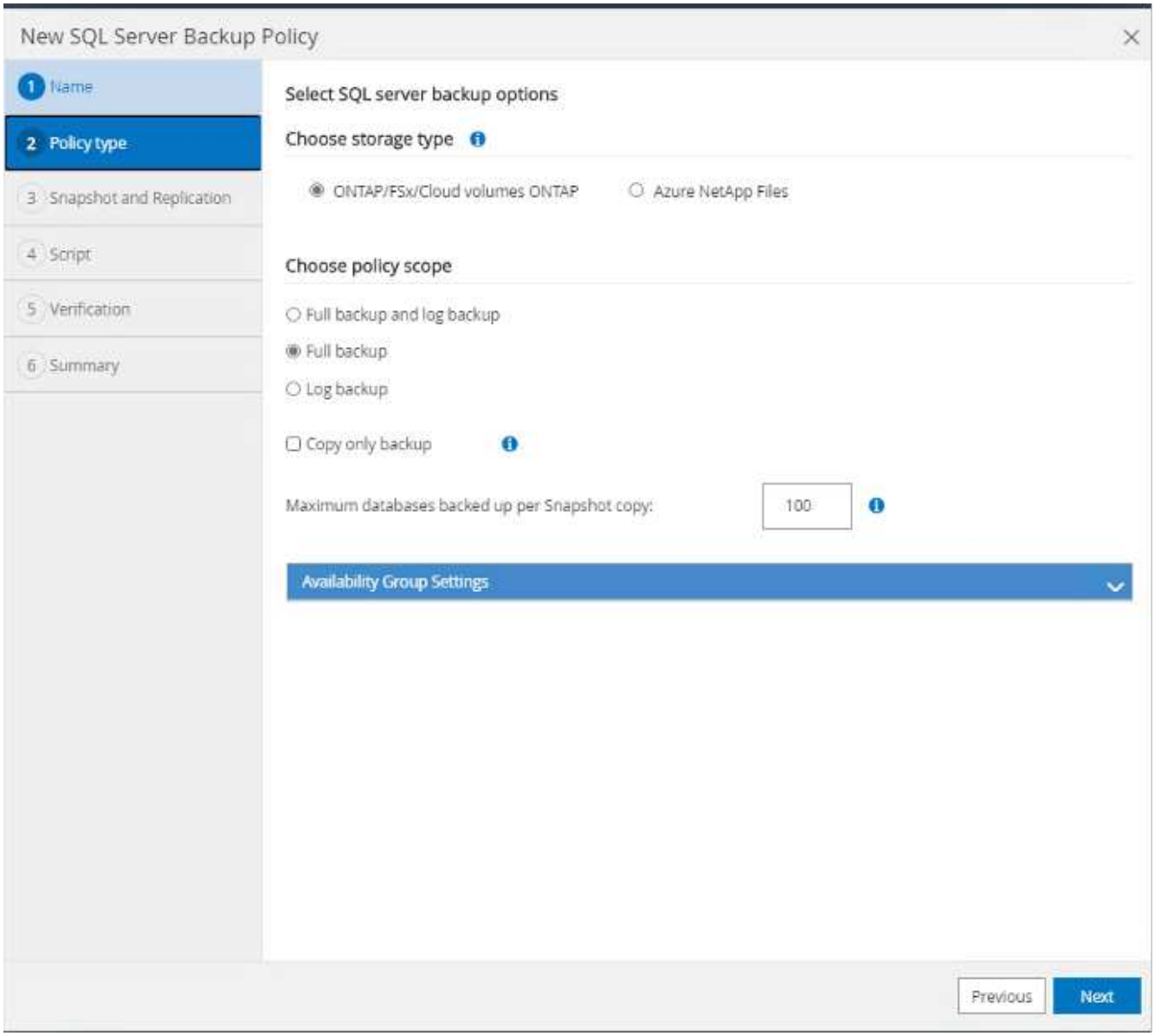
> Las validaciones se realizan contra una base de datos SQL Server que se ejecuta en la máquina virtual invitada.



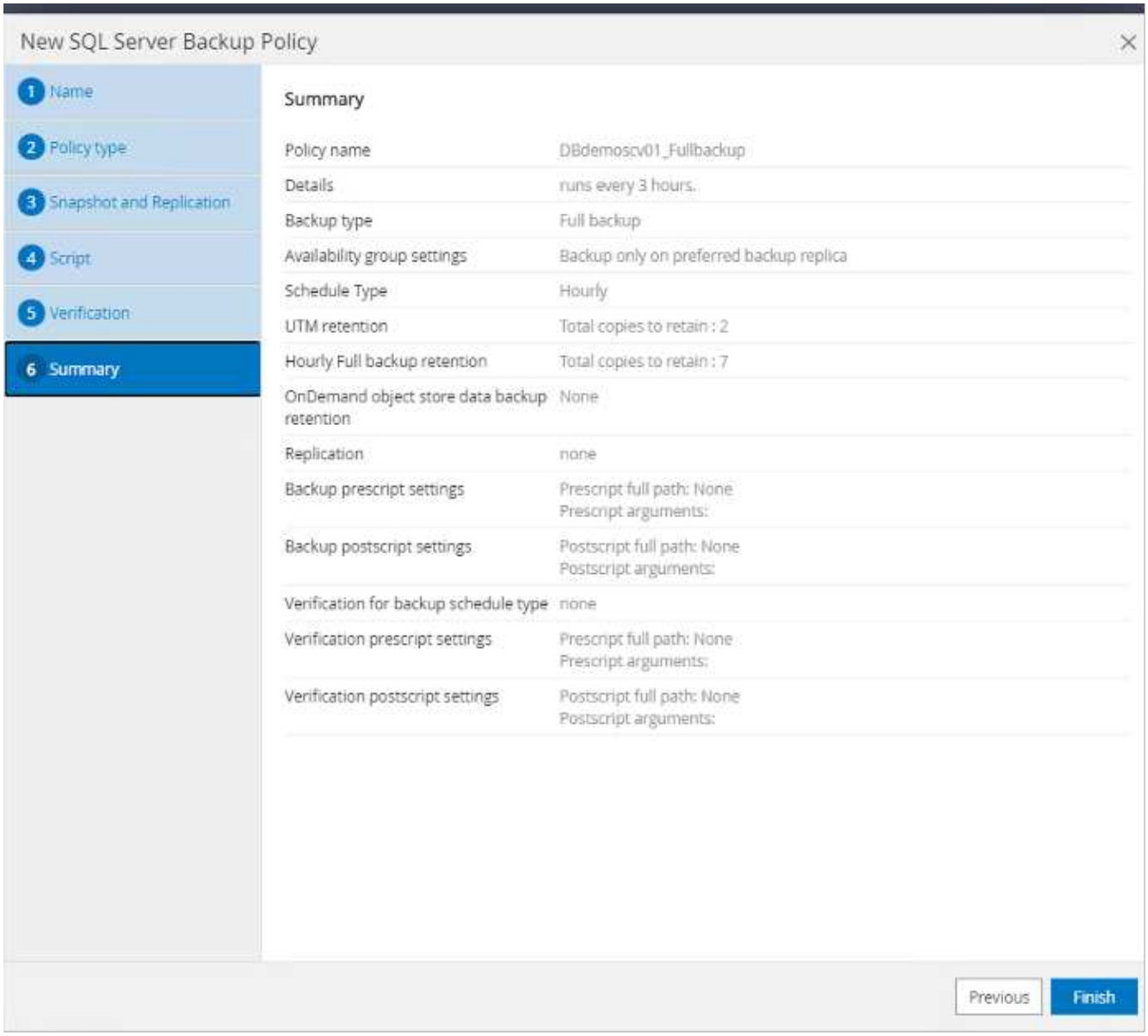
2. Haz clic en el icono del signo más para configurar una política de backup de SQL Server.



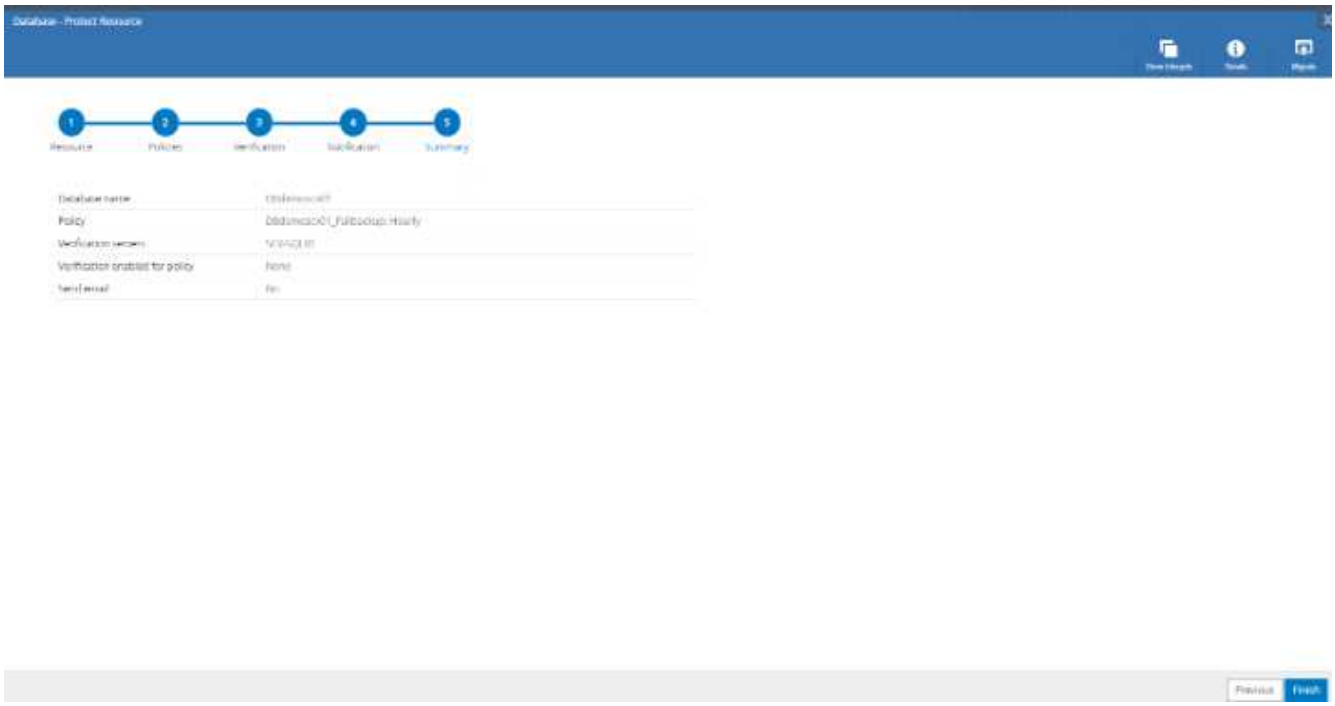
3. En esta demo, está seleccionado "backup completo". Selecciona "Siguiente" para continuar.



4. En la página de resumen, selecciona "Finalizar".



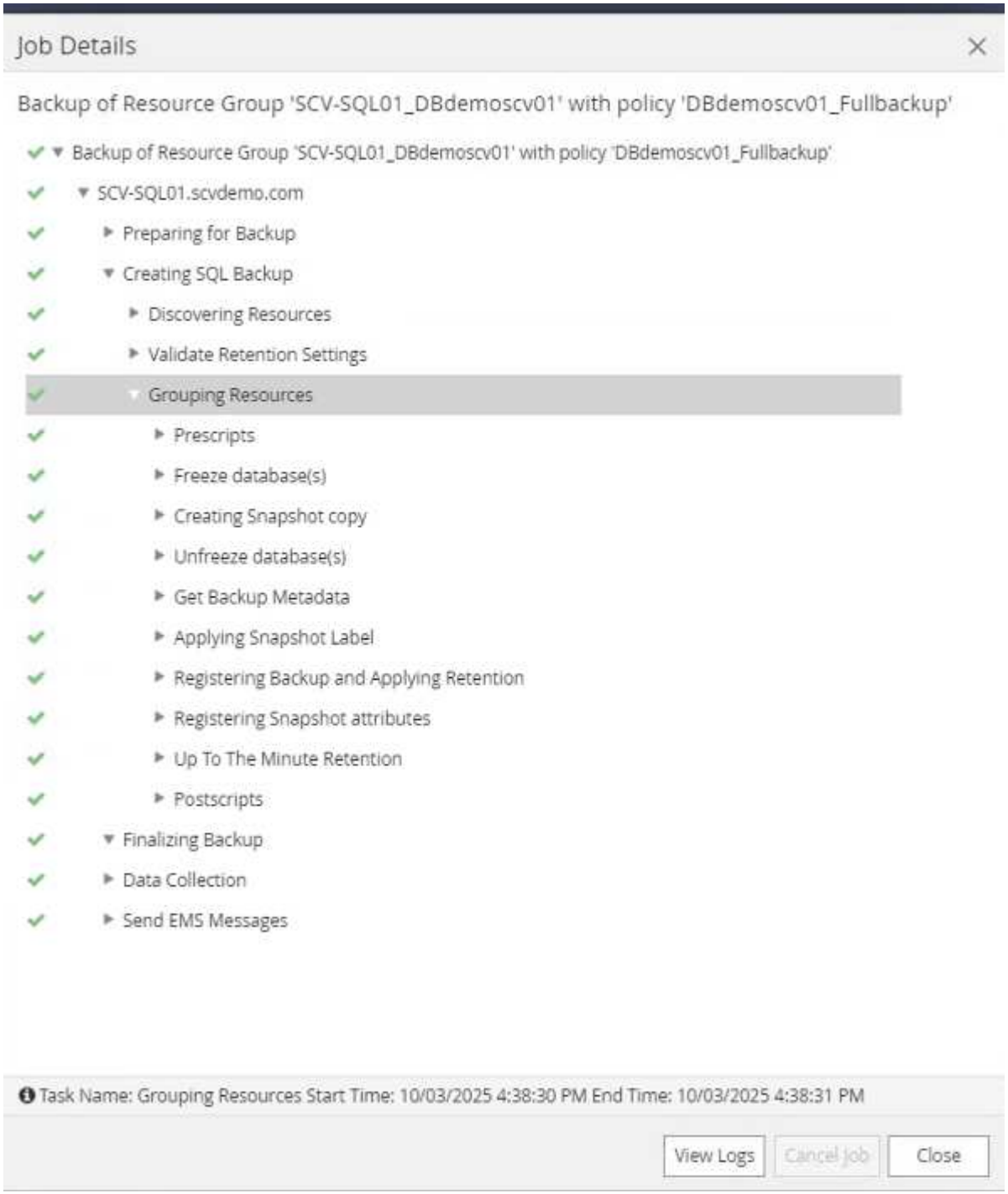
5. Continúa a "Finalizar".



Supervisar una copia de seguridad

Una vez que hayas configurado una política de backup, puedes supervisar tus operaciones de backup a medida que se realizan. Puedes hacer esto haciendo clic en Backup now para iniciar una operación de backup bajo demanda o esperando a que tu política de backup programada entre en acción.

1. Supervisa el progreso del trabajo usando **Monitor › Jobs**.
2. Selecciona el trabajo de copia de seguridad y luego haz clic en "Detalles" para ver los detalles del trabajo como se muestra abajo.

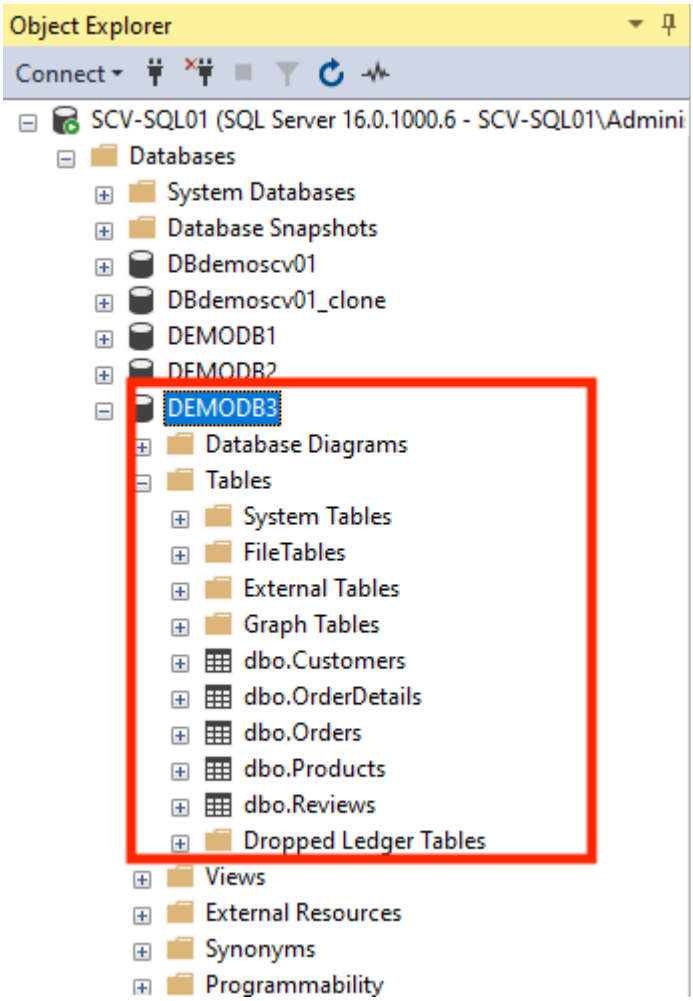


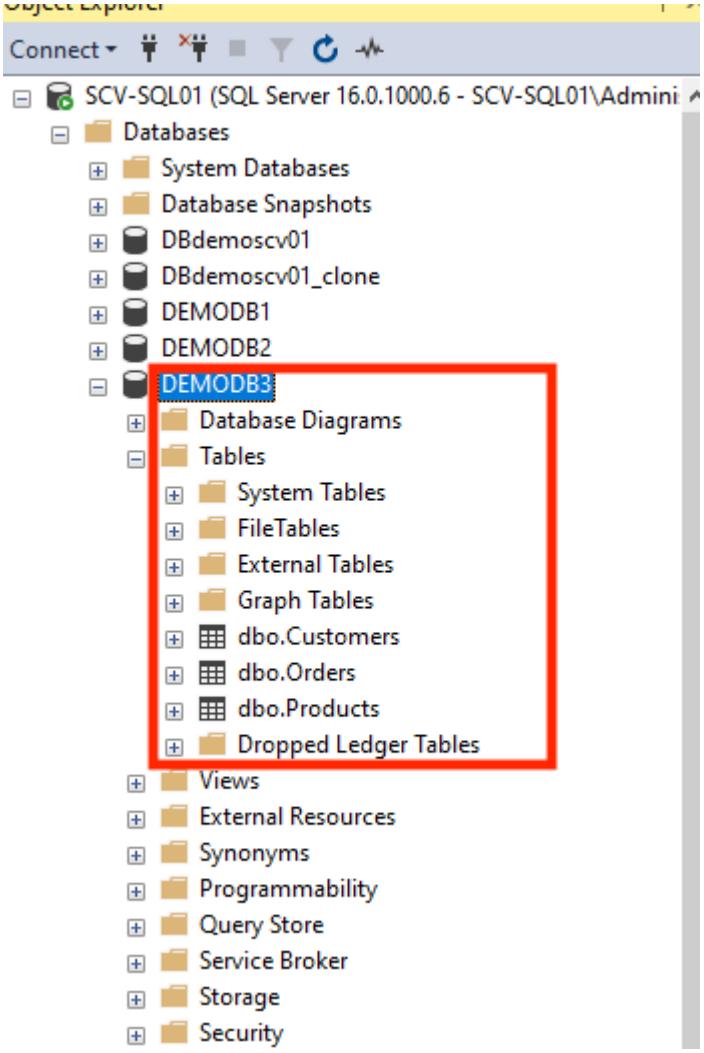
Restauración de bases de datos que residen en los VMDKs

La base de datos en el VMDK se puede restaurar a un momento específico.

Podemos simular la importancia de esto borrando algunas tablas en tu base de datos, que luego se corregirán realizando una restauración a un momento específico.

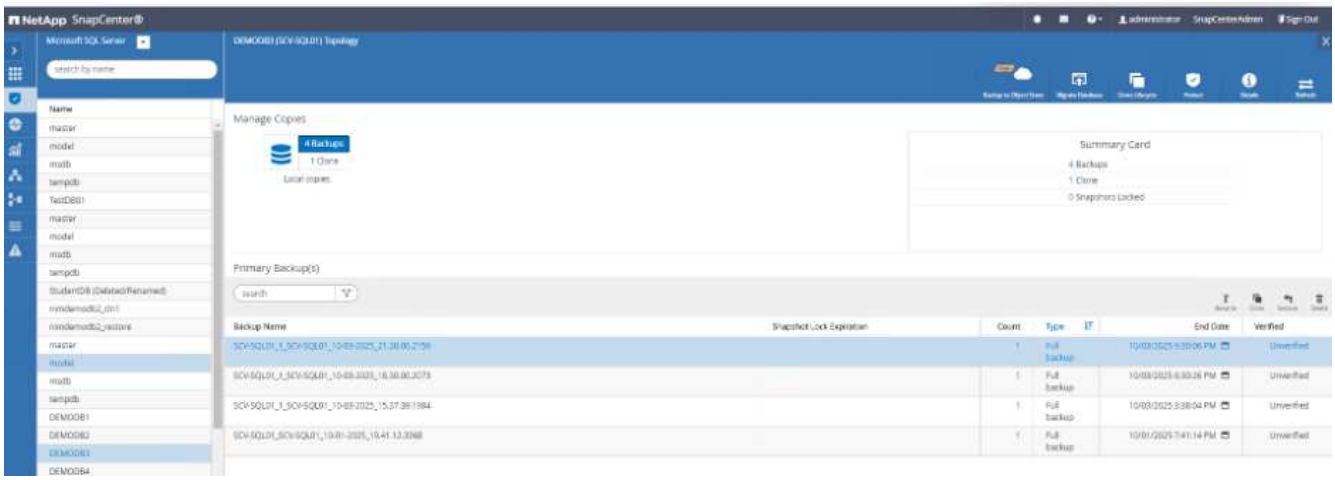
A continuación puedes ver que varias tablas de nuestra base de datos mostradas en la primera captura de pantalla han sido eliminadas en la segunda captura de pantalla:


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

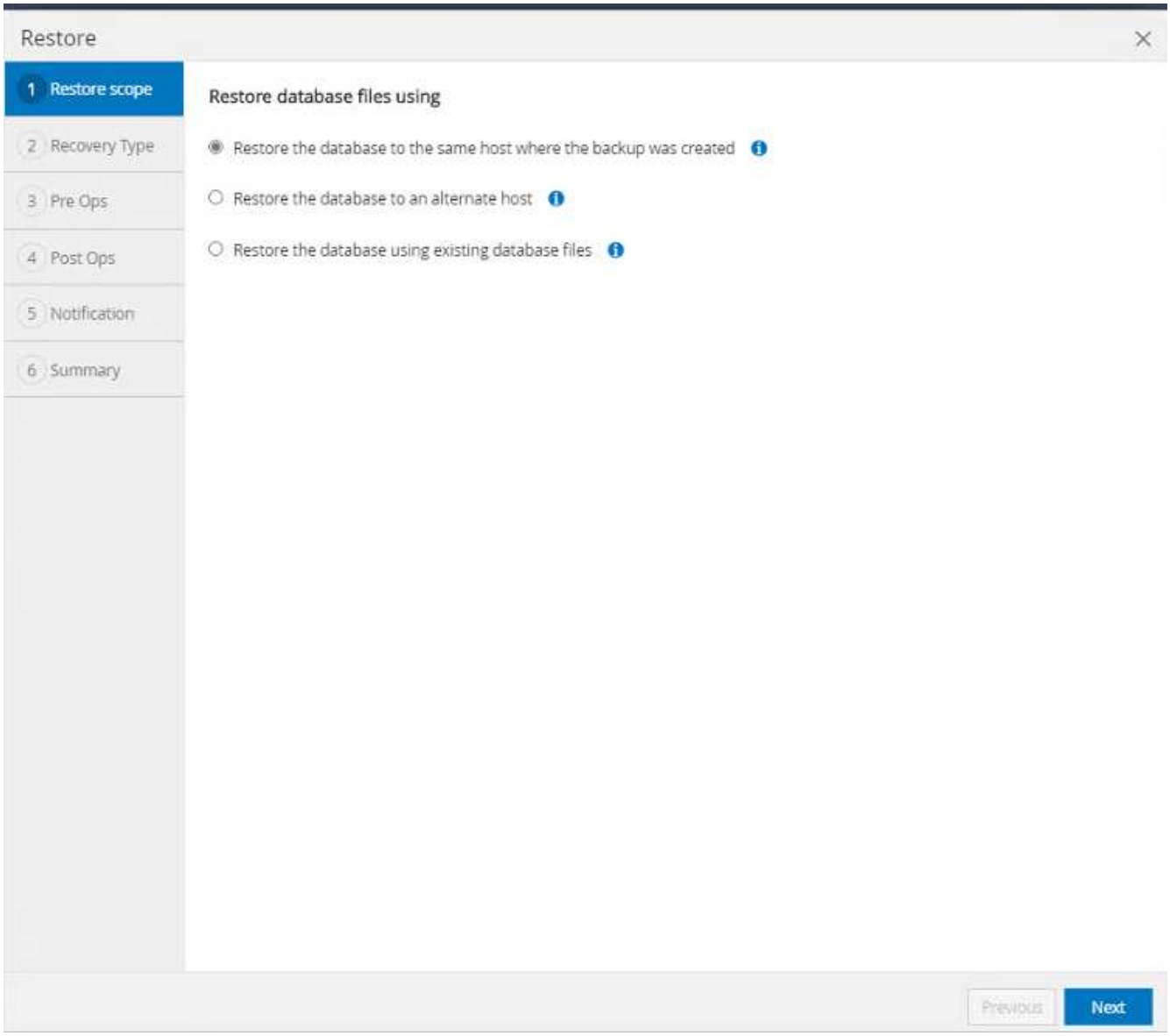


Los siguientes pasos muestran cómo llevar a cabo una restauración para recuperar esas tablas eliminadas:

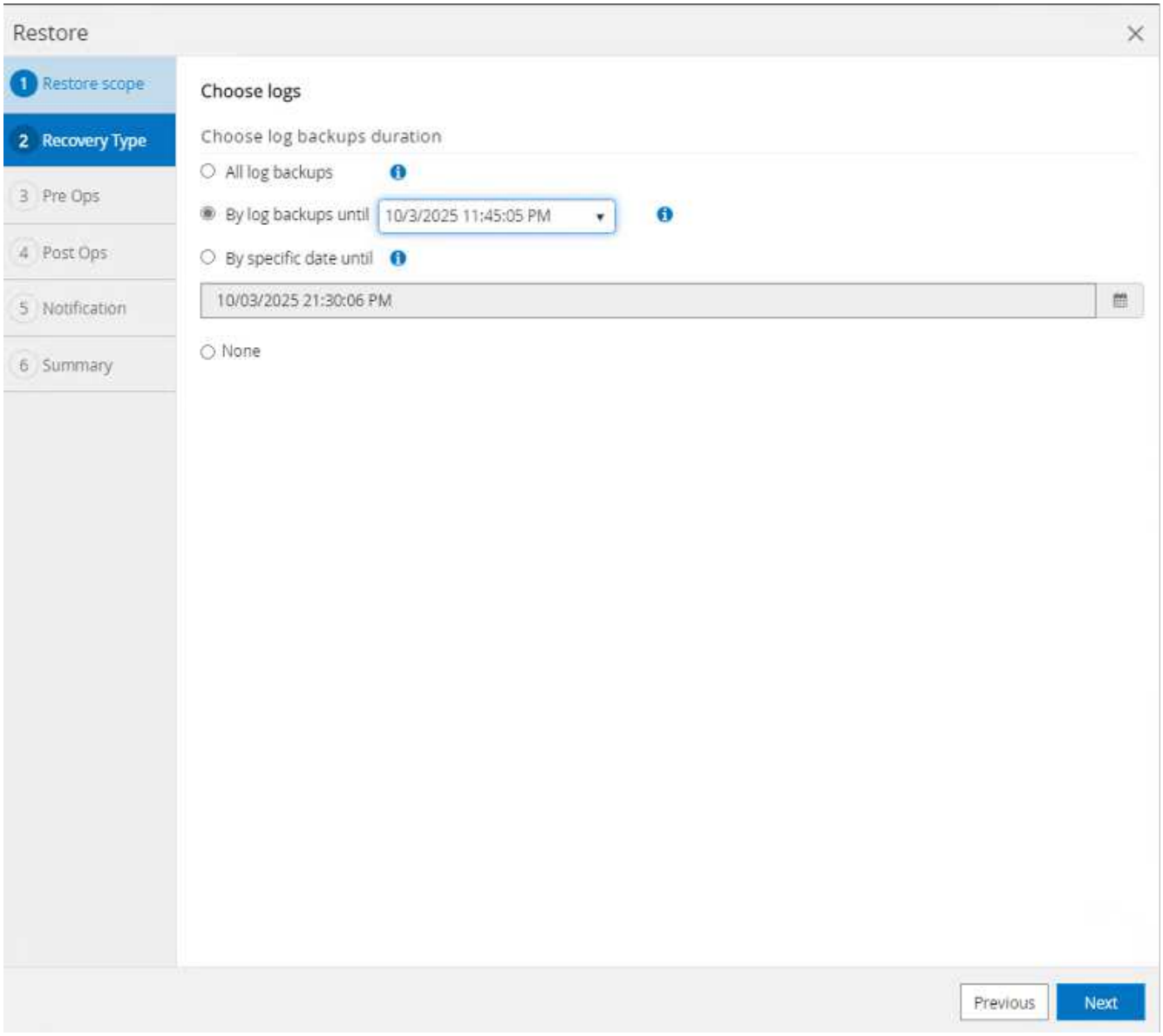
1. Selecciona la base de datos del grupo de recursos.



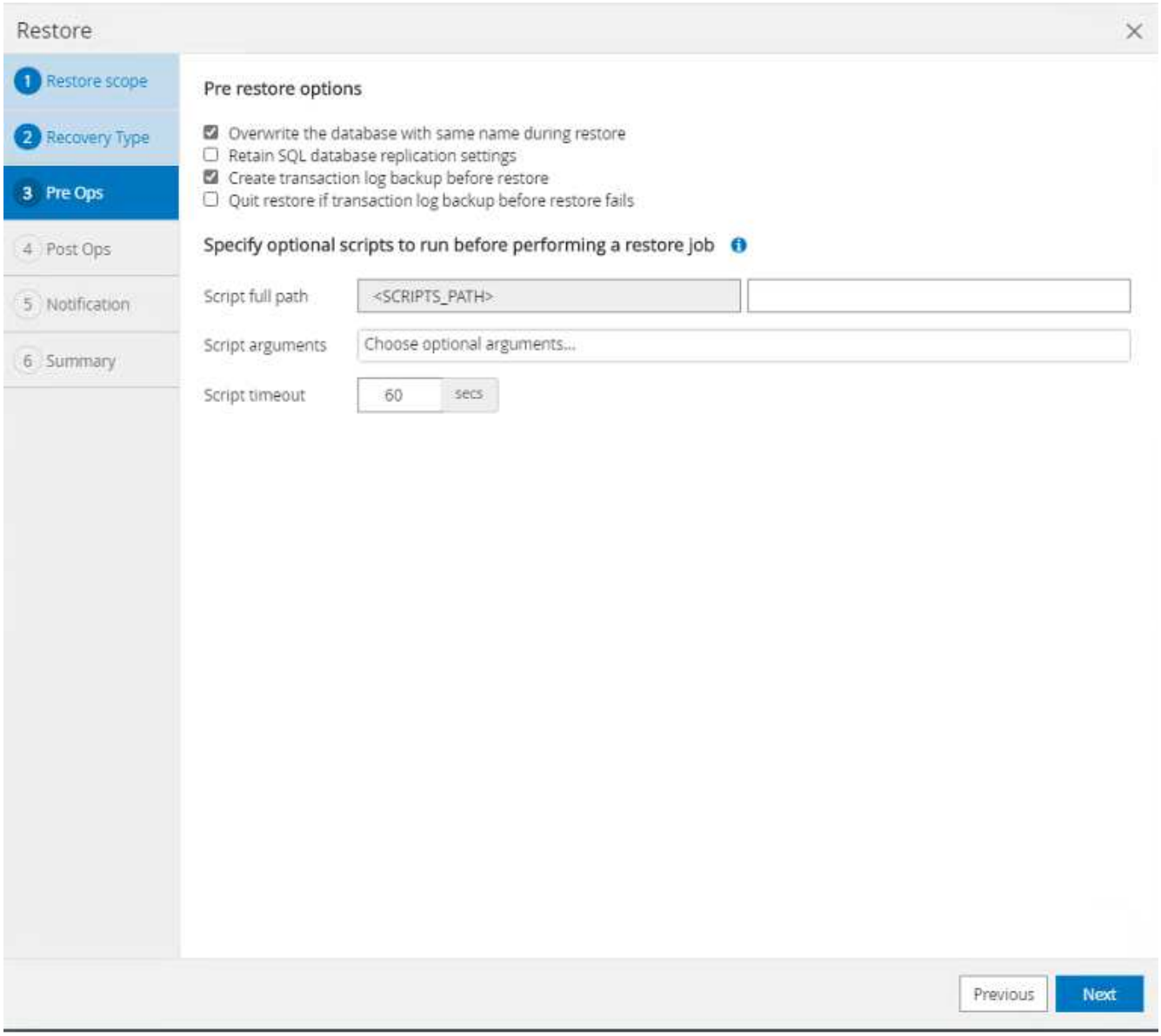
2. En la página Restaurar, selecciona la opción "Restaurar la base de datos en el mismo host donde se creó el backup".



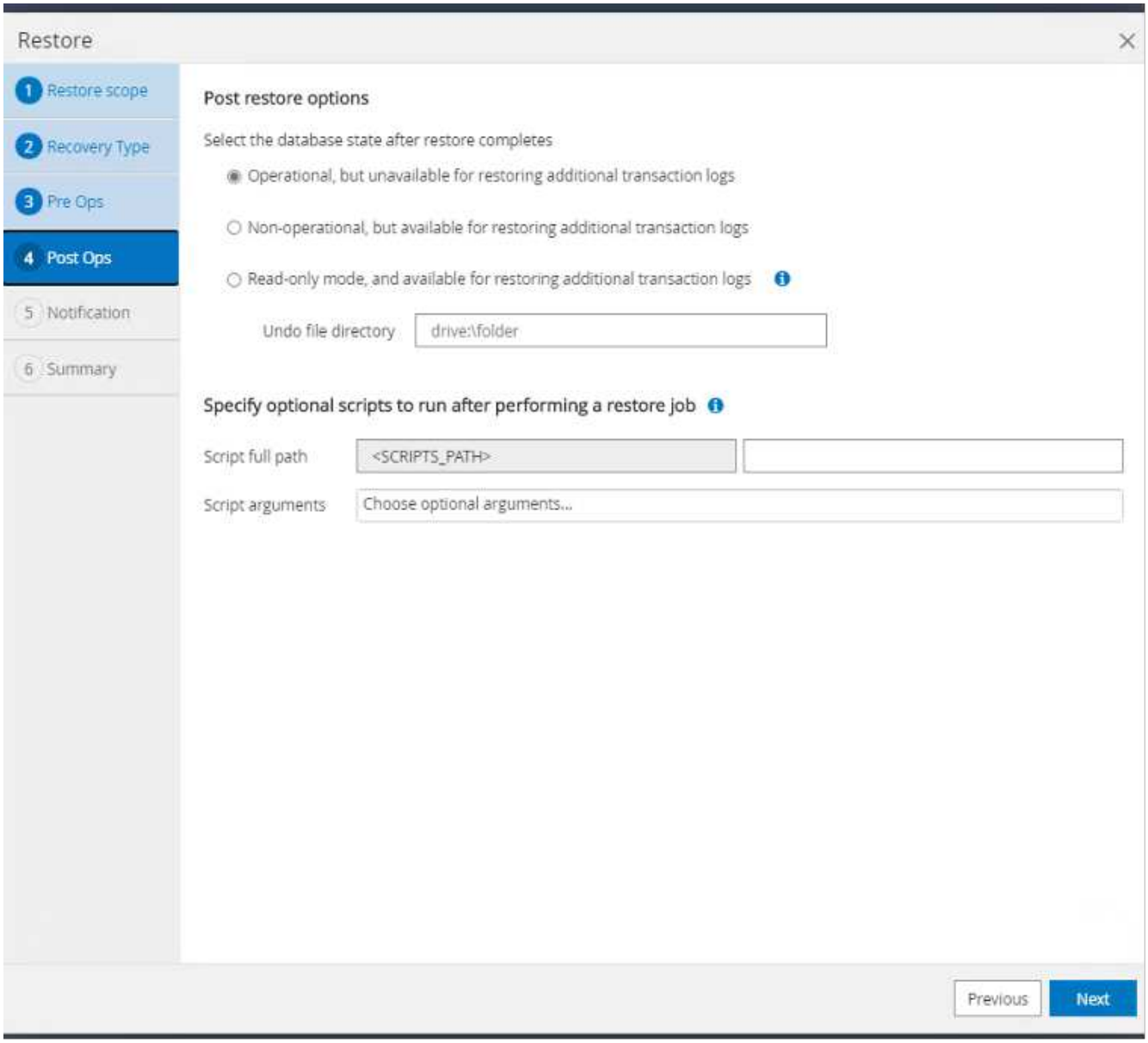
3. Selecciona la opción para usar una copia de seguridad del registro hasta un momento específico.



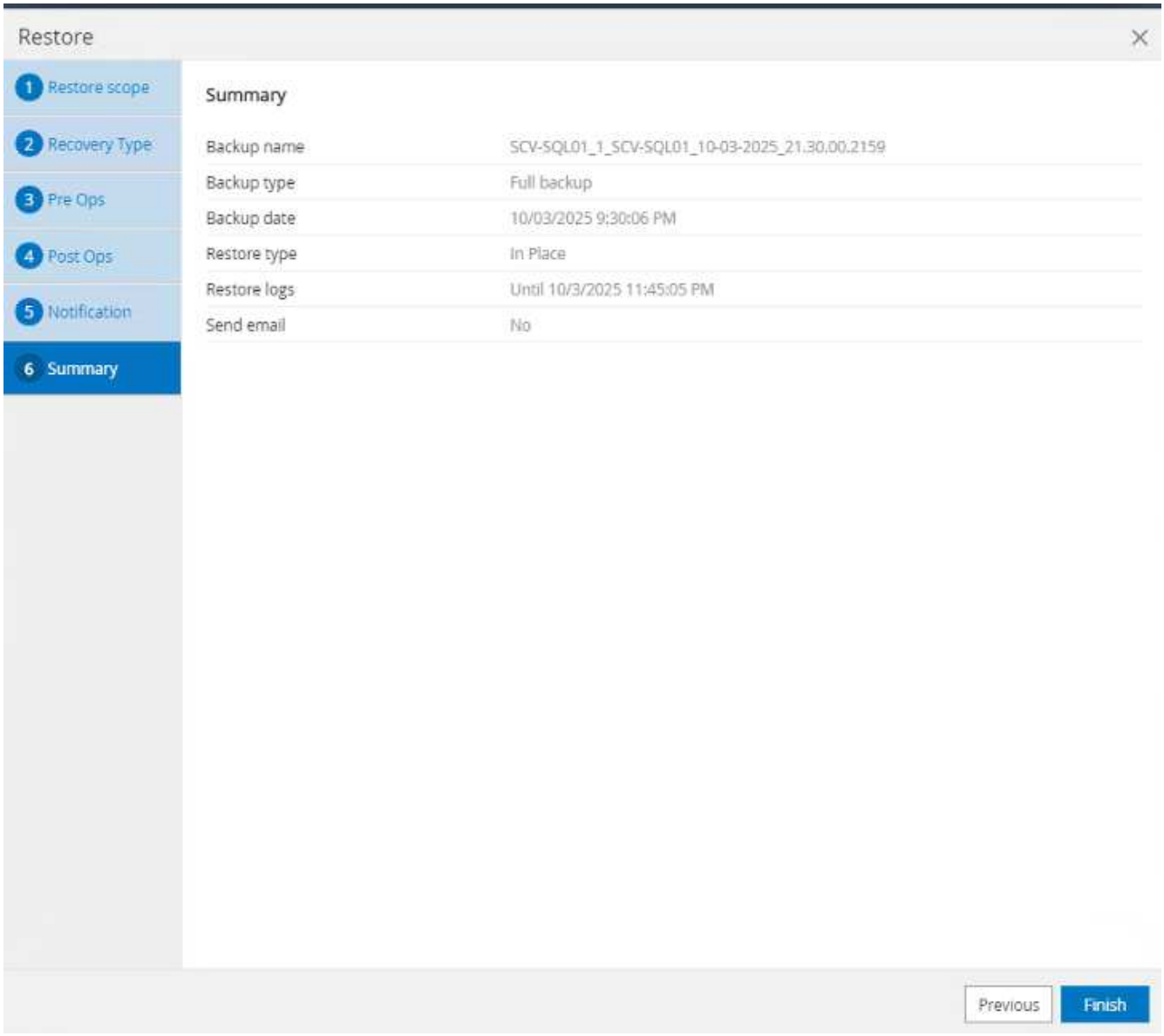
4. Selecciona "Sobrescribir base de datos con el mismo nombre durante la restauración, Crear copia de seguridad del registro de transacciones antes de la restauración" y selecciona "Siguiente".



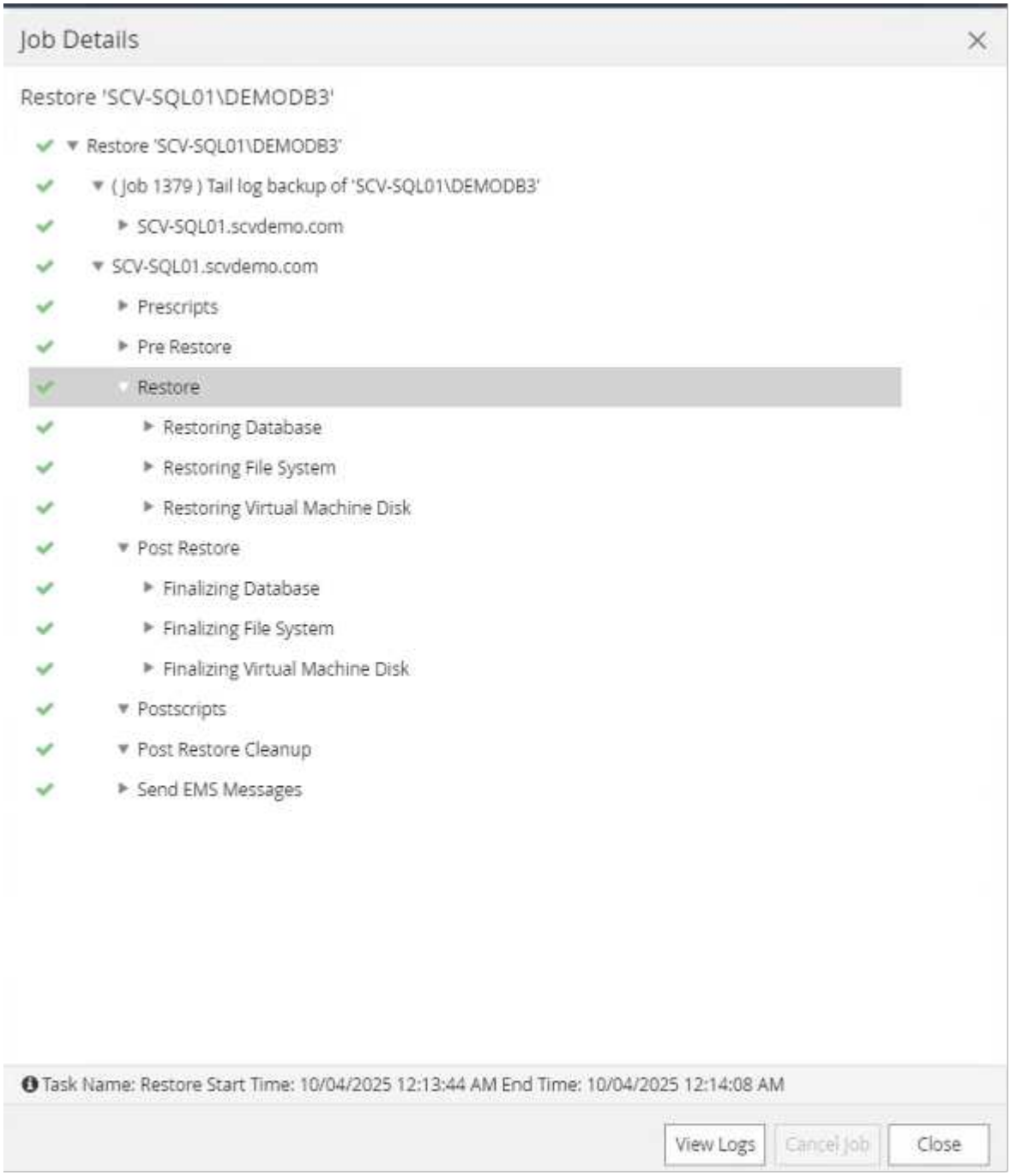
5. Selecciona el estado posterior a la restauración que quieres que adopte la base de datos de la lista de opciones y selecciona "Siguiente".



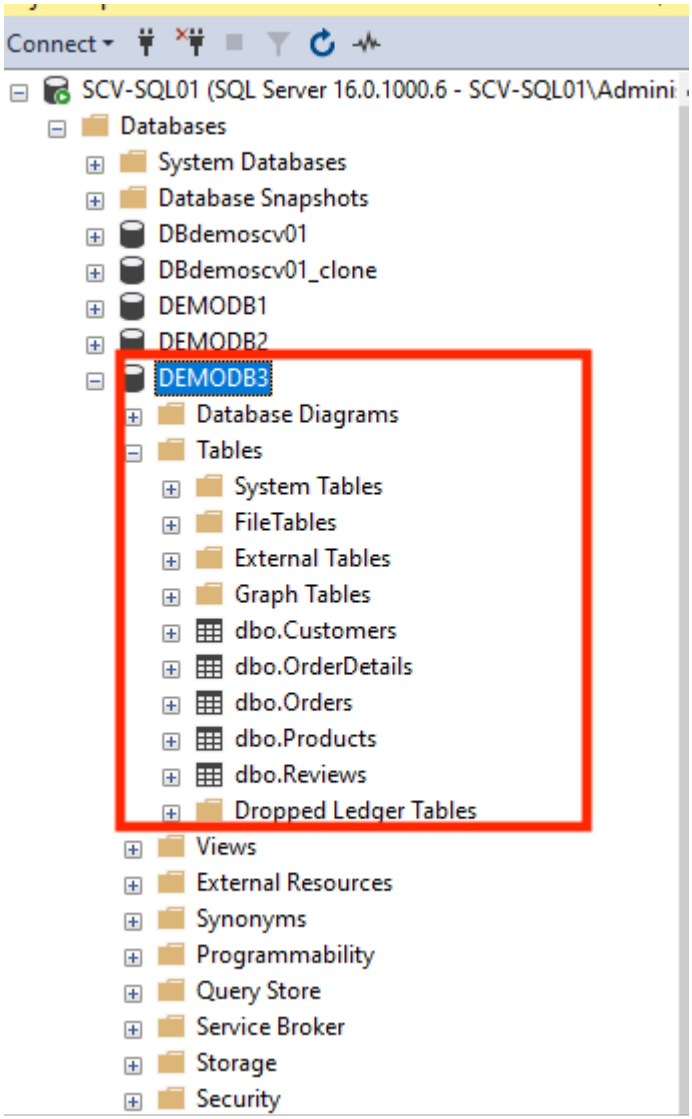
6. En la página de resumen, selecciona "Finalizar".



7. Supervisa el trabajo hasta que termine.



8. Verifica que las tablas eliminadas se hayan restaurado correctamente.



Conclusión

En este documento, te damos una guía detallada paso a paso para desplegar, configurar y usar SCV y "SnapCenter Plug-in for SQL Server (SCSQL)" mientras usas FSx para ONTAP como datastore complementario con clústeres de Amazon EVS.

Conclusión

En resumen, cuando usas FSx para ONTAP para optimizar el TCO de un despliegue de Amazon EVS, SCV ofrece un método sencillo y eficiente para hacer backup de VMs. Puede hacer backup y restaurar VMs de manera rápida y sin complicaciones, ya que se basa en copias Snapshot, que tardan literalmente segundos en completarse.

"Prueba gratis el plug-in SnapCenter para VMware ahora".

NetApp para Azure/AVS

Capacidades de NetApp para Azure AVS

Obtenga más información sobre las capacidades que NetApp aporta a Azure VMware Solution (AVS), desde NetApp como un dispositivo de almacenamiento conectado invitado o un almacén de datos NFS complementario hasta la migración de flujos de trabajo, la extensión/ampliación a la nube, la copia de seguridad/restauración y la recuperación ante desastres.

Salte a la sección del contenido deseado seleccionando entre las siguientes opciones:

- "Configuración de AVS en Azure"
- "Opciones de almacenamiento de NetApp para AVS"
- "Soluciones en la nube NetApp /VMware"

Configuración de AVS en Azure

Al igual que en las instalaciones locales, la planificación de un entorno de virtualización basado en la nube es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

En esta sección se describe cómo configurar y administrar Azure VMware Solution y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

> El almacenamiento en el invitado es el único método compatible para conectar Cloud Volumes ONTAP a Azure VMware Solution.

El proceso de configuración se puede dividir en los siguientes pasos:

- Registrar el proveedor de recursos y crear una nube privada
- Conectarse a una puerta de enlace de red virtual ExpressRoute nueva o existente
- Validar la conectividad de la red y acceder a la nube privada

Ver el detalle"Pasos de configuración para AVS" .

Opciones de almacenamiento de NetApp para AVS

El almacenamiento de NetApp se puede utilizar de varias maneras, ya sea como almacenamiento conectado por instancia o como un almacén de datos NFS complementario, dentro de Azure AVS.

Por favor visite"Opciones de almacenamiento de NetApp compatibles" Para más información.

Azure admite el almacenamiento de NetApp en las siguientes configuraciones:

- Azure NetApp Files (ANF) como almacenamiento conectado invitado
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- Azure NetApp Files (ANF) como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para AVS" . Ver el detalle"Opciones de almacén de datos NFS complementarias para AVS" .

Casos de uso de soluciones

Con las soluciones de nube de NetApp y VMware, muchos casos de uso son fáciles de implementar en Azure AVS. Estos casos se definen para cada una de las áreas de nube definidas por VMware:

- Proteger (incluye recuperación ante desastres y copia de seguridad/restauración)
- Extender
- Emigrar

"Explorar las soluciones de NetApp para Azure AVS"

Proteger las cargas de trabajo en Azure/AVS

Recuperación ante desastres con ANF y JetStream

La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos (por ejemplo, ransomware). Con el marco VMware VAIO, las cargas de trabajo locales de VMware se pueden replicar en el almacenamiento de Azure Blob y recuperar, lo que permite una pérdida de datos mínima o casi nula y un RTO cercano a cero.

JetStream DR se puede utilizar para recuperar sin problemas las cargas de trabajo replicadas desde las instalaciones locales a AVS y, específicamente, a Azure NetApp Files. Permite una recuperación ante desastres rentable mediante el uso de recursos mínimos en el sitio de recuperación ante desastres y un almacenamiento en la nube rentable. JetStream DR automatiza la recuperación a almacenes de datos ANF a través de Azure Blob Storage. JetStream DR recupera máquinas virtuales independientes o grupos de máquinas virtuales relacionadas en la infraestructura del sitio de recuperación de acuerdo con el mapeo de la red y proporciona recuperación en un punto en el tiempo para la protección contra ransomware.

Este documento proporciona una comprensión de los principios de operaciones de JetStream DR y sus componentes principales.

▼ Descripción general de la implementación de la solución

1. Instale el software JetStream DR en el centro de datos local.
    a. Descargue el paquete de software JetStream DR de Azure Marketplace (ZIP) e implemente JetStream DR MSA (OVA) en el clúster designado.
    b. Configure el clúster con el paquete de filtro de E/S (instale JetStream VIB).
    c. Aprovisione Azure Blob (cuenta de almacenamiento de Azure) en la misma región que el clúster DR AVS.
    d. Implemente dispositivos DRVA y asigne volúmenes de registro de replicación (VMDK desde un almacén de datos existente o almacenamiento iSCSI compartido).
    e. Cree dominios protegidos (grupos de máquinas virtuales relacionadas) y asigne DRVA y Azure Blob Storage/ANF.
    f. Protección de inicio.
2. Instale el software JetStream DR en la nube privada de Azure VMware Solution.
    a. Utilice el comando Ejecutar para instalar y configurar JetStream DR.
    b. Agregue el mismo contenedor de blobs de Azure y descubra dominios mediante la opción Escanear dominios.

c. Implementar los dispositivos DRVA necesarios.

d. Cree volúmenes de registro de replicación utilizando almacenes de datos vSAN o ANF disponibles.

e. Importe dominios protegidos y configure RocVA (VA de recuperación) para usar el almacén de datos ANF para las ubicaciones de máquinas virtuales.

f. Seleccione la opción de conmutación por error adecuada e inicie la rehidratación continua para dominios o máquinas virtuales con RTO cercano a cero.

3. Durante un evento de desastre, active la conmutación por error a los almacenes de datos de Azure NetApp Files en el sitio de AVS DR designado.
4. Invocar la conmutación por error al sitio protegido después de que este se haya recuperado. Antes de comenzar, asegúrese de que se cumplan los requisitos previos como se indica en este "enlace" y también ejecutar la herramienta de prueba de ancho de banda (BWT) proporcionada por JetStream Software para evaluar el rendimiento potencial del almacenamiento de blobs de Azure y su ancho de banda de replicación cuando se usa con el software JetStream DR. Una vez que se cumplan los requisitos previos, incluida la conectividad, configure y suscríbase a JetStream DR para AVS desde "Azure Marketplace" . Después de descargar el paquete de software, continúe con el proceso de instalación descrito anteriormente.

Al planificar e iniciar la protección para una gran cantidad de máquinas virtuales (por ejemplo, más de 100), utilice la herramienta de planificación de capacidad (CPT) del kit de herramientas de automatización de DR de JetStream. Proporcione una lista de máquinas virtuales que se protegerán junto con sus preferencias de RTO y grupo de recuperación y luego ejecute CPT.

El CPT realiza las siguientes funciones:

- Combinar máquinas virtuales en dominios de protección según su RTO.
- Definir el número óptimo de DRVAs y sus recursos.
- Estimación del ancho de banda de replicación requerido.
- Identificar las características del volumen del registro de replicación (capacidad, ancho de banda, etc.).
- Estimación de la capacidad de almacenamiento de objetos requerida y más.

> La cantidad y el contenido de los dominios prescritos dependen de varias características de la máquina virtual, como el IOPS promedio, la capacidad total, la prioridad (que define el orden de conmutación por error), el RTO y otros.

Instalar JetStream DR en el centro de datos local

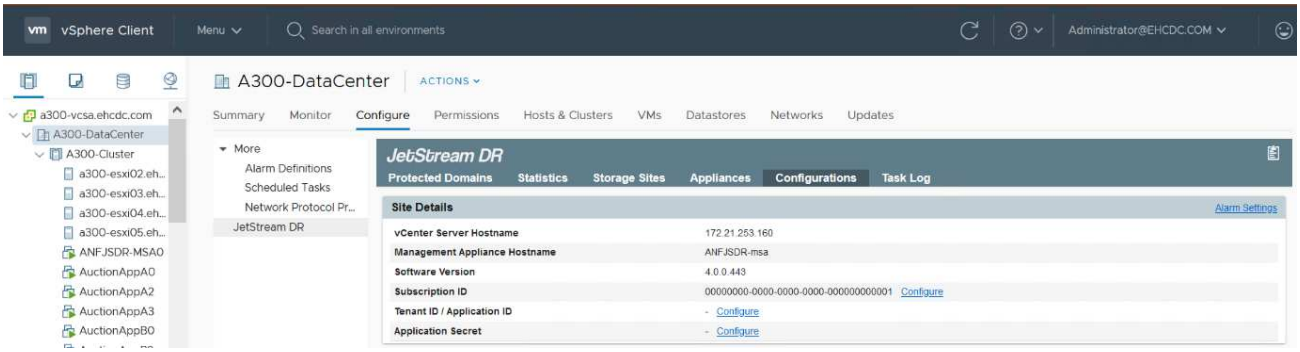
El software JetStream DR consta de tres componentes principales: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) y componentes de host (paquetes de filtros de E/S). MSA se utiliza para instalar y configurar componentes del host en el clúster de cómputo y luego para administrar el software JetStream DR. La siguiente lista proporciona una descripción de alto nivel del proceso de instalación:

▼ Cómo instalar JetStream DR en instalaciones locales

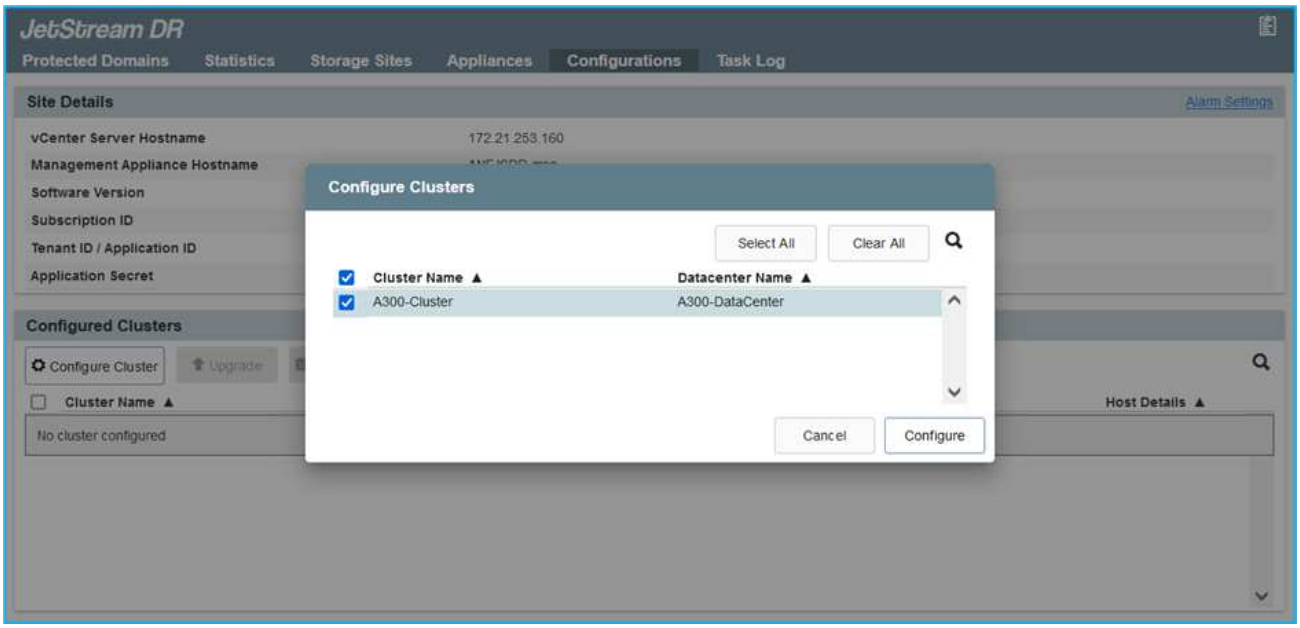
1. Consulte los requisitos previos.
2. Ejecute la herramienta de planificación de capacidad para obtener recomendaciones de recursos y configuración (opcional pero recomendado para pruebas de concepto).
3. Implemente JetStream DR MSA en un host vSphere en el clúster designado.
4. Inicie el MSA utilizando su nombre DNS en un navegador.
5. Registre el servidor vCenter con MSA. Para realizar la instalación, complete los siguientes pasos

detallados:

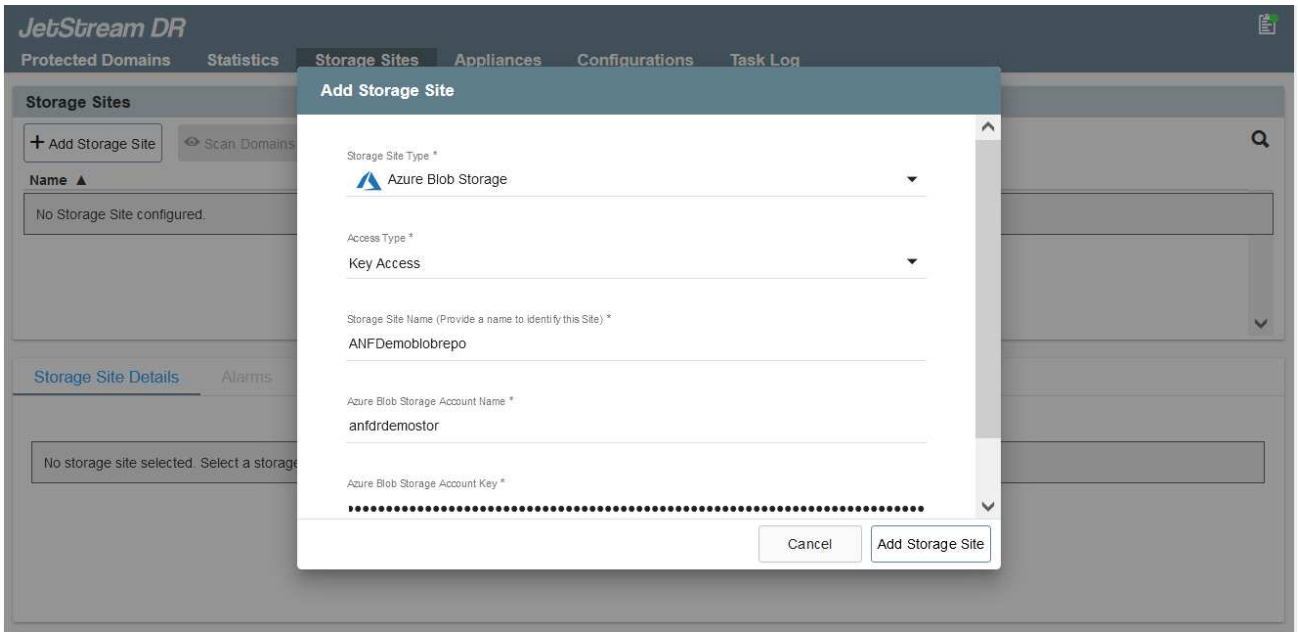
6. Una vez implementado JetStream DR MSA y registrado vCenter Server, acceda al complemento JetStream DR mediante vSphere Web Client. Esto se puede hacer navegando a Centro de datos > Configurar > JetStream DR.



7. Desde la interfaz de JetStream DR, seleccione el clúster apropiado.



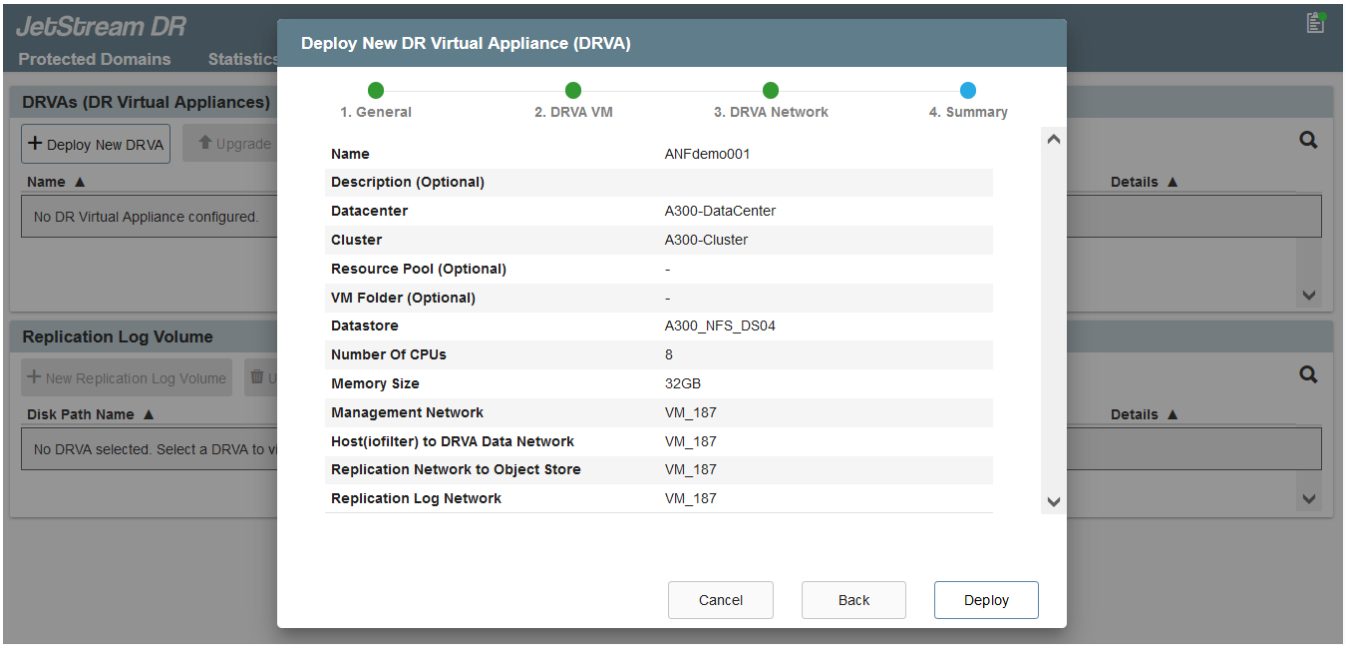
8. Configure el clúster con el paquete de filtro de E/S.



9. Agregue Azure Blob Storage ubicado en el sitio de recuperación.
10. Implemente un dispositivo virtual de recuperación ante desastres (DRVA) desde la pestaña Dispositivos.

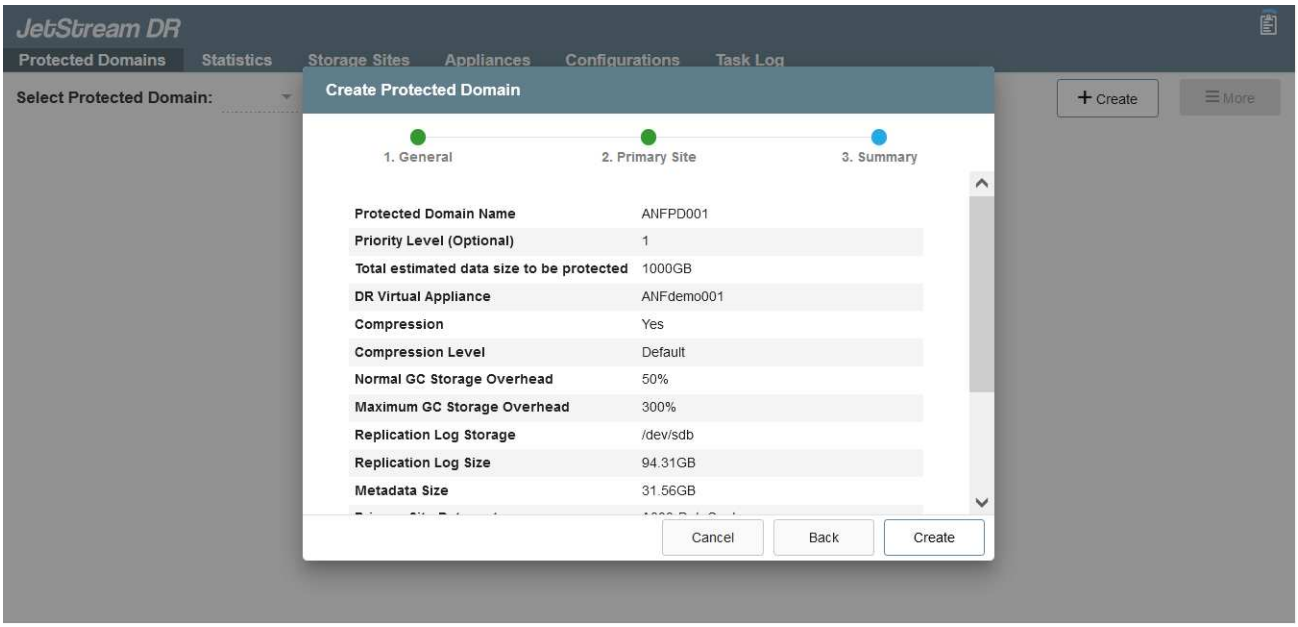
> CPT puede crear DRVA automáticamente, pero para pruebas de POC recomendamos configurar y ejecutar el ciclo de DR manualmente (iniciar protección > conmutación por error > conmutación por recuperación).

JetStream DRVA es un dispositivo virtual que facilita funciones clave en el proceso de replicación de datos. Un clúster protegido debe contener al menos un DRVA y, normalmente, se configura un DRVA por host. Cada DRVA puede administrar múltiples dominios protegidos.



En este ejemplo, se crearon cuatro DRVA para 80 máquinas virtuales.

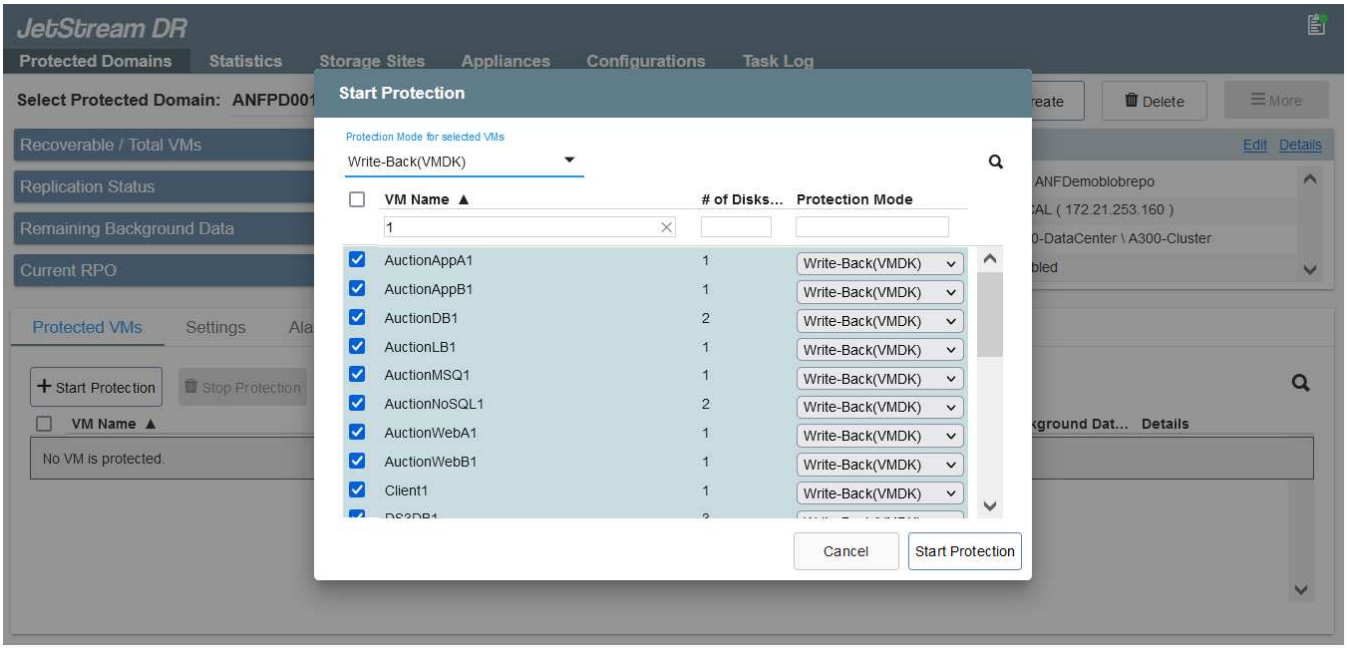
1. Cree volúmenes de registro de replicación para cada DRVA utilizando VMDK desde los almacenes de datos disponibles o grupos de almacenamiento iSCSI compartidos independientes.
2. Desde la pestaña Dominios protegidos, cree la cantidad necesaria de dominios protegidos utilizando información sobre el sitio de Azure Blob Storage, la instancia de DRVA y el registro de replicación. Un dominio protegido define una máquina virtual específica o un conjunto de máquinas virtuales dentro del clúster que están protegidas juntas y a las que se les asigna un orden de prioridad para operaciones de conmutación por error/recuperación.



3. Seleccione las máquinas virtuales que desee proteger e inicie la protección de las máquinas virtuales del dominio protegido. Esto inicia la replicación de datos en el Blob Store designado.

Verifique que se utilice el mismo modo de protección para todas las máquinas virtuales en un dominio protegido.

El modo de escritura diferida (VMDK) puede ofrecer un mayor rendimiento.



Verifique que los volúmenes del registro de replicación estén ubicados en un almacenamiento de alto rendimiento.

> Los libros de ejecución de conmutación por error se pueden configurar para agrupar las máquinas virtuales (llamado grupo de recuperación), establecer la secuencia de orden de arranque y modificar las configuraciones de CPU/memoria junto con las configuraciones de IP.

Instale JetStream DR para AVS en una nube privada de Azure VMware Solution mediante el comando Ejecutar

Una práctica recomendada para un sitio de recuperación (AVS) es crear con anticipación un clúster piloto de tres nodos. Esto permite preconfigurar la infraestructura del sitio de recuperación, incluidos los siguientes elementos:

- Segmentos de red de destino, firewalls, servicios como DHCP y DNS, etc.
- Instalación de JetStream DR para AVS
- Configuración de volúmenes ANF como almacenes de datos y másJetStream DR admite el modo RTO casi cero para dominios de misión crítica. Para estos dominios, el almacenamiento de destino debe estar preinstalado. ANF es el tipo de almacenamiento recomendado en este caso.

> La configuración de la red, incluida la creación de segmentos, debe configurarse en el clúster AVS para que coincida con los requisitos locales.

Dependiendo de los requisitos de SLA y RTO, se puede utilizar el modo de conmutación por error continuo o el modo de conmutación por error regular (estándar). En caso de RTO cercano a cero, se debe iniciar la rehidratación continua en el sitio de recuperación.

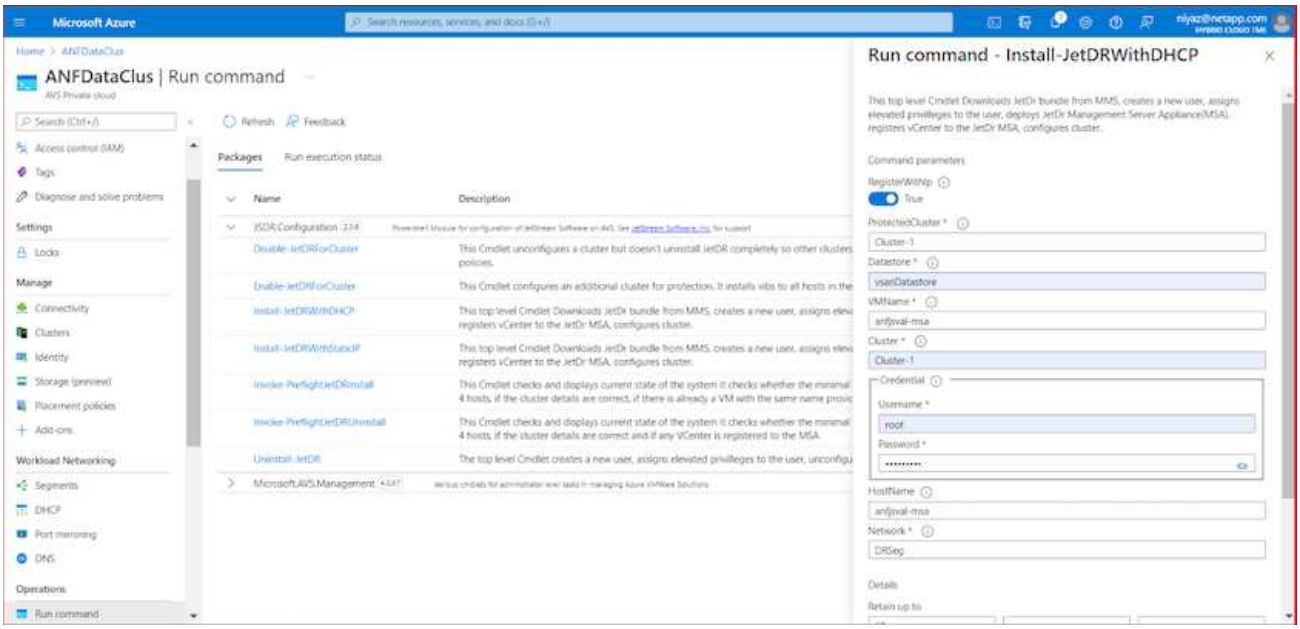
▼ Cómo instalar JetStream DR para AVS en una nube privada

Para instalar JetStream DR para AVS en una nube privada de Azure VMware Solution, complete los siguientes pasos:

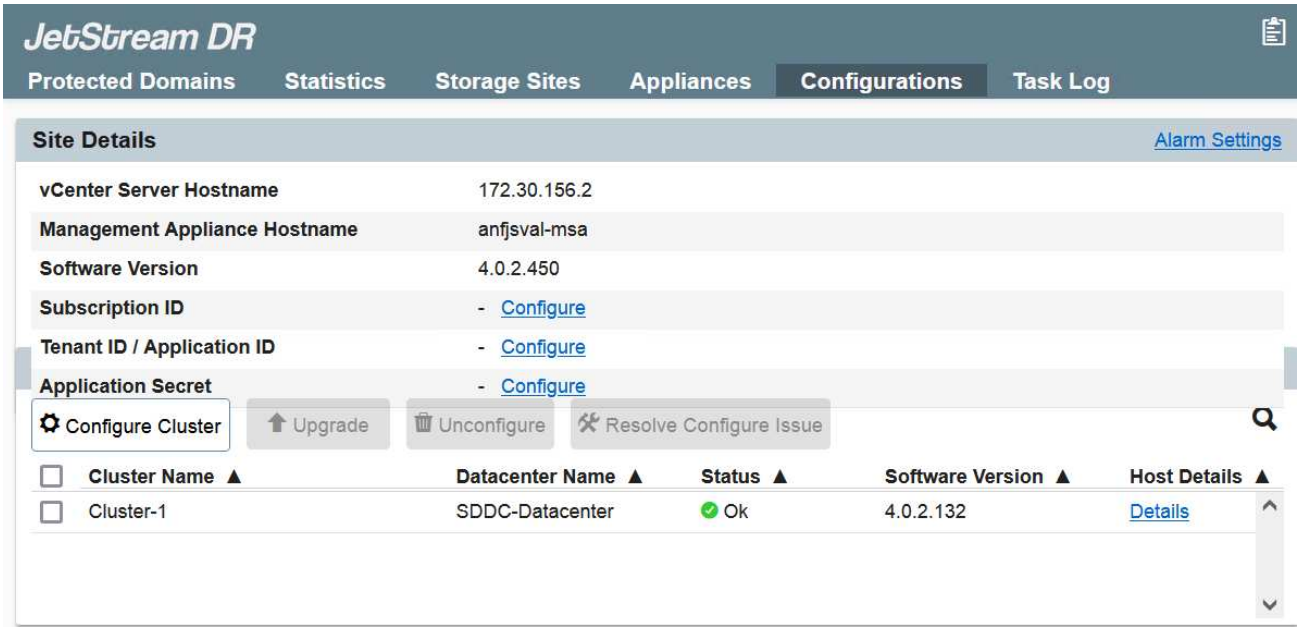
1. Desde el portal de Azure, vaya a la solución Azure VMware, seleccione la nube privada y seleccione Ejecutar comando > Paquetes > JSDR.Configuration.

El usuario CloudAdmin predeterminado en Azure VMware Solution no tiene privilegios suficientes para instalar JetStream DR para AVS. Azure VMware Solution permite una instalación simplificada y automatizada de JetStream DR invocando el comando Ejecutar de Azure VMware Solution para JetStream DR.

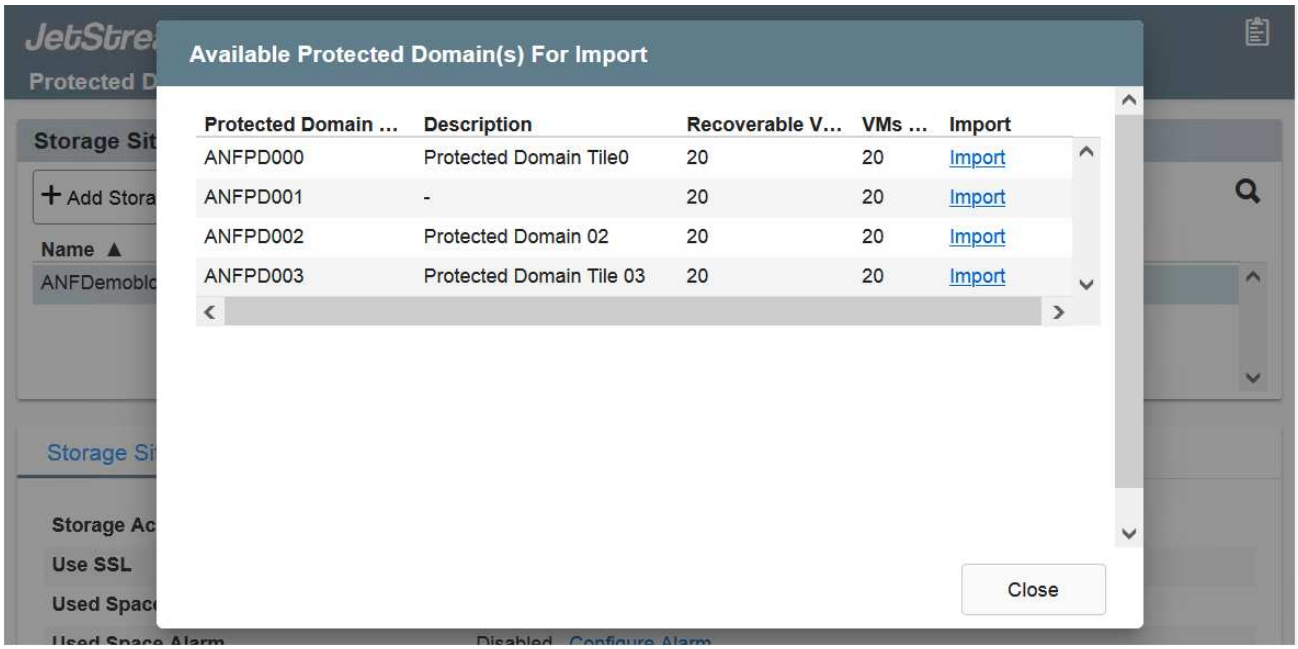
La siguiente captura de pantalla muestra la instalación utilizando una dirección IP basada en DHCP.



2. Una vez completada la instalación de JetStream DR para AVS, actualice el navegador. Para acceder a la interfaz de usuario de JetStream DR, vaya a SDDC Datacenter > Configurar > JetStream DR.



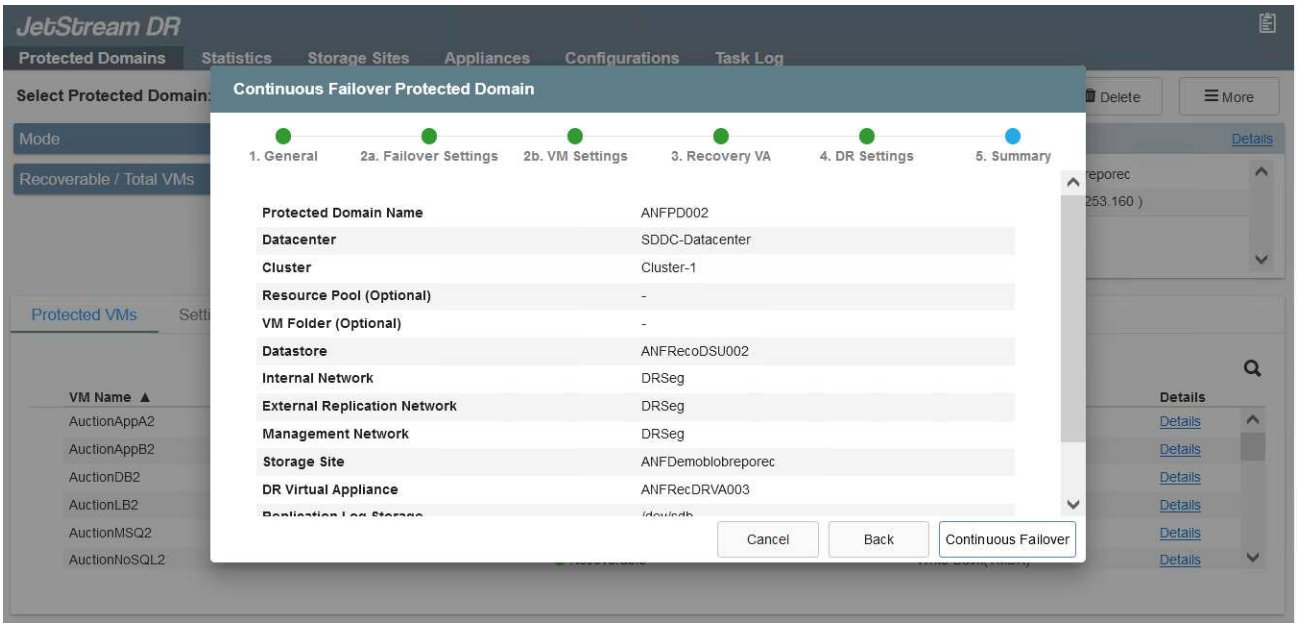
3. Desde la interfaz de JetStream DR, agregue la cuenta de Azure Blob Storage que se usó para proteger el clúster local como un sitio de almacenamiento y luego ejecute la opción Escanear dominios.



4. Una vez importados los dominios protegidos, implemente los dispositivos DRVA. En este ejemplo, la rehidratación continua se inicia manualmente desde el sitio de recuperación mediante la interfaz de usuario JetStream DR.

> Estos pasos también se pueden automatizar utilizando planes creados por CPT.

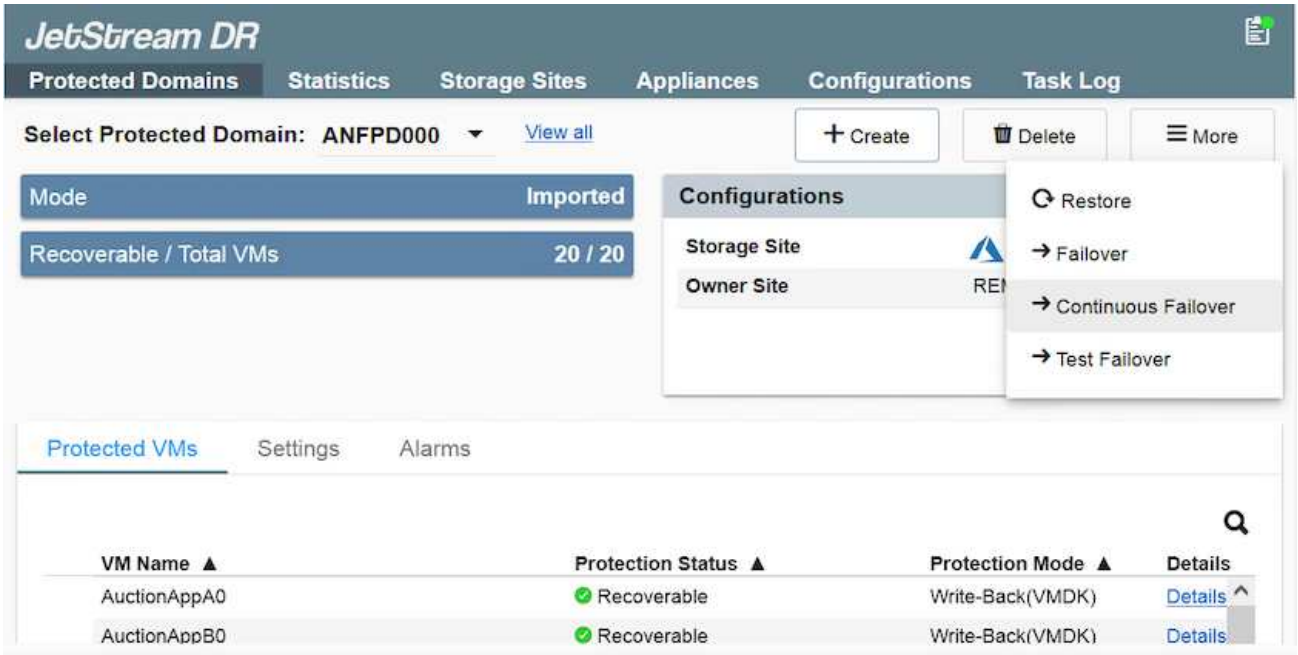
5. Cree volúmenes de registro de replicación utilizando almacenes de datos vSAN o ANF disponibles.
6. Importe los dominios protegidos y configure Recovery VA para usar el almacén de datos ANF para las ubicaciones de VM.



> Asegúrese de que DHCP esté habilitado en el segmento seleccionado y que haya suficientes IP disponibles. Las IP dinámicas se utilizan temporalmente mientras los dominios se recuperan. Cada VM en recuperación (incluida la rehidratación continua) requiere una IP dinámica individual. Una vez completada la recuperación, la IP se libera

y se puede reutilizar.

7. Seleccione la opción de conmutación por error adecuada (conmutación por error continua o conmutación por error). En este ejemplo, se selecciona la rehidratación continua (conmutación por error continua).



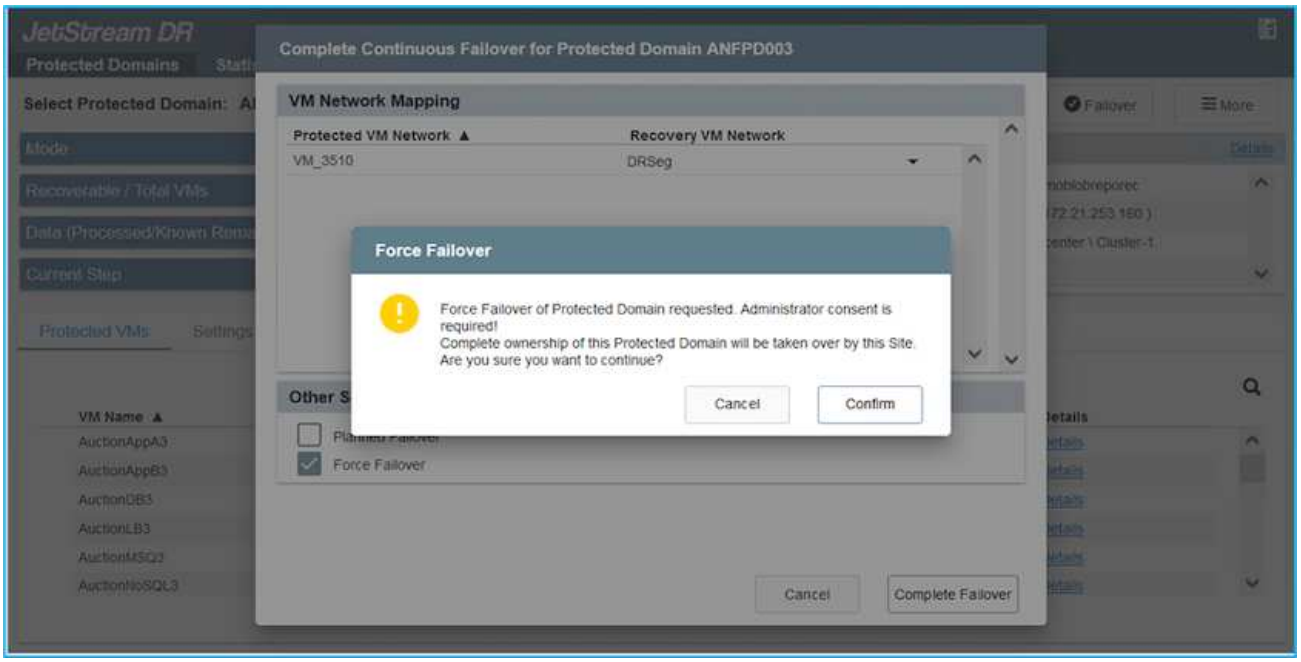
Realizar conmutación por error/recuperación

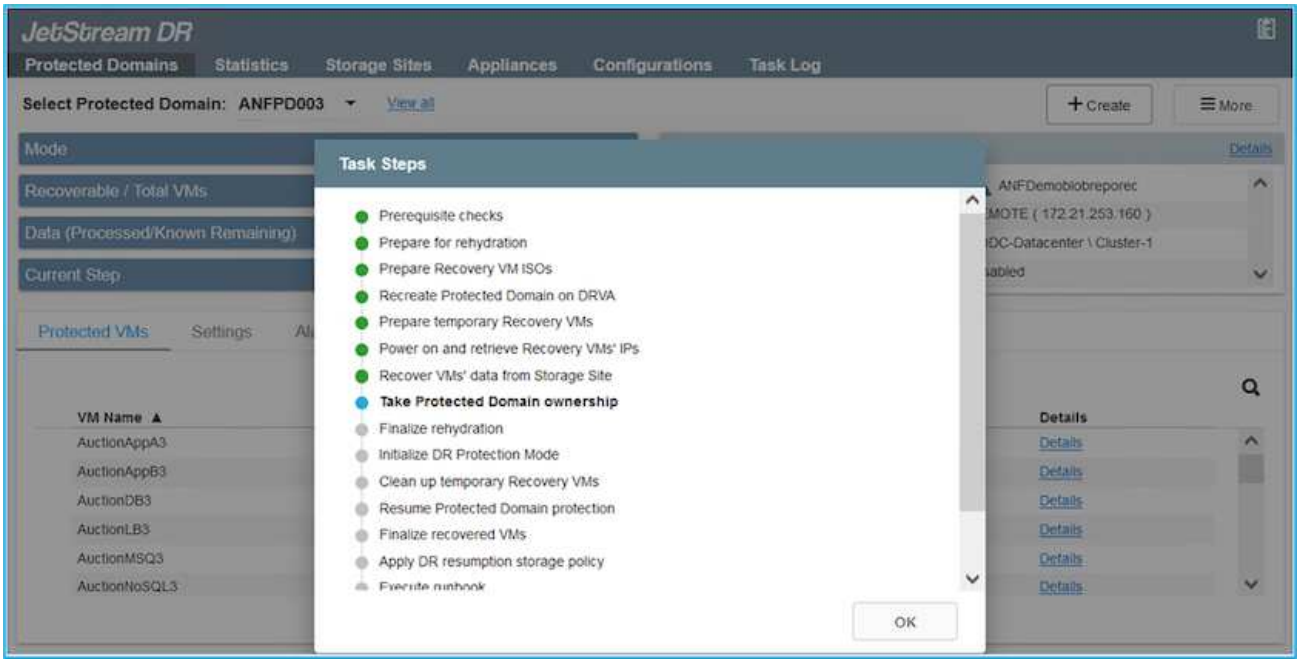
▼ Cómo realizar una conmutación por error/retorno

1. Después de que ocurre un desastre en el clúster protegido del entorno local (falla parcial o total), active la conmutación por error.

CPT se puede usar para ejecutar el plan de conmutación por error para recuperar las máquinas virtuales de Azure Blob Storage en el sitio de recuperación del clúster AVS.

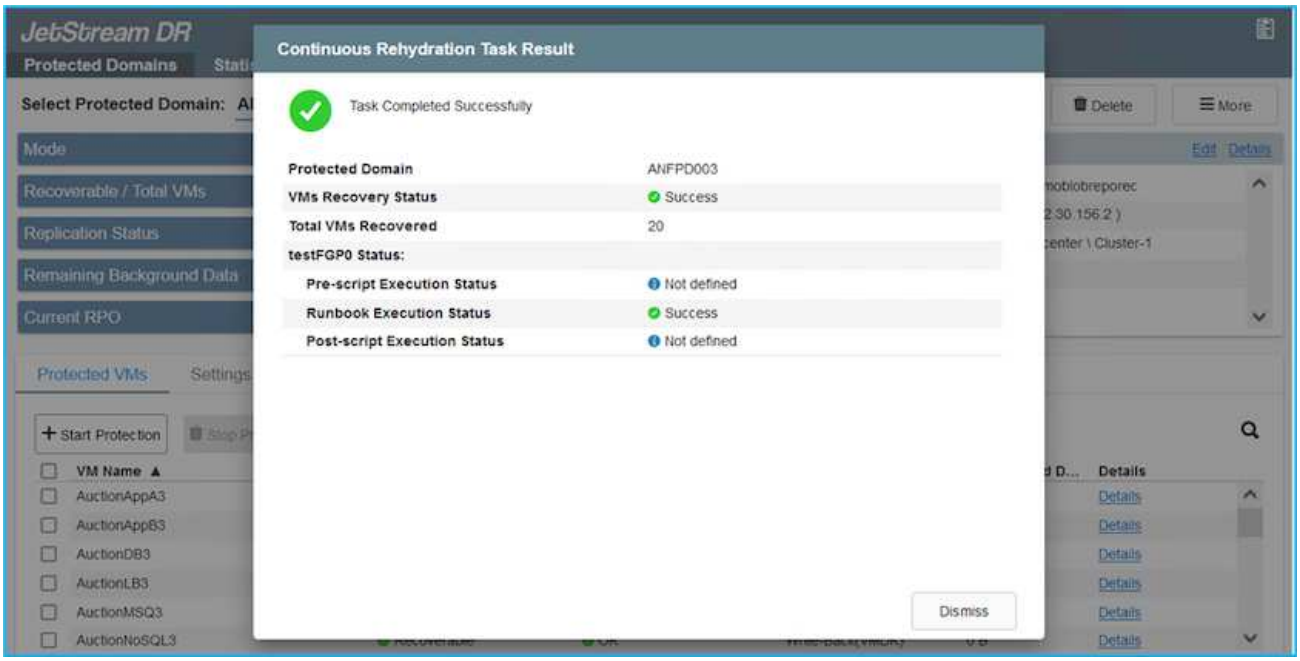
Después de la conmutación por error (para rehidratación continua o estándar), cuando las máquinas virtuales protegidas se han iniciado en AVS, la protección se reanuda automáticamente y JetStream DR continúa replicando sus datos en los contenedores apropiados/originales en Azure Blob Storage.





La barra de tareas muestra el progreso de las actividades de conmutación por error.

2. Una vez finalizada la tarea, acceda a las máquinas virtuales recuperadas y el negocio continúa normalmente.

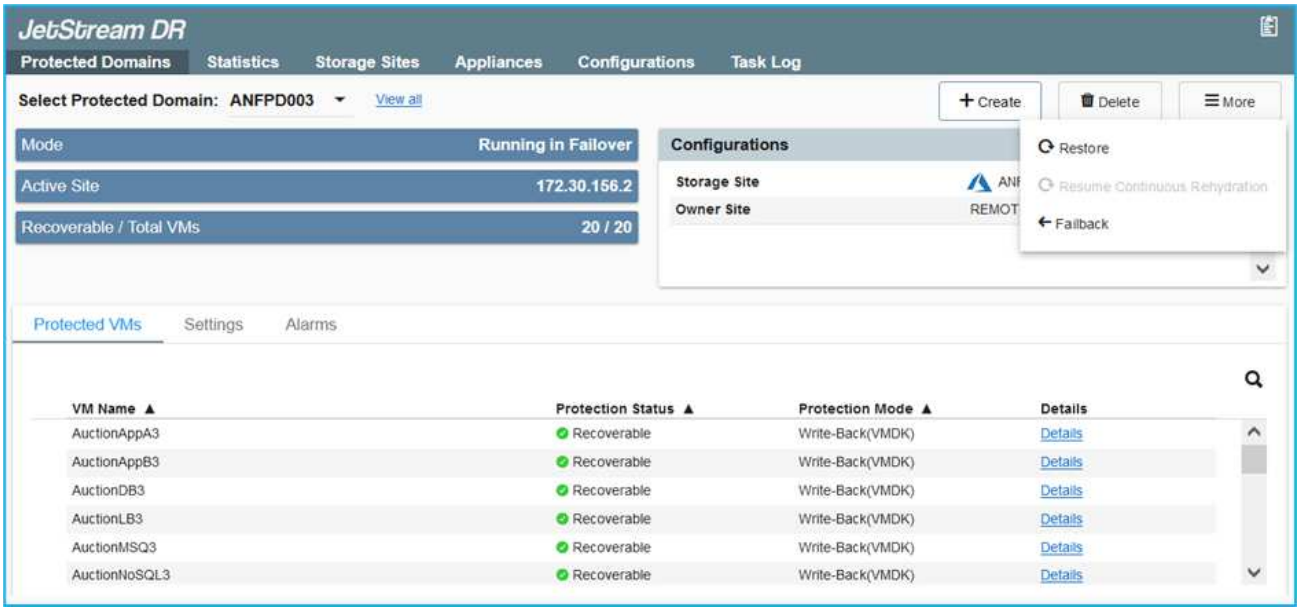


Una vez que el sitio principal esté funcionando nuevamente, se puede realizar una conmutación por recuperación. Se reanuda la protección de la máquina virtual y se debe verificar la consistencia de los datos.

3. Restaurar el entorno local. Dependiendo del tipo de incidente de desastre, podría ser necesario restaurar y/o verificar la configuración del clúster protegido. Si es necesario, es posible que sea necesario reinstalar el software JetStream DR.

> Nota: El `recovery_utility_prepare_failback` El script proporcionado en Automation Toolkit se puede usar para ayudar a limpiar el sitio protegido original de cualquier máquina virtual obsoleta, información de dominio, etc.

4. Acceda al entorno local restaurado, vaya a la interfaz de usuario de Jetstream DR y seleccione el dominio protegido adecuado. Una vez que el sitio protegido esté listo para la conmutación por recuperación, seleccione la opción Conmutación por recuperación en la interfaz de usuario.



El plan de conmutación por error generado por CPT también se puede utilizar para iniciar el retorno de las máquinas virtuales y sus datos desde el almacén de objetos al entorno VMware original.

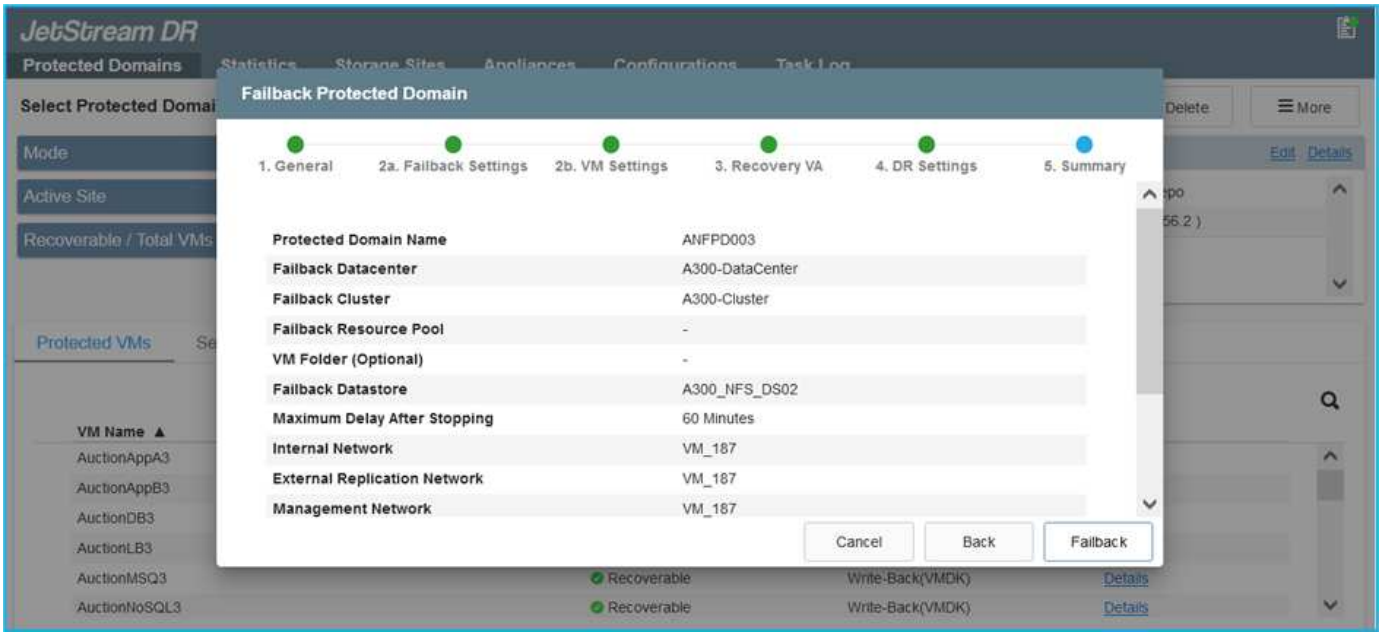
Especifique el retraso máximo después de pausar las máquinas virtuales en el sitio de recuperación y reiniciarlas en el sitio protegido. Este tiempo incluye completar la replicación después de detener las máquinas virtuales de conmutación por error, el tiempo para limpiar el sitio de recuperación y el tiempo para recrear las máquinas virtuales en el sitio protegido. El valor recomendado NetApp es 10 minutos.

Complete el proceso de conmutación por error y luego confirme la reanudación de la protección de la máquina virtual y la consistencia de los datos.

Recuperación de ransomeware

Recuperarse de un ransomware puede ser una tarea abrumadora. En concreto, puede resultar difícil para las organizaciones de TI determinar el punto de retorno seguro y, una vez determinado, cómo garantizar que las cargas de trabajo recuperadas estén protegidas de ataques recurrentes (de malware inactivo o de aplicaciones vulnerables).

JetStream DR para AVS junto con los almacenes de datos de Azure NetApp Files pueden abordar estas inquietudes al permitir que las organizaciones se recuperen desde puntos disponibles en el tiempo, de modo que las cargas de trabajo se recuperen en una red funcional y aislada si es necesario. La recuperación permite que las aplicaciones funcionen y se comuniquen entre sí sin exponerlas al tráfico de norte a sur, lo que brinda a los equipos de seguridad un lugar seguro para realizar análisis forenses y otras reparaciones necesarias.



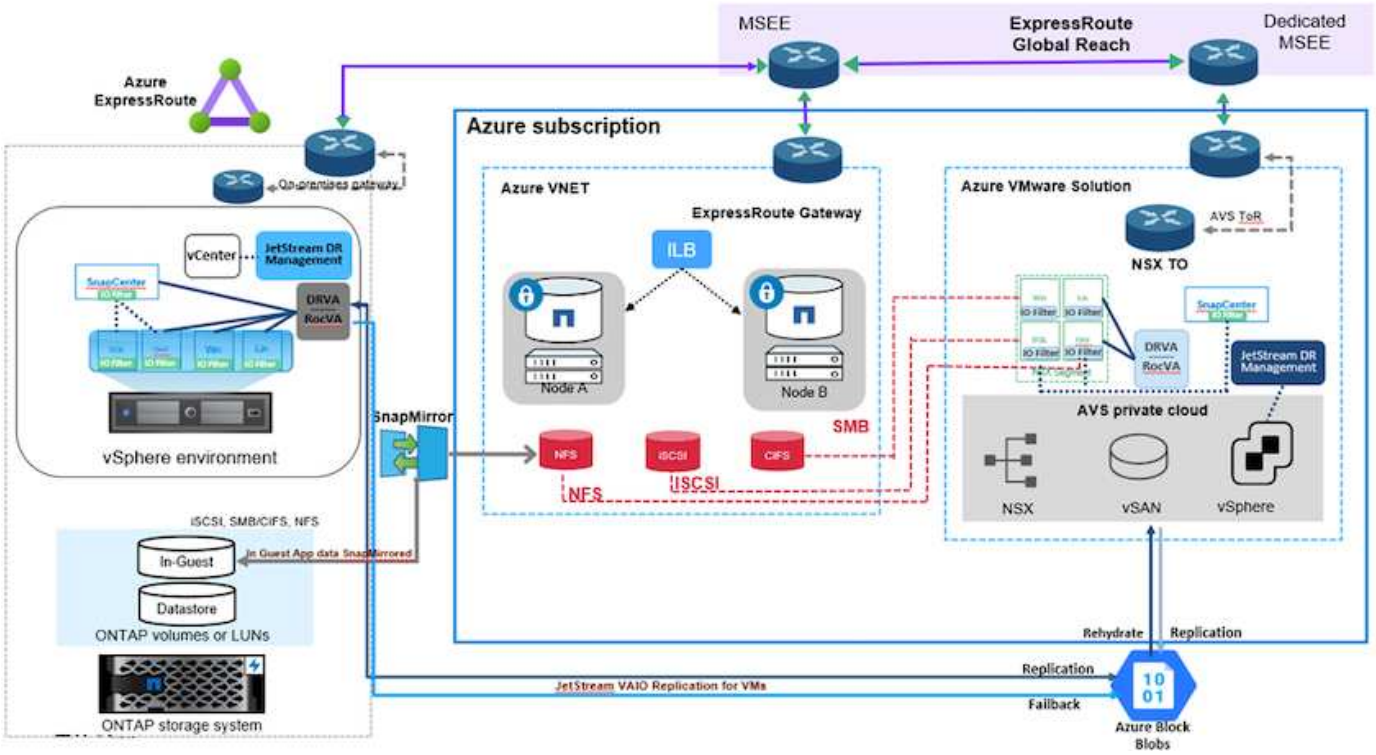
Recuperación ante desastres con CVO y AVS (almacenamiento conectado a invitados)

La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos como ransomware. Con NetApp SnapMirror, las cargas de trabajo locales de VMware que usan almacenamiento conectado a invitados se pueden replicar en NetApp Cloud

Volumes ONTAP que se ejecuta en Azure.

Descripción general

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
Este documento proporciona un enfoque paso a paso para configurar y
realizar la recuperación ante desastres que utiliza NetApp SnapMirror,
JetStream y Azure VMware Solution (AVS).
```



Suposiciones

Este documento se centra en el almacenamiento interno de datos de aplicaciones (también conocido como almacenamiento conectado por invitado) y asumimos que el entorno local utiliza SnapCenter para realizar copias de seguridad consistentes con las aplicaciones.

> Este documento se aplica a cualquier solución de copia de seguridad o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las mejores prácticas para crear políticas de respaldo que cumplan con los SLA de la organización.

Para la conectividad entre el entorno local y la red virtual de Azure, utilice la ruta rápida Global Reach o una WAN virtual con una puerta de enlace VPN. Los segmentos deben crearse según el diseño de VLAN local.

Existen múltiples opciones para conectar centros de datos locales a Azure, lo que nos impide delinear un flujo de trabajo específico en este documento. Consulte la documentación de Azure para conocer el método de conectividad local a Azure adecuado.

Implementación de la solución de recuperación ante desastres

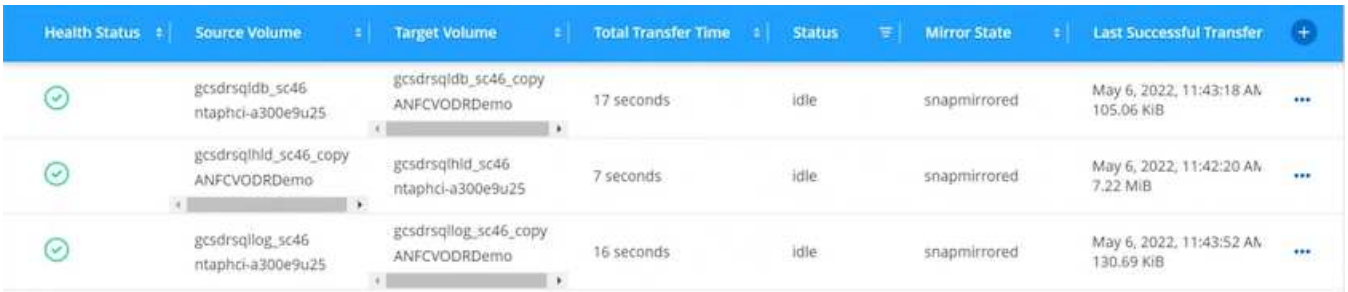
Descripción general de la implementación de la solución

1. Asegúrese de que los datos de la aplicación estén respaldados mediante SnapCenter con los requisitos de RPO necesarios.
2. Aprovisione Cloud Volumes ONTAP con el tamaño de instancia correcto utilizando Cloud Manager dentro de la suscripción y la red virtual adecuadas.
   a. Configure SnapMirror para los volúmenes de aplicación relevantes.
   b. Actualice las políticas de respaldo en SnapCenter para activar las actualizaciones de SnapMirror después de los trabajos programados.
3. Instale el software JetStream DR en el centro de datos local e inicie la protección para máquinas virtuales.
4. Instale el software JetStream DR en la nube privada de Azure VMware Solution.
5. Durante un evento de desastre, interrumpa la relación de SnapMirror mediante Cloud Manager y active la conmutación por error de las máquinas virtuales a Azure NetApp Files o a los almacenes de datos de vSAN en el sitio de AVS DR designado.
   a. Vuelva a conectar los LUN ISCSI y los montajes NFS para las máquinas virtuales de la aplicación.
6. Invoque la conmutación por error al sitio protegido mediante la resincronización inversa de SnapMirror después de que se haya recuperado el sitio principal.

Detalles de la implementación

▼ Configurar CVO en Azure y replicar volúmenes en CVO

El primer paso es configurar Cloud Volumes ONTAP en Azure ("Enlace") y replique los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retenciones de instantáneas deseadas.



▼ Configurar los hosts AVS y el acceso a los datos CVO

Dos factores importantes a tener en cuenta al implementar el SDDC son el tamaño del clúster SDDC en la solución Azure VMware y cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costos operativos generales. El SDDC puede ser tan pequeño como tres hosts, o incluso un clúster de múltiples hosts en una implementación a gran escala.

La decisión de implementar un clúster AVS se basa principalmente en los requisitos de RPO/RTO. Con la solución Azure VMware, el SDDC se puede aprovisionar justo a tiempo para prepararse para pruebas o para un evento de desastre real. Un SDDC implementado justo a tiempo ahorra costos de host ESXi

cuando no se enfrenta a un desastre. Sin embargo, esta forma de implementación afecta el RTO en algunas horas mientras se aprovisiona el SDDC.

La opción implementada más común es tener el SDDC funcionando en un modo de operación siempre activo y con luz piloto. Esta opción proporciona un espacio reducido de tres hosts que están siempre disponibles y también acelera las operaciones de recuperación al proporcionar una línea base en funcionamiento para actividades de simulación y verificaciones de cumplimiento, evitando así el riesgo de desviaciones operativas entre los sitios de producción y de recuperación ante desastres. El grupo de luces piloto se puede ampliar rápidamente al nivel deseado cuando sea necesario para manejar un evento de DR real.

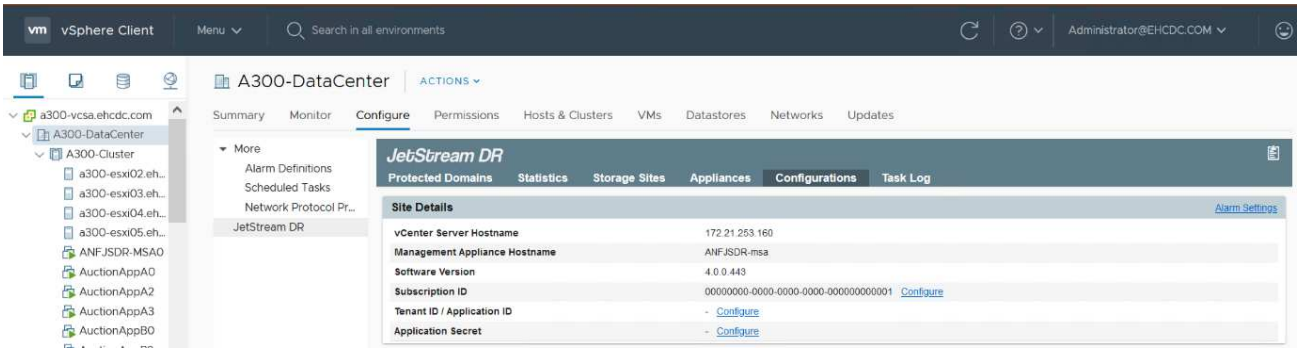
Para configurar AVS SDDC (ya sea a pedido o en modo piloto), consulte"Implementar y configurar el entorno de virtualización en Azure" . Como requisito previo, verifique que las máquinas virtuales invitadas que residen en los hosts AVS puedan consumir datos de Cloud Volumes ONTAP una vez que se haya establecido la conectividad.

Una vez que Cloud Volumes ONTAP y AVS se hayan configurado correctamente, comience a configurar Jetstream para automatizar la recuperación de cargas de trabajo locales en AVS (máquinas virtuales con VMDK de aplicaciones y máquinas virtuales con almacenamiento invitado) mediante el mecanismo VAIO y aprovechando SnapMirror para las copias de volúmenes de aplicaciones en Cloud Volumes ONTAP.

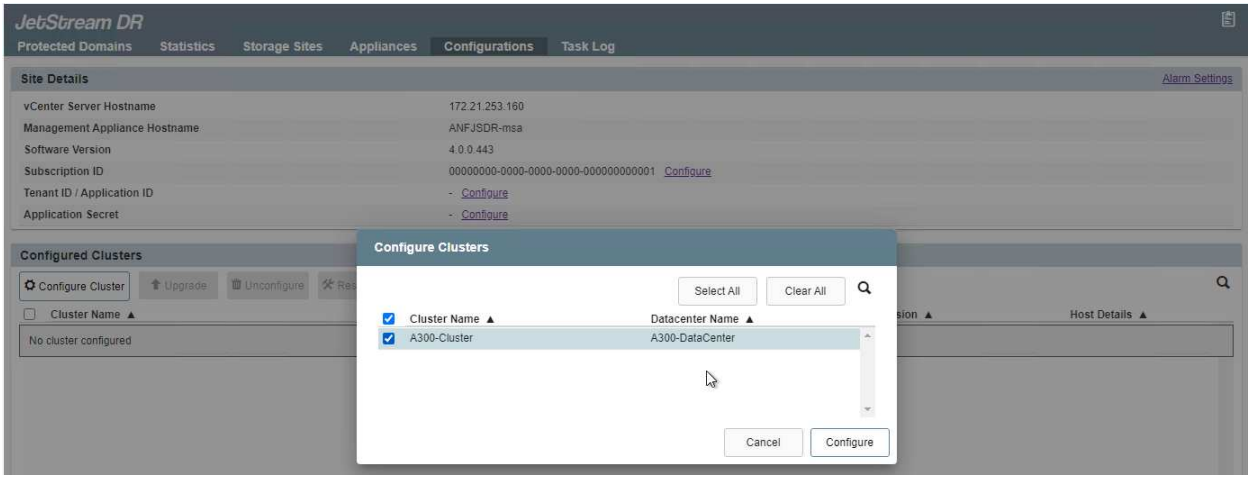
▼ Instalar JetStream DR en el centro de datos local

El software JetStream DR consta de tres componentes principales: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) y componentes de host (paquetes de filtros de E/S). El MSA se utiliza para instalar y configurar componentes del host en el clúster de cómputo y luego para administrar el software JetStream DR. El proceso de instalación es el siguiente:

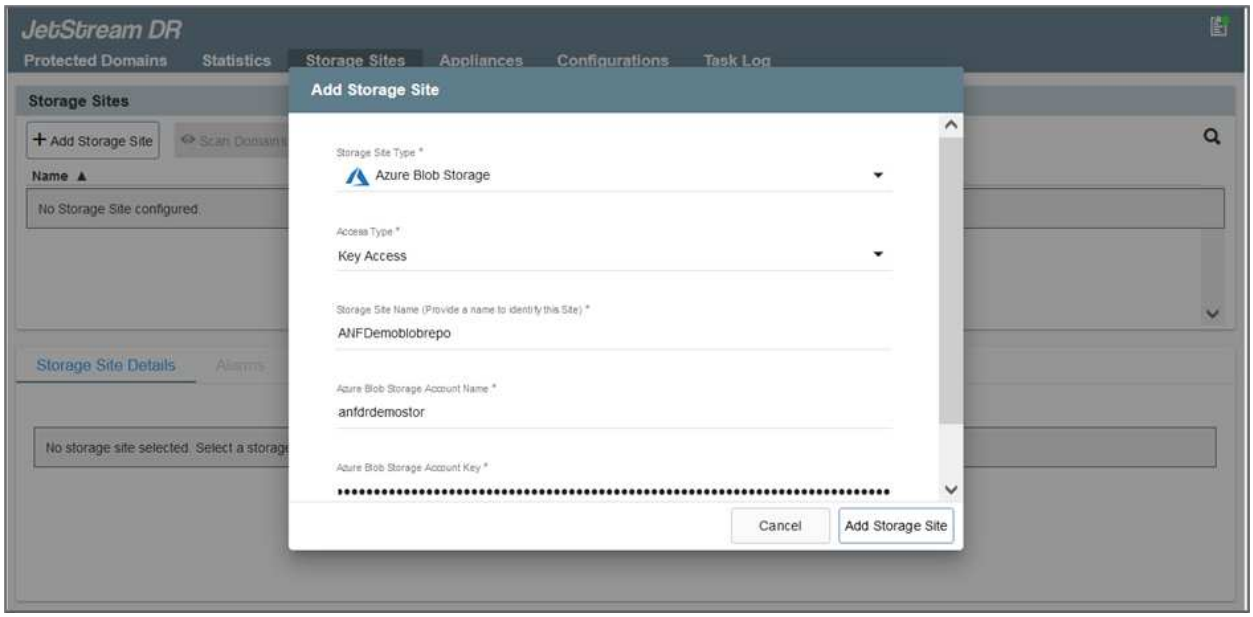
1. Consulte los requisitos previos.
2. Ejecute la herramienta de planificación de capacidad para obtener recomendaciones de recursos y configuración.
3. Implemente JetStream DR MSA en cada host vSphere en el clúster designado.
4. Inicie el MSA utilizando su nombre DNS en un navegador.
5. Registre el servidor vCenter con MSA.
6. Una vez implementado JetStream DR MSA y registrado vCenter Server, navegue hasta el complemento JetStream DR con vSphere Web Client. Esto se puede hacer navegando a Centro de datos > Configurar > JetStream DR.



7. Desde la interfaz de JetStream DR, complete las siguientes tareas:
   a. Configure el clúster con el paquete de filtro de E/S.



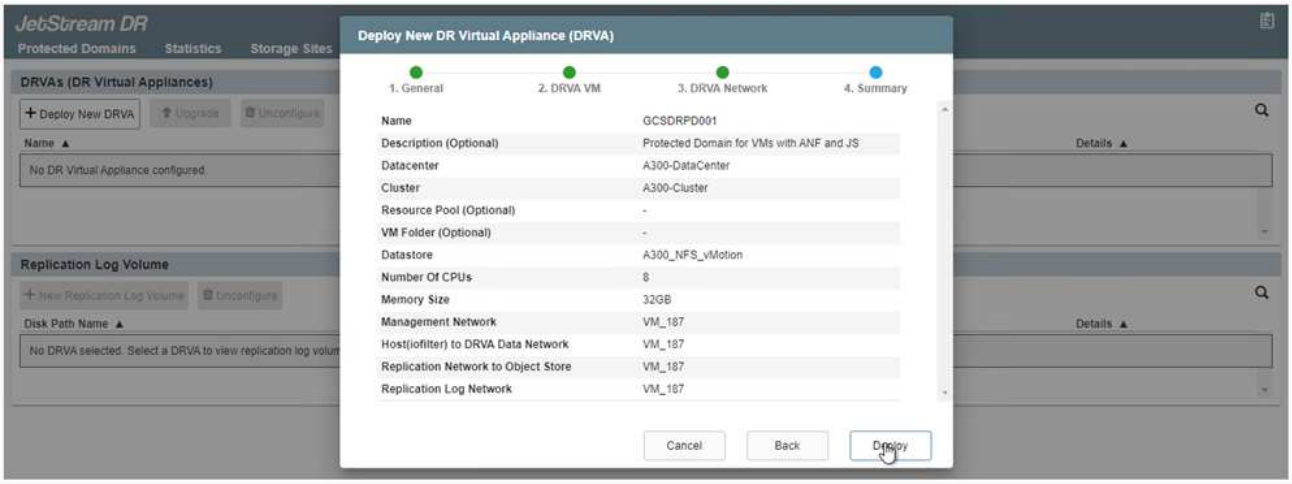
b. Agregue el almacenamiento de blobs de Azure ubicado en el sitio de recuperación.



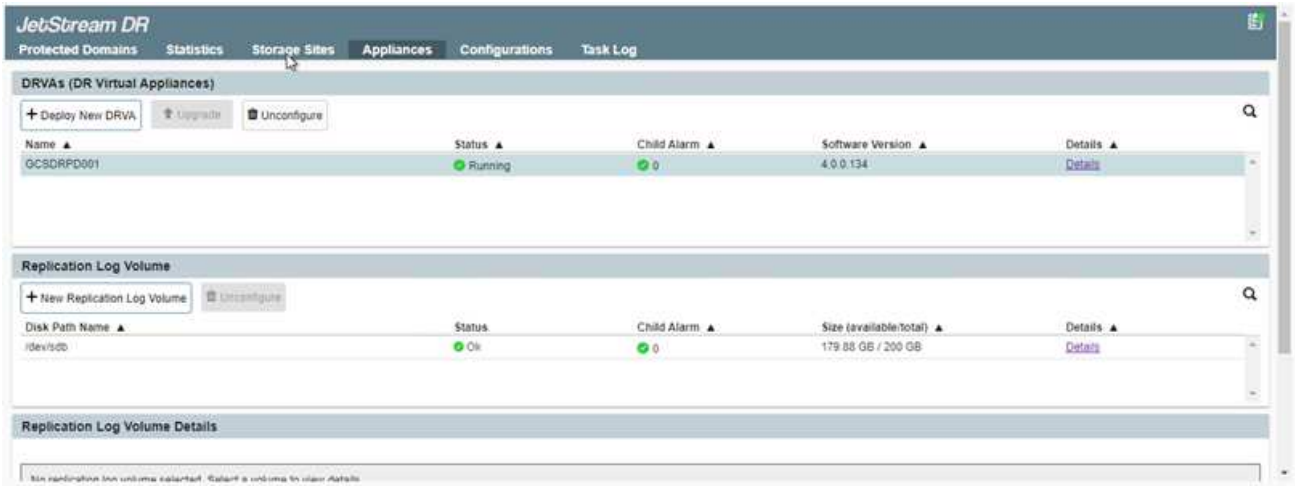
8. Implemente la cantidad necesaria de dispositivos virtuales de recuperación ante desastres (DRVA) desde la pestaña Dispositivos.

Utilice la herramienta de planificación de capacidad para estimar la cantidad de DRVA necesarios.

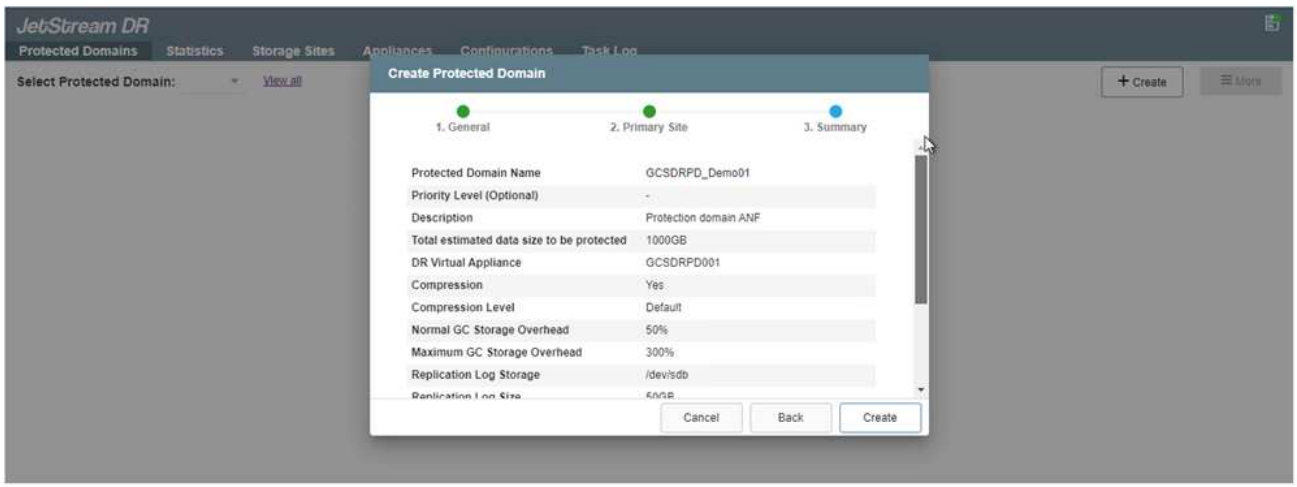


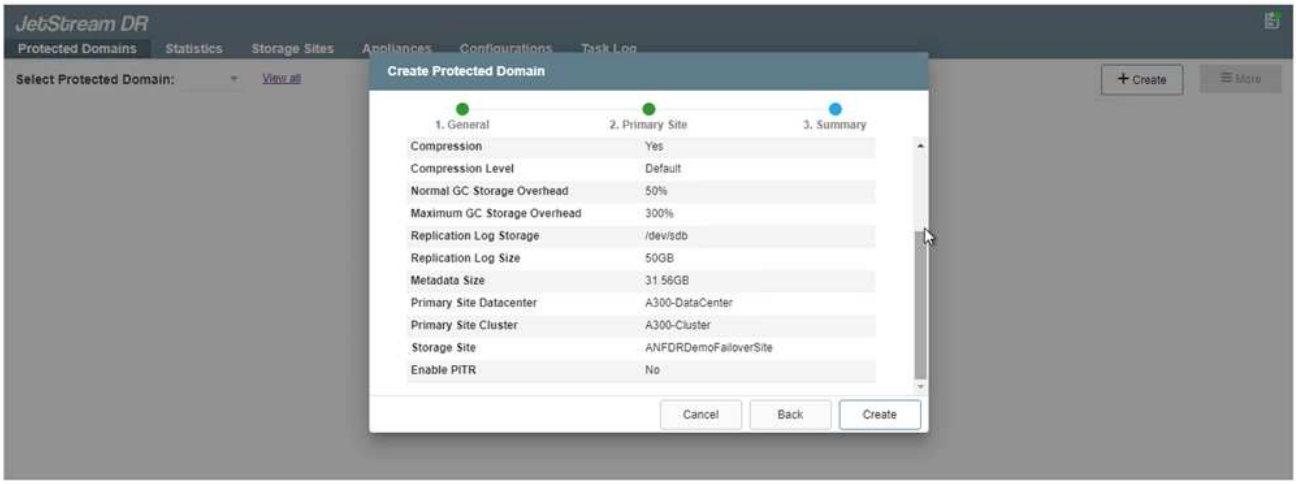


9. Cree volúmenes de registro de replicación para cada DRVA utilizando el VMDK de los almacenes de datos disponibles o el grupo de almacenamiento iSCSI compartido independiente.



10. Desde la pestaña Dominios protegidos, cree la cantidad necesaria de dominios protegidos utilizando información sobre el sitio de Azure Blob Storage, la instancia de DRVA y el registro de replicación. Un dominio protegido define una máquina virtual específica o un conjunto de máquinas virtuales de aplicación dentro del clúster que están protegidas juntas y a las que se les asigna un orden de prioridad para operaciones de conmutación por error/recuperación.

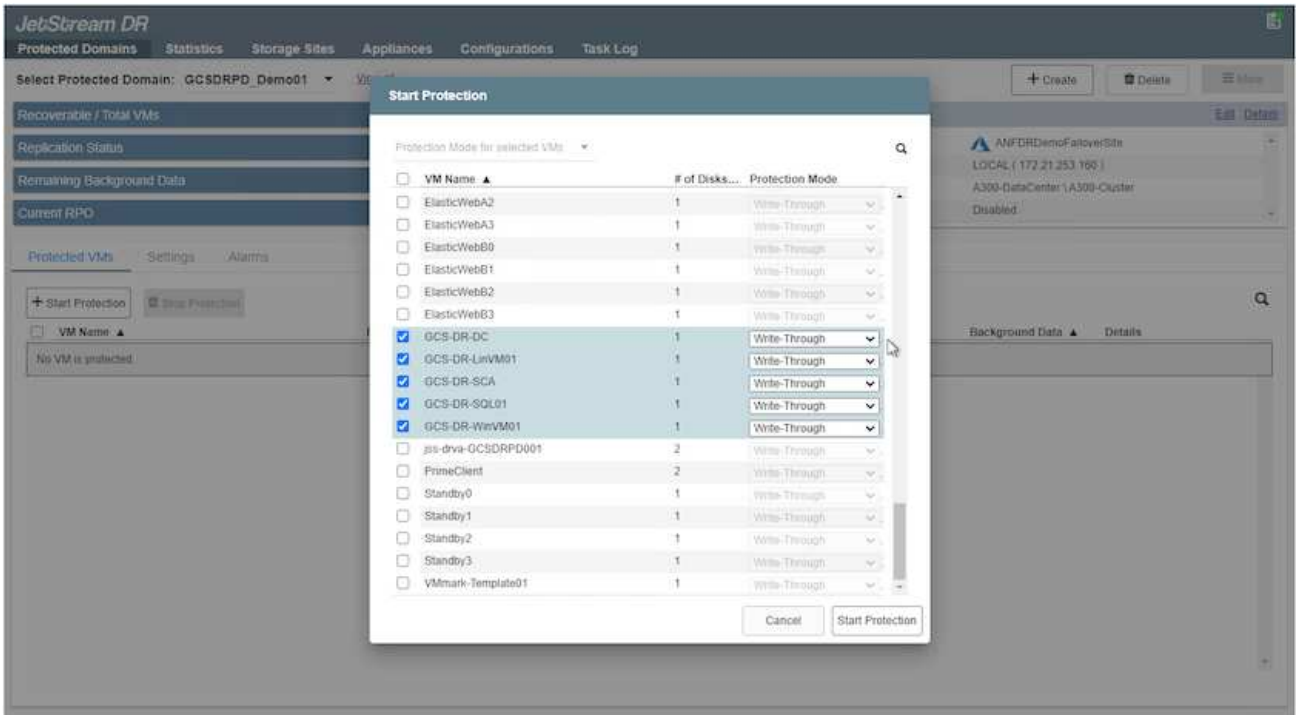




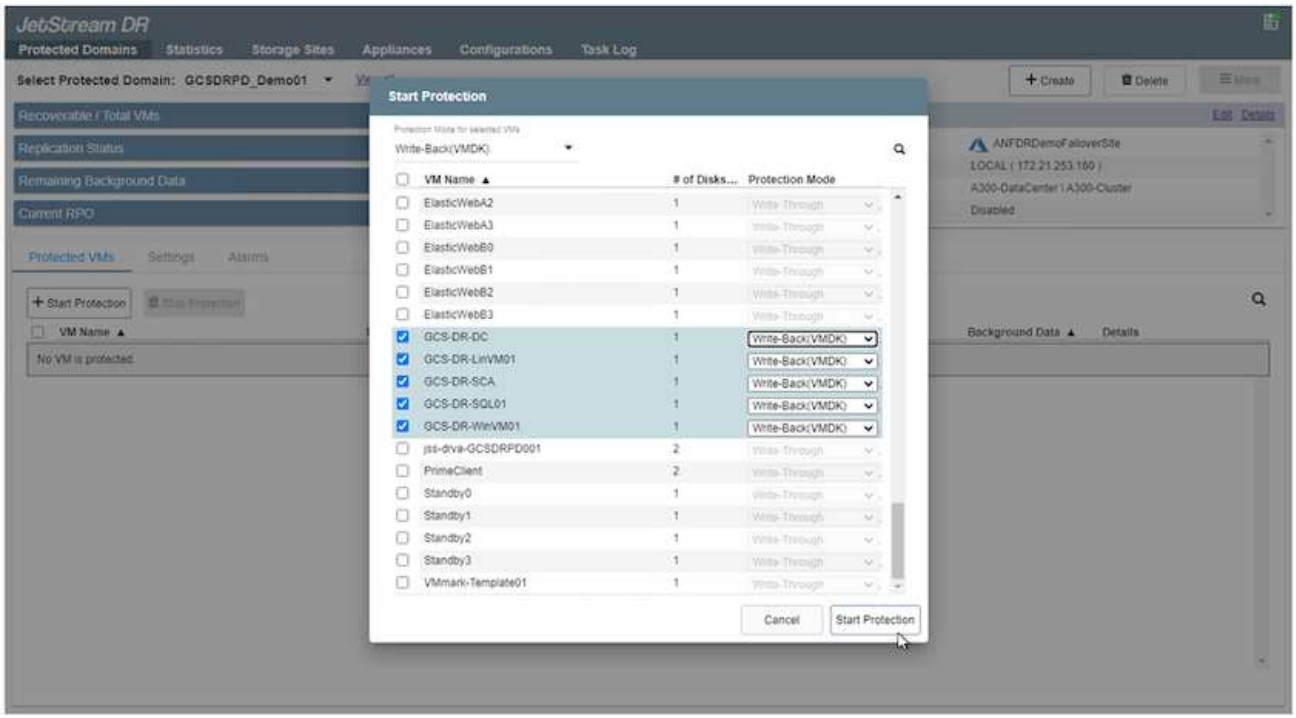
11. Seleccione las máquinas virtuales que desea proteger y agrúpelas en grupos de aplicaciones según la dependencia. Las definiciones de aplicación le permiten agrupar conjuntos de máquinas virtuales en grupos lógicos que contienen sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones opcionales que se pueden ejecutar durante la recuperación.

Asegúrese de que se utilice el mismo modo de protección para todas las máquinas virtuales en un dominio protegido.

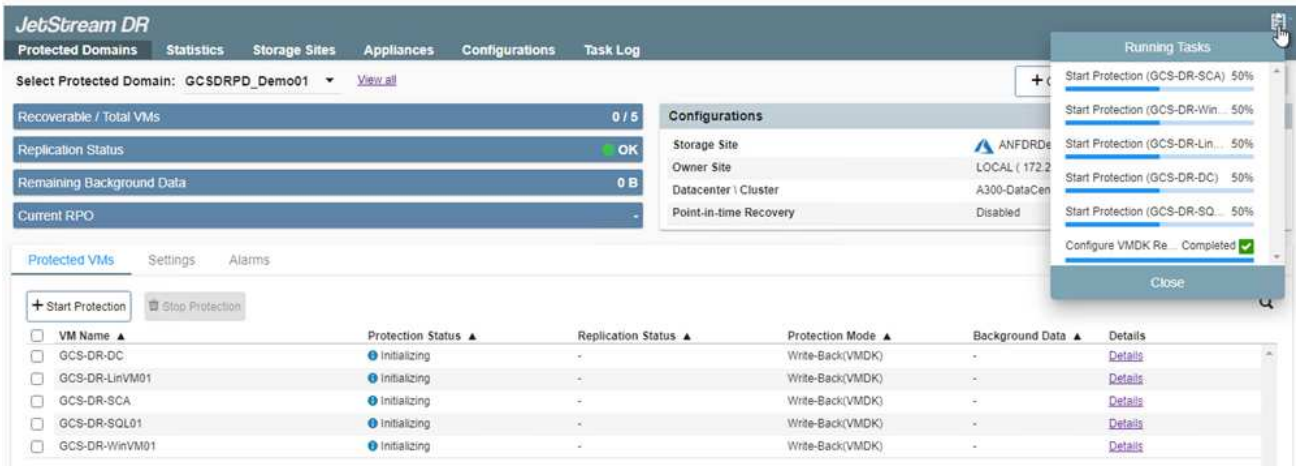
El modo de escritura diferida (VMDK) ofrece un mayor rendimiento.



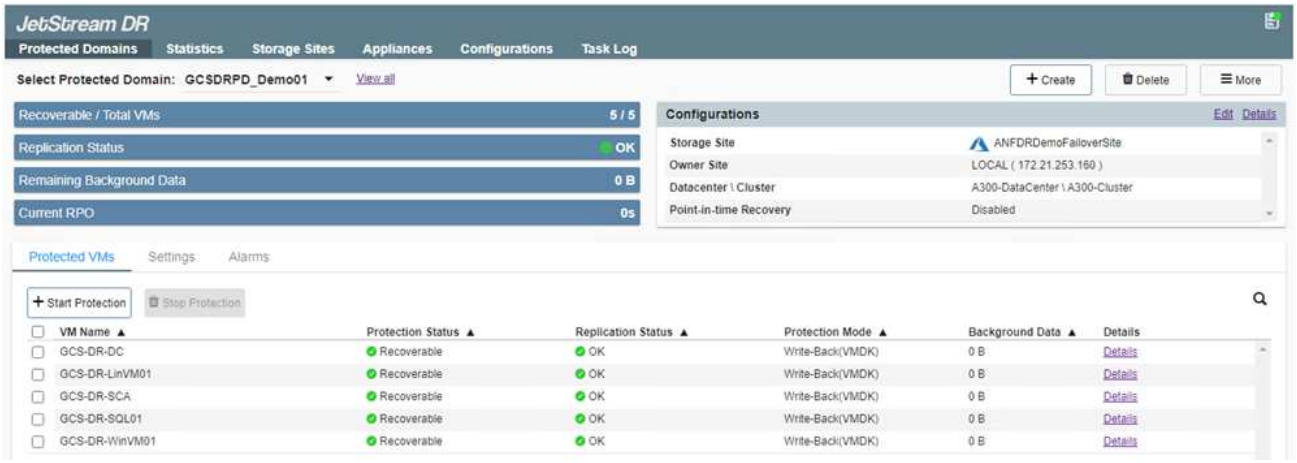
12. Asegúrese de que los volúmenes de registro de replicación estén ubicados en un almacenamiento de alto rendimiento.



13. Una vez que haya terminado, haga clic en Iniciar protección para el dominio protegido. Esto inicia la replicación de datos de las máquinas virtuales seleccionadas en el almacén de blobs designado.



14. Una vez completada la replicación, el estado de protección de la máquina virtual se marca como Recuperable.



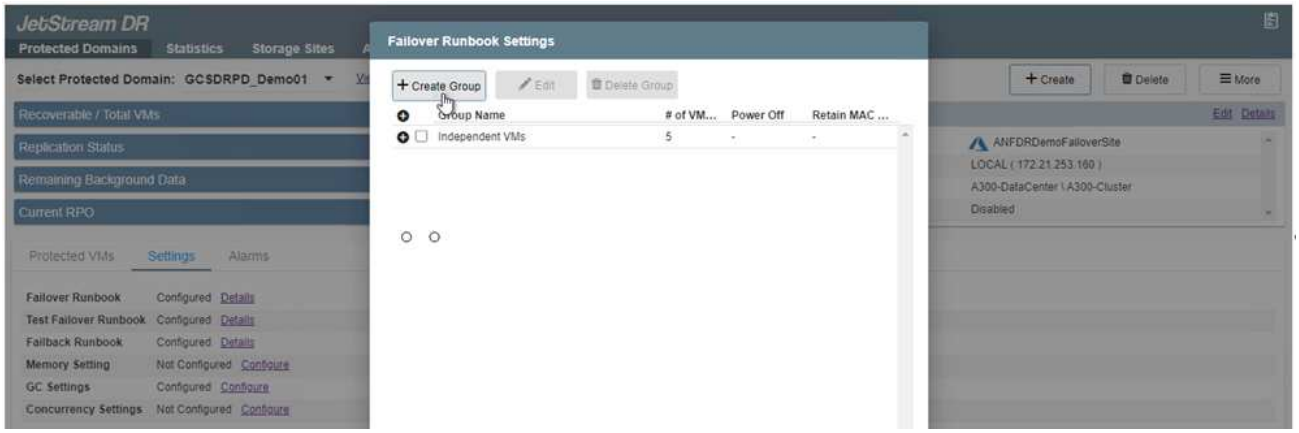
Los libros de ejecución de conmutación por error se pueden configurar para agrupar las máquinas virtuales (llamado grupo de recuperación), establecer la secuencia de orden de arranque y modificar las configuraciones de CPU/memoria junto con las configuraciones de IP.

15. Haga clic en Configuración y luego en el vínculo Configurar del libro de ejecución para configurar el grupo de libros de ejecución.

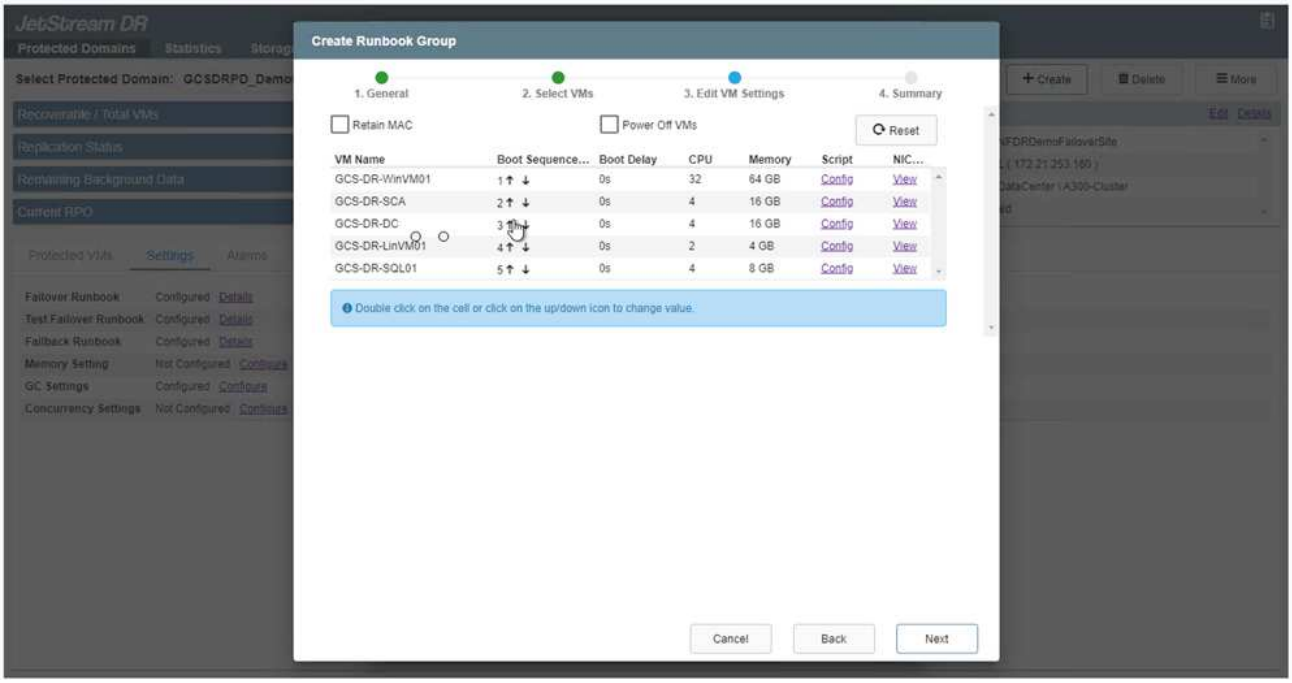


16. Haga clic en el botón Crear grupo para comenzar a crear un nuevo grupo de libros de ejecución.

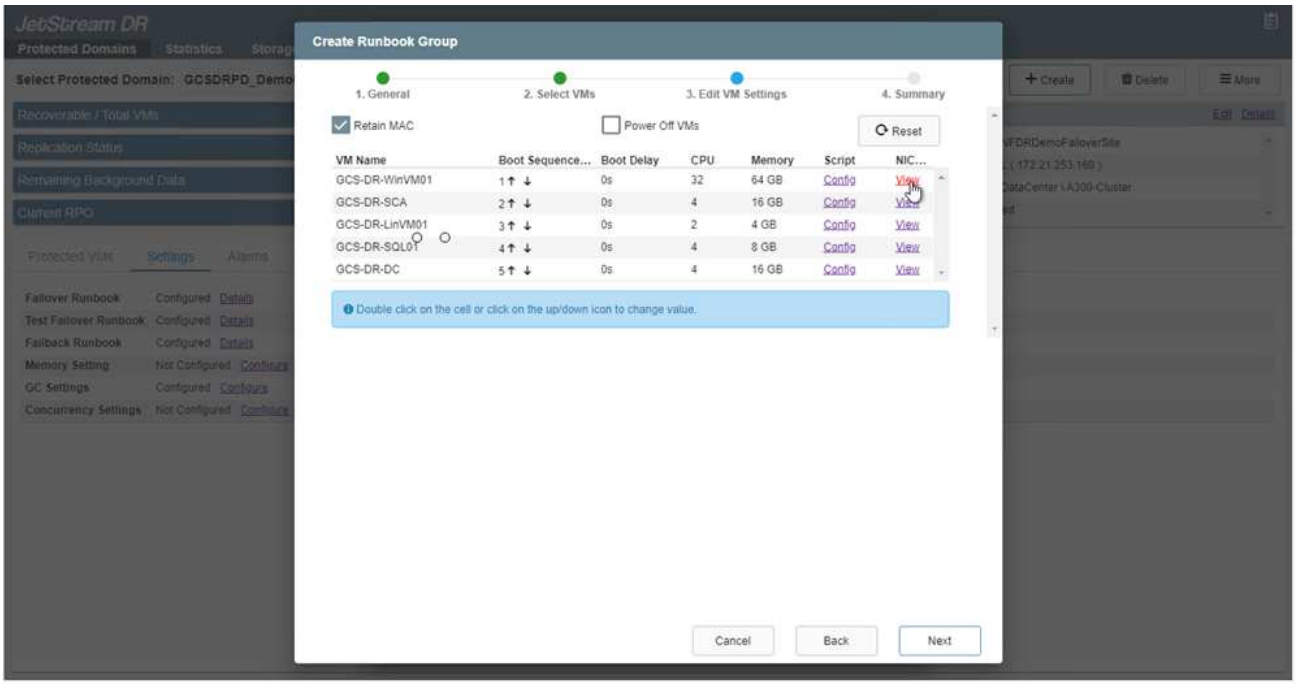
Si es necesario, en la parte inferior de la pantalla, aplique pre-scripts y post-scripts personalizados para que se ejecuten automáticamente antes y después de la operación del grupo de libros de ejecución. Asegúrese de que los scripts de Runbook residan en el servidor de administración.



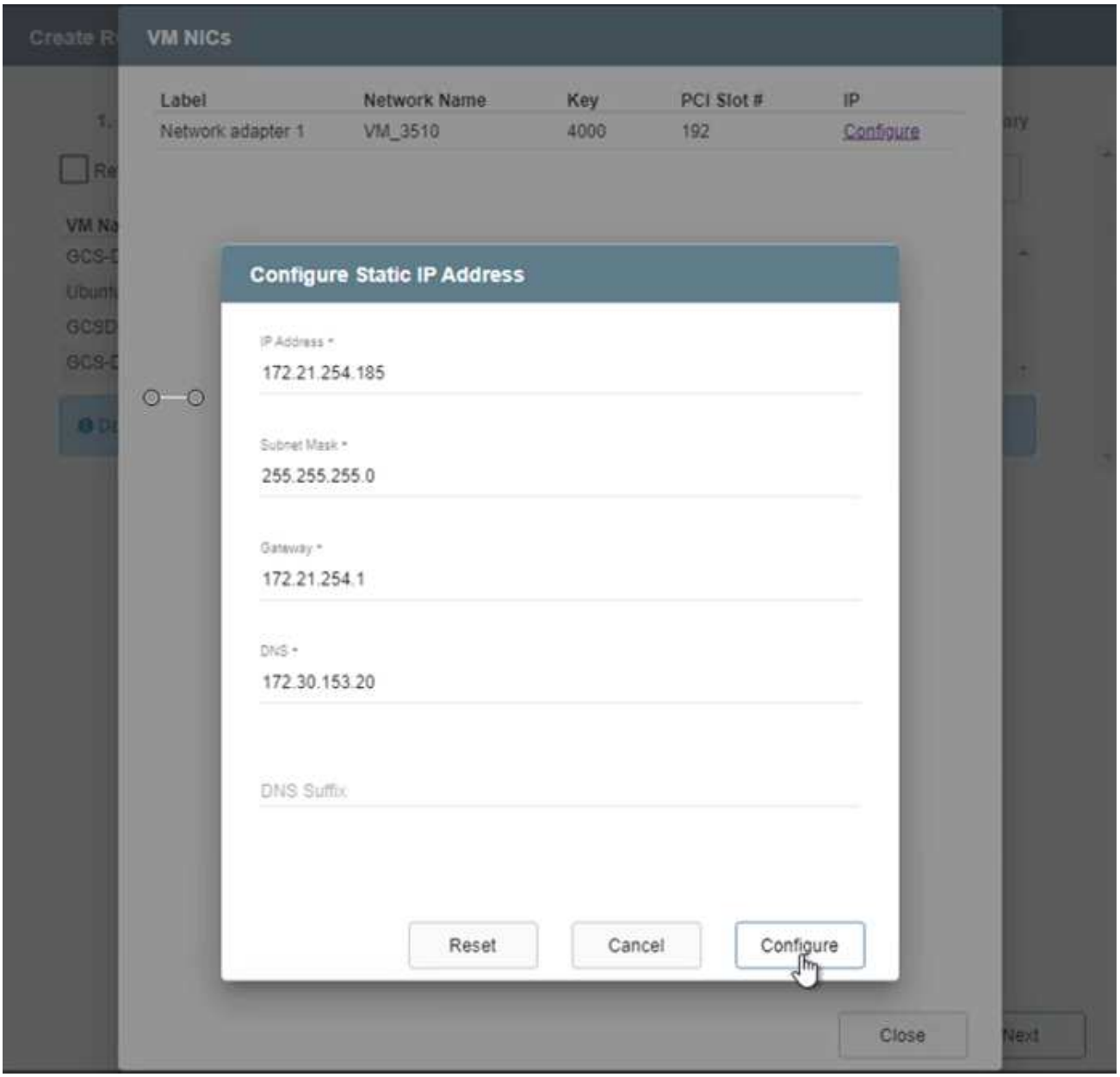
17. Edite la configuración de la máquina virtual según sea necesario. Especifique los parámetros para recuperar las máquinas virtuales, incluida la secuencia de arranque, el retraso de arranque (especificado en segundos), la cantidad de CPU y la cantidad de memoria a asignar. Cambie la secuencia de arranque de las máquinas virtuales haciendo clic en las flechas hacia arriba o hacia abajo. También se proporcionan opciones para conservar MAC.

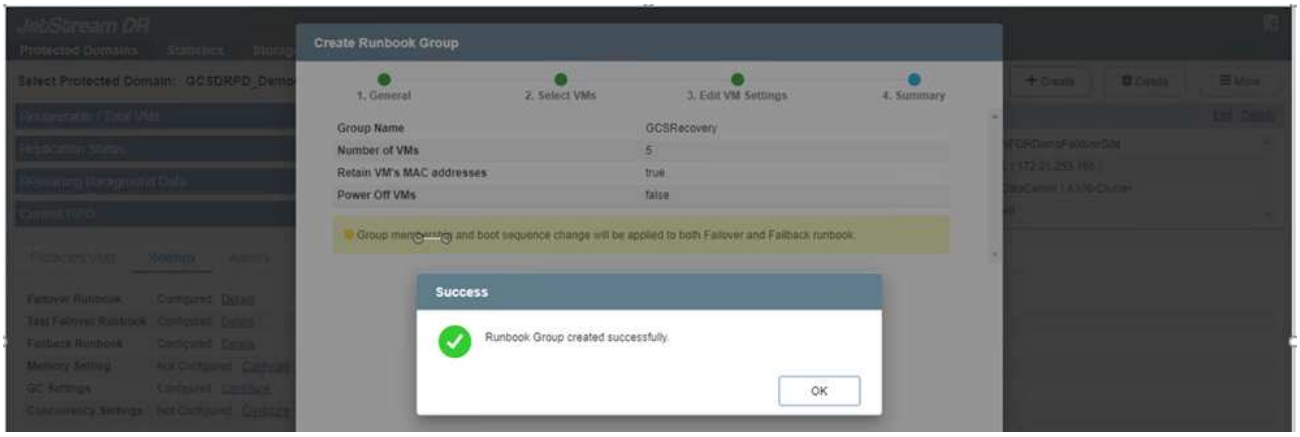


18. Las direcciones IP estáticas se pueden configurar manualmente para las máquinas virtuales individuales del grupo. Haga clic en el enlace Vista NIC de una VM para configurar manualmente sus ajustes de dirección IP.



19. Haga clic en el botón Configurar para guardar la configuración de NIC para las respectivas máquinas virtuales.





El estado de los libros de ejecución de conmutación por error y de recuperación ahora aparece como Configurado. Los grupos de libros de ejecución de conmutación por error y recuperación se crean en pares utilizando el mismo grupo inicial de máquinas virtuales y configuraciones. Si es necesario, es posible personalizar individualmente la configuración de cualquier grupo de runbooks haciendo clic en su enlace

Detalles correspondiente y realizando cambios.

▼ Instalar JetStream DR para AVS en la nube privada

Una práctica recomendada para un sitio de recuperación (AVS) es crear con anticipación un clúster piloto de tres nodos. Esto permite preconfigurar la infraestructura del sitio de recuperación, incluido lo siguiente:

- Segmentos de red de destino, firewalls, servicios como DHCP y DNS, etc.
- Instalación de JetStream DR para AVS
- Configuración de volúmenes ANF como almacenes de datos y más

JetStream DR admite un modo RTO casi cero para dominios de misión crítica. Para estos dominios, el almacenamiento de destino debe estar preinstalado. ANF es el tipo de almacenamiento recomendado en este caso.

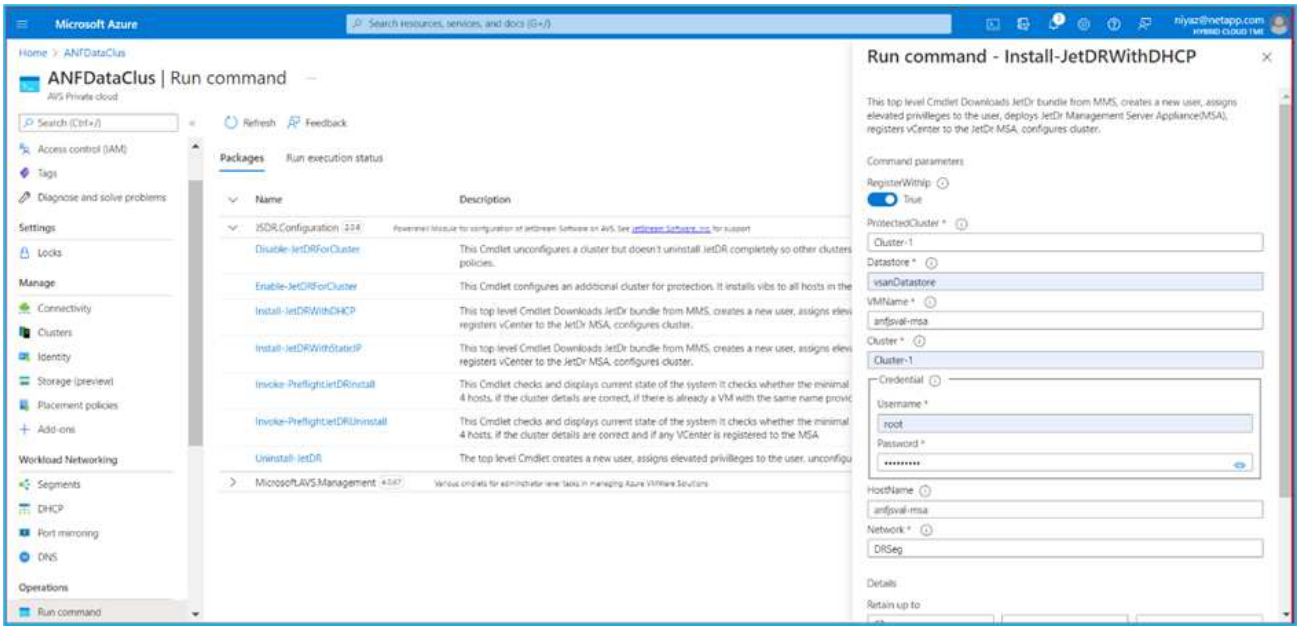
> La configuración de la red, incluida la creación de segmentos, debe configurarse en el clúster AVS para que coincida con los requisitos locales.

> Dependiendo de los requisitos de SLA y RTO, puede utilizar el modo de conmutación por error continuo o el modo de conmutación por error regular (estándar). Para un RTO cercano a cero, debe comenzar la rehidratación continua en el sitio de recuperación.

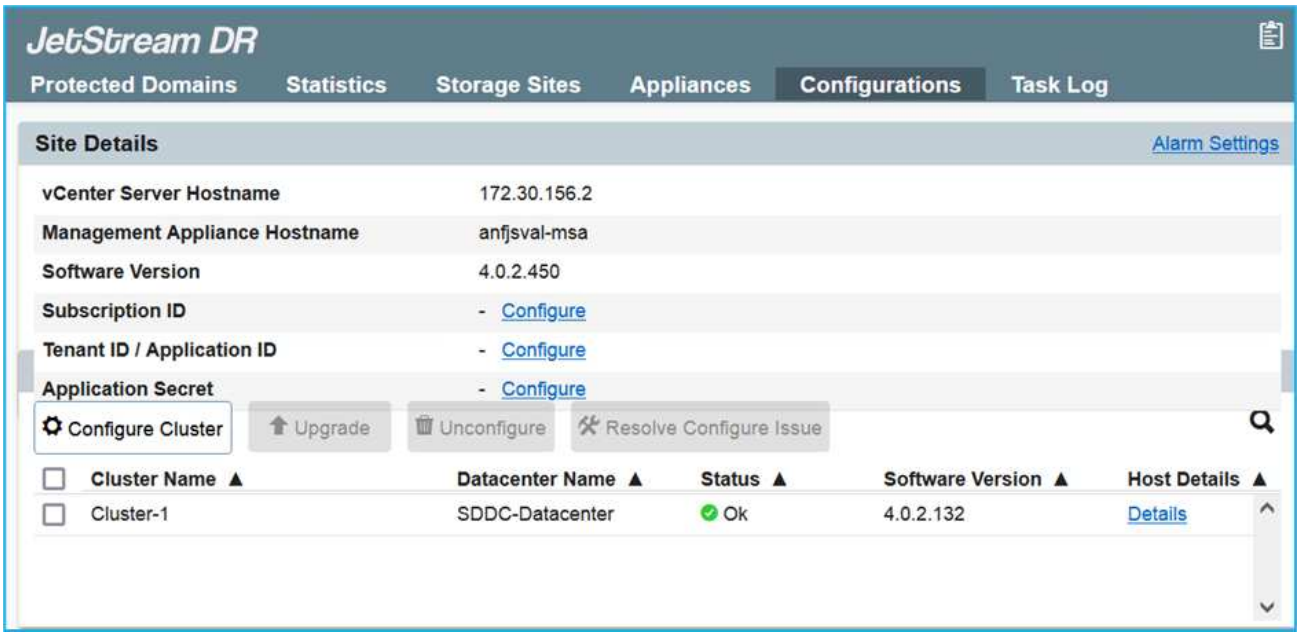
1. Para instalar JetStream DR para AVS en una nube privada de Azure VMware Solution, use el comando Ejecutar. Desde el portal de Azure, vaya a la solución Azure VMware, seleccione la nube privada y seleccione Ejecutar comando > Paquetes > JSDR.Configuration.

> El usuario CloudAdmin predeterminado de Azure VMware Solution no tiene privilegios suficientes para instalar JetStream DR para AVS. La solución Azure VMware permite una instalación simplificada y automatizada de JetStream DR invocando el comando Ejecutar de la solución Azure VMware para JetStream DR.

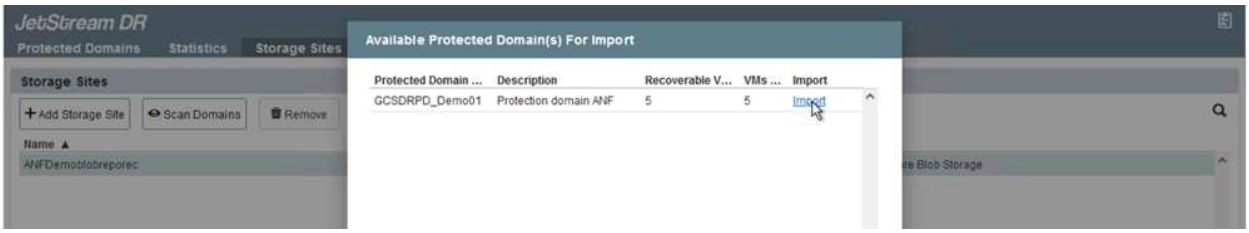
La siguiente captura de pantalla muestra la instalación utilizando una dirección IP basada en DHCP.



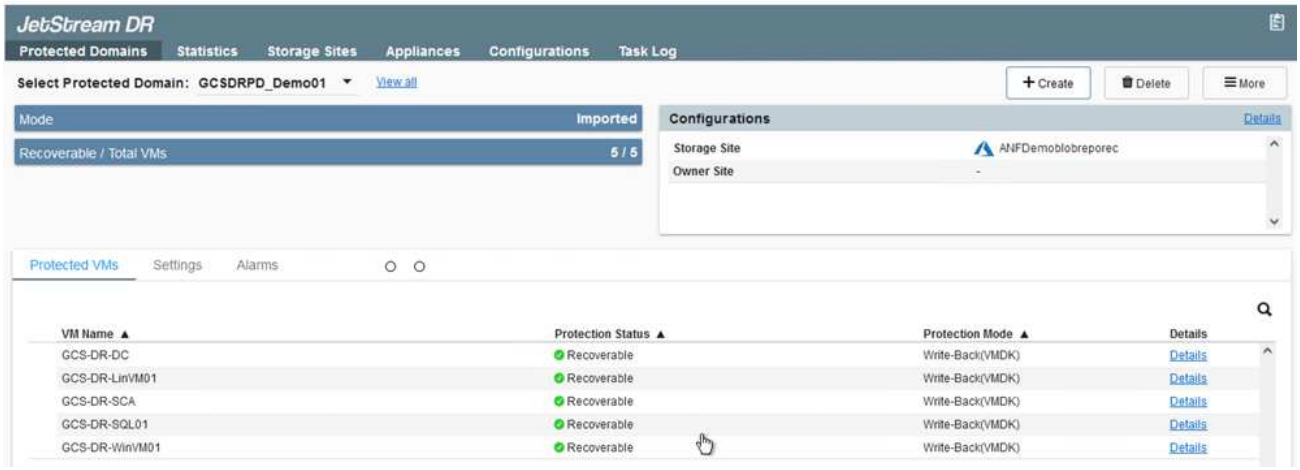
2. Una vez completada la instalación de JetStream DR para AVS, actualice el navegador. Para acceder a la interfaz de usuario de JetStream DR, vaya a SDDC Datacenter > Configurar > JetStream DR.



3. Desde la interfaz de JetStream DR, complete las siguientes tareas:
   a. Agregue la cuenta de Azure Blob Storage que se usó para proteger el clúster local como un sitio de almacenamiento y luego ejecute la opción Escanear dominios.
   b. En la ventana de diálogo emergente que aparece, seleccione el dominio protegido que desea importar y luego haga clic en su enlace Importar.



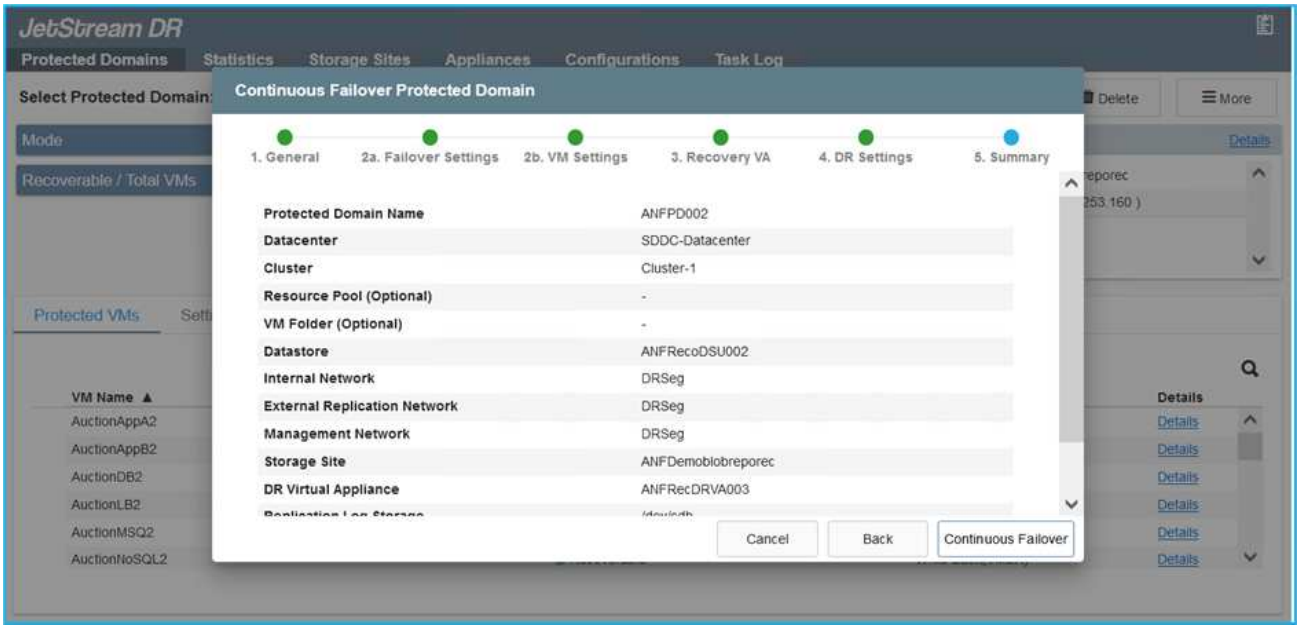
4. El dominio se importa para su recuperación. Vaya a la pestaña Dominios protegidos y verifique que se haya seleccionado el dominio deseado o elija el deseado en el menú Seleccionar dominio protegido. Se muestra una lista de las máquinas virtuales recuperables en el dominio protegido.



5. Una vez importados los dominios protegidos, implemente los dispositivos DRVA.

Estos pasos también se pueden automatizar utilizando planes creados por CPT.

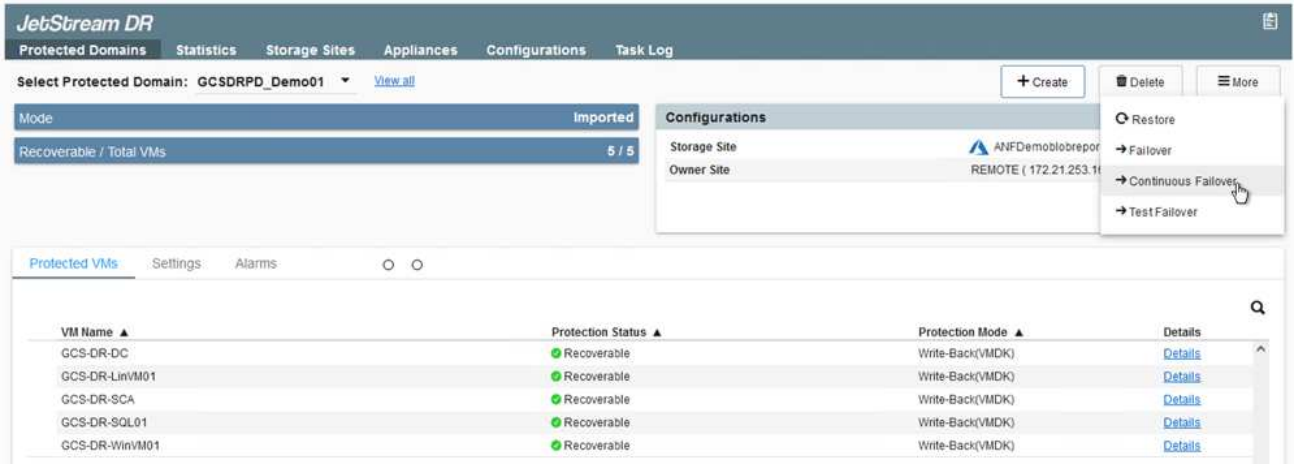
6. Cree volúmenes de registro de replicación utilizando almacenes de datos vSAN o ANF disponibles.
7. Importe los dominios protegidos y configure el VA de recuperación para utilizar un almacén de datos ANF para las ubicaciones de VM.



Asegúrese de que DHCP esté habilitado en el segmento seleccionado y que haya suficientes IP disponibles. Las IP dinámicas se utilizan temporalmente mientras los dominios se recuperan. Cada VM en recuperación (incluida la rehidratación continua) requiere una IP dinámica individual. Una vez completada la recuperación, la IP se libera y se puede reutilizar.

8. Seleccione la opción de conmutación por error adecuada (conmutación por error continua o conmutación por error). En este ejemplo, se selecciona la rehidratación continua (conmutación por error continua).

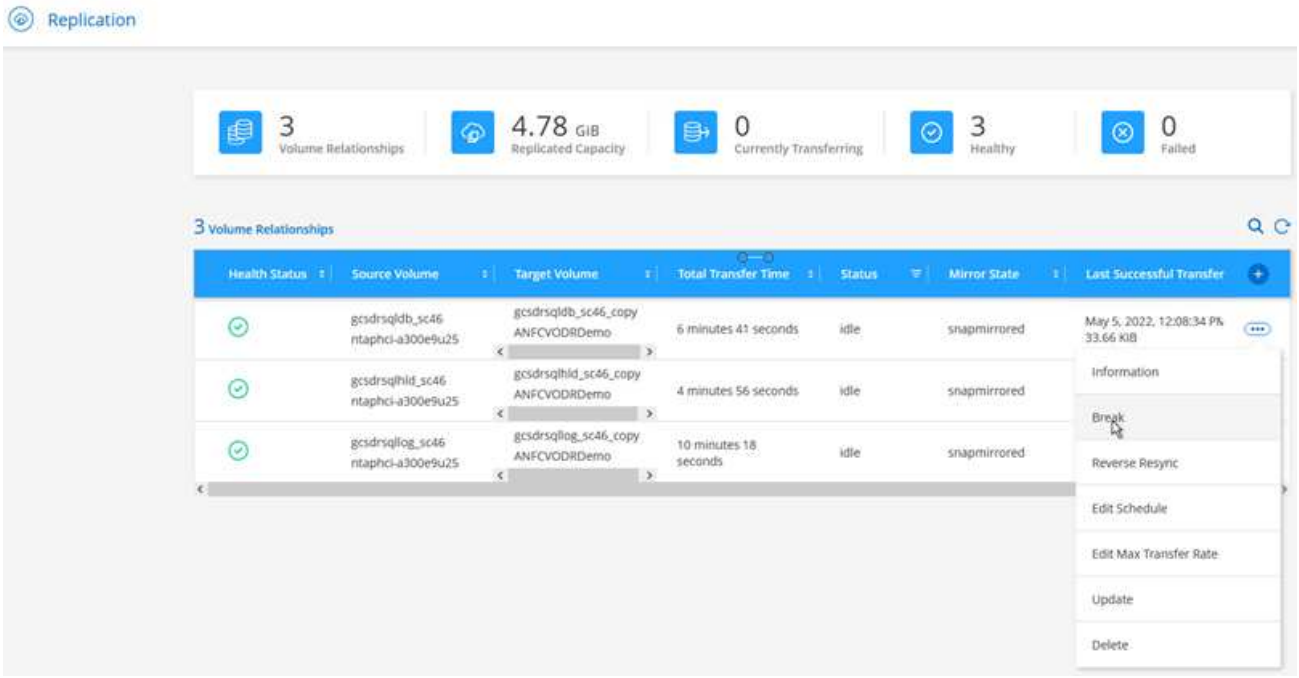
Aunque los modos de conmutación por error continua y conmutación por error difieren en cuanto al momento en que se realiza la configuración, ambos modos de conmutación por error se configuran utilizando los mismos pasos. Los pasos de conmutación por error se configuran y se ejecutan juntos en respuesta a un evento de desastre. La conmutación por error continua se puede configurar en cualquier momento y luego permitir que se ejecute en segundo plano durante el funcionamiento normal del sistema. Después de que ocurre un evento de desastre, se completa una conmutación por error continua para transferir de inmediato la propiedad de las máquinas virtuales protegidas al sitio de recuperación (RTO cercano a cero).

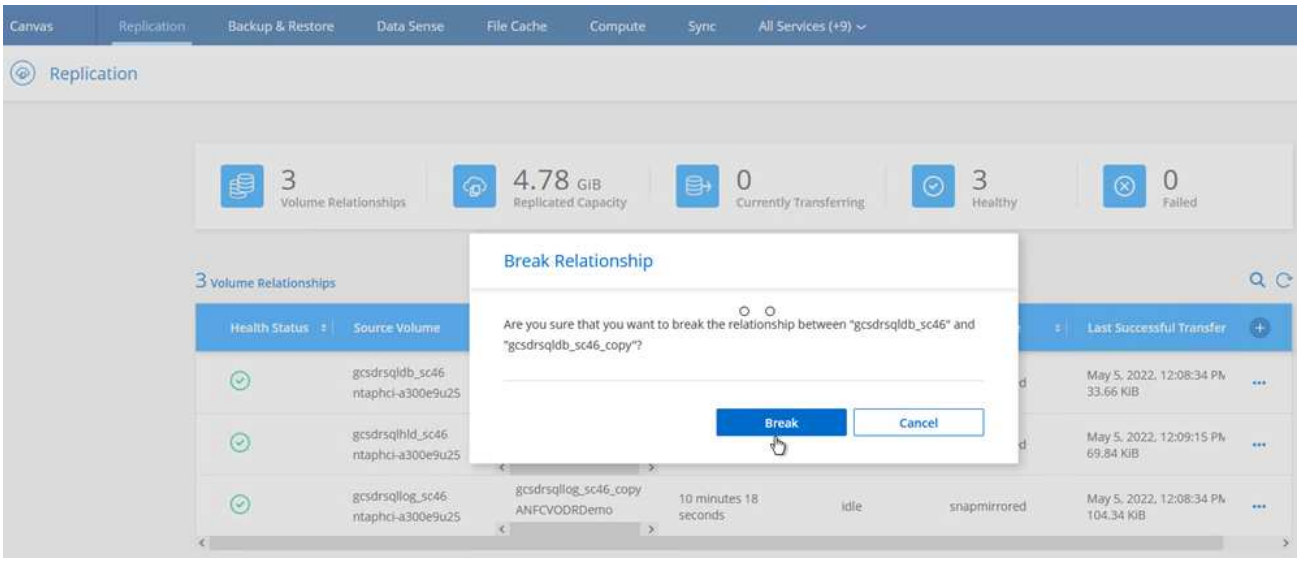


Comienza el proceso de conmutación por error continua y su progreso se puede supervisar desde la interfaz de usuario. Al hacer clic en el ícono azul en la sección Paso actual, se abre una ventana emergente que muestra detalles del paso actual del proceso de conmutación por error.

▼ **Conmutación por error y recuperación**

1. Después de que ocurre un desastre en el clúster protegido del entorno local (falla parcial o completa), puede activar la conmutación por error para las máquinas virtuales mediante Jetstream después de romper la relación SnapMirror para los respectivos volúmenes de la aplicación.

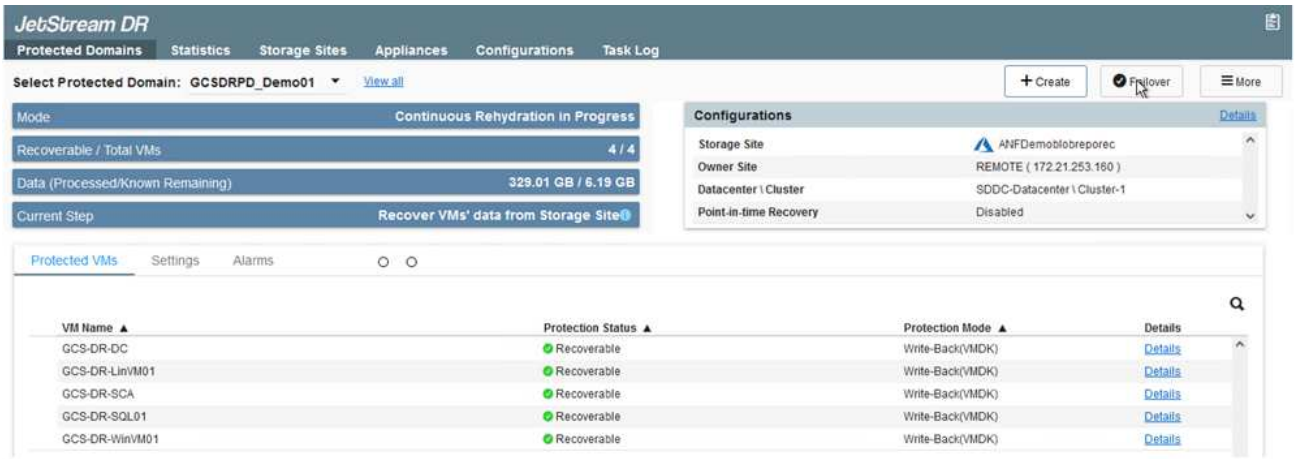


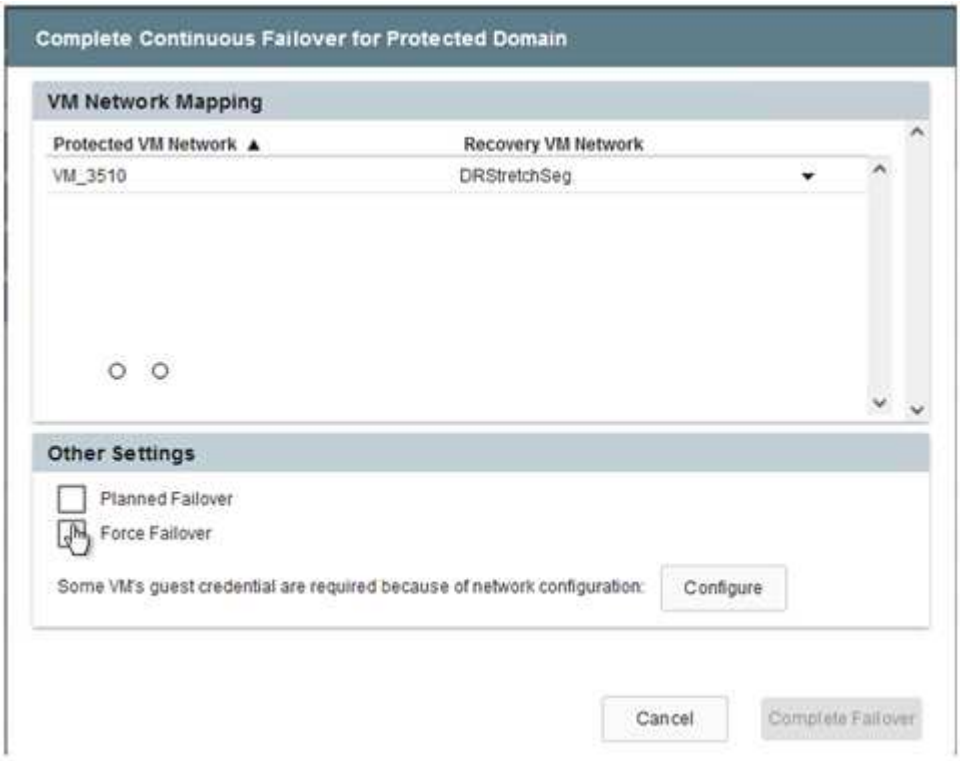


Este paso se puede automatizar fácilmente para facilitar el proceso de recuperación.

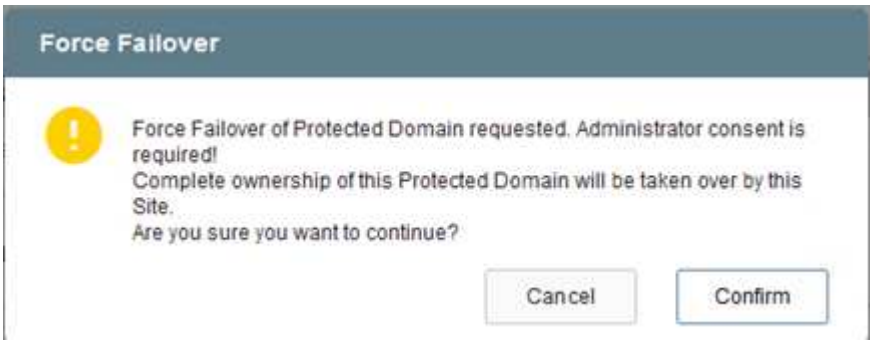
2. Acceda a la interfaz de usuario de Jetstream en AVS SDDC (lado de destino) y active la opción de conmutación por error para completar la conmutación por error. La barra de tareas muestra el progreso de las actividades de conmutación por error.

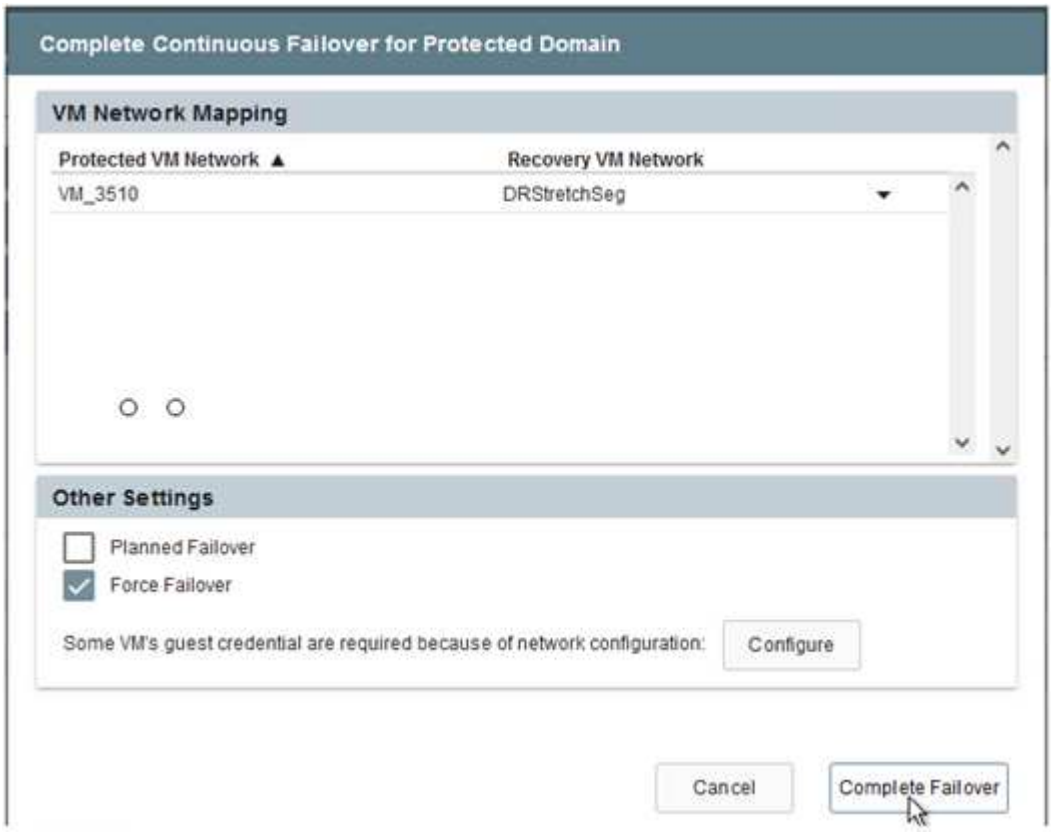
   En la ventana de diálogo que aparece al completar la conmutación por error, se puede especificar la tarea de conmutación por error como planificada o asumir que será forzada.





La conmutación por error forzada supone que el sitio principal ya no es accesible y que la propiedad del dominio protegido debe ser asumida directamente por el sitio de recuperación.





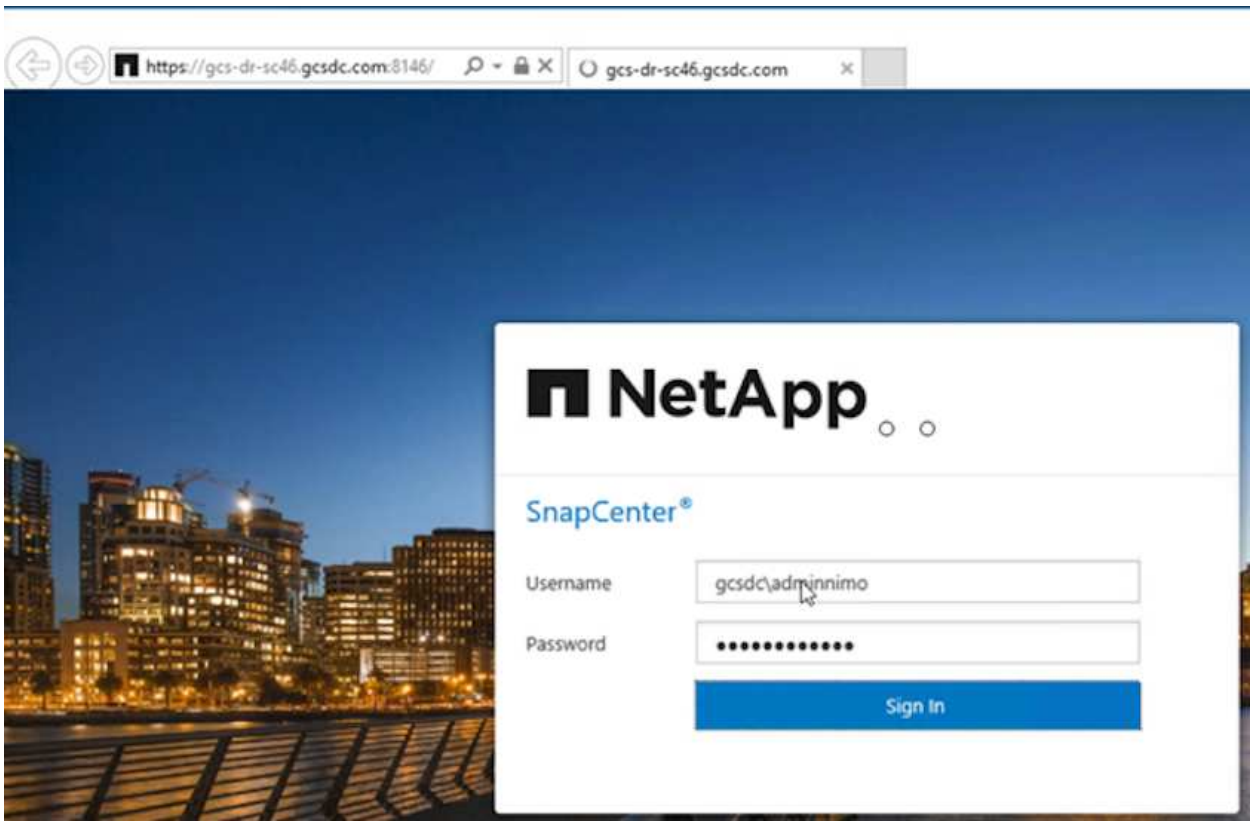
3. Una vez completada la conmutación por error continua, aparece un mensaje que confirma la finalización de la tarea. Una vez completada la tarea, acceda a las máquinas virtuales recuperadas para configurar sesiones ISCSI o NFS.

El modo de conmutación por error cambia a Ejecutándose en conmutación por error y el estado de la VM es Recuperable. Todas las máquinas virtuales del dominio protegido ahora se están ejecutando en el sitio de recuperación en el estado especificado por la configuración del libro de ejecución de conmutación por error.

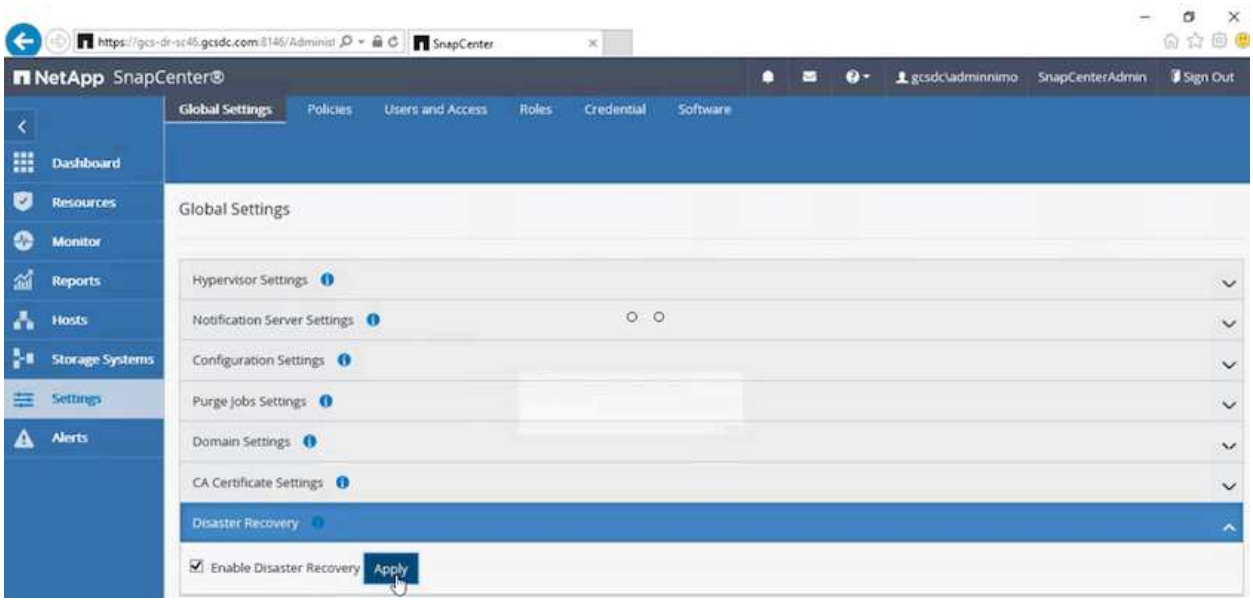
Para verificar la configuración y la infraestructura de conmutación por error, JetStream DR se puede utilizar en modo de prueba (opción de conmutación por error de prueba) para observar la recuperación de las máquinas virtuales y sus datos desde el almacén de objetos a un entorno de recuperación de prueba. Cuando se ejecuta un procedimiento de conmutación por error en modo de prueba, su funcionamiento se asemeja a un proceso de conmutación por error real.



4. Una vez recuperadas las máquinas virtuales, utilice la recuperación ante desastres de almacenamiento para el almacenamiento invitado. Para demostrar este proceso, en este ejemplo se utiliza el servidor SQL.
5. Inicie sesión en la máquina virtual SnapCenter recuperada en AVS SDDC y habilite el modo DR.
   a. Acceda a la interfaz de usuario de SnapCenter mediante el navegadorN.



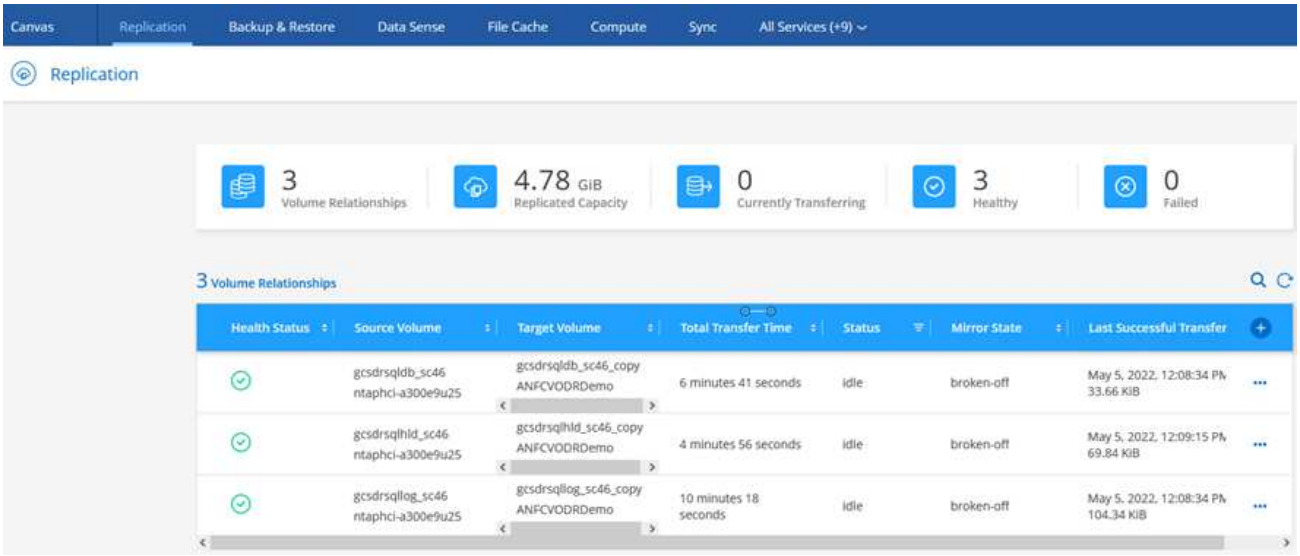
   b. En la página de Configuración, navegue a Configuración > Configuración global > Recuperación ante desastres.
   c. Seleccione Habilitar recuperación ante desastres.
   d. Haga clic en Aplicar.



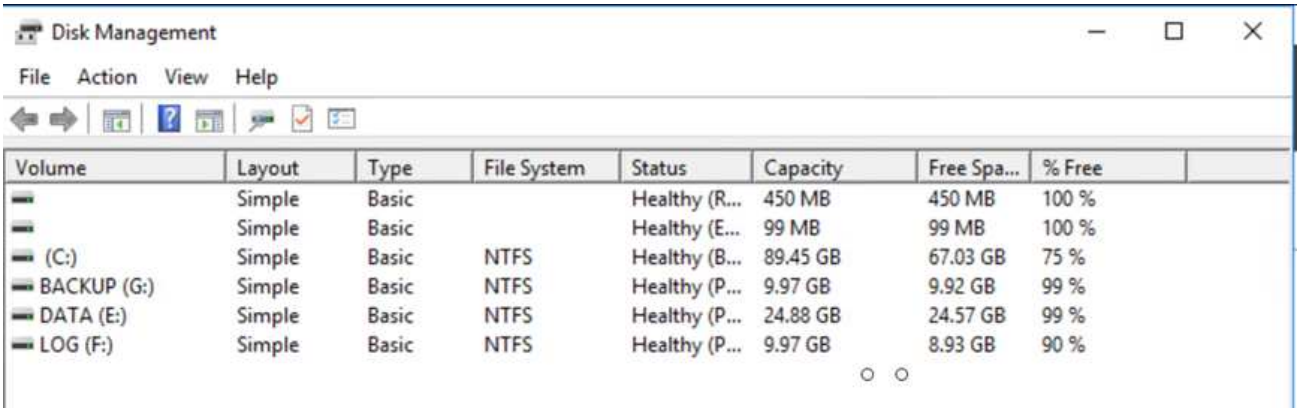
e. Verifique si el trabajo de DR está habilitado haciendo clic en Monitorear > Trabajos.

> Se debe utilizar NetApp SnapCenter 4.6 o posterior para la recuperación ante desastres de almacenamiento. Para versiones anteriores, se deben utilizar instantáneas consistentes con la aplicación (replicadas mediante SnapMirror) y se debe ejecutar una recuperación manual en caso de que se deban recuperar copias de seguridad anteriores en el sitio de recuperación ante desastres.

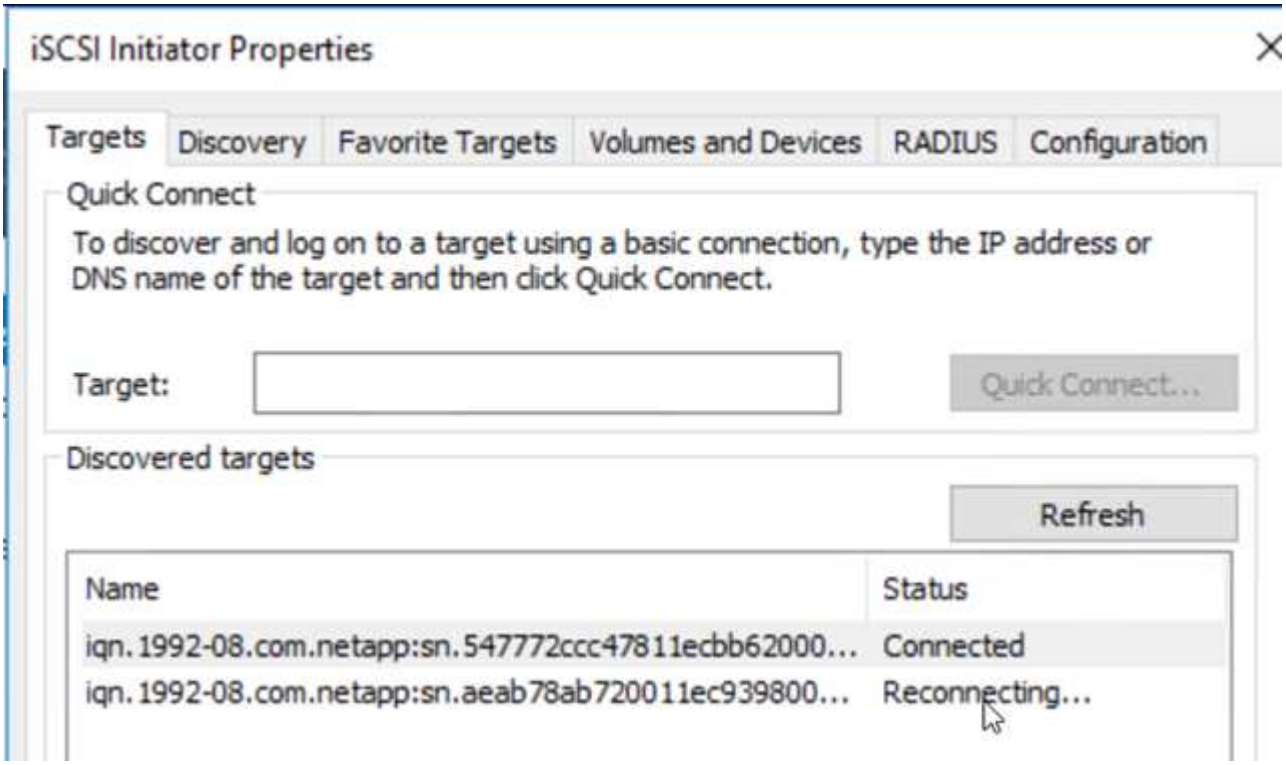
6. Asegúrese de que la relación SnapMirror esté rota.



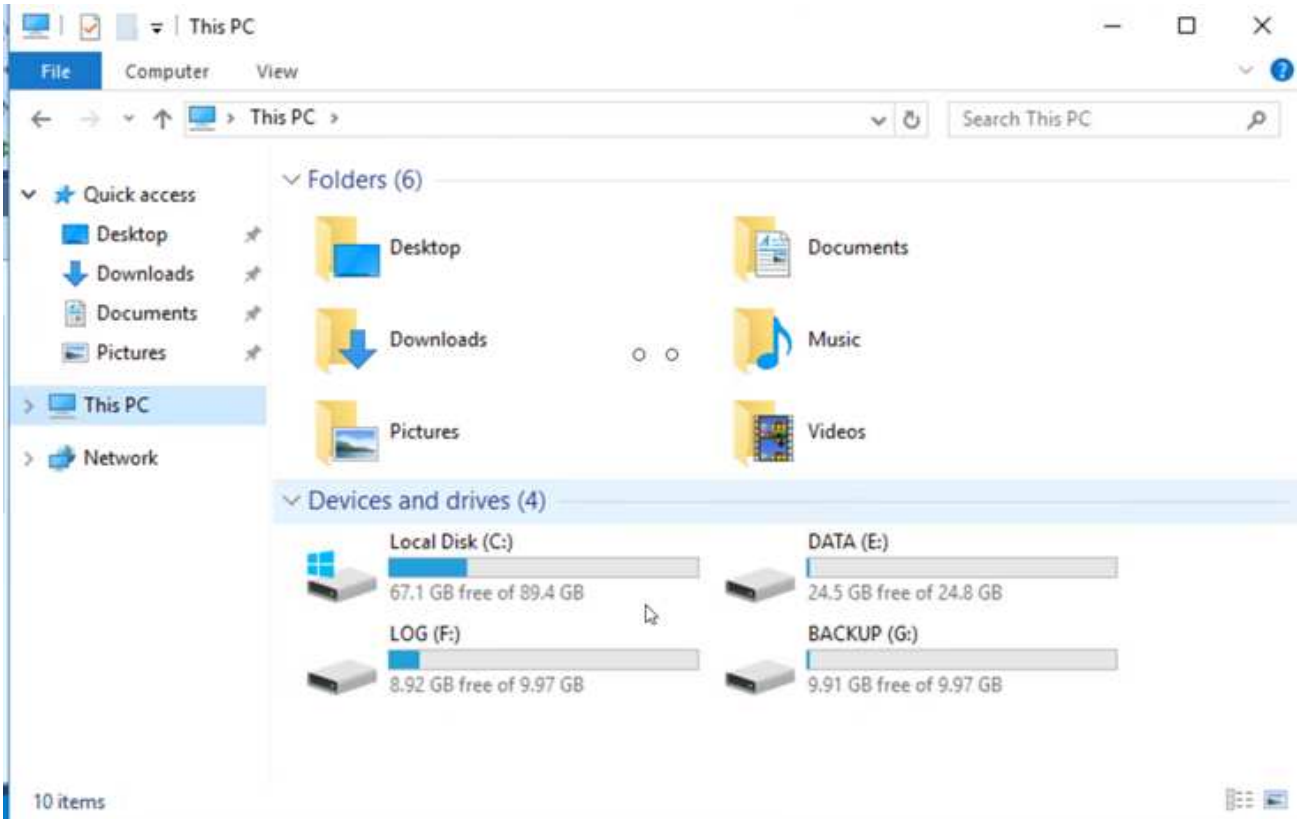
7. Adjunte el LUN de Cloud Volumes ONTAP a la máquina virtual invitada SQL recuperada con las mismas letras de unidad.



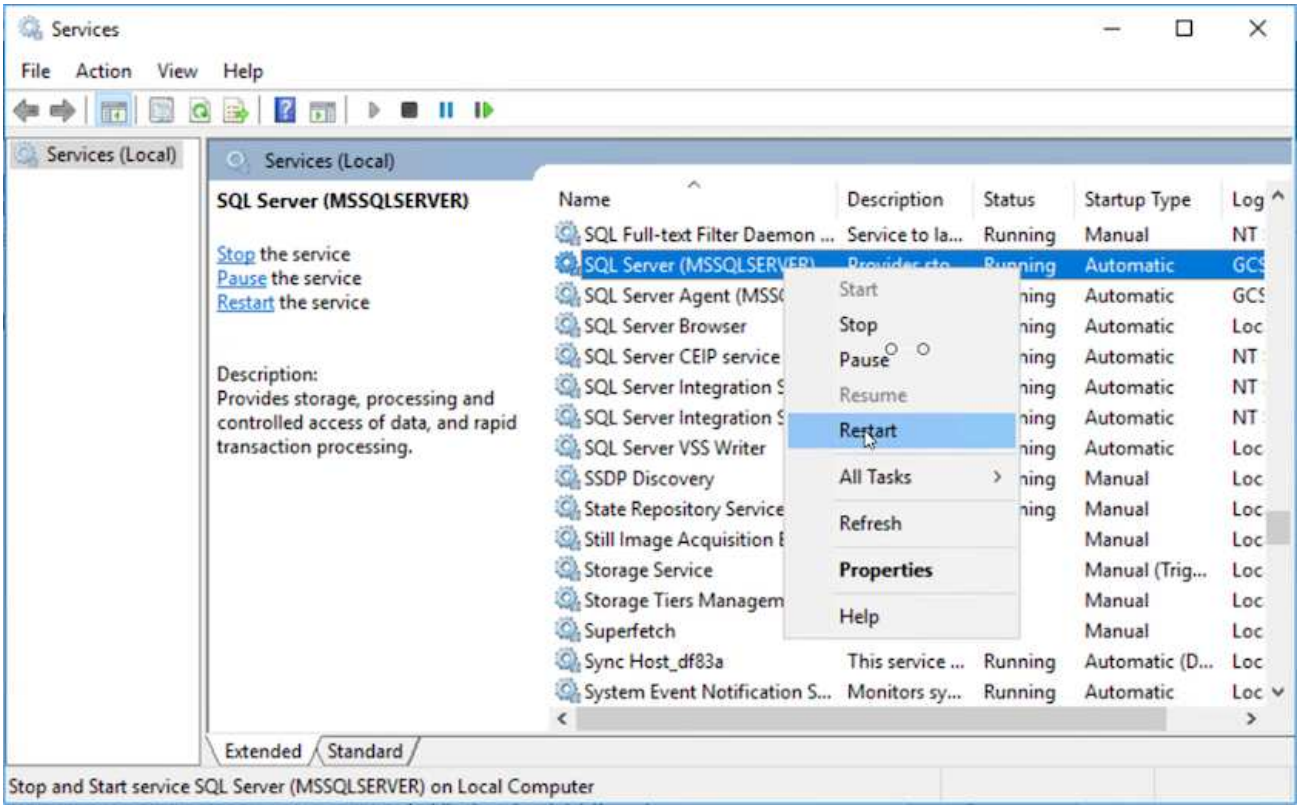
8. Abra el iniciador iSCSI, borre la sesión desconectada anterior y agregue el nuevo destino junto con la ruta múltiple para los volúmenes de Cloud Volumes ONTAP replicados.



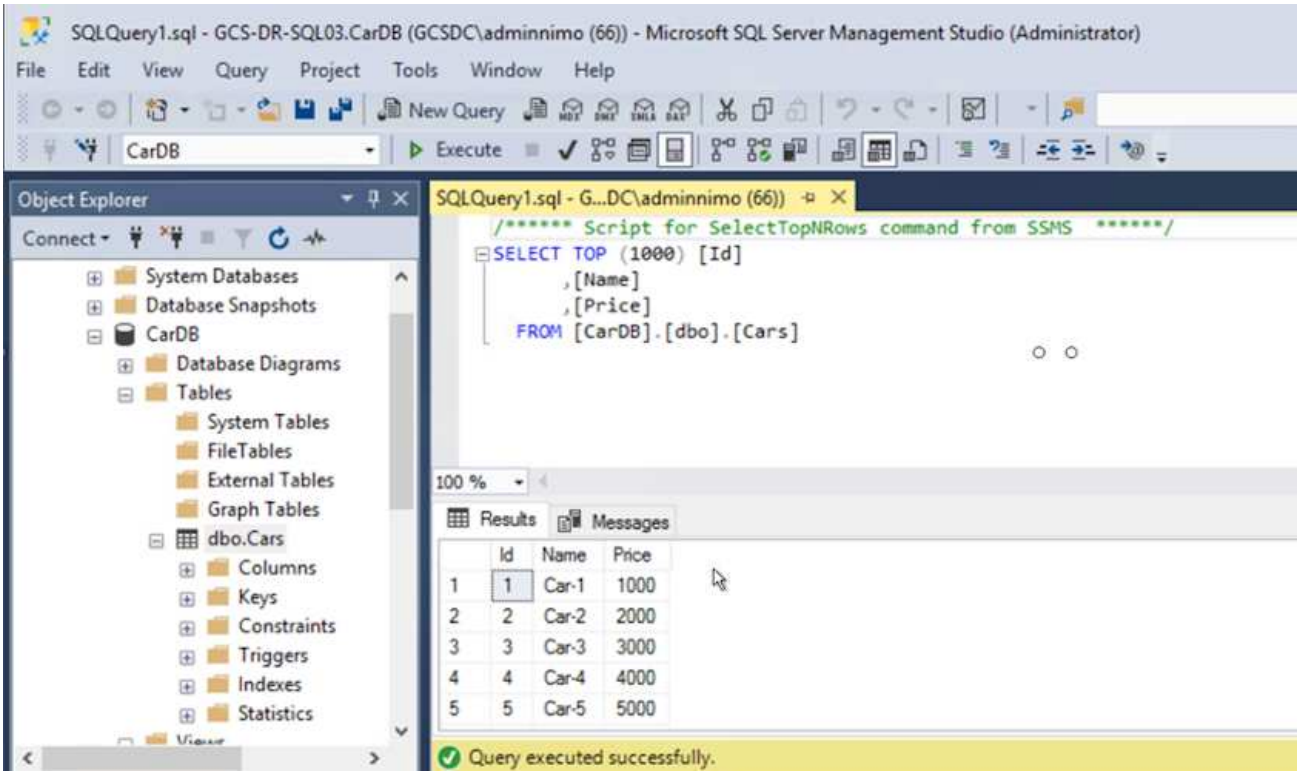
9. Asegúrese de que todos los discos estén conectados utilizando las mismas letras de unidad que se usaron antes de la recuperación ante desastres.



10. Reinicie el servicio del servidor MSSQL.



11. Asegúrese de que los recursos de SQL vuelvan a estar en línea.



En el caso de NFS, adjunte los volúmenes usando el comando mount y actualice el `/etc/fstab` entradas.

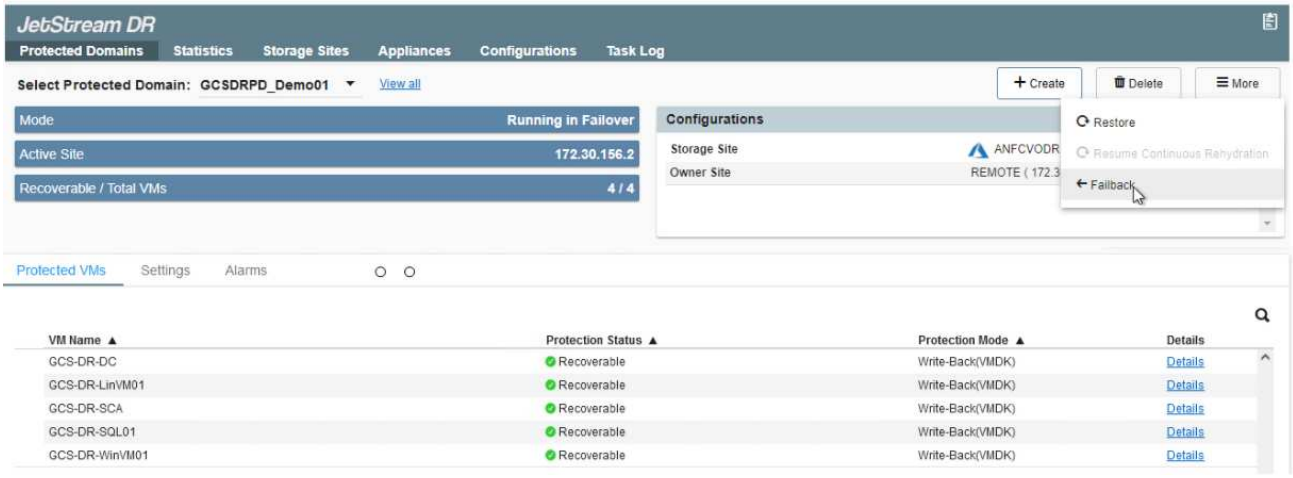
En este punto, las operaciones pueden ejecutarse y el negocio continúa normalmente.

En el extremo NSX-T, se puede crear una puerta de enlace de nivel 1 dedicada e independiente para simular escenarios de conmutación por error. Esto garantiza que todas las cargas de trabajo puedan comunicarse entre sí, pero que ningún tráfico pueda entrar o salir del entorno, de modo que cualquier tarea de clasificación, contención o refuerzo se pueda realizar sin riesgo de contaminación cruzada. Esta operación está fuera del alcance de este documento, pero se puede lograr fácilmente para simular el aislamiento.

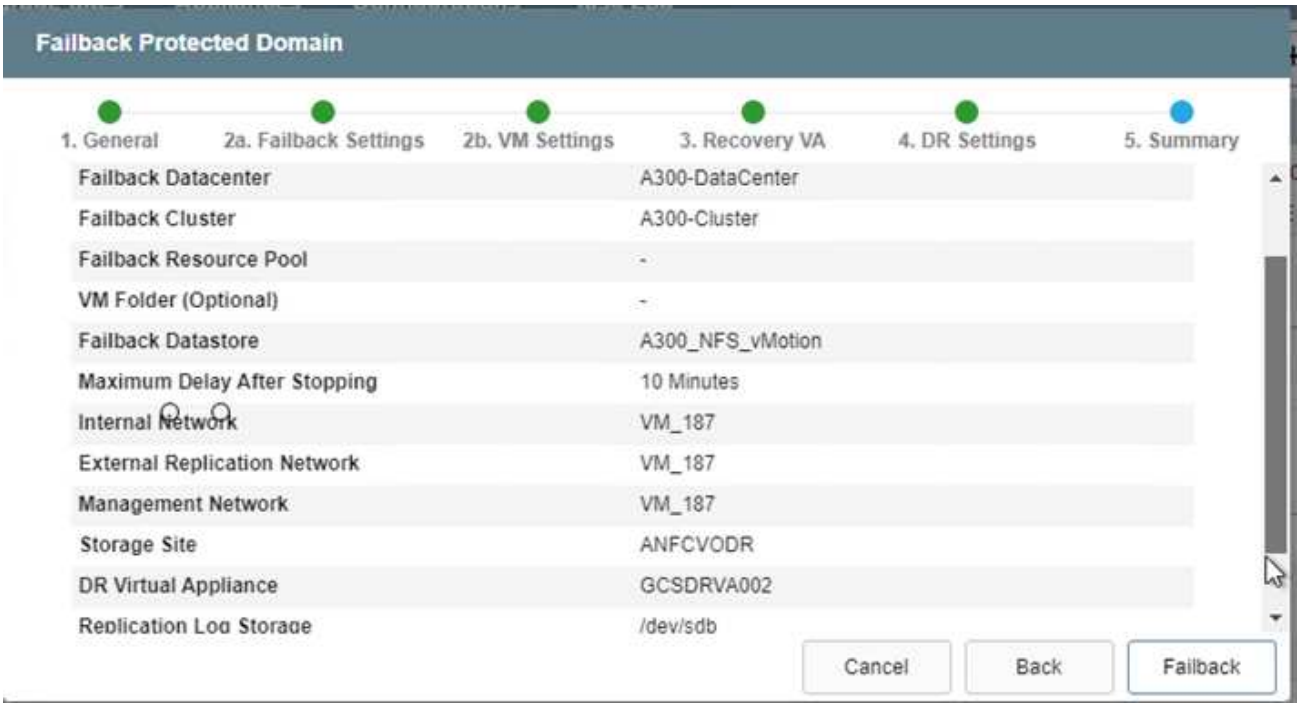
Una vez que el sitio principal esté funcionando nuevamente, puedes realizar una conmutación por error. Jetstream reanuda la protección de la máquina virtual y se debe revertir la relación de SnapMirror .

1. Restaurar el entorno local. Dependiendo del tipo de incidente de desastre, podría ser necesario restaurar y/o verificar la configuración del clúster protegido. Si es necesario, es posible que sea necesario reinstalar el software JetStream DR.
2. Acceda al entorno local restaurado, vaya a la interfaz de usuario de Jetstream DR y seleccione el dominio protegido adecuado. Una vez que el sitio protegido esté listo para la conmutación por recuperación, seleccione la opción Conmutación por recuperación en la interfaz de usuario.

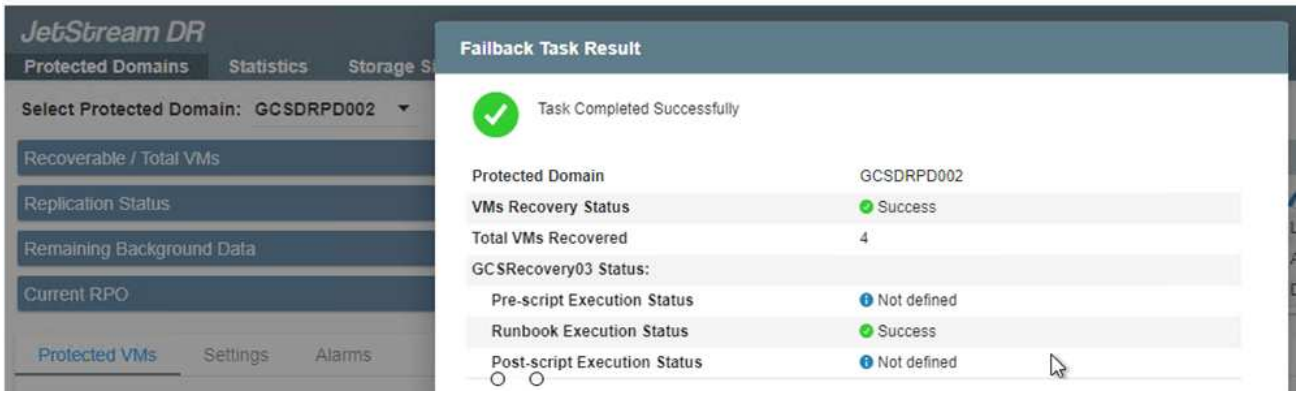
El plan de conmutación por error generado por CPT también se puede utilizar para iniciar el retorno de las máquinas virtuales y sus datos desde el almacén de objetos al entorno VMware original.



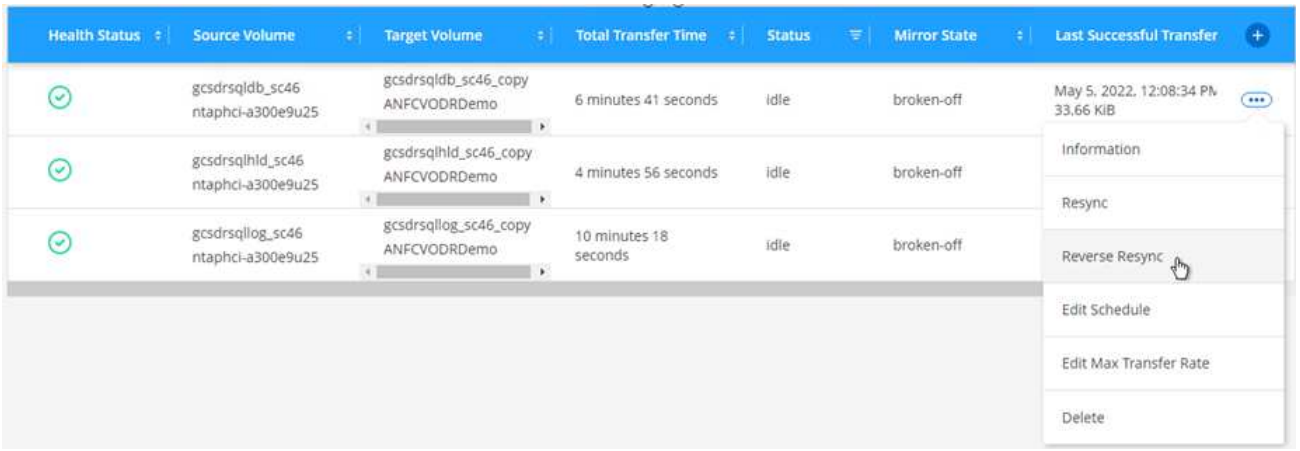
Especifique el retraso máximo después de pausar las máquinas virtuales en el sitio de recuperación y reiniciarlas en el sitio protegido. El tiempo necesario para completar este proceso incluye la finalización de la replicación después de detener las máquinas virtuales de conmutación por error, el tiempo necesario para limpiar el sitio de recuperación y el tiempo necesario para recrear las máquinas virtuales en el sitio protegido. NetApp recomienda 10 minutos.

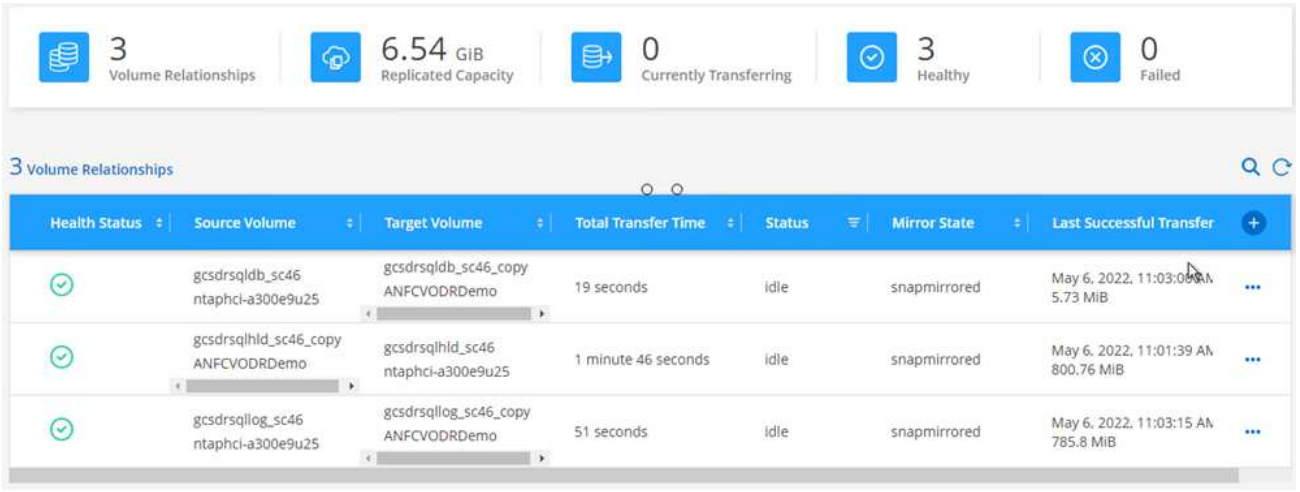


3. Complete el proceso de conmutación por error y luego confirme la reanudación de la protección de la máquina virtual y la consistencia de los datos.

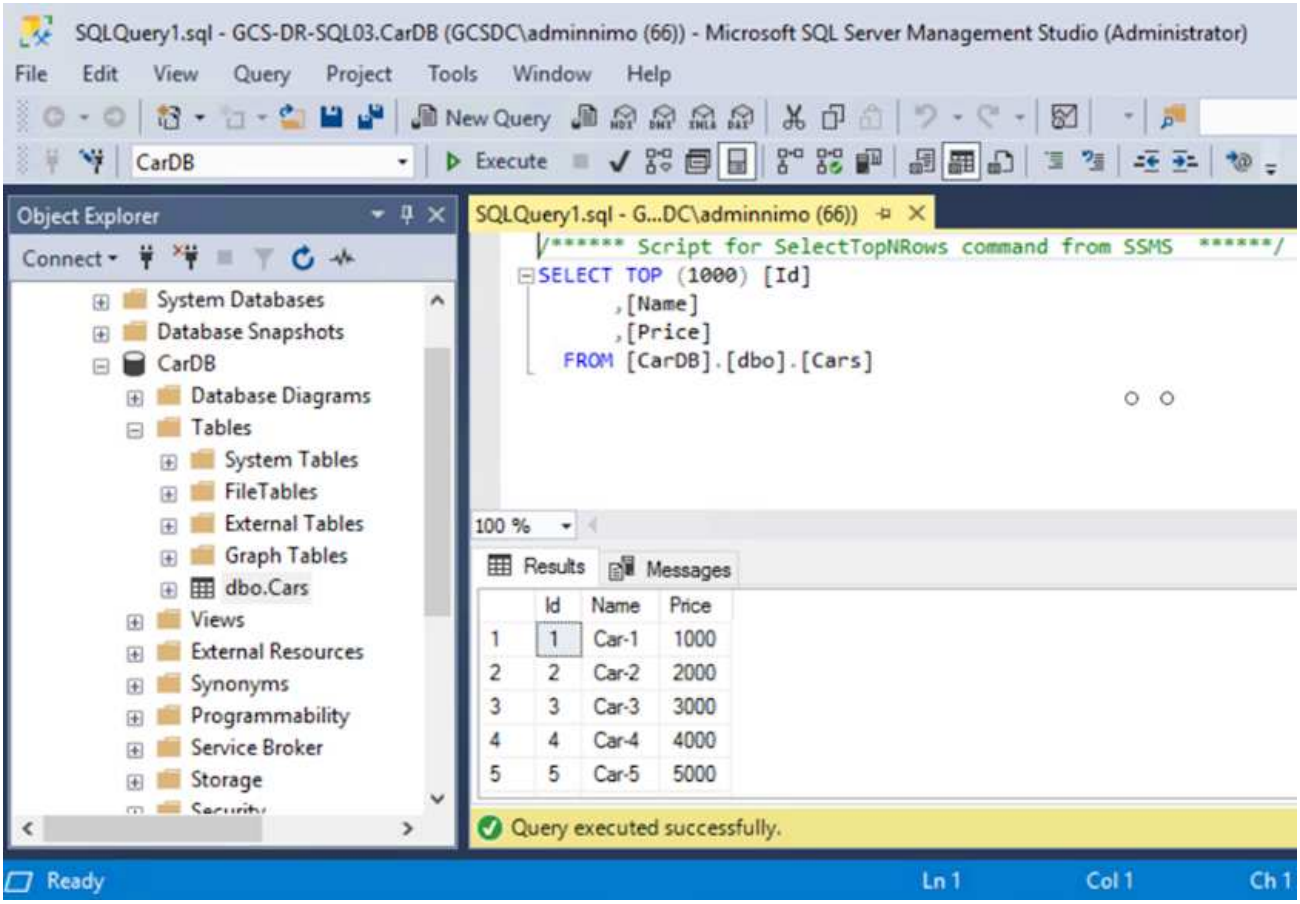


4. Una vez recuperadas las máquinas virtuales, desconecte el almacenamiento secundario del host y conéctese al almacenamiento primario.





5. Reinicie el servicio del servidor MSSQL.
6. Verifique que los recursos SQL estén nuevamente en línea.



Para volver al almacenamiento principal, asegúrese de que la dirección de la relación siga siendo la misma que antes de la conmutación por error realizando una operación de resincronización inversa.

Para conservar las funciones de almacenamiento primario y secundario después de la operación de resincronización inversa, realice la operación de resincronización inversa nuevamente.

Este proceso es aplicable a otras aplicaciones como Oracle, bases de datos similares y cualquier otra aplicación que utilice almacenamiento conectado a invitados.

Como siempre, pruebe los pasos necesarios para recuperar las cargas de trabajo críticas antes de trasladarlas a producción.

Beneficios de esta solución

- Utiliza la replicación eficiente y resistente de SnapMirror.
- Se recupera a cualquier punto disponible en el tiempo con retención de instantáneas ONTAP .
- La automatización completa está disponible para todos los pasos necesarios para recuperar cientos a miles de máquinas virtuales, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonación que no modifican el volumen replicado.
  - Esto evita el riesgo de corrupción de datos en volúmenes e instantáneas.
  - Evita interrupciones de replicación durante los flujos de trabajo de prueba de DR.

- Aprovecha los datos de DR para flujos de trabajo más allá de DR, como desarrollo y prueba, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas de remediación.

- La optimización de la CPU y la RAM puede ayudar a reducir los costos de la nube al permitir la recuperación a clústeres de cómputo más pequeños.

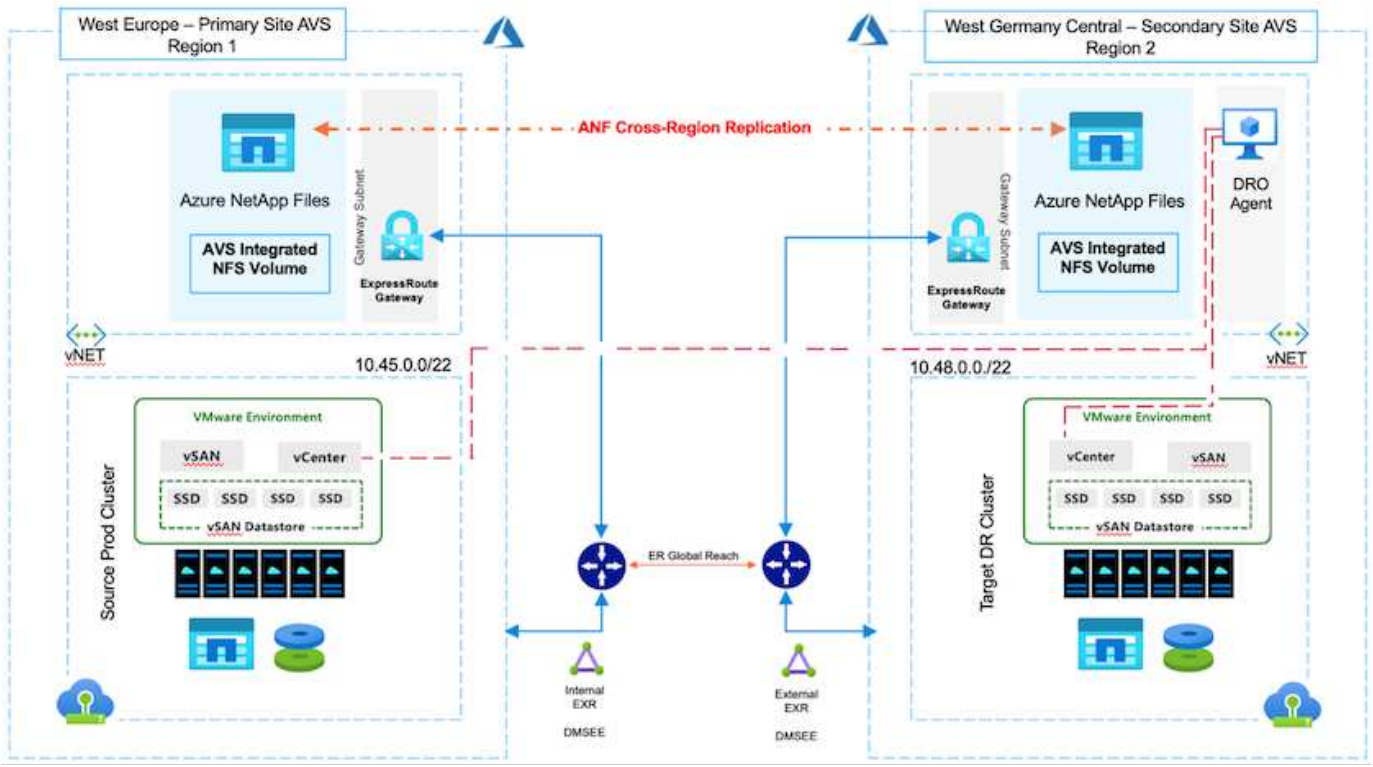
TR-4955: Recuperación ante desastres con Azure NetApp Files (ANF) y Azure VMware Solution (AVS)

La recuperación ante desastres mediante la replicación a nivel de bloques entre regiones dentro de la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos (por ejemplo, ransomware).

Descripción general

Con la replicación de volúmenes entre regiones de archivos Azure NetApp (ANF), las cargas de trabajo de VMware que se ejecutan en un sitio SDDC de Azure VMware Solution (AVS) que usa volúmenes de archivos Azure NetApp como un almacén de datos NFS en el sitio AVS principal se pueden replicar en un sitio AVS secundario designado en la región de recuperación de destino.

Disaster Recovery Orchestrator (DRO) (una solución con script y una interfaz de usuario) se puede utilizar para recuperar sin problemas cargas de trabajo replicadas de un SDDC de AVS a otro. DRO automatiza la recuperación interrumpiendo el emparejamiento de replicación y luego montando el volumen de destino como un almacén de datos, a través del registro de VM en AVS, hasta asignaciones de red directamente en NSX-T (incluido con todas las nubes privadas de AVS).



Prerrequisitos y recomendaciones generales

- Verifique que haya habilitado la replicación entre regiones mediante la creación de un emparejamiento de replicación. Ver "Crear replicación de volumen para Azure NetApp Files" .

- Debe configurar ExpressRoute Global Reach entre las nubes privadas de Azure VMware Solution de origen y destino.
- Debe tener una entidad de servicio que pueda acceder a los recursos.
- Se admite la siguiente topología: sitio AVS principal a sitio AVS secundario.
- Configurar el "replicación" Programe cada volumen de manera adecuada según las necesidades del negocio y la tasa de cambio de datos.

No se admiten topologías en cascada ni de entrada y salida en abanico.

Empezando

Implementar la solución VMware de Azure

El "Solución VMware de Azure" (AVS) es un servicio de nube híbrida que proporciona SDDC de VMware completamente funcionales dentro de una nube pública de Microsoft Azure. AVS es una solución propia totalmente administrada y respaldada por Microsoft y verificada por VMware que utiliza la infraestructura de Azure. Por lo tanto, los clientes obtienen VMware ESXi para la virtualización informática, vSAN para el almacenamiento hiperconvergente y NSX para redes y seguridad, todo ello mientras aprovechan la presencia global de Microsoft Azure, las instalaciones de centros de datos líderes en su clase y la proximidad al rico ecosistema de servicios y soluciones nativos de Azure. Una combinación de Azure VMware Solution SDDC y Azure NetApp Files proporciona el mejor rendimiento con una latencia de red mínima.

Para configurar una nube privada de AVS en Azure, siga los pasos de este"enlace" para la documentación de NetApp y en este "enlace" para la documentación de Microsoft. Se puede utilizar un entorno de luz piloto configurado con una configuración mínima para fines de recuperación ante desastres. Esta configuración solo contiene componentes básicos para soportar aplicaciones críticas, y puede escalar y generar más hosts para asumir la mayor parte de la carga si ocurre una conmutación por error.

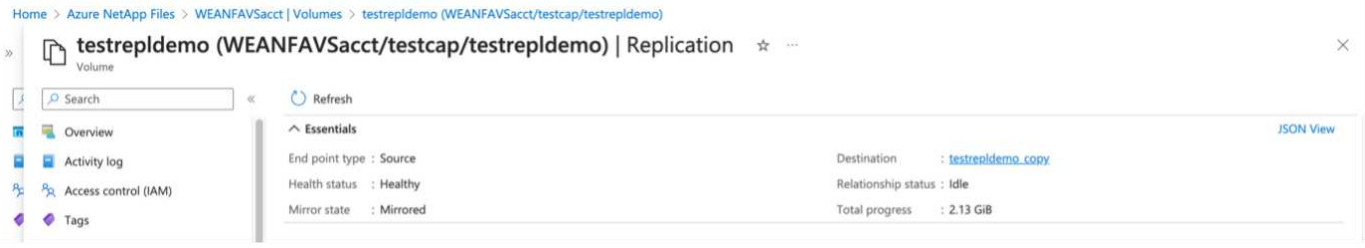
En la versión inicial, DRO admite un clúster SDDC de AVS existente. La creación de SDDC a pedido estará disponible en una próxima versión.

Aprovisionar y configurar Azure NetApp Files

"Azure NetApp Files"Es un servicio de almacenamiento de archivos medido, de clase empresarial y de alto rendimiento. Siga los pasos de este "enlace" para aprovisionar y configurar Azure NetApp Files como un almacén de datos NFS para optimizar las implementaciones de nube privada de AVS.

Crear replicación de volumen para volúmenes de almacén de datos con tecnología Azure NetApp Files

El primer paso es configurar la replicación entre regiones para los volúmenes de almacén de datos deseados desde el sitio principal de AVS al sitio secundario de AVS con las frecuencias y retenciones adecuadas.



Siga los pasos de este "enlace" para configurar la replicación entre regiones mediante la creación de un peering de replicación. El nivel de servicio del grupo de capacidad de destino puede coincidir con el del grupo

de capacidad de origen. Sin embargo, para este caso de uso específico, puede seleccionar el nivel de servicio estándar y luego "modificar el nivel de servicio" en caso de un desastre real o simulaciones de DR.

Una relación de replicación entre regiones es un requisito previo y debe crearse de antemano.

Instalación de DRO

Para comenzar a utilizar DRO, use el sistema operativo Ubuntu en la máquina virtual de Azure designada y asegúrese de cumplir con los requisitos previos. Luego instala el paquete.

Prerrequisitos:

- Principal de servicio que puede acceder a los recursos.
- Asegúrese de que exista conectividad adecuada con las instancias de SDDC y de Azure NetApp Files de origen y destino.
- La resolución de DNS debe estar implementada si está utilizando nombres DNS. De lo contrario, utilice direcciones IP para vCenter.

Requisitos del sistema operativo:

- Ubuntu Focal 20.04 (LTS)Los siguientes paquetes deben instalarse en la máquina virtual del agente designado:
- Docker
- Docker-componer
- JqChange `docker.sock` A este nuevo permiso: `sudo chmod 666 /var/run/docker.sock` .

El `deploy.sh` El script ejecuta todos los requisitos previos necesarios.

Los pasos son los siguientes:

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

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

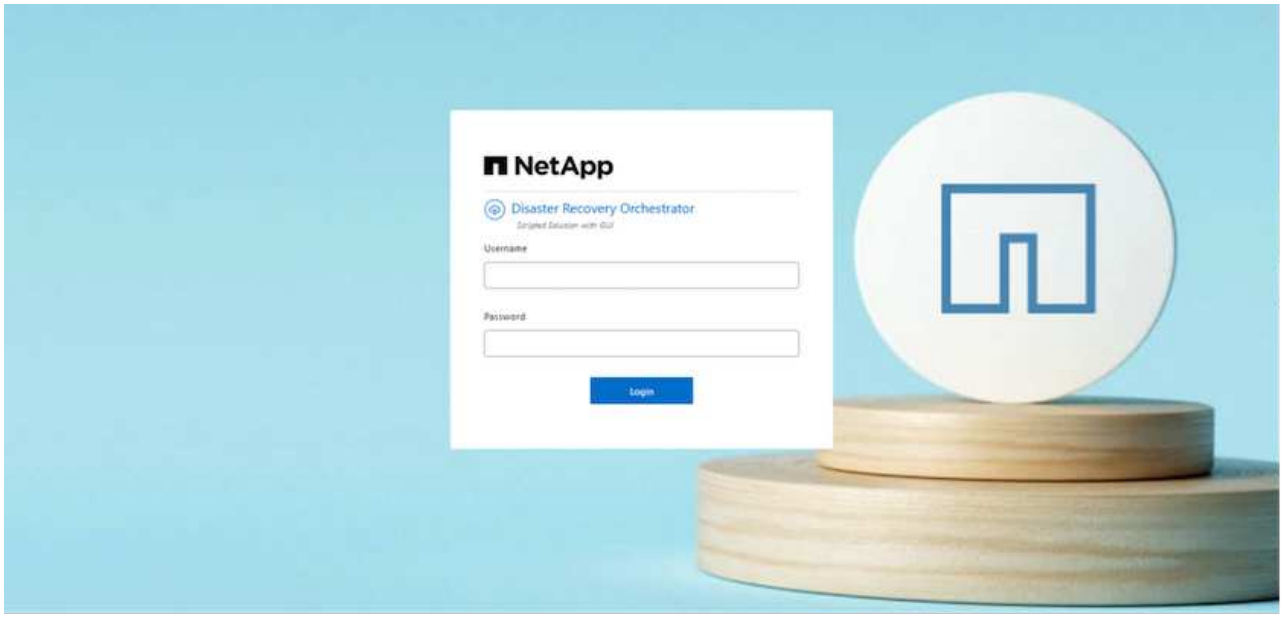
El agente debe instalarse en la región del sitio AVS secundario o en la región del sitio AVS primario en una zona de disponibilidad (AZ) separada del SDDC.

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

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Acceda a la interfaz de usuario utilizando las siguientes credenciales:
   - Nombre de usuario: `admin`

- Contraseña: `admin`



Configuración de DRO

Una vez que Azure NetApp Files y AVS se hayan configurado correctamente, puede comenzar a configurar DRO para automatizar la recuperación de cargas de trabajo desde el sitio de AVS principal al sitio de AVS secundario. NetApp recomienda implementar el agente DRO en el sitio AVS secundario y configurar la conexión de puerta de enlace de ExpressRoute para que el agente DRO pueda comunicarse a través de la red con los componentes AVS y Azure NetApp Files adecuados.

El primer paso es agregar credenciales. DRO requiere permiso para descubrir Azure NetApp Files y Azure VMware Solution. Puede otorgar los permisos necesarios a una cuenta de Azure creando y configurando una aplicación de Azure Active Directory (AD) y obteniendo las credenciales de Azure que DRO necesita. Debe vincular la entidad de servicio a su suscripción de Azure y asignarle un rol personalizado que tenga los permisos necesarios correspondientes. Cuando agrega entornos de origen y destino, se le solicita que seleccione las credenciales asociadas con la entidad de servicio. Debe agregar estas credenciales a DRO antes de poder hacer clic en Agregar nuevo sitio.

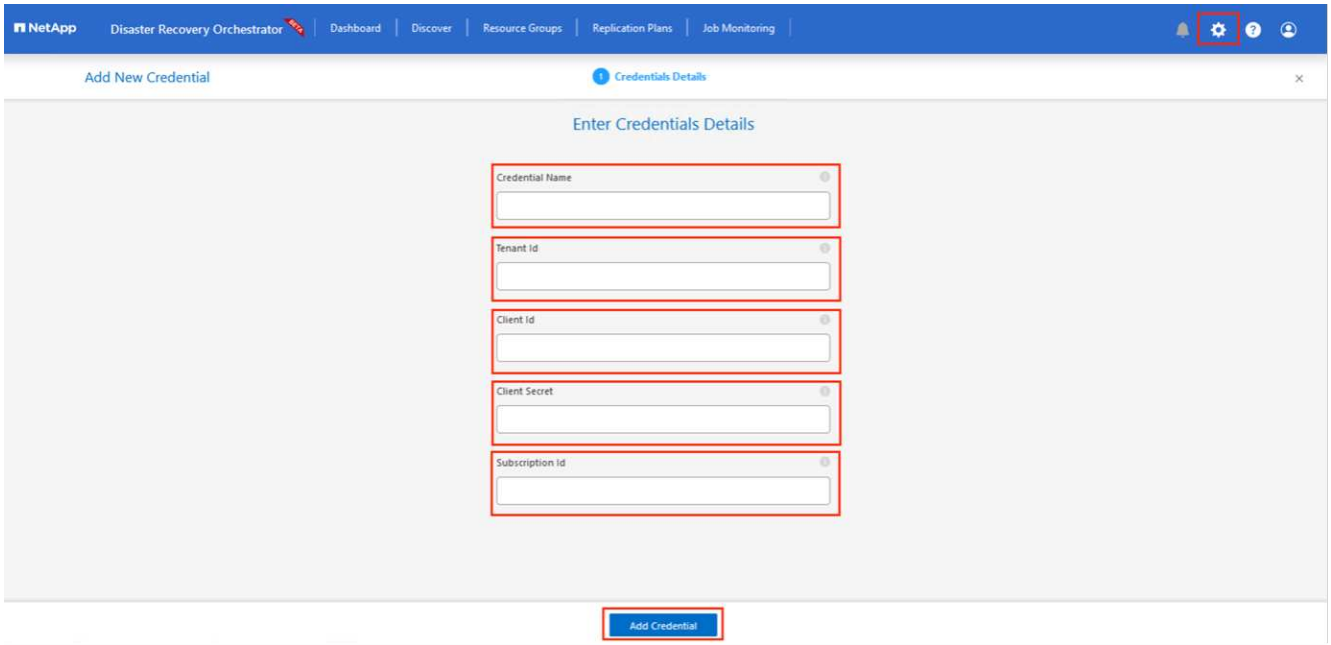
Para realizar esta operación, complete los siguientes pasos:

1. Abra DRO en un navegador compatible y use el nombre de usuario y la contraseña predeterminados/`admin`/`admin`). La contraseña se puede restablecer después del primer inicio de sesión utilizando la opción Cambiar contraseña.
2. En la parte superior derecha de la consola DRO, haga clic en el ícono **Configuración** y seleccione **Credenciales**.
3. Haga clic en Agregar nueva credencial y siga los pasos del asistente.
4. Para definir las credenciales, ingrese información sobre la entidad de servicio de Azure Active Directory que otorga los permisos necesarios:
   - Nombre de la credencial
   - Identificación del inquilino
   - ID de cliente
   - Secreto del cliente

- ID de suscripción

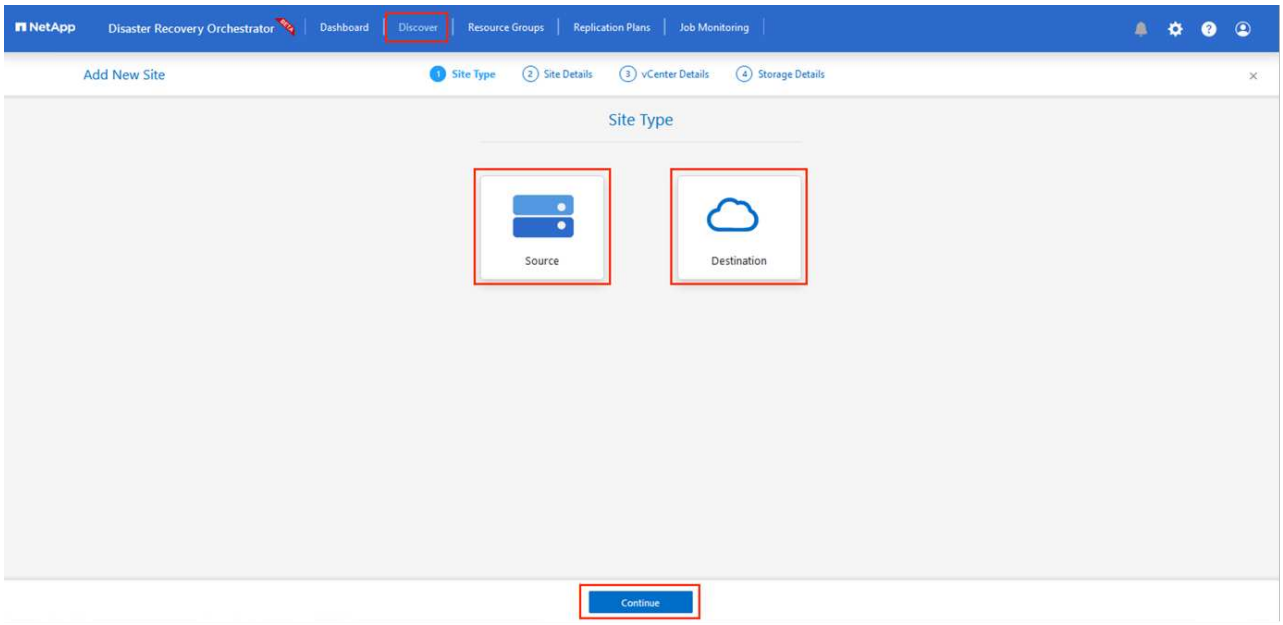
  Deberías haber capturado esta información cuando creaste la aplicación AD.

5. Confirme los detalles sobre las nuevas credenciales y haga clic en Agregar credencial.



Después de agregar las credenciales, es momento de descubrir y agregar los sitios AVS principales y secundarios (tanto vCenter como la cuenta de almacenamiento de archivos de Azure NetApp) a DRO. Para agregar el sitio de origen y destino, complete los siguientes pasos:

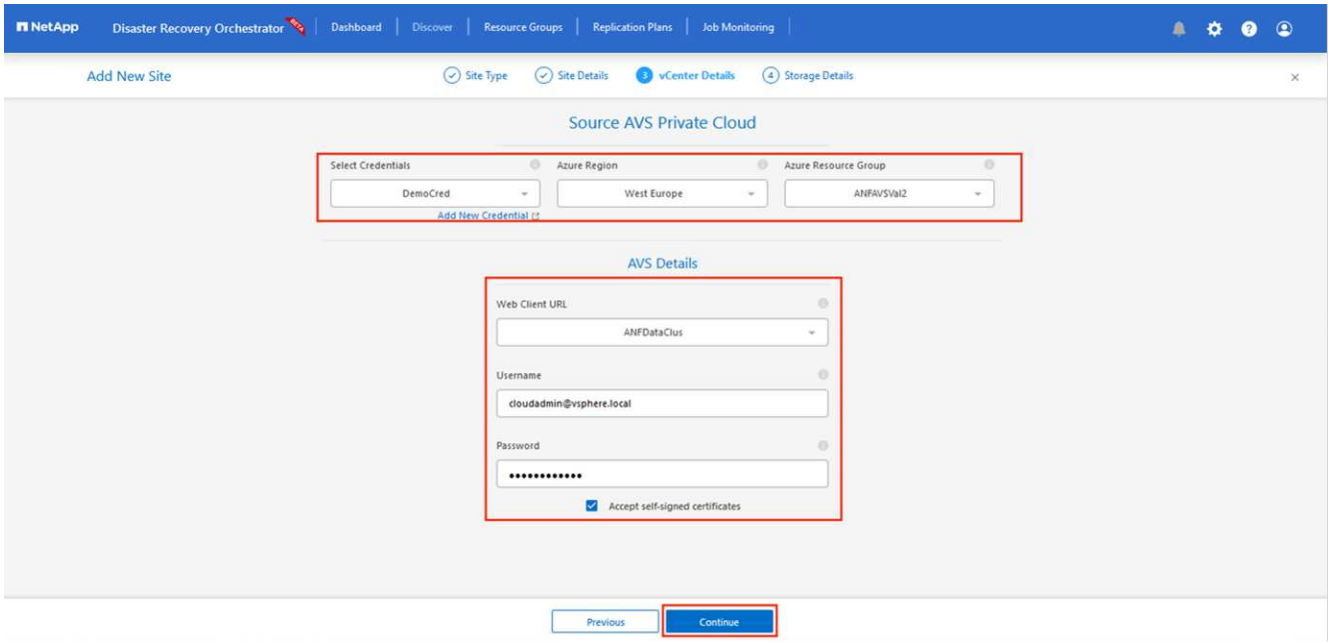
6. Vaya a la pestaña **Descubrir**.
7. Haga clic en **Agregar nuevo sitio**.
8. Agregue el siguiente sitio AVS principal (designado como **Fuente** en la consola).
   - vCenter de SDDC
   - Cuenta de almacenamiento de Azure NetApp Files
9. Agregue el siguiente sitio AVS secundario (designado como **Destino** en la consola).
   - vCenter de SDDC
   - Cuenta de almacenamiento de Azure NetApp Files



10. Agregue detalles del sitio haciendo clic en **Fuente**, ingresando un nombre de sitio descriptivo y seleccionando el conector. Luego haga clic en **Continuar**.

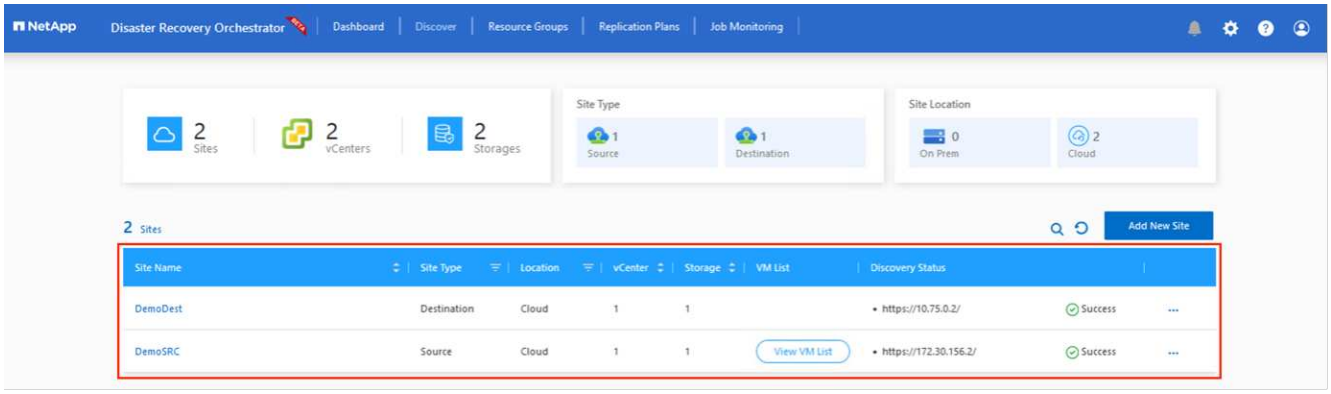
> Para fines de demostración, en este documento se explica cómo agregar un sitio de origen.

11. Actualice los detalles de vCenter. Para ello, seleccione las credenciales, la región de Azure y el grupo de recursos del menú desplegable para el SDDC de AVS principal.
12. DRO enumera todos los SDDC disponibles dentro de la región. Seleccione la URL de la nube privada designada en el menú desplegable.
13. Entrar en el `cloudadmin@vsphere.local` credenciales de usuario. Se puede acceder desde el Portal de Azure. Siga los pasos mencionados en este "enlace" . Una vez hecho esto, haga clic en **Continuar**.

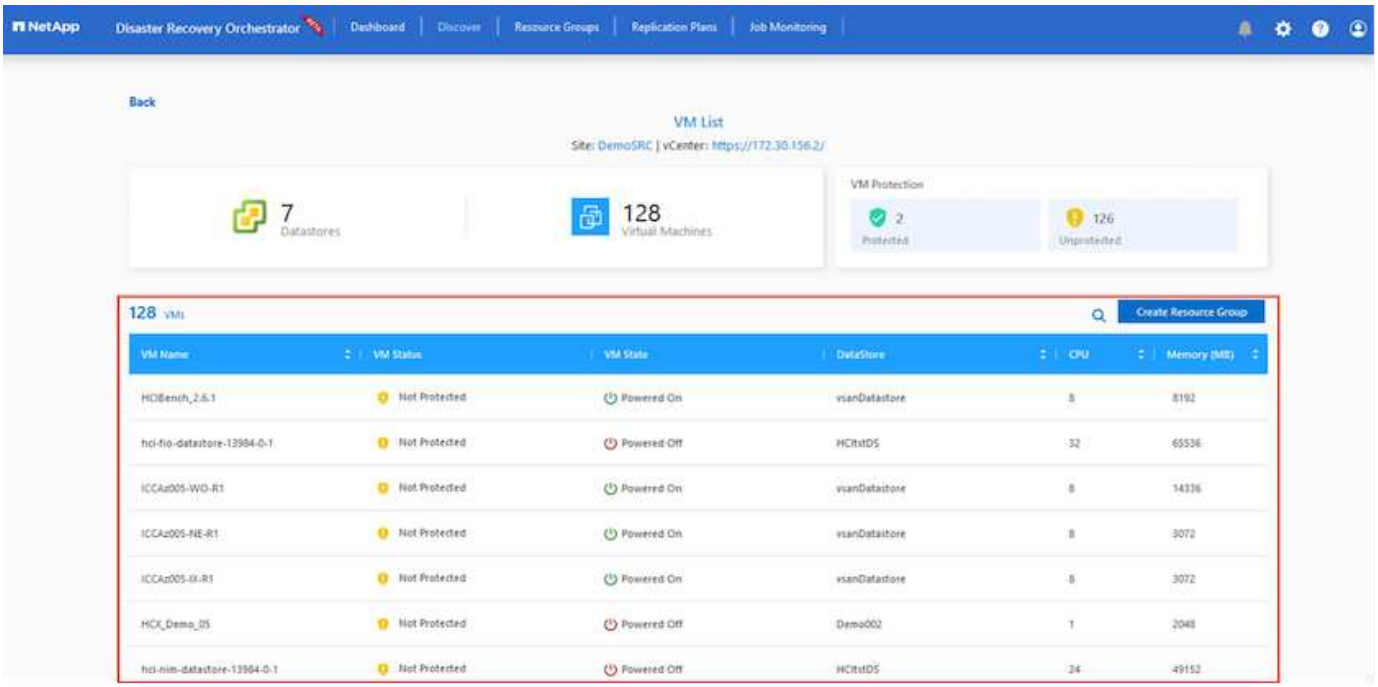


14. Seleccione los detalles del almacenamiento de origen (ANF) seleccionando el grupo de recursos de Azure y la cuenta de NetApp .

15. Haga clic en **Crear sitio**.



Una vez agregado, DRO realiza un descubrimiento automático y muestra las máquinas virtuales que tienen réplicas entre regiones correspondientes desde el sitio de origen al sitio de destino. DRO detecta automáticamente las redes y los segmentos utilizados por las máquinas virtuales y los completa.



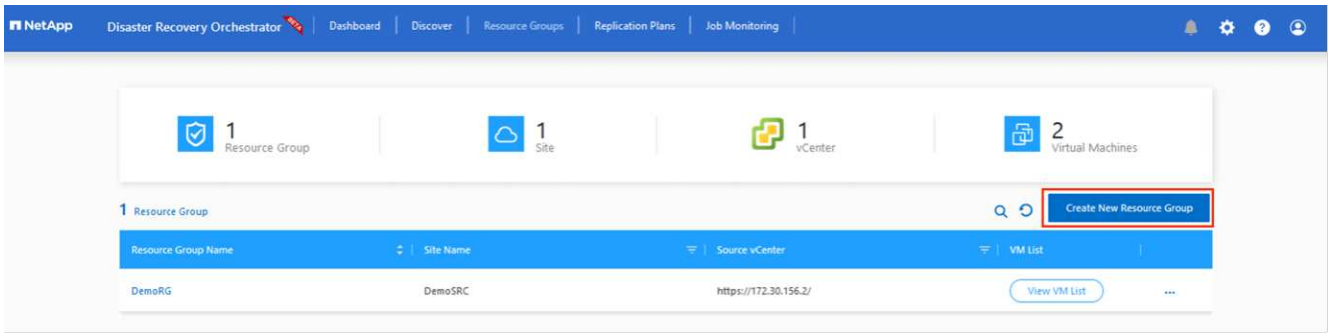
El siguiente paso es agrupar las máquinas virtuales necesarias en sus grupos funcionales como grupos de recursos.

Agrupaciones de recursos

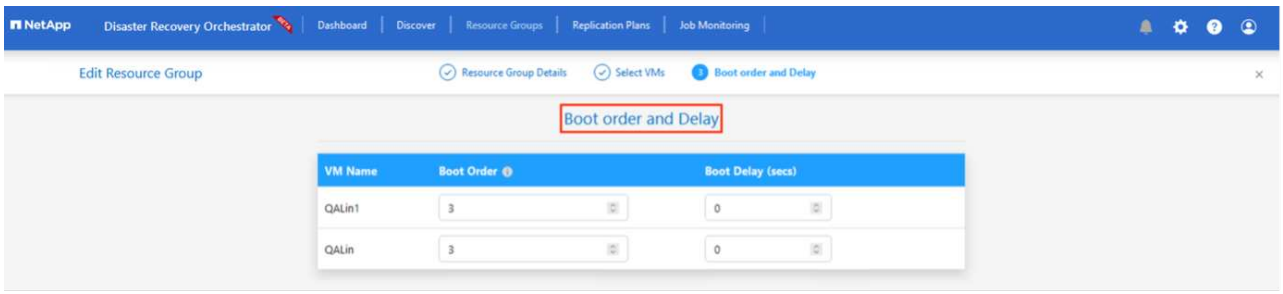
Una vez agregadas las plataformas, agrupe las máquinas virtuales que desea recuperar en grupos de recursos. Los grupos de recursos DRO le permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones opcionales que se pueden ejecutar durante la recuperación.

Para comenzar a crear grupos de recursos, haga clic en el elemento de menú **Crear nuevo grupo de recursos**.

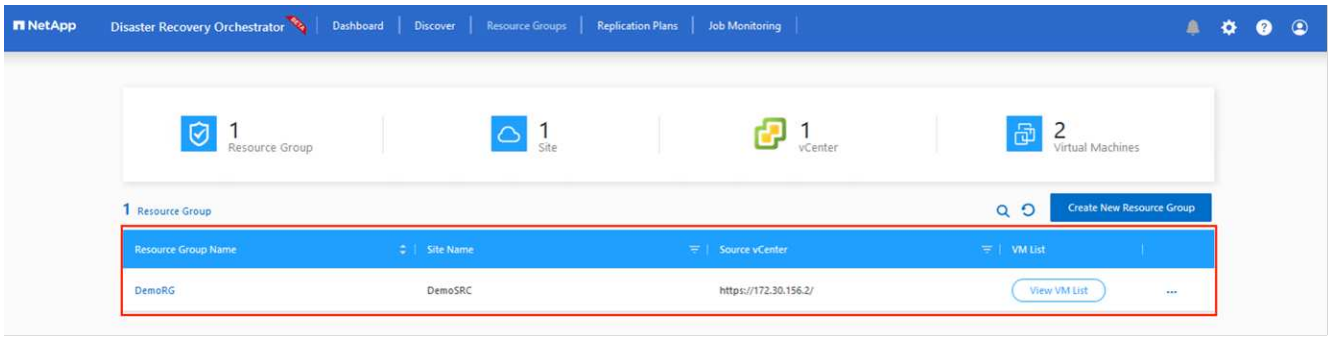
1. Acceda a **Grupos de recursos** y haga clic en **Crear nuevo grupo de recursos**.



2. En Nuevo grupo de recursos, seleccione el sitio de origen en el menú desplegable y haga clic en **Crear**.
3. Proporcione los detalles del grupo de recursos y haga clic en **Continuar**.
4. Seleccione las máquinas virtuales adecuadas mediante la opción de búsqueda.
5. Seleccione el **Orden de arranque** y el **Retraso de arranque** (segundos) para todas las máquinas virtuales seleccionadas. Establezca el orden de la secuencia de encendido seleccionando cada máquina virtual y configurando su prioridad. El valor predeterminado para todas las máquinas virtuales es 3. Las opciones son las siguientes:
   - La primera máquina virtual en encenderse
   - Por defecto
   - La última máquina virtual en encenderse



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

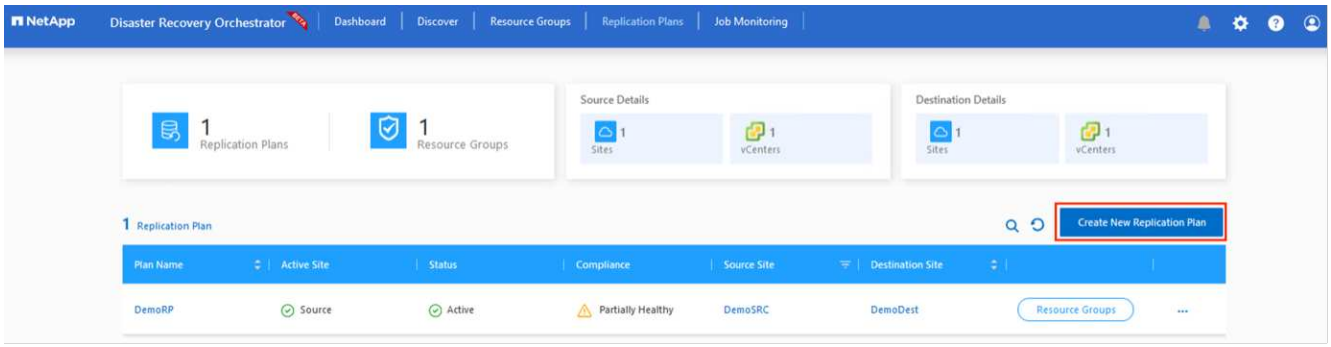


Planes de replicación

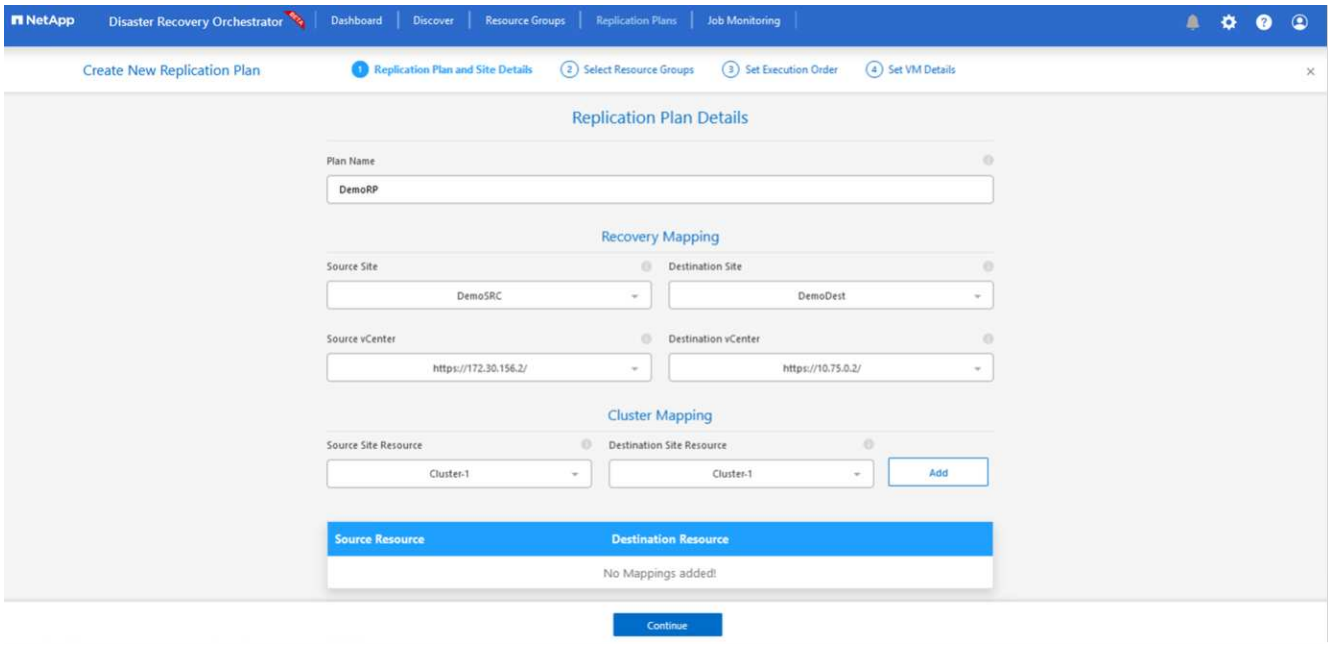
Debe tener un plan para recuperar aplicaciones en caso de desastre. Seleccione las plataformas de vCenter de origen y destino en el menú desplegable, elija los grupos de recursos que se incluirán en este plan y también incluya la agrupación de cómo se deben restaurar y encender las aplicaciones (por ejemplo, controladores de dominio, nivel 1, nivel 2, etc.). A los planes también se les suele llamar planos. Para definir el plan de recuperación, vaya a la pestaña Plan de replicación y haga clic en **Nuevo plan de replicación**.

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

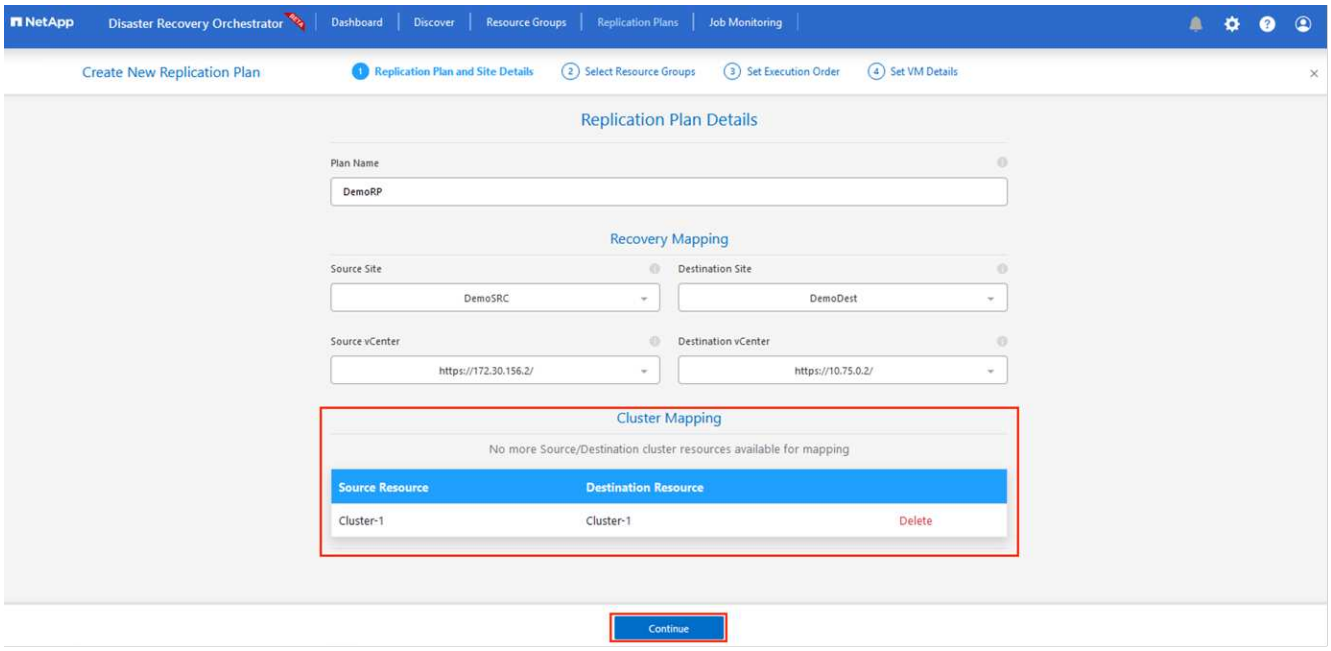
1. Vaya a **Planes de replicación** y haga clic en **Crear nuevo plan de replicación**.



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

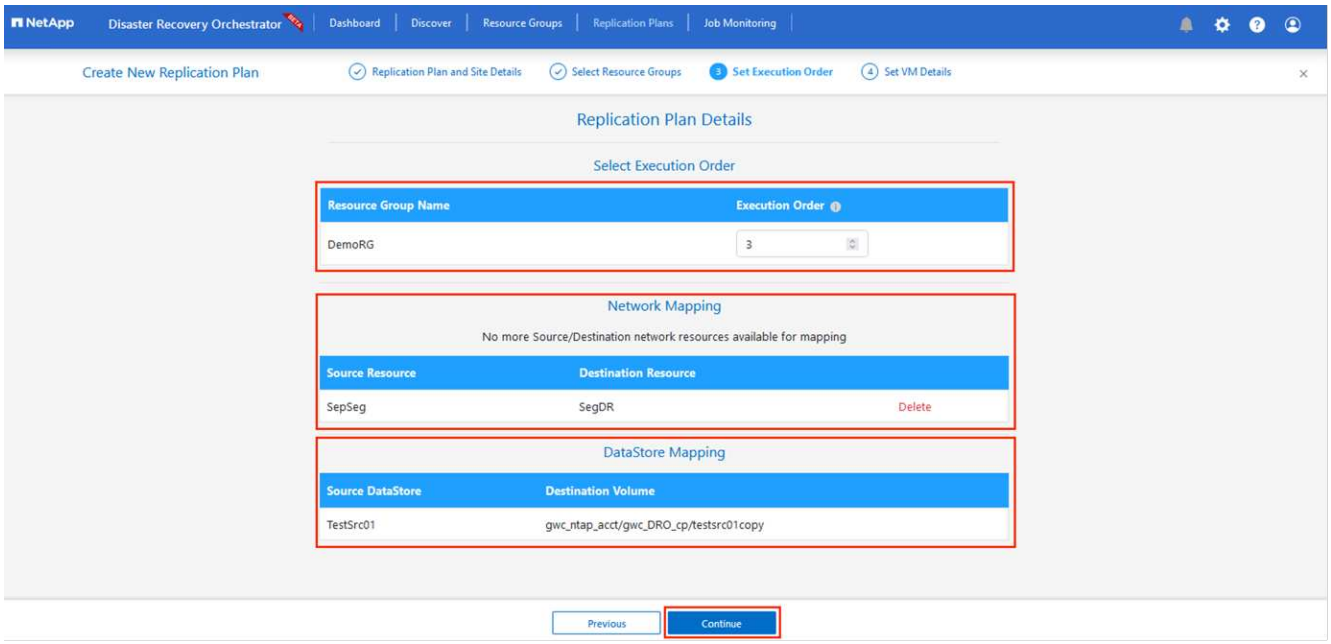


3. Una vez completado el mapeo de recuperación, seleccione **Mapeo de clúster**.

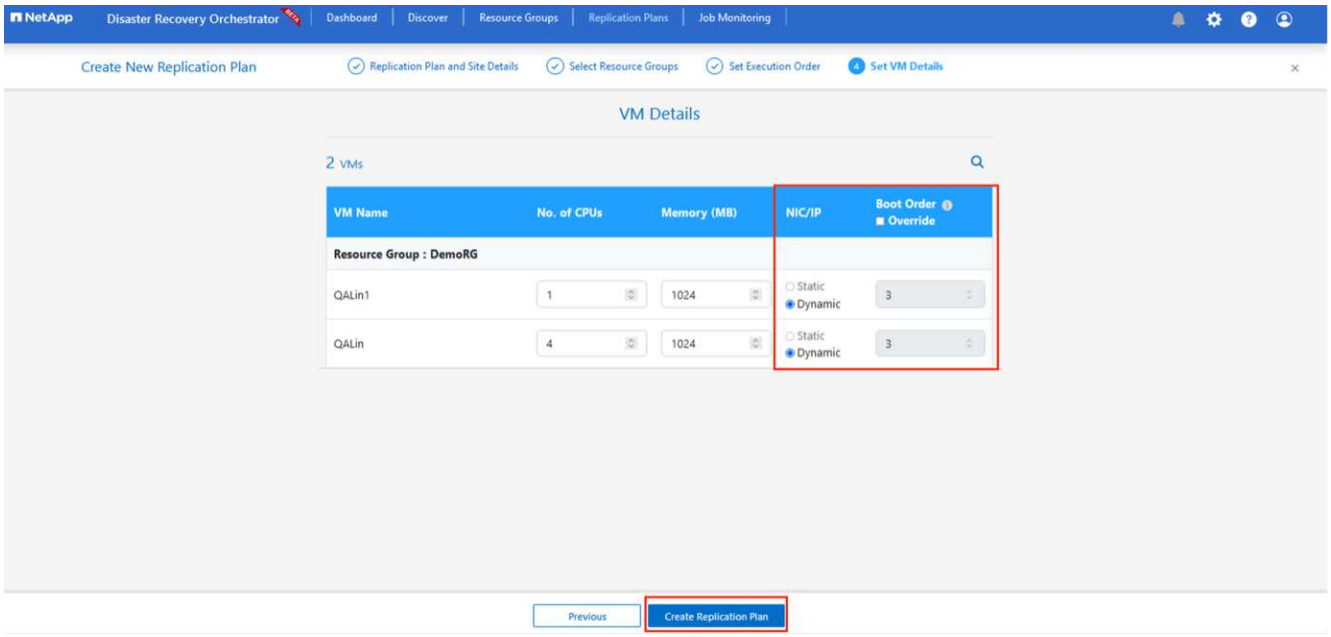


4. Seleccione **Detalles del grupo de recursos** y haga clic en **Continuar**.
5. Establecer el orden de ejecución para el grupo de recursos. Esta opción le permite seleccionar la secuencia de operaciones cuando existen múltiples grupos de recursos.
6. Una vez hecho esto, configure la asignación de red en el segmento apropiado. Los segmentos ya deben estar aprovisionados en el clúster AVS secundario y, para asignar las máquinas virtuales a ellos, seleccione el segmento apropiado.
7. Las asignaciones de almacenes de datos se seleccionan automáticamente en función de la selección de máquinas virtuales.

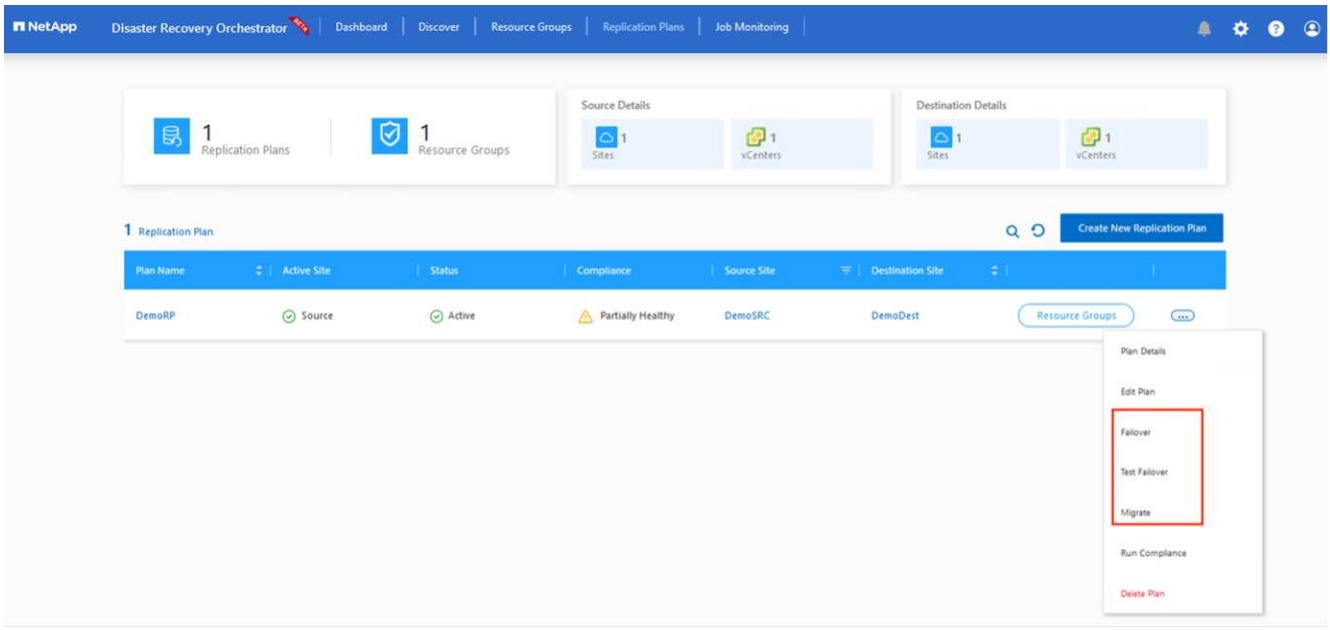
> ⓘ La replicación entre regiones (CRR) se produce a nivel de volumen. Por lo tanto, todas las máquinas virtuales que residen en el volumen respectivo se replican en el destino CRR. Asegúrese de seleccionar todas las máquinas virtuales que forman parte del almacén de datos, porque solo se procesan las máquinas virtuales que forman parte del plan de replicación.



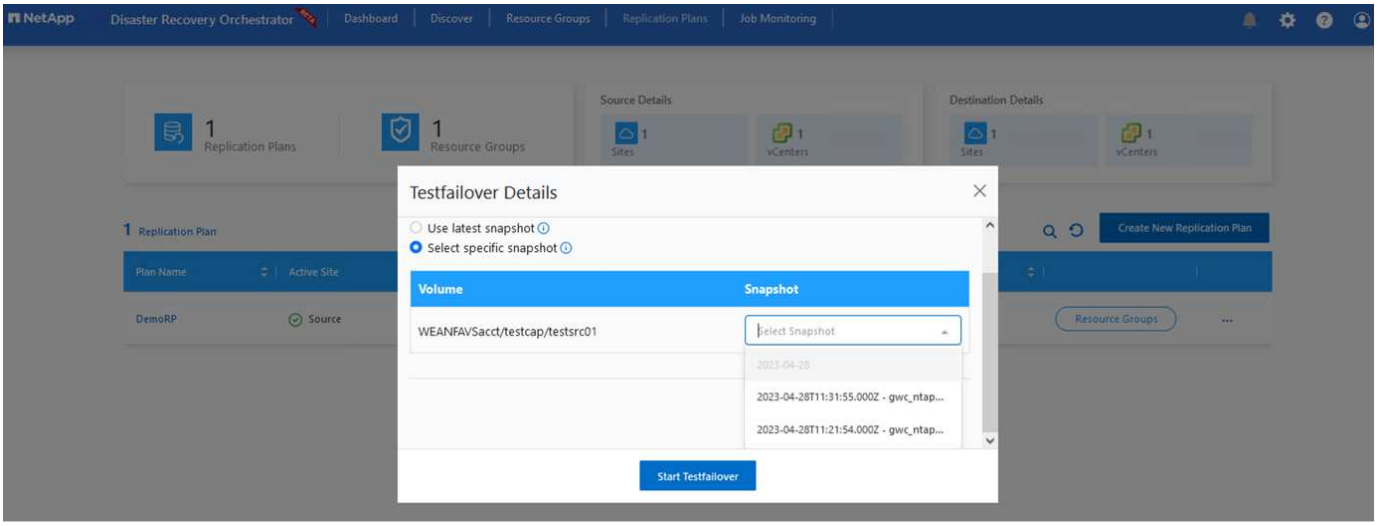
8. En Detalles de la máquina virtual, puede modificar opcionalmente el tamaño de los parámetros de CPU y RAM de la máquina virtual. Esto puede ser muy útil cuando se recuperan entornos grandes en clústeres de destino más pequeños o cuando se realizan pruebas de recuperación ante desastres sin tener que aprovisionar una infraestructura física VMware uno a uno. Además, modifique el orden de arranque y el retraso de arranque (segundos) para todas las máquinas virtuales seleccionadas en los grupos de recursos. Hay una opción adicional para modificar el orden de arranque si se requieren cambios respecto de lo seleccionado durante la selección del orden de arranque del grupo de recursos. De forma predeterminada, se utiliza el orden de arranque seleccionado durante la selección del grupo de recursos, sin embargo, cualquier modificación se puede realizar en esta etapa.



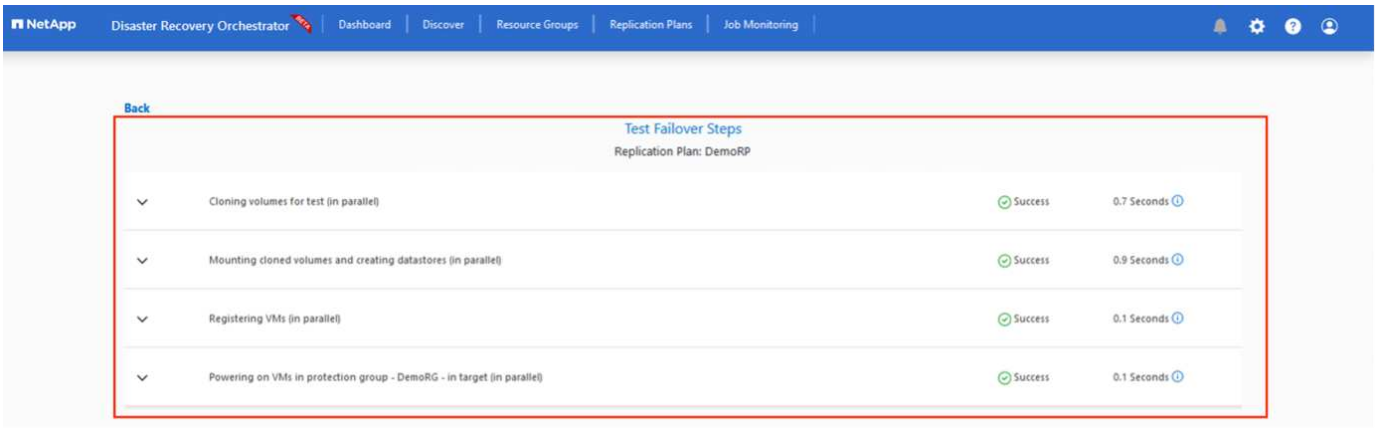
9. Haga clic en **Crear plan de replicación**. Una vez creado el plan de replicación, puede ejecutar las opciones de conmutación por error, conmutación por error de prueba o migración según sus requisitos.



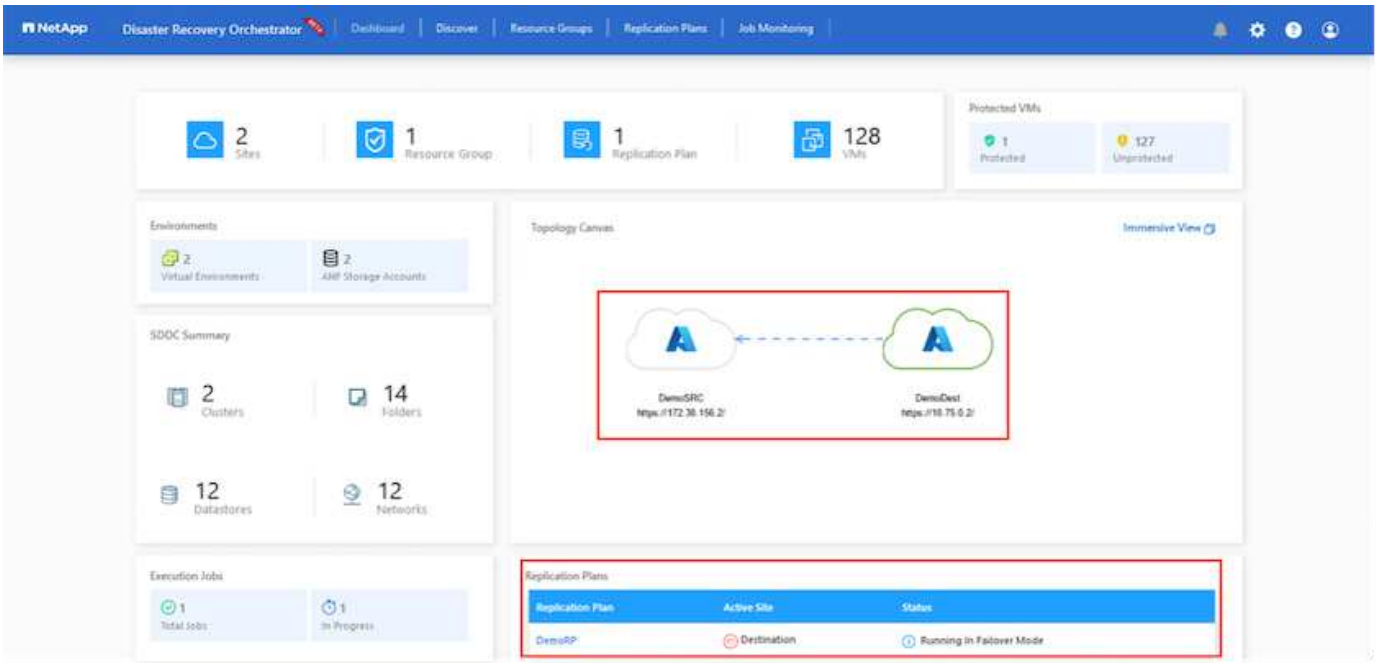
Durante las opciones de conmutación por error y conmutación por error de prueba, se utiliza la instantánea más reciente o se puede seleccionar una instantánea específica de una instantánea de un momento determinado. La opción de punto en el tiempo puede ser muy beneficiosa si se enfrenta a un evento de corrupción como ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. DRO muestra todos los puntos de tiempo disponibles.



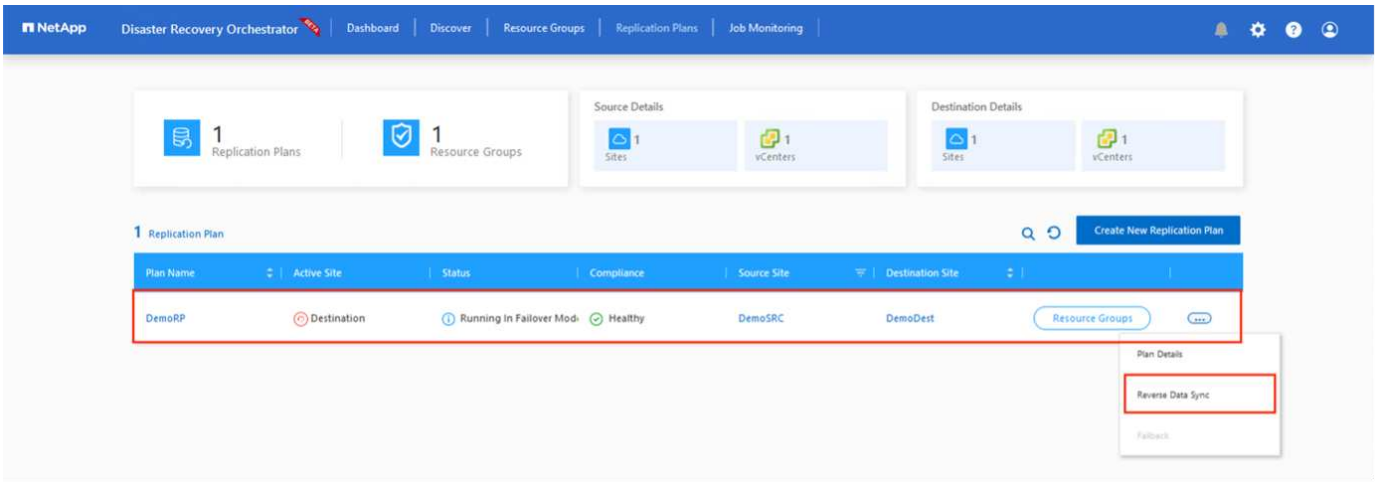
Para activar o probar la conmutación por error con la configuración especificada en el plan de replicación, puede hacer clic en **Conmutación por error** o **Probar conmutación por error**. Puede supervisar el plan de replicación en el menú de tareas.



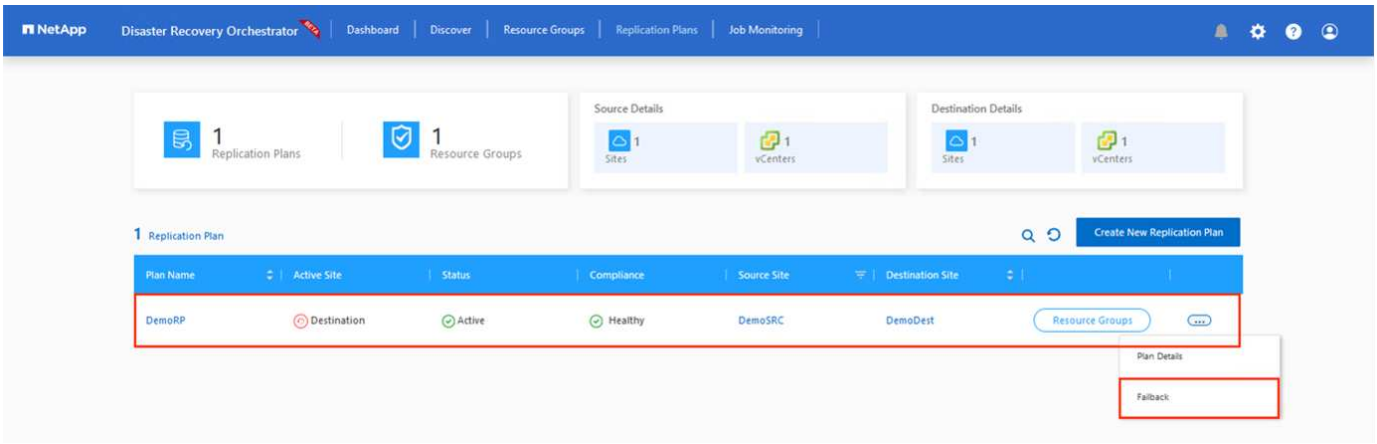
Una vez activada la conmutación por error, los elementos recuperados se pueden ver en el vCenter del SDDC de AVS del sitio secundario (máquinas virtuales, redes y almacenes de datos). De forma predeterminada, las máquinas virtuales se recuperan en la carpeta de carga de trabajo.

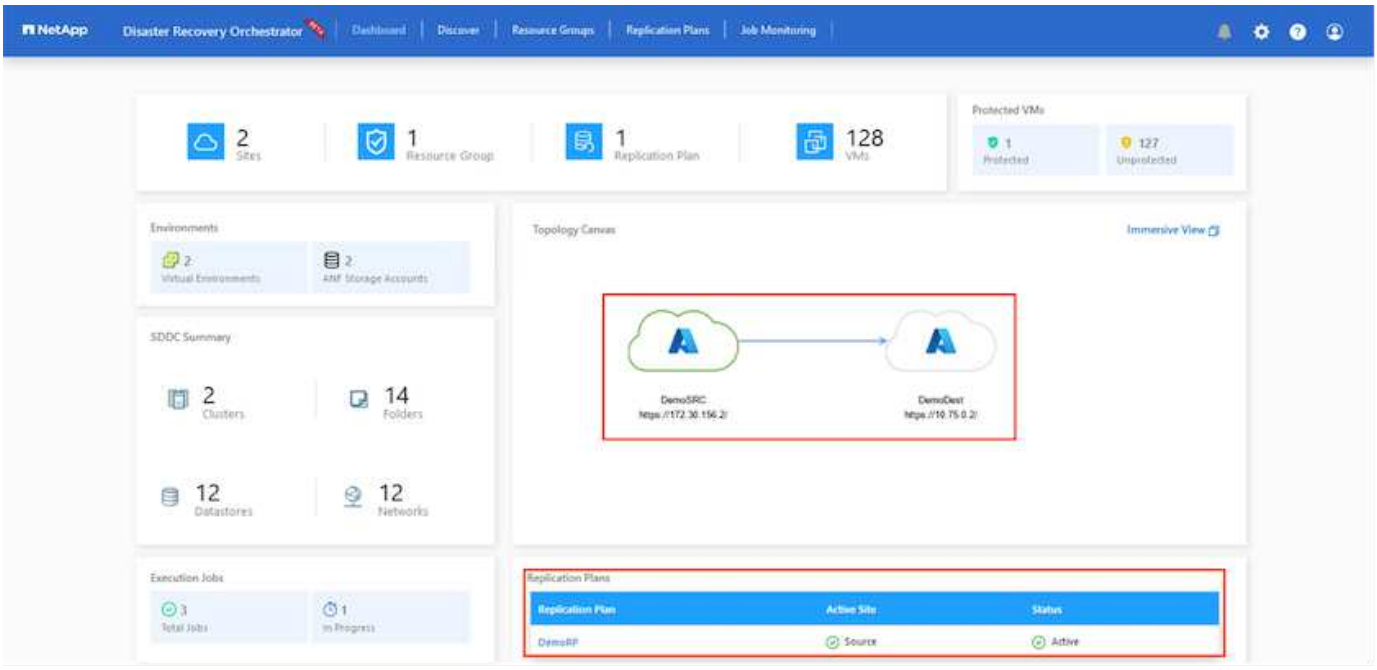


La conmutación por recuperación se puede activar en el nivel del plan de replicación. En caso de una conmutación por error de prueba, se puede utilizar la opción de desmantelamiento para revertir los cambios y eliminar el volumen recién creado. Las recuperaciones relacionadas con la conmutación por error son un proceso de dos pasos. Seleccione el plan de replicación y seleccione **Sincronización inversa de datos**.



Una vez completado este paso, active la conmutación por error para regresar al sitio AVS principal.





Desde el portal de Azure, podemos ver que se ha interrumpido el estado de la replicación para los volúmenes adecuados que se asignaron al SDDC de AVS del sitio secundario como volúmenes de lectura y escritura. Durante la conmutación por error de prueba, DRO no asigna el volumen de destino ni de réplica. En lugar de

ello, crea un nuevo volumen de la instantánea de replicación entre regiones requerida y expone el volumen como un almacén de datos, lo que consume capacidad física adicional del grupo de capacidad y garantiza que el volumen de origen no se modifique. En particular, los trabajos de replicación pueden continuar durante las pruebas de recuperación ante desastres o los flujos de trabajo de clasificación. Además, este proceso garantiza que la recuperación se pueda limpiar sin el riesgo de que la réplica se destruya si ocurren errores o se recuperan datos dañados.

Recuperación de ransomware

Recuperarse de un ransomware puede ser una tarea abrumadora. En concreto, puede resultar difícil para las organizaciones de TI determinar cuál es el punto de retorno seguro y, una vez determinado, cómo garantizar que las cargas de trabajo recuperadas estén protegidas de ataques recurrentes (por ejemplo, de malware inactivo o de aplicaciones vulnerables).

DRO aborda estas preocupaciones al permitir que las organizaciones se recuperen desde cualquier momento disponible. Las cargas de trabajo luego se recuperan en redes funcionales pero aisladas, de modo que las aplicaciones puedan funcionar y comunicarse entre sí pero no queden expuestas a ningún tráfico norte-sur. Este proceso brinda a los equipos de seguridad un lugar seguro para realizar análisis forenses e identificar cualquier malware oculto o inactivo.

Conclusión

La solución de recuperación ante desastres de Azure NetApp Files y Azure VMware le brindan los siguientes beneficios:

- Aproveche la replicación entre regiones eficiente y resistente de Azure NetApp Files .
- Recupere cualquier punto en el tiempo disponible con retención de instantáneas.
- Automatice completamente todos los pasos necesarios para recuperar cientos a miles de máquinas virtuales de los pasos de almacenamiento, computación, red y validación de aplicaciones.
- La recuperación de carga de trabajo aprovecha el proceso "Crear nuevos volúmenes a partir de las instantáneas más recientes", que no manipula el volumen replicado.
- Evite cualquier riesgo de corrupción de datos en los volúmenes o instantáneas.
- Evite interrupciones de replicación durante los flujos de trabajo de pruebas de DR.
- Aproveche los datos de DR y los recursos de computación en la nube para flujos de trabajo más allá de DR, como desarrollo y prueba, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas de remediación.
- La optimización de la CPU y la RAM puede ayudar a reducir los costos de la nube al permitir la recuperación a clústeres de cómputo más pequeños.

Dónde encontrar información adicional

Para obtener más información sobre la información que se describe en este documento, revise los siguientes documentos y/o sitios web:

- Crear replicación de volumen para Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replicación entre regiones de volúmenes de Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Solución VMware de Azure"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Implementar y configurar el entorno de virtualización en Azure

  "Configurar AVS en Azure"

- Implementar y configurar Azure VMware Solution

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Uso de Veeam Replication y el almacén de datos de Azure NetApp Files para la recuperación ante desastres en Azure VMware Solution

Los almacenes de datos de Azure NetApp Files (ANF) desacoplan el almacenamiento del procesamiento y liberan la flexibilidad necesaria para que cualquier organización lleve sus cargas de trabajo a la nube. Proporciona a los clientes una infraestructura de almacenamiento flexible y de alto rendimiento que escala independientemente de los recursos computacionales. El almacén de datos de Azure NetApp Files simplifica y optimiza la implementación junto con Azure VMware Solution (AVS) como un sitio de recuperación ante desastres para entornos VMWare locales.

Descripción general

Los almacenes de datos NFS basados en volúmenes de Azure NetApp Files (ANF) se pueden usar para replicar datos desde instalaciones locales mediante cualquier solución de terceros validada que proporcione capacidad de replicación de máquinas virtuales. Al agregar almacenes de datos de Azure NetApp Files , se permitirá una implementación con costos optimizados en comparación con la creación de un SDDC de Azure VMware Solution con una enorme cantidad de hosts ESXi para acomodar el almacenamiento. Este enfoque se denomina "grupo de luces piloto". Un clúster de luz piloto es una configuración de host AVS mínima (3 nodos AVS) junto con la capacidad del almacén de datos de Azure NetApp Files .

El objetivo es mantener una infraestructura de bajo costo con todos los componentes básicos para manejar una conmutación por error. Un clúster de luz piloto puede escalar horizontalmente y aprovisionar más hosts AVS si ocurre una conmutación por error. Y una vez que se completa la conmutación por error y se restablecen las operaciones normales, el grupo de luces piloto puede volver a un modo de operaciones de bajo costo.

Propósitos de este documento

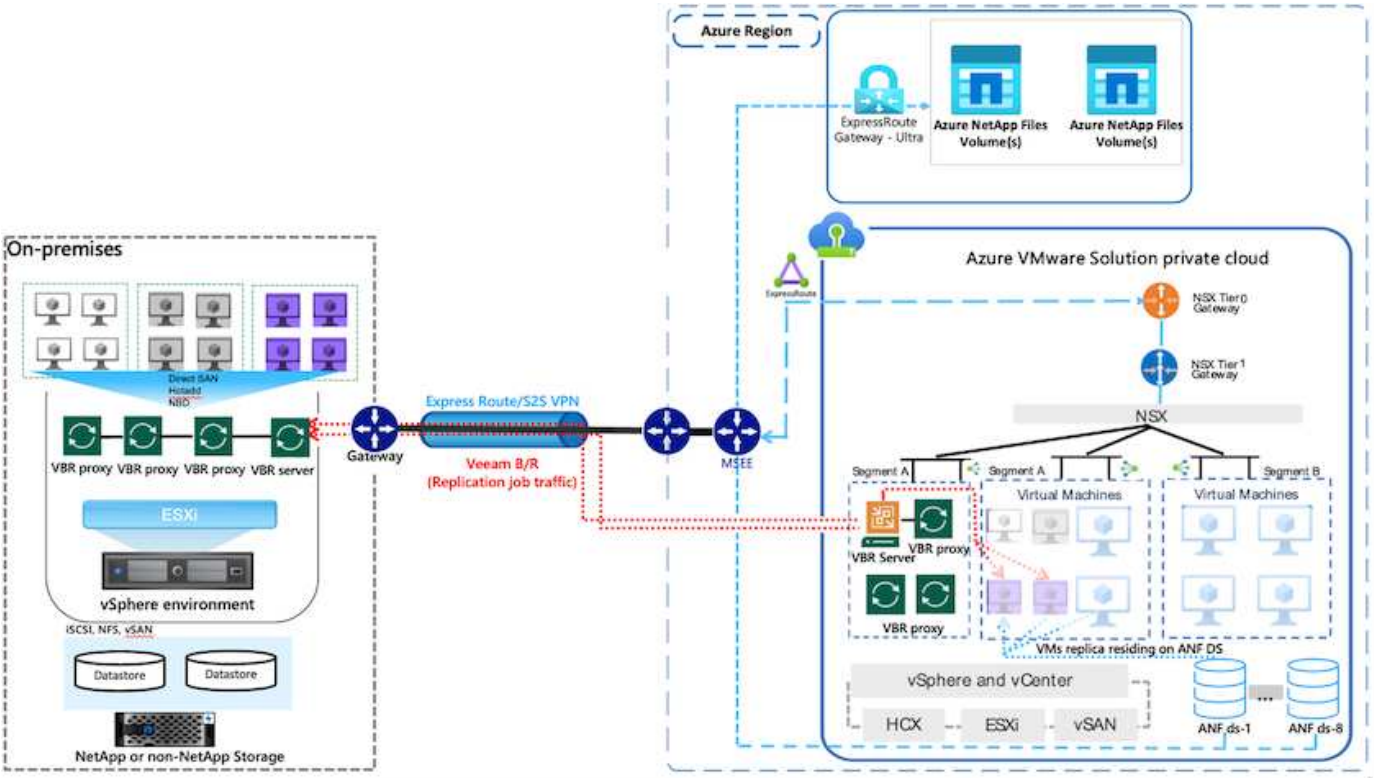
En este artículo se describe cómo usar el almacén de datos de Azure NetApp Files con Veeam Backup and Replication para configurar la recuperación ante desastres de las máquinas virtuales VMware locales (AVS) mediante la funcionalidad del software de replicación de máquinas virtuales de Veeam.

Veeam Backup & Replication es una aplicación de backup y replicación para entornos virtuales. Cuando se replican máquinas virtuales, Veeam Backup & Replication se replica desde AVS, el software creará una copia exacta de las máquinas virtuales en el formato nativo de VMware vSphere en el clúster SDDC de AVS de destino. Veeam Backup & Replication mantendrá la copia sincronizada con la VM original. La replicación proporciona el mejor objetivo de tiempo de recuperación (RTO) ya que hay una copia montada de una máquina virtual en el sitio de recuperación ante desastres en un estado listo para iniciarse.

Este mecanismo de replicación garantiza que las cargas de trabajo puedan iniciarse rápidamente en un SDDC de AVS en caso de un desastre. El software Veeam Backup & Replication también optimiza la transmisión de

tráfico para la replicación a través de WAN y conexiones lentas. Además, también filtra bloques de datos duplicados, bloques de datos cero, archivos de intercambio y "archivos del sistema operativo invitado de VM excluidos". El software también comprimirá el tráfico de réplicas. Para evitar que los trabajos de replicación consuman todo el ancho de banda de la red, se pueden utilizar aceleradores de WAN y reglas de limitación de red.

El proceso de replicación en Veeam Backup & Replication está impulsado por trabajos, lo que significa que la replicación se realiza mediante la configuración de trabajos de replicación. En el caso de un evento de desastre, se puede activar la conmutación por error para recuperar las máquinas virtuales mediante la conmutación por error a su copia de réplica. Cuando se realiza una conmutación por error, una VM replicada asume el rol de la VM original. La conmutación por error se puede realizar al último estado de una réplica o a cualquiera de sus puntos de restauración conocidos. Esto permite la recuperación de ransomware o pruebas aisladas según sea necesario. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.



Implementación de la solución

Pasos de alto nivel

1. El software Veeam Backup and Replication se ejecuta en un entorno local con conectividad de red adecuada.
2. "Implementar Azure VMware Solution (AVS)"nube privada y"Adjuntar almacenes de datos de Azure NetApp Files" a los hosts de Azure VMware Solution.

   Se puede utilizar un entorno de luz piloto configurado con una configuración mínima para fines de recuperación ante desastres. Las máquinas virtuales conmutarán a este clúster en caso de un incidente y se podrán agregar nodos adicionales).

3. Configure el trabajo de replicación para crear réplicas de máquinas virtuales mediante Veeam Backup and Replication.

4. Cree un plan de conmutación por error y realice la conmutación por error.
5. Vuelva a las máquinas virtuales de producción una vez que se complete el evento de desastre y el sitio principal esté activo.

Requisitos previos para la replicación de máquinas virtuales de Veeam en almacenes de datos AVS y ANF

1. Asegúrese de que la máquina virtual de respaldo de Veeam Backup & Replication esté conectada a los clústeres AVS SDDC de origen y de destino.
2. El servidor de respaldo debe poder resolver nombres cortos y conectarse a los vCenter de origen y de destino.
3. El almacén de datos de destino de Azure NetApp Files debe tener suficiente espacio libre para almacenar los VMDK de las máquinas virtuales replicadas.

Para obtener información adicional, consulte el apartado "Consideraciones y limitaciones""aquí" .

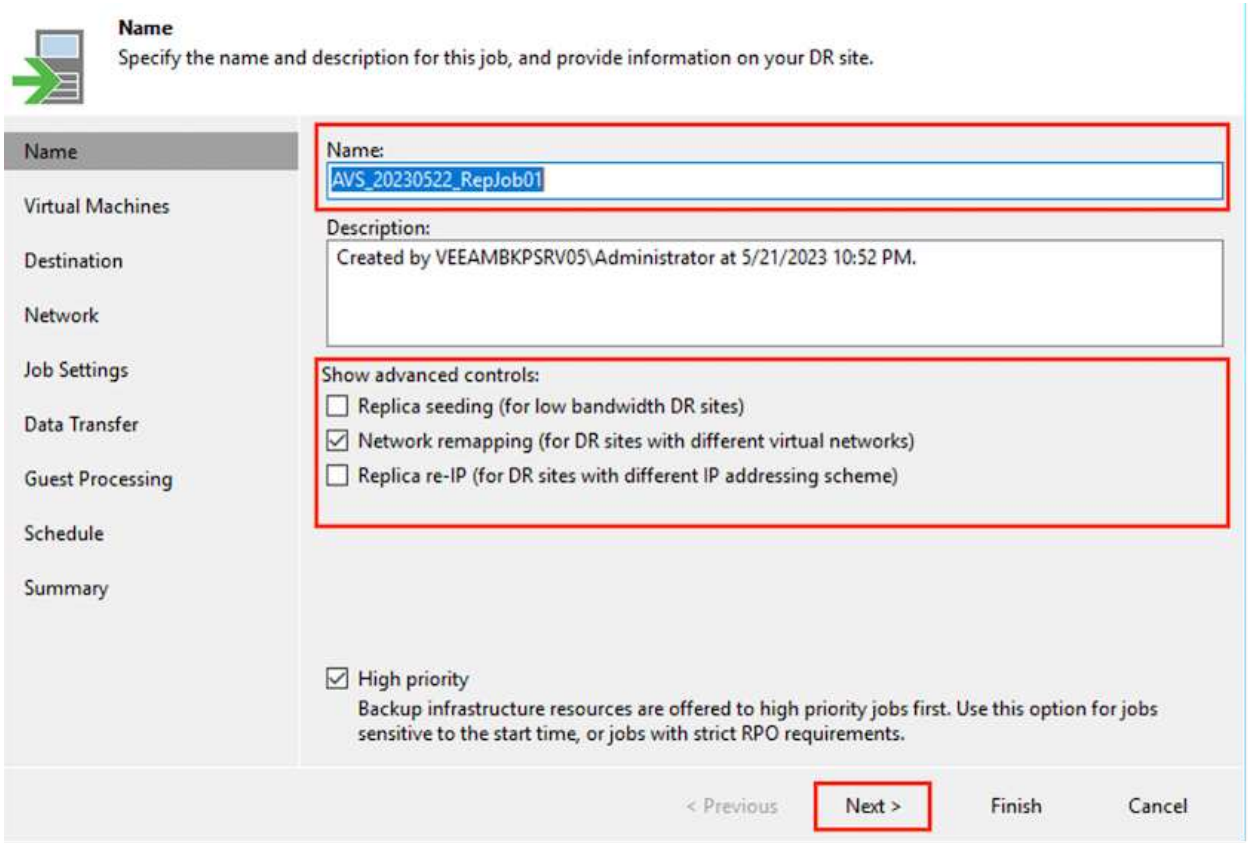
Detalles de la implementación

▼ **Paso 1: replicar máquinas virtuales**

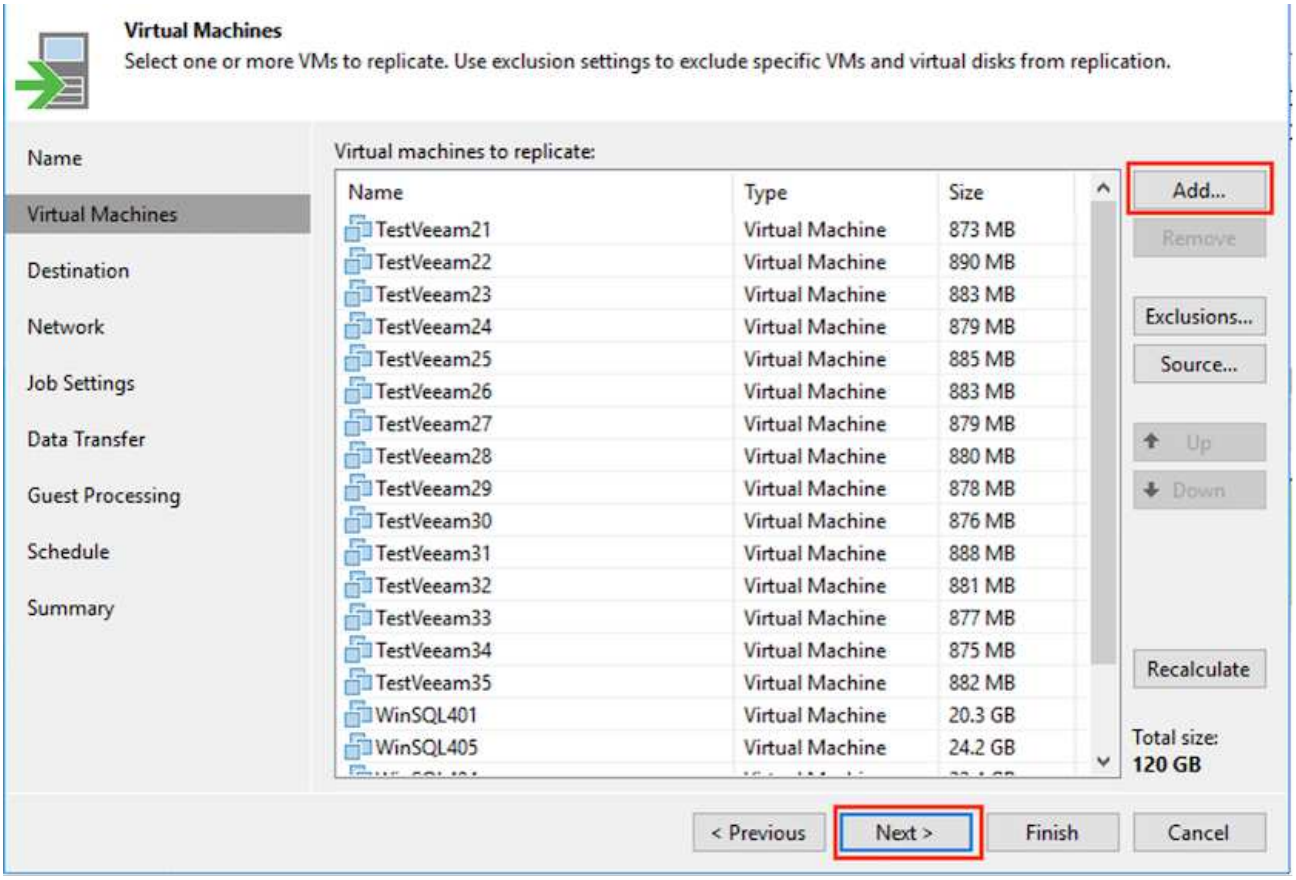
Veeam Backup & Replication aprovecha las capacidades de instantáneas de VMware vSphere. Durante la replicación, Veeam Backup & Replication solicita a VMware vSphere que cree una instantánea de la máquina virtual. La instantánea de VM es la copia puntual de una VM que incluye discos virtuales, estado del sistema, configuración y metadatos. Veeam Backup & Replication utiliza la instantánea como fuente de datos para la replicación.

Para replicar máquinas virtuales, siga los pasos a continuación:

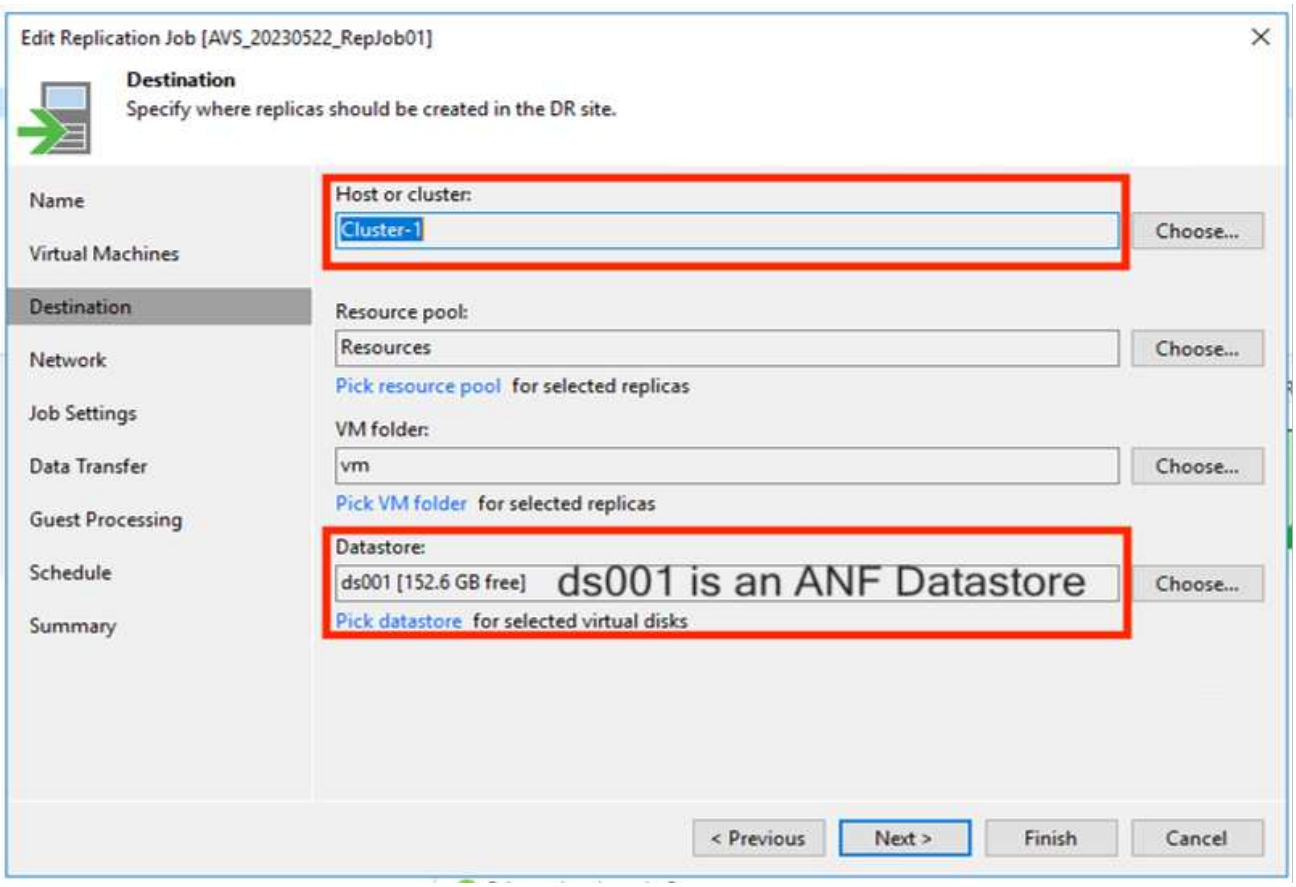
1. Abra la consola de Veeam Backup & Replication.
2. En la vista de inicio. Haga clic con el botón derecho en el nodo de trabajos y seleccione Trabajo de replicación > Máquina virtual.
3. Especifique un nombre de trabajo y seleccione la casilla de verificación de control avanzado adecuada. Haga clic en Siguiente.
    - Seleccione la casilla de verificación Siembra de réplicas si la conectividad entre las instalaciones locales y Azure tiene un ancho de banda restringido. *Seleccione la casilla de verificación Reasignación de red (para sitios AVS SDDC con redes diferentes) si los segmentos en Azure VMware Solution 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 AVS de destino, seleccione la casilla de verificación Re-IP de réplica (para sitios DR con esquema de direccionamiento IP diferente).



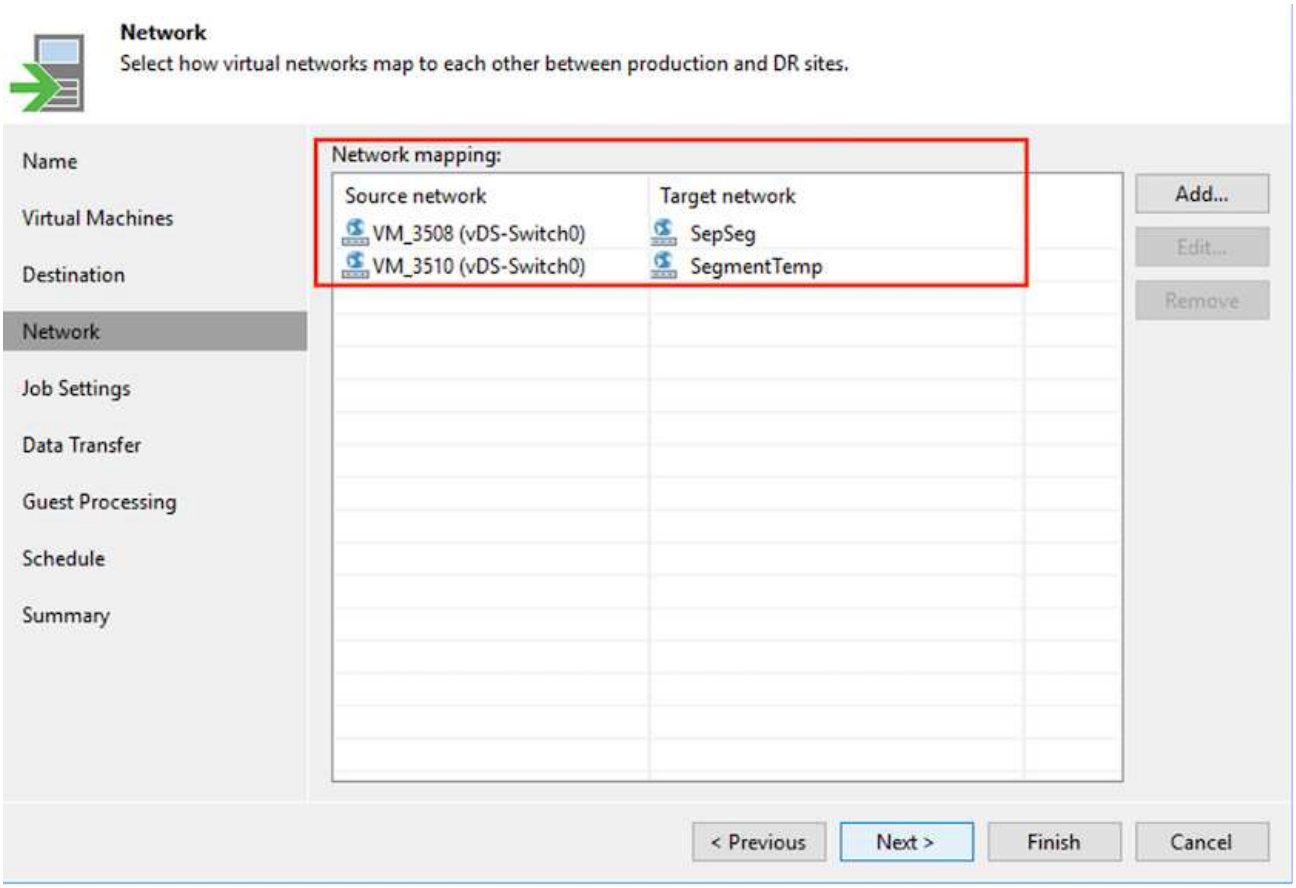
4. Seleccione las máquinas virtuales que se replicarán en el almacén de datos de Azure NetApp Files conectado a un SDDC de Azure VMware Solution en el paso **Máquinas virtuales**. Las máquinas virtuales se pueden colocar en vSAN para llenar la capacidad del almacén de datos de vSAN disponible. En un clúster de luz piloto, la capacidad utilizable de un clúster de 3 nodos será limitada. El resto de los datos se pueden colocar fácilmente en almacenes de datos de Azure NetApp Files para que las máquinas virtuales se puedan recuperar y el clúster se pueda expandir para cumplir con los requisitos de CPU/memoria. Haga clic en **Agregar**, luego en la ventana **Agregar objeto** seleccione las máquinas virtuales o los contenedores de máquinas virtuales necesarios y haga clic en **Agregar**. Haga clic en **Siguiente**.



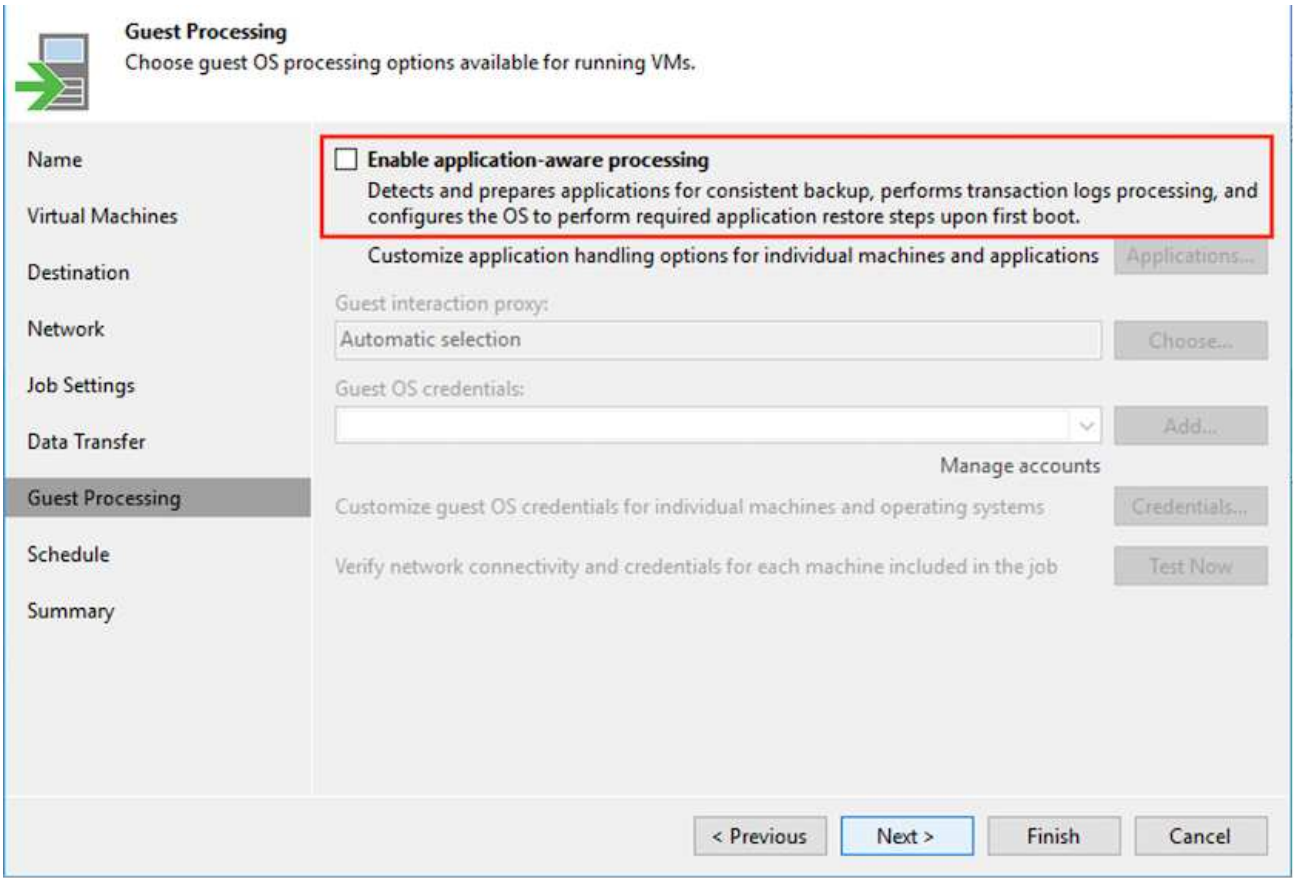
5. Después de eso, seleccione el destino como clúster/host SDDC de Azure VMware Solution y el grupo de recursos adecuado, la carpeta de VM y el almacén de datos FSx ONTAP para las réplicas de VM. Luego haga clic en **Siguiente**.



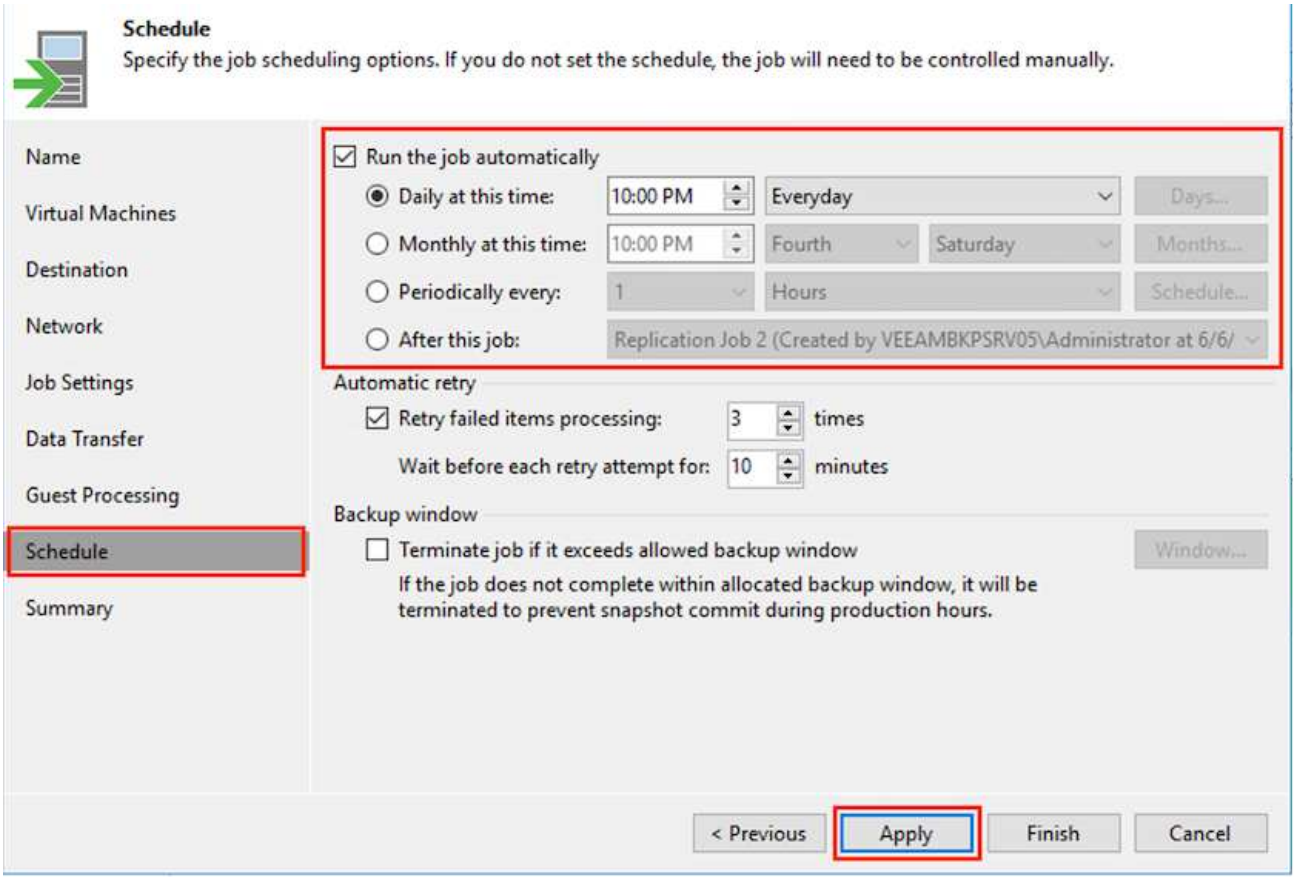
6. En el siguiente paso, cree la asignación entre la red virtual de origen y de destino según sea necesario.



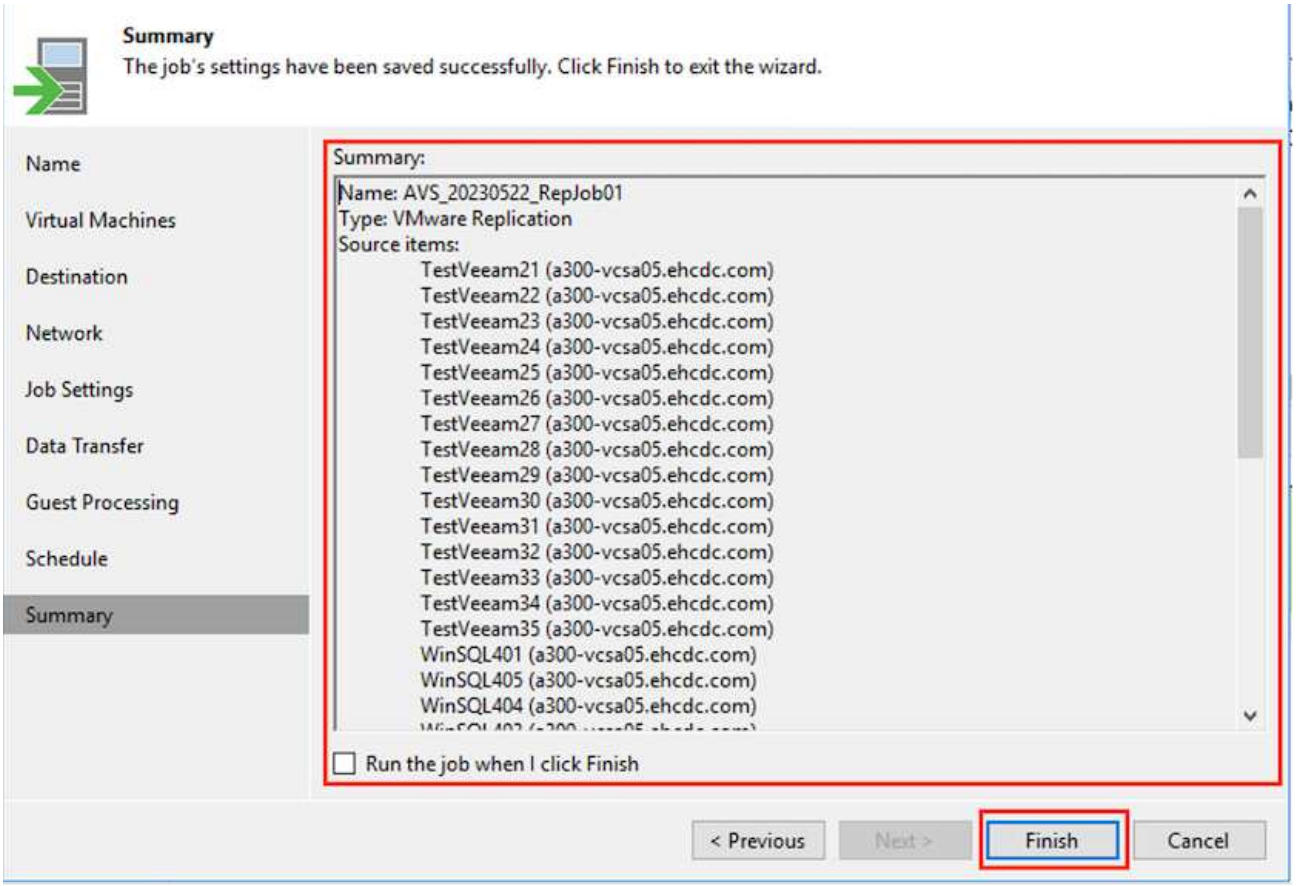
7. En el paso **Configuración del trabajo**, especifique el repositorio de respaldo que almacenará metadatos para las réplicas de VM, la política de retención, etc.
8. Actualice los servidores proxy **Origen** y **Destino** en el paso **Transferencia de datos** y deje la selección **Automática** (predeterminada) y mantenga seleccionada la opción **Directa** y haga clic en **Siguiente**.
9. En el paso **Procesamiento de invitado**, seleccione la opción **Habilitar procesamiento consciente de la aplicación** según sea necesario. Haga clic en **Siguiente**.



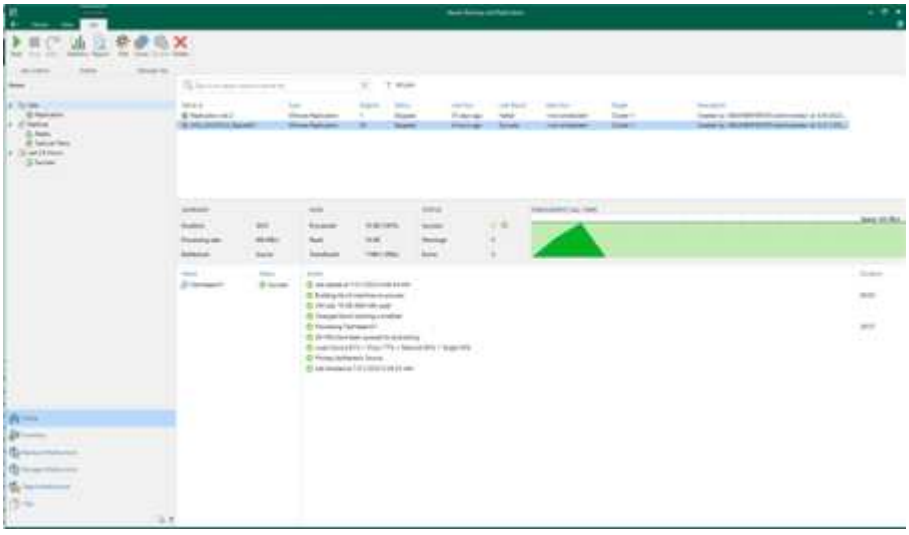
10. Seleccione la programación de replicación para ejecutar el trabajo de replicación de manera periódica.



11. En el paso **Resumen** del asistente, revise los detalles del trabajo de replicación. Para iniciar el trabajo inmediatamente después de cerrar el asistente, seleccione la casilla de verificación **Ejecutar el trabajo al hacer clic en Finalizar**; de lo contrario, deje la casilla de verificación sin seleccionar. Luego haga clic en **Finalizar** para cerrar el asistente.



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



Para obtener información adicional sobre la replicación de Veeam, consulte"Cómo funciona la replicación"

▼ Paso 2: Crear un plan de conmutación por error

Cuando se complete la replicación o siembra inicial, cree el plan de conmutación por error. El plan de conmutación por error ayuda a realizar la conmutación por error de las máquinas virtuales dependientes una por una o como grupo de manera automática. El plan de conmutación por error es el modelo para el orden en que se procesan las máquinas virtuales, incluidos los retrasos en el arranque. El plan de conmutación por error también ayuda a garantizar que las máquinas virtuales dependientes críticas ya

estén en ejecución.

Para crear el plan, navegue a la nueva subsección llamada **Réplicas** y seleccione **Plan de conmutación por error**. Seleccione las máquinas virtuales adecuadas. 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.

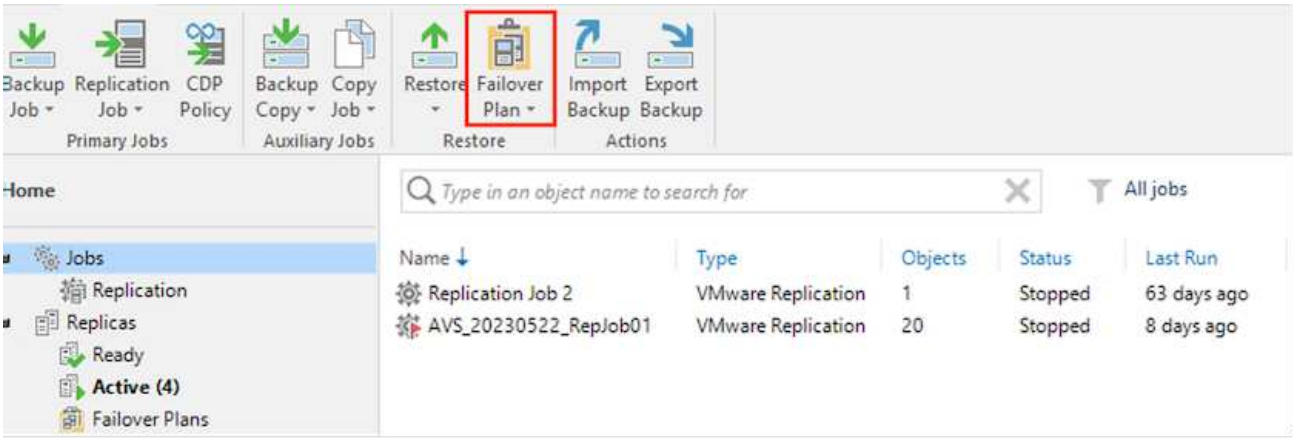
> El plan de conmutación por error solo se puede agregar una vez que se completa la replicación inicial y las réplicas de la máquina virtual están en estado Listo.

> La cantidad máxima de máquinas virtuales que se pueden iniciar simultáneamente cuando se ejecuta un plan de conmutación por error es 10

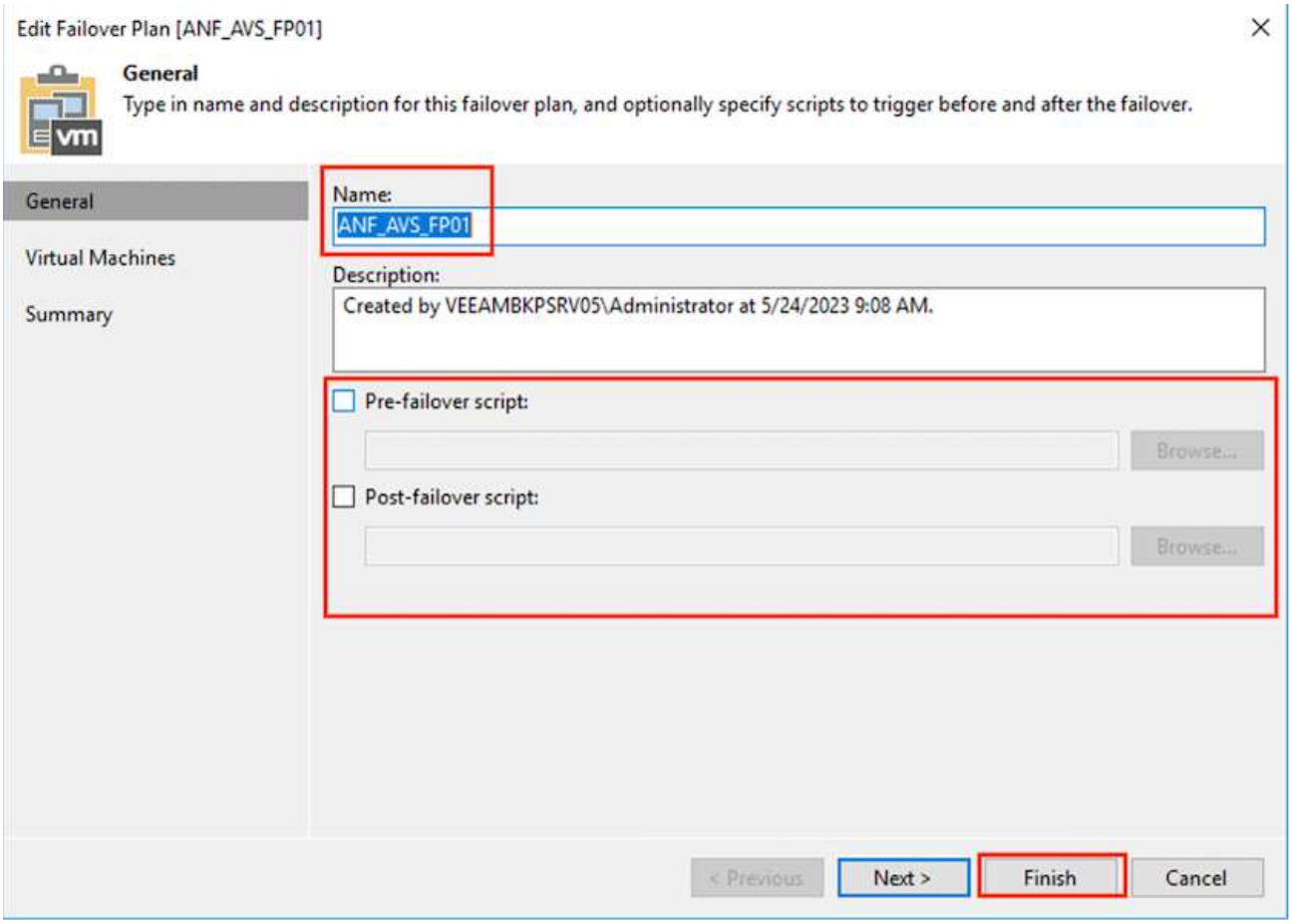
> Durante el proceso de conmutación por error, las máquinas virtuales de origen no se apagarán

Para crear el **Plan de conmutación por error**, haga lo siguiente:

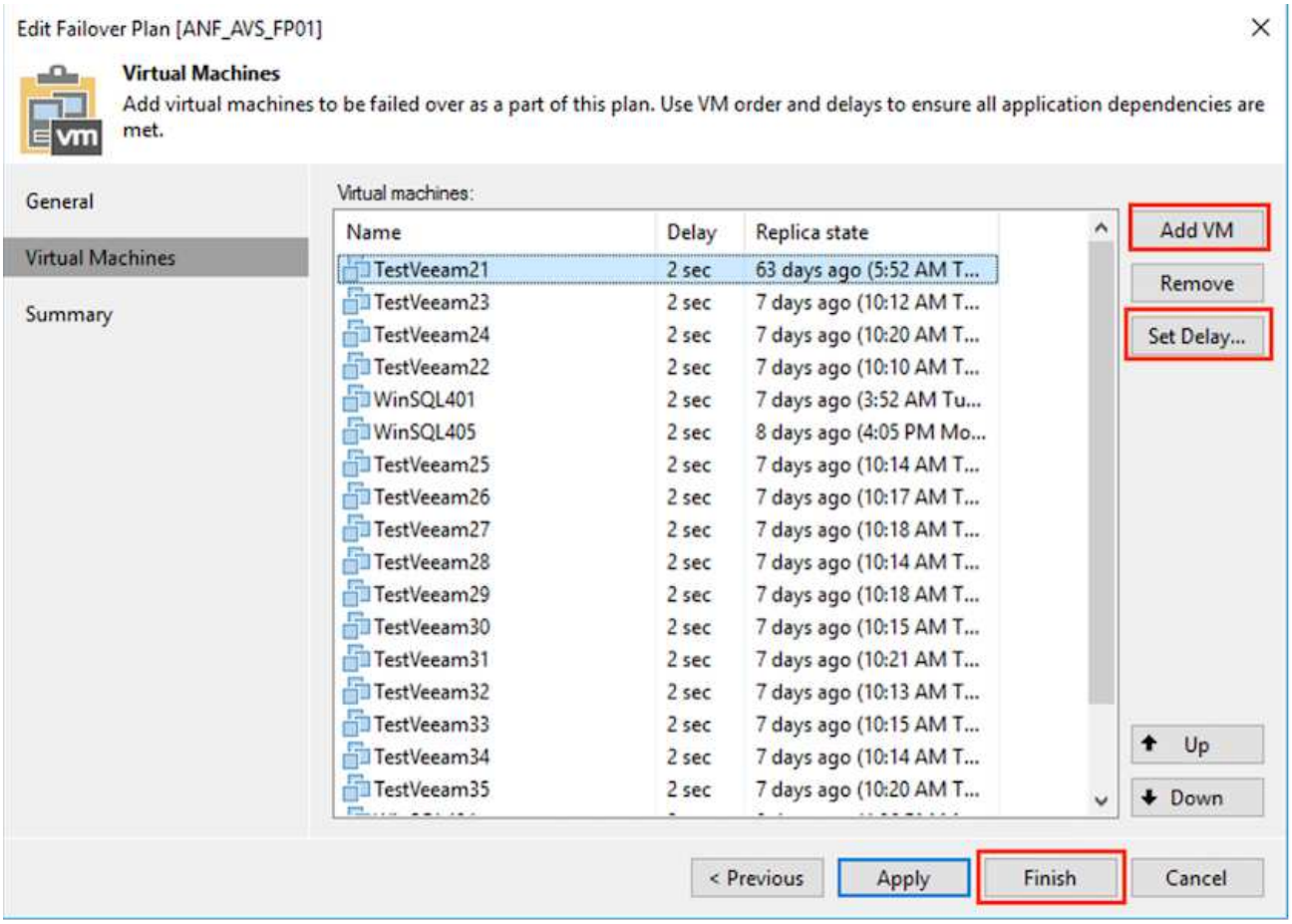
1. En la vista de inicio. Haga clic con el botón derecho en el nodo Réplicas y seleccione Planes de conmutación por error > Plan de conmutación por error > VMware vSphere.



2. A continuación, proporcione un nombre y una descripción al plan. Se pueden agregar scripts previos y posteriores a la conmutación por error según sea necesario. Por ejemplo, ejecute un script para apagar las máquinas virtuales antes de iniciar las máquinas virtuales replicadas.



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



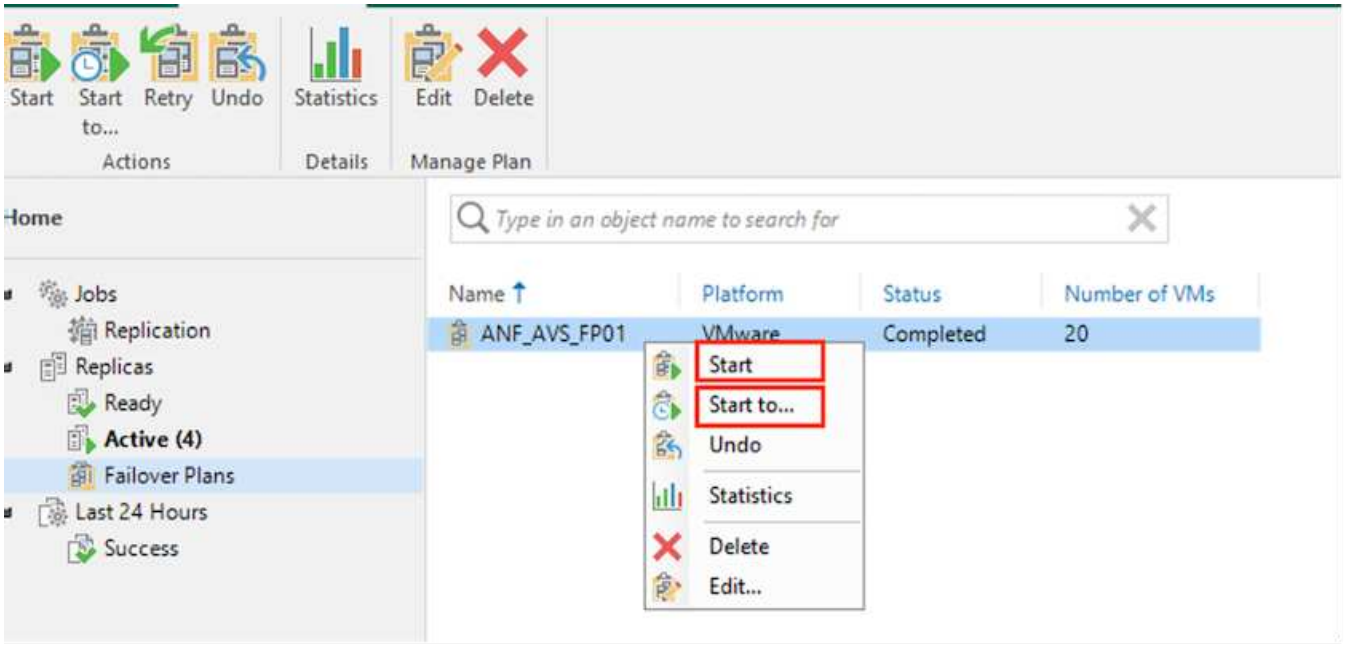
Para obtener información adicional sobre la creación de trabajos de replicación, consulte"Creación de trabajos de replicación" .

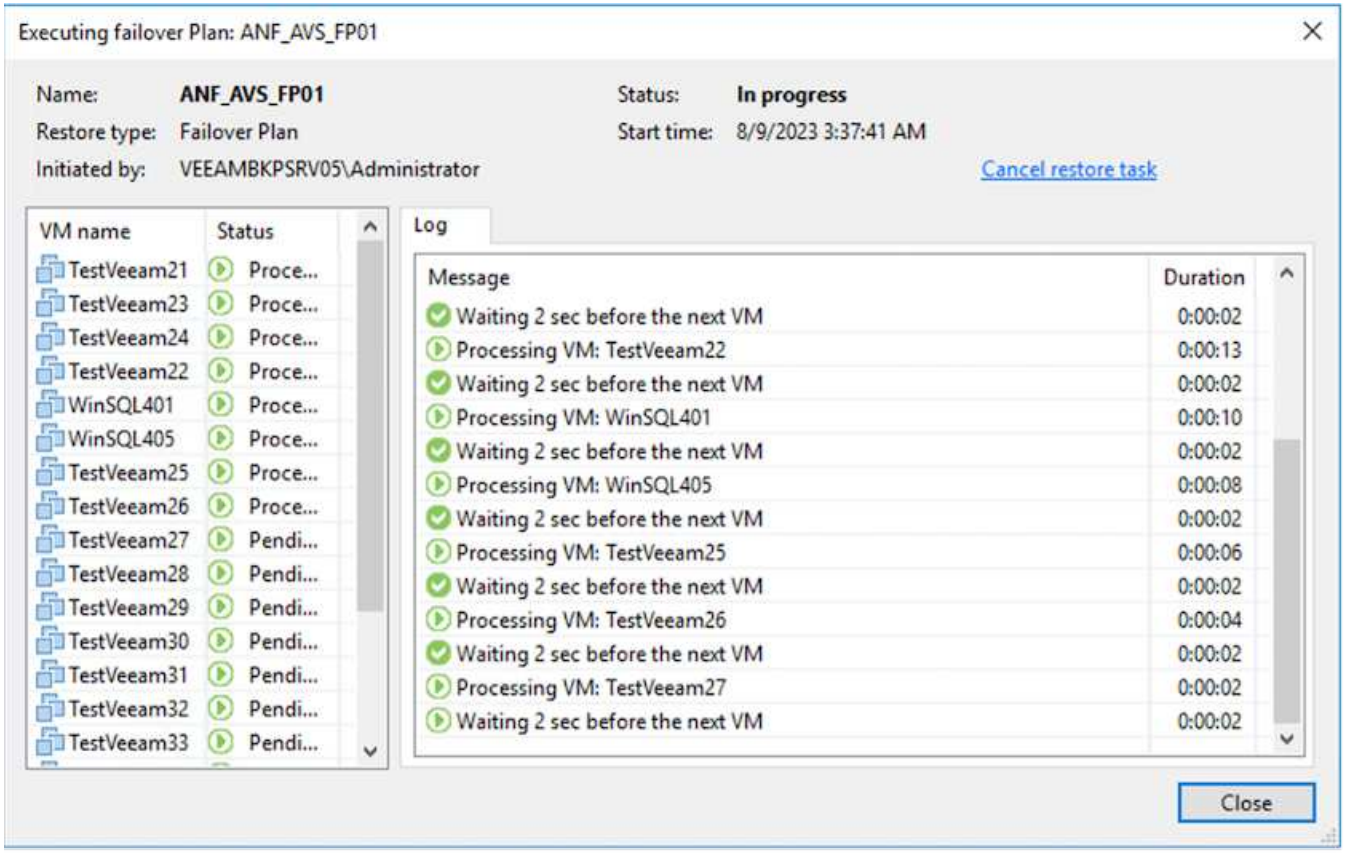
▼ **Paso 3: Ejecutar el plan de conmutación por error**

Durante la conmutación por error, la máquina virtual de origen en el sitio de producción se cambia a su réplica en el sitio de recuperación ante desastres. Como parte del proceso de conmutación por error, Veeam Backup & Replication restaura la réplica de la máquina virtual al punto de restauración requerido y mueve todas las actividades de E/S de la máquina virtual de origen a su réplica. Las réplicas se pueden utilizar no sólo en caso de desastre, sino también para simular simulacros de recuperación ante desastres. Durante la simulación de conmutación por error, la máquina virtual de origen permanece en ejecución. Una vez que se hayan realizado todas las pruebas necesarias, puede deshacer la conmutación por error y volver a las operaciones normales.

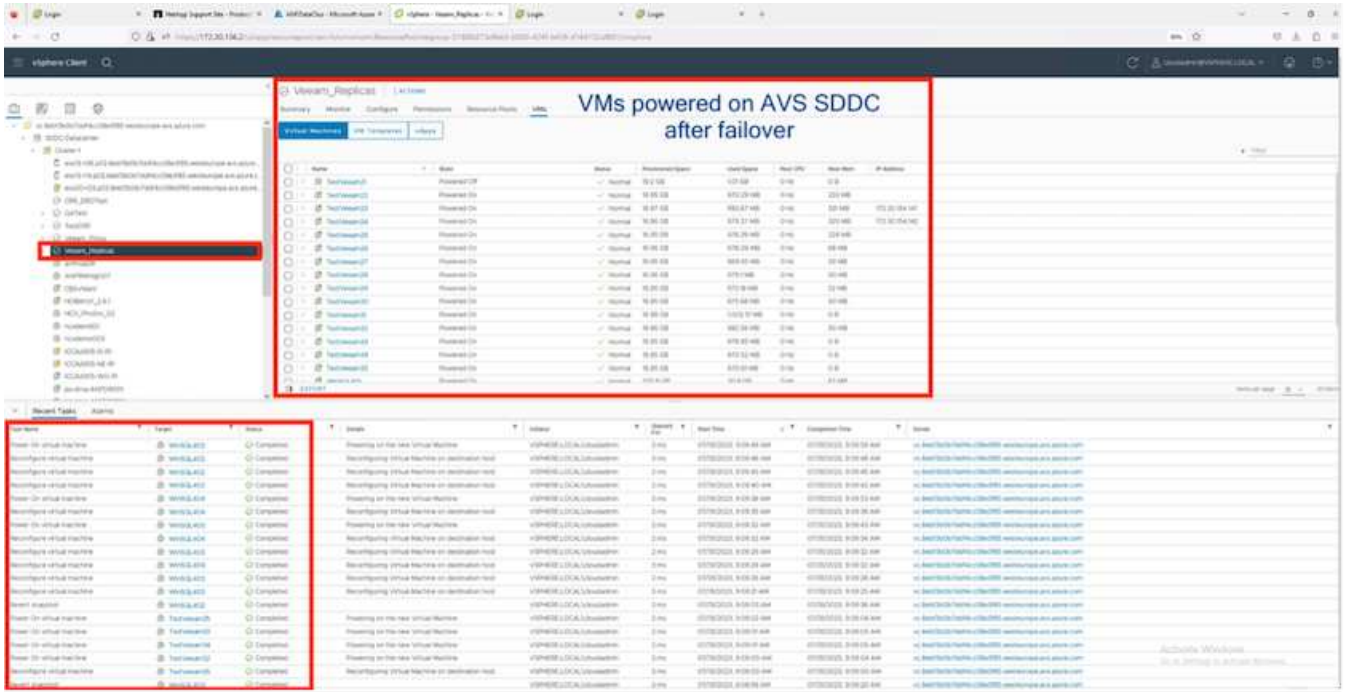
ⓘ Asegúrese de que la segmentación de la red esté implementada para evitar conflictos de IP durante la conmutación por error.

Para iniciar el plan de conmutación por error, simplemente haga clic en la pestaña **Planes de conmutación por error** y haga clic derecho en su plan de conmutación por error. Seleccione ***Inicio**. Esto conmutará por error utilizando los últimos puntos de restauración de las réplicas de VM. Para conmutar por error a puntos de restauración específicos de réplicas de máquinas virtuales, seleccione **Iniciar en**.

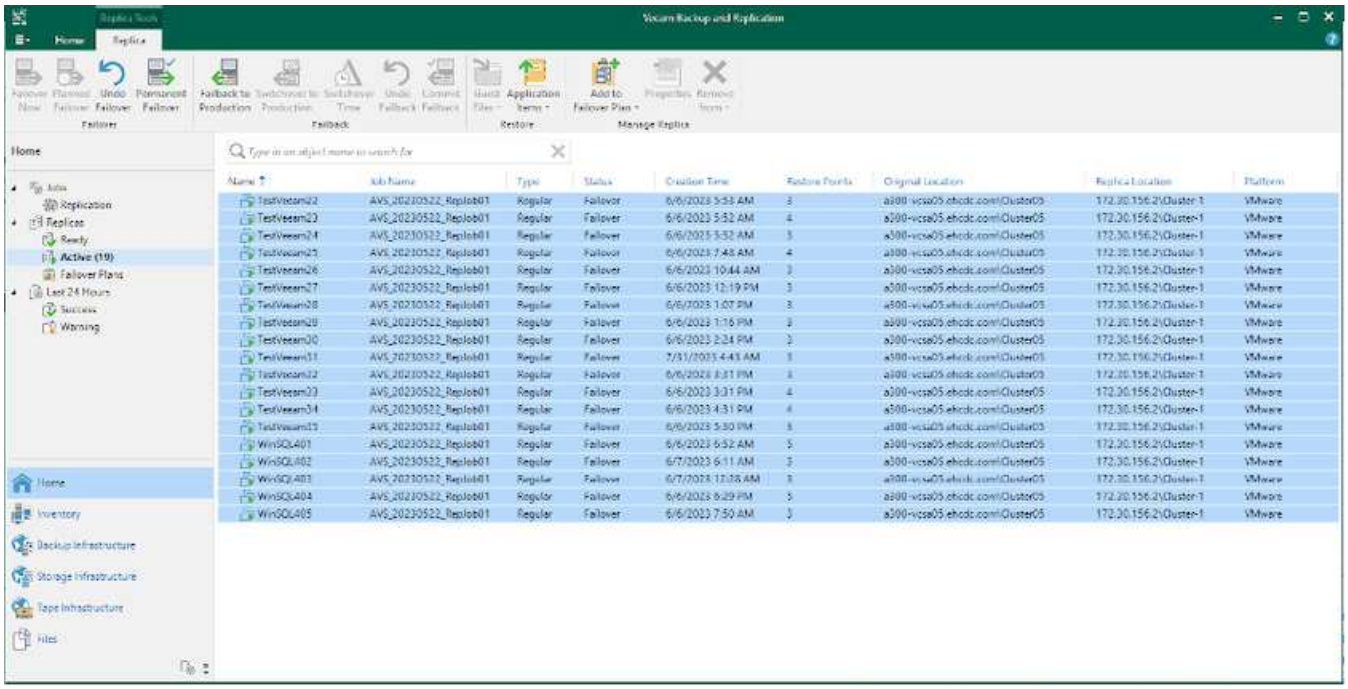




El estado de la réplica de la máquina virtual cambia de Listo a Conmutación por error y las máquinas virtuales se iniciarán en el host/clúster SDDC de Azure VMware Solution (AVS) de destino.



Una vez completada la conmutación por error, el estado de las máquinas virtuales cambiará a "Conmutación por error".



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

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

▼ **Paso 4: Retorno al sitio de producción**

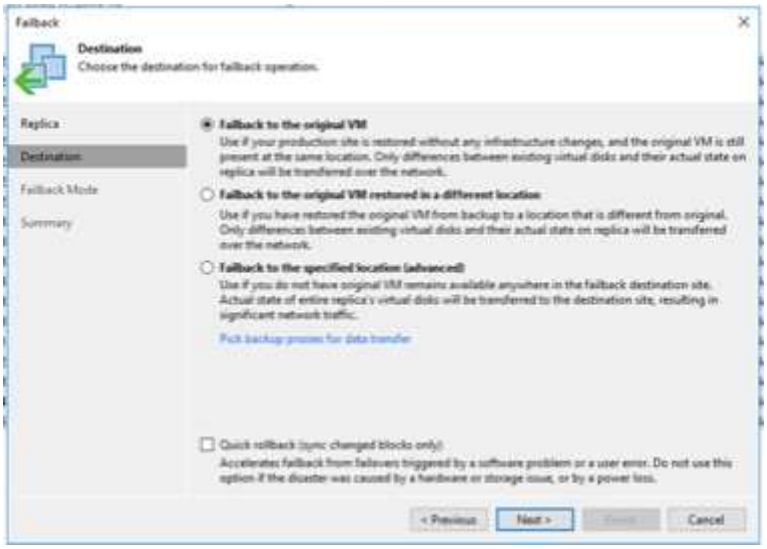
Cuando se ejecuta el plan de conmutación por error, se lo considera un paso intermedio y debe finalizarse según el requisito. Las opciones incluyen lo siguiente:

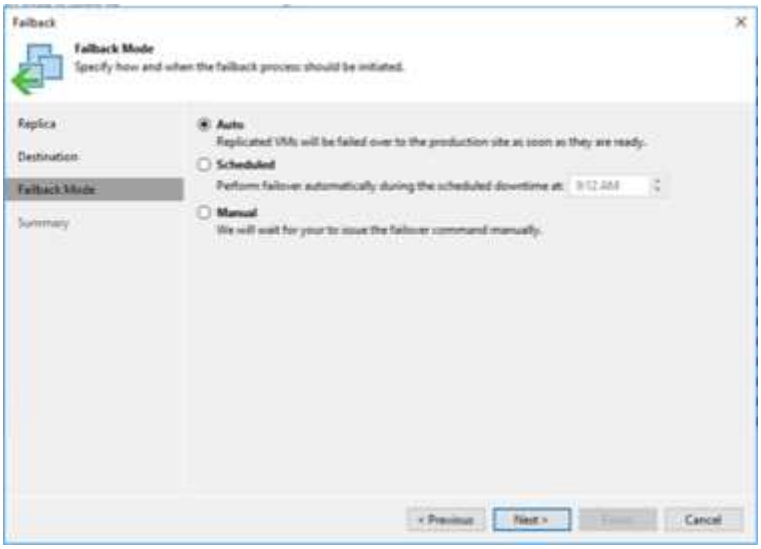
- **Retorno a producción**: vuelve a la máquina virtual original y transfiere todos los cambios que tuvieron lugar mientras la réplica de la máquina virtual estaba en ejecución a la máquina virtual original.

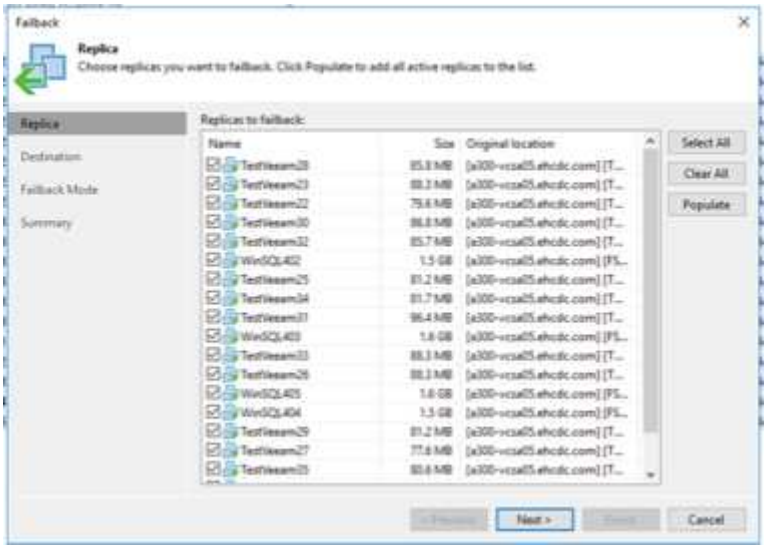
> Al realizar una conmutación por error, los cambios solo se transfieren, pero no se publican. Seleccione **Confirmar conmutación por error** (una vez que se confirme que la VM original funciona como se espera) o Deshacer conmutación por error para volver a la réplica de la VM si la VM original no funciona como se espera.

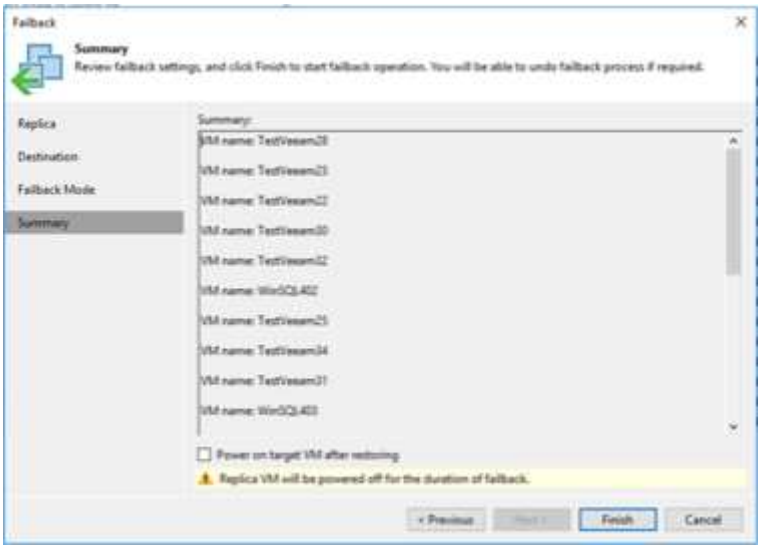
- **Deshacer conmutación por error**: vuelve a la máquina virtual original y descarta todos los cambios realizados en la réplica de la máquina virtual mientras estaba en ejecución.
- **Conmutación por error permanente**: cambia de forma permanente de la máquina virtual original a una réplica de máquina virtual y utiliza esta réplica como la máquina virtual original.

En esta demostración, se eligió Failback a producción. Se seleccionó la opción de retorno a la máquina virtual original durante el paso Destino del asistente y se habilitó la casilla de verificación "Encender la máquina virtual después de restaurar".



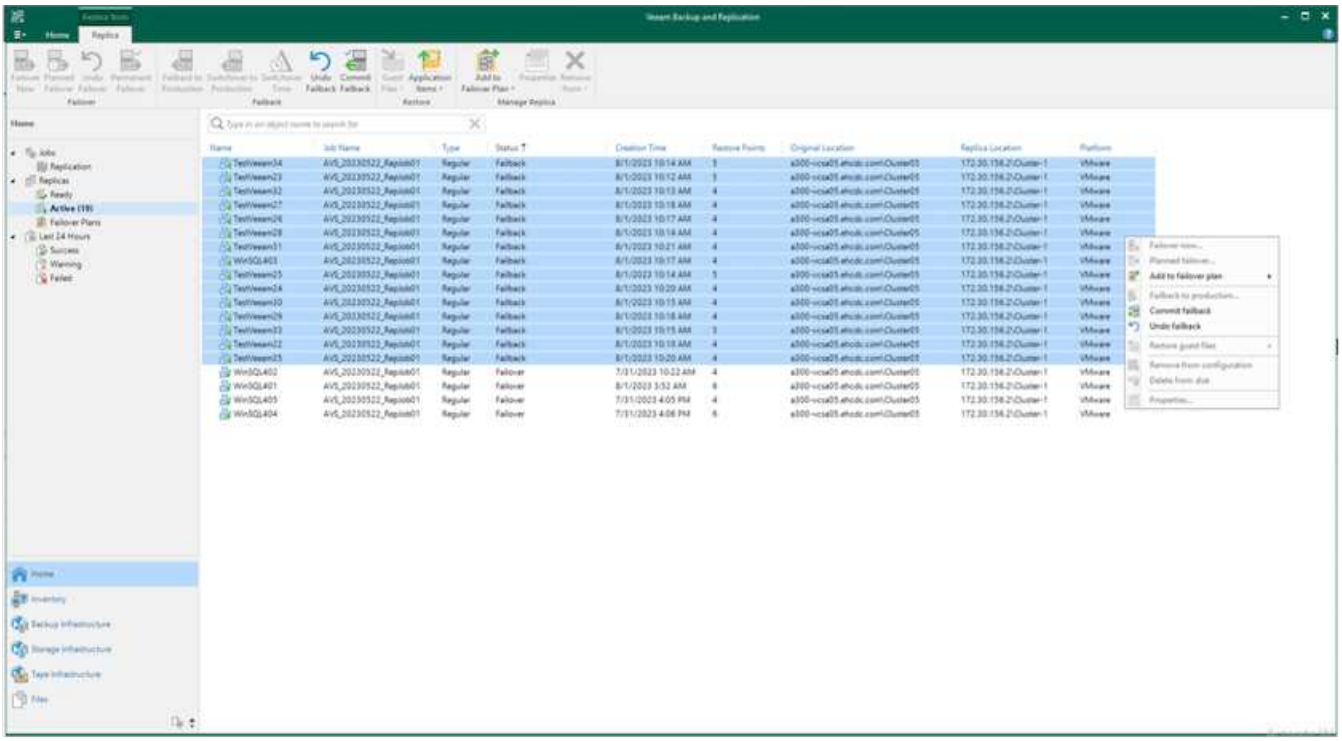




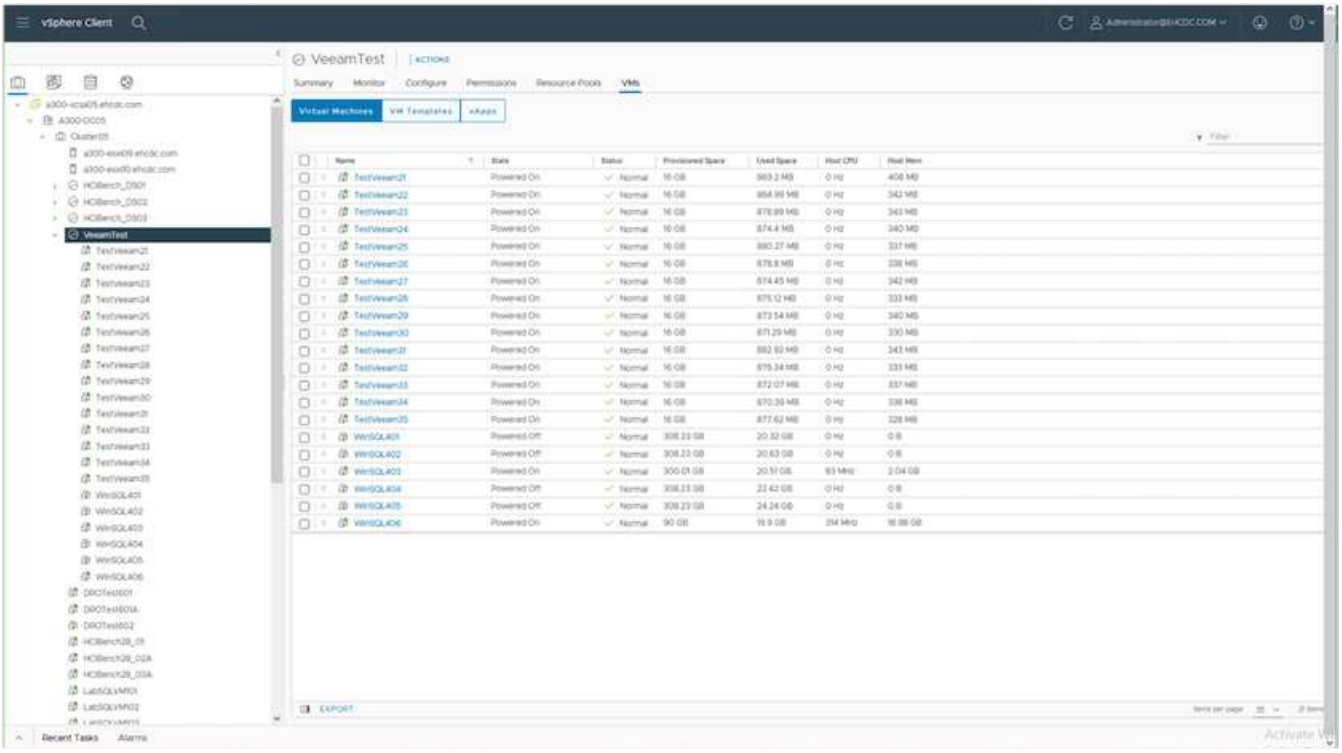


La confirmación de conmutación por error es una de las formas de finalizar la operación de conmutación por error. Cuando se confirma la conmutación por error, se confirma que los cambios enviados a la máquina virtual que se conmutó (la máquina virtual de producción) funcionan como se esperaba. Después de 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 error, consulte la documentación de Veeam."Conmutación por error y recuperación para replicación" .



Una vez que la conmutación a producción es exitosa, todas las máquinas virtuales se restauran al sitio de producción original.



Conclusión

La capacidad de almacenamiento de datos de Azure NetApp Files permite que Veeam o cualquier herramienta de terceros validada proporcione una solución de recuperación ante desastres de bajo costo al aprovechar clústeres Pilot Light en lugar de crear un clúster grande solo para acomodar réplicas de máquinas virtuales. Esto proporciona una manera eficaz de gestionar un plan de recuperación ante desastres personalizado y

adaptado, y de reutilizar los productos de respaldo existentes internamente para DR, lo que permite una recuperación ante desastres basada en la nube al salir de los centros de datos de DR locales. Es posible realizar una conmutación por error haciendo clic en un botón en caso de desastre o realizar una conmutación por error automáticamente si ocurre un desastre.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Migrar cargas de trabajo en Azure/AVS

TR-4940: Migración de cargas de trabajo al almacén de datos de Azure NetApp Files mediante VMware HCX - Guía de inicio rápido

Uno de los casos de uso más comunes del almacén de datos de Azure VMware Solution y Azure NetApp Files es la migración de cargas de trabajo de VMware. VMware HCX es una opción preferida y proporciona varios mecanismos de migración para trasladar máquinas virtuales (VM) locales y sus datos a almacenes de datos de Azure NetApp Files .

Descripción general: Migración de máquinas virtuales con VMware HCX, almacenes de datos de Azure NetApp Files y la solución Azure VMware

VMware HCX es principalmente una plataforma de migración diseñada para simplificar la migración de aplicaciones, el reequilibrio de la carga de trabajo e incluso la continuidad del negocio en las nubes. Se incluye como parte de Azure VMware Solution Private Cloud y ofrece muchas formas de migrar cargas de trabajo y se puede utilizar para operaciones de recuperación ante desastres (DR).

Este documento proporciona una guía paso a paso para aprovisionar un almacén de datos de Azure NetApp Files, seguido de la descarga, la implementación y la configuración de VMware HCX, incluidos todos sus componentes principales en las instalaciones locales y en el lado de Azure VMware Solution, incluida la interconexión, la extensión de red y la optimización de WAN para habilitar varios mecanismos de migración de VM.

> VMware HCX funciona con cualquier tipo de almacén de datos, ya que la migración se realiza a nivel de máquina virtual. Por lo tanto, este documento es aplicable a clientes existentes de NetApp y a clientes que no son de NetApp que planean implementar Azure NetApp Files con Azure VMware Solution para una implementación de nube VMware rentable.

▼ **Pasos de alto nivel**

Esta lista proporciona los pasos de alto nivel necesarios para instalar y configurar HCX Cloud Manager en el lado de la nube de Azure e instalar HCX Connector en las instalaciones:

1. Instale HCX a través del portal de Azure.
2. Descargue e implemente el instalador de HCX Connector Open Virtualization Appliance (OVA) en el servidor VMware vCenter local.
3. Active HCX con la clave de licencia.
4. Empareje el conector VMware HCX local con Azure VMware Solution HCX Cloud Manager.
5. Configurar el perfil de red, el perfil de cómputo y la malla de servicio.
6. (Opcional) Realice la extensión de la red para evitar la re-IP durante las migraciones.

7. Validar el estado del dispositivo y asegurarse de que la migración sea posible.
8. Migrar las cargas de trabajo de la máquina virtual.

▼ Prerrequisitos

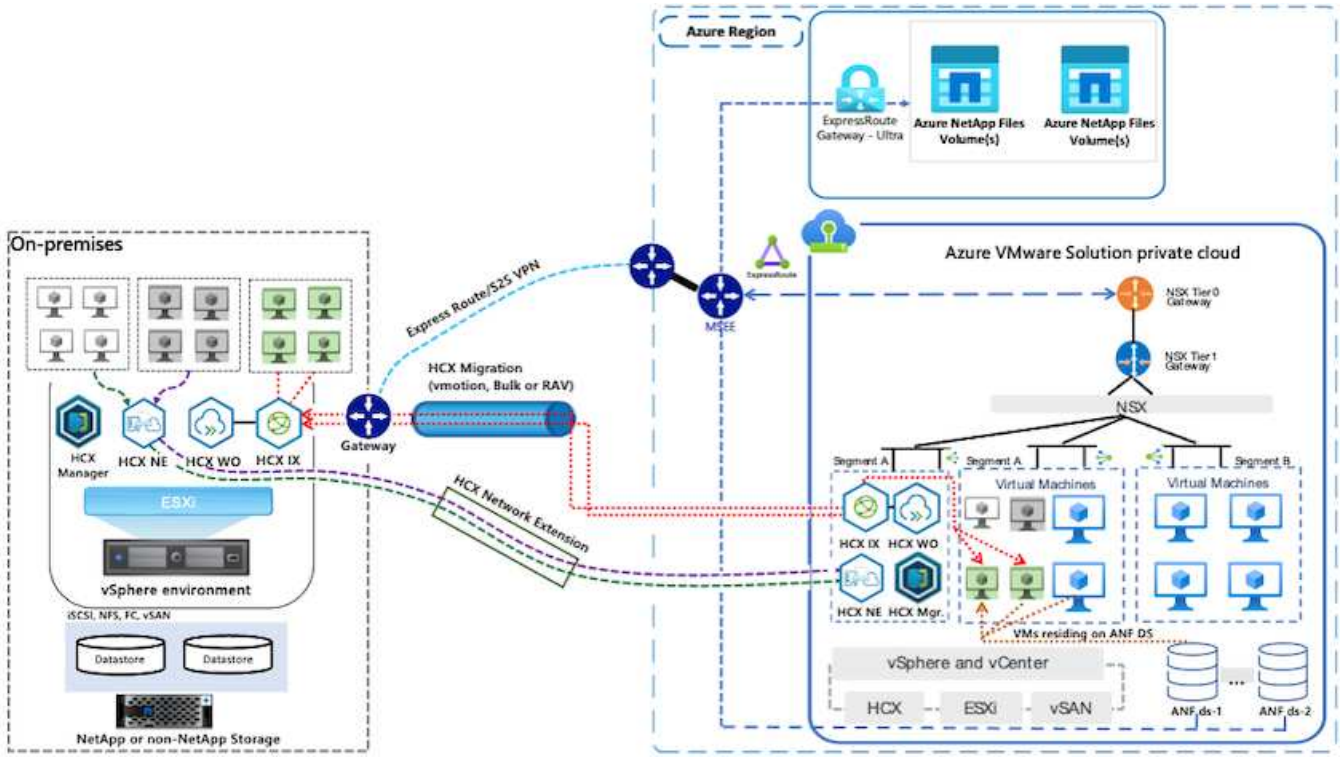
Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte este "enlace" . Una vez cumplidos los requisitos previos, incluida la conectividad, configure y active HCX generando la clave de licencia desde el portal de Azure VMware Solution. Después de descargar el instalador de OVA, continúe con el proceso de instalación como se describe a continuación.

> ⓘ HCX Advanced es la opción predeterminada y la edición VMware HCX Enterprise también está disponible a través de un ticket de soporte y recibe soporte sin costo adicional.

- Utilice un centro de datos definido por software (SDDC) de la solución VMware de Azure existente o cree una nube privada mediante este"Enlace de NetApp" o esto "Enlace de Microsoft" .
- La migración de máquinas virtuales y datos asociados desde el centro de datos local habilitado para VMware vSphere requiere conectividad de red desde el centro de datos al entorno SDDC. Antes de migrar cargas de trabajo, "Configurar una conexión VPN de sitio a sitio o una conexión de alcance global de Express Route" entre el entorno local y la respectiva nube privada.
- La ruta de red desde el entorno local de VMware vCenter Server a la nube privada de Azure VMware Solution debe admitir la migración de máquinas virtuales mediante vMotion.
- Asegúrese de que se cumplan los requisitos "reglas y puertos de firewall" Se permiten para el tráfico de vMotion entre el servidor vCenter local y el vCenter de SDDC. En la nube privada, el enrutamiento en la red vMotion está configurado de forma predeterminada.
- El volumen NFS de Azure NetApp Files debe montarse como un almacén de datos en Azure VMware Solution. Siga los pasos detallados en este "enlace" para conectar almacenes de datos de Azure NetApp Files a los hosts de Azure VMware Solutions.

▼ Arquitectura de alto nivel

Para fines de prueba, el entorno de laboratorio local utilizado para esta validación se conectó a través de una VPN de sitio a sitio, lo que permite la conectividad local con Azure VMware Solution.



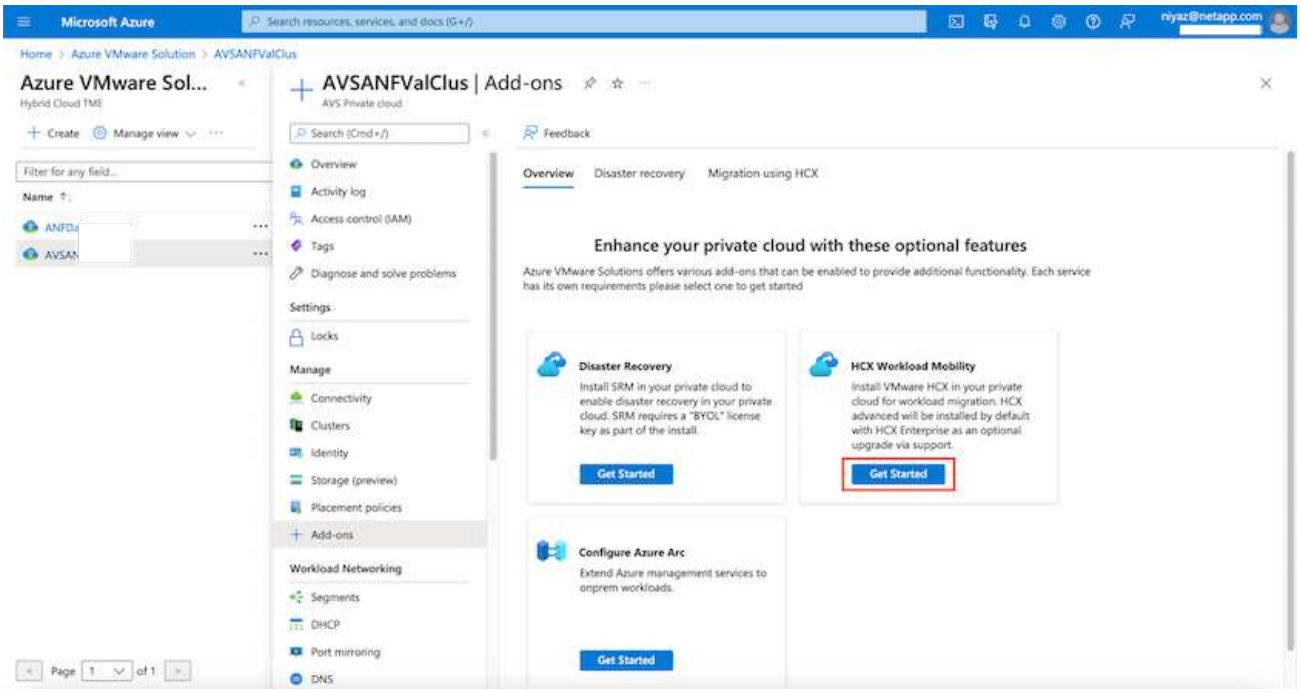
Implementación de la solución

Siga la serie de pasos para completar la implementación de esta solución:

▼ **Paso 1: Instale HCX a través del Portal de Azure usando la opción Complementos**

Para realizar la instalación, complete los siguientes pasos:

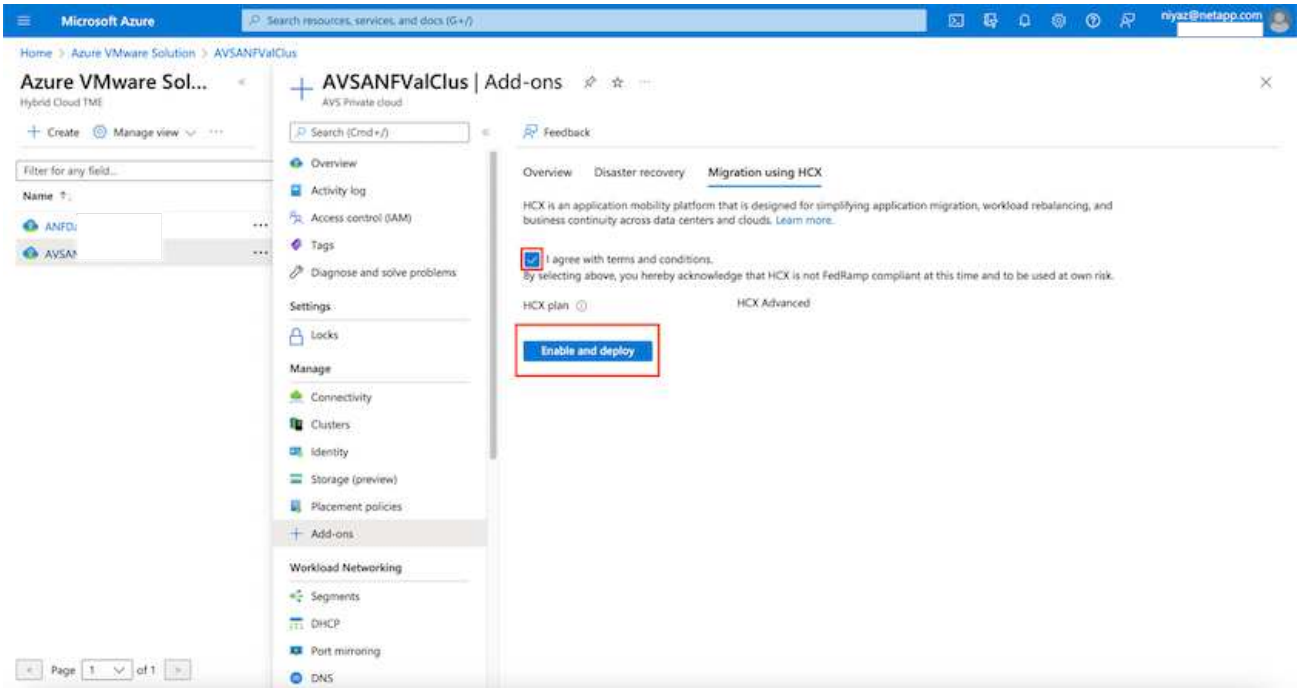
1. Inicie sesión en el Portal de Azure y acceda a la nube privada de Azure VMware Solution.
2. Seleccione la nube privada adecuada y acceda a Complementos. Esto se puede hacer navegando a **Administrar > Complementos**.
3. En la sección Movilidad de carga de trabajo de HCX, haga clic en **Comenzar**.



4. Seleccione la opción **Acepto los términos y condiciones** y haga clic en **Habilitar e implementar**.

> La implementación predeterminada es HCX Advanced. Abra una solicitud de soporte para habilitar la edición Enterprise.

> La implementación demora aproximadamente entre 25 y 30 minutos.



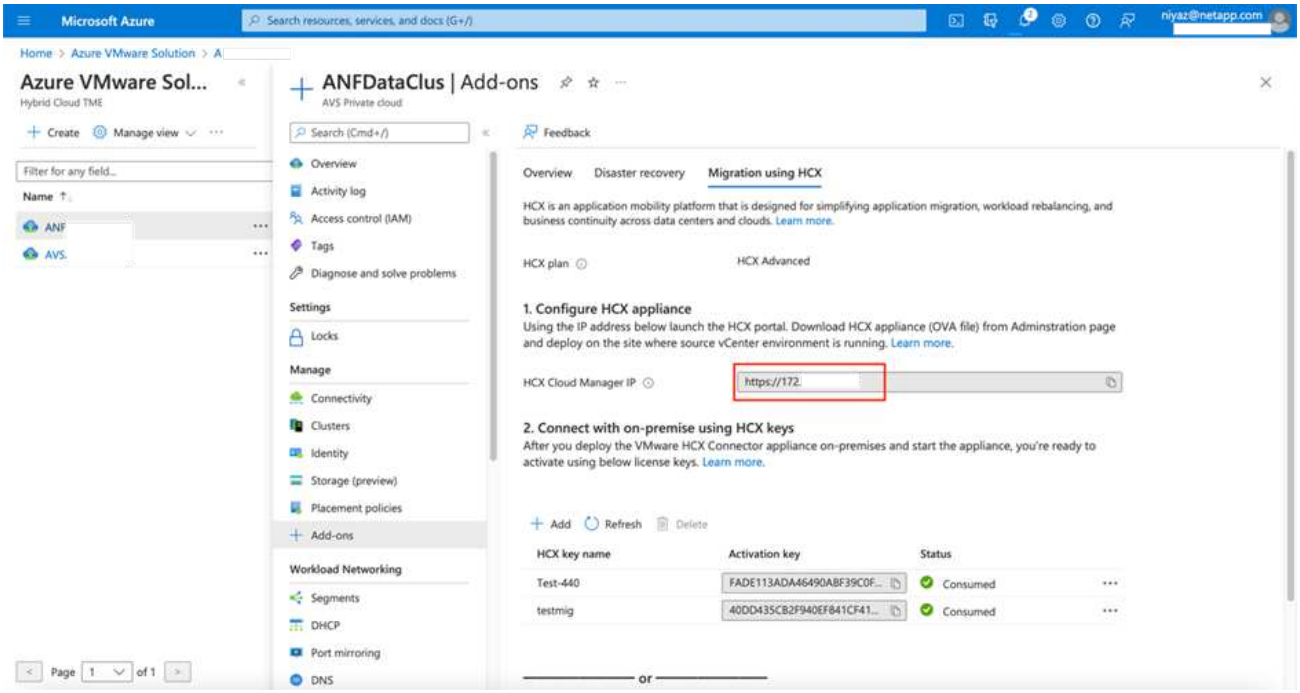
▼ **Paso 2: Implementar el instalador OVA en el servidor vCenter local**

Para que el conector local se conecte al HCX Manager en Azure VMware Solution, asegúrese de que los puertos de firewall adecuados estén abiertos en el entorno local.

Para descargar e instalar HCX Connector en el vCenter Server local, complete los siguientes pasos:

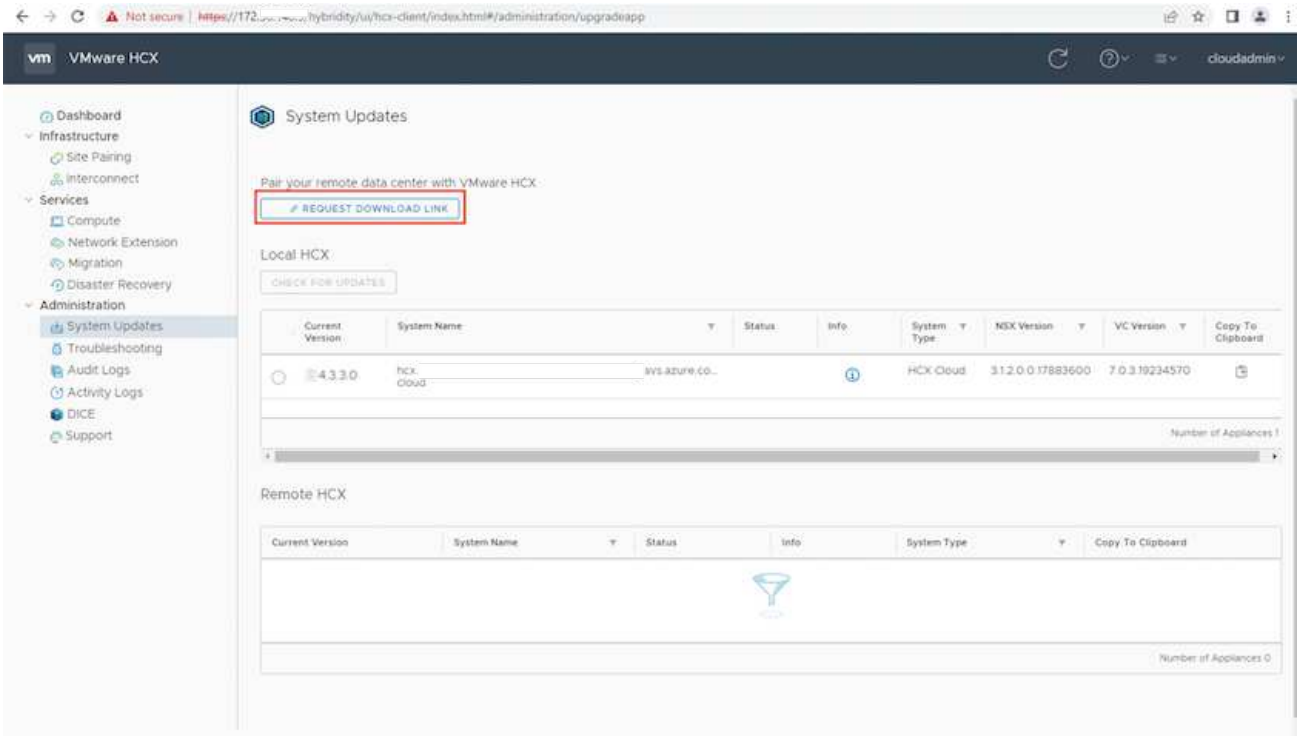
1. Desde el portal de Azure, vaya a Azure VMware Solution, seleccione la nube privada y seleccione **Administrar > Complementos > Migración** usando HCX y copie el portal de HCX Cloud Manager para descargar el archivo OVA.

   Utilice las credenciales de usuario CloudAdmin predeterminadas para acceder al portal HCX.

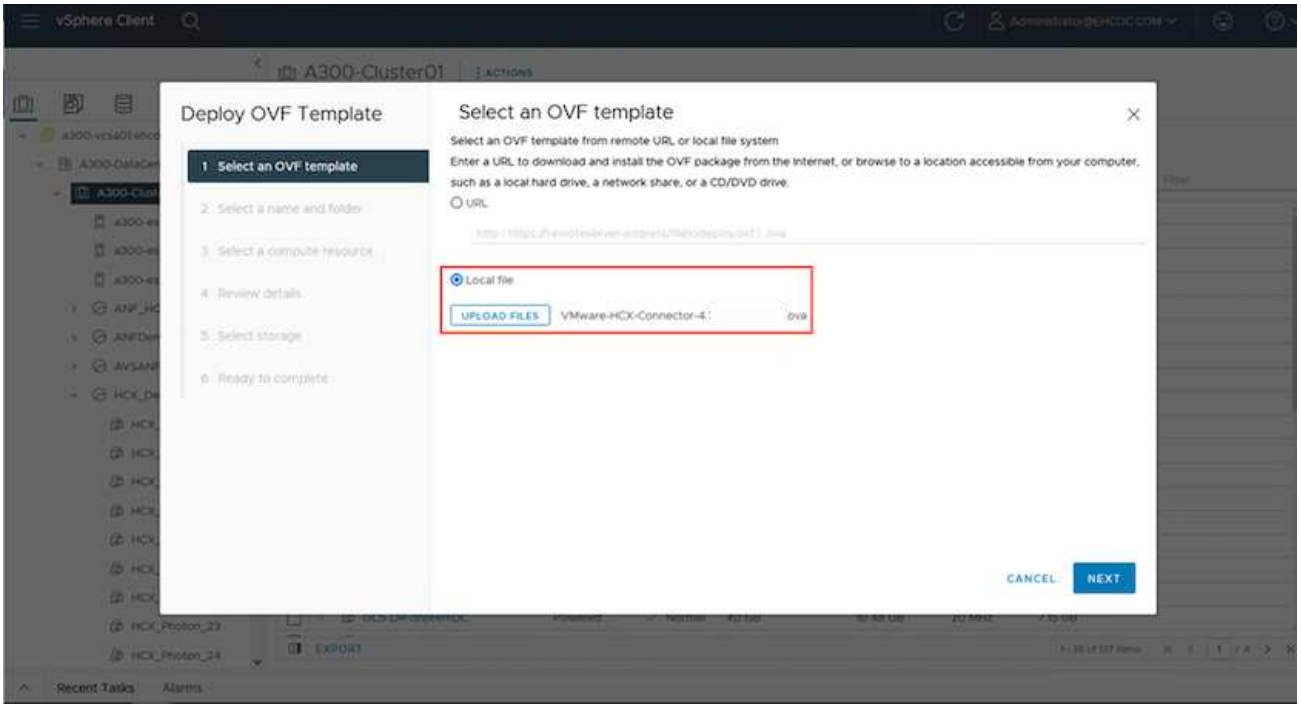


2. Después de acceder al portal HCX con cloudadmin@vsphere.local usando jumphost, navegue a **Administración > Actualizaciones del sistema** y haga clic en **Solicitar enlace de descarga**.

   Descargue o copie el enlace al OVA y péguelo en un navegador para comenzar el proceso de descarga del archivo OVA de VMware HCX Connector para implementarlo en el servidor vCenter local.



3. Una vez descargado el OVA, impleméntelo en el entorno local de VMware vSphere utilizando la opción **Implementar plantilla OVF**.



4. Ingrese toda la información requerida para la implementación de OVA, haga clic en **Siguiente** y luego haga clic en **Finalizar** para implementar el OVA del conector VMware HCX.

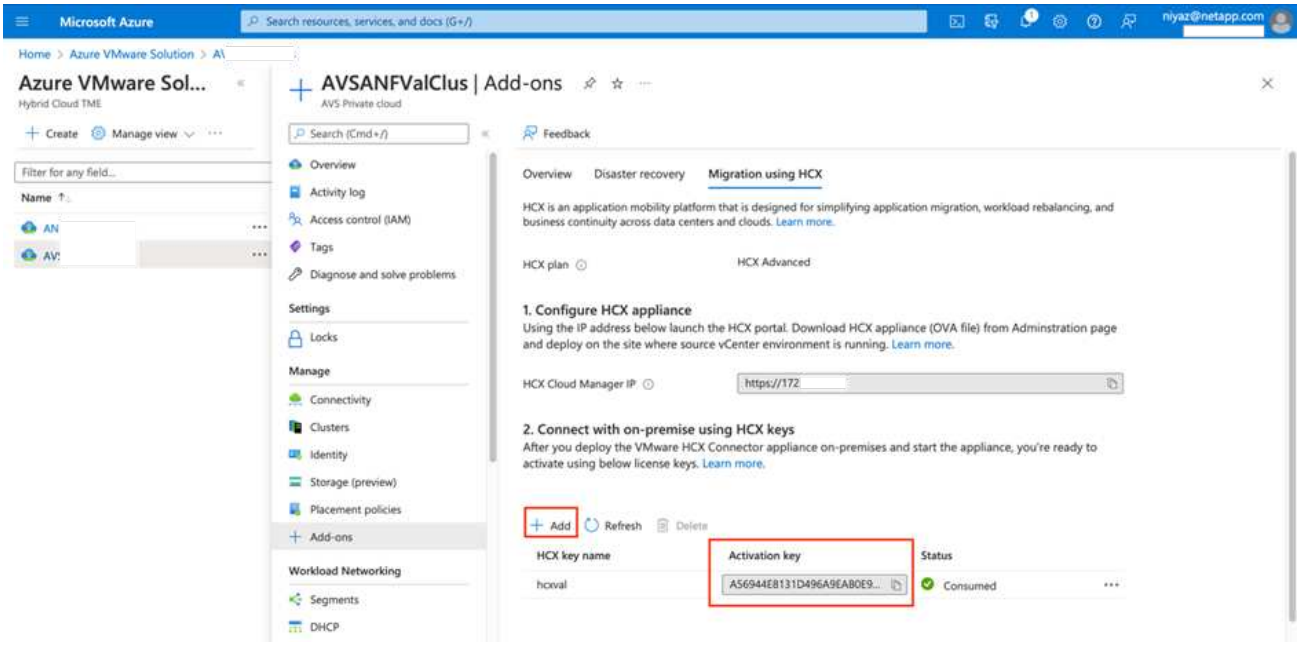
Encienda el dispositivo virtual manualmente.

Para obtener instrucciones paso a paso, consulte la "Guía del usuario de VMware HCX" .

▼ Paso 3: Activar el conector HCX con la clave de licencia

Después de implementar VMware HCX Connector OVA en las instalaciones e iniciar el dispositivo, complete los siguientes pasos para activar HCX Connector. Genere la clave de licencia desde el portal de Azure VMware Solution y actívela en VMware HCX Manager.

1. Desde el portal de Azure, vaya a Azure VMware Solution, seleccione la nube privada y seleccione **Administrar > Complementos > Migración mediante HCX**.
2. En **Conectarse con las instalaciones locales mediante claves HCX**, haga clic en **Agregar** y copie la clave de activación.



> Se requiere una clave separada para cada conector HCX local que se implemente.

3. Inicie sesión en VMware HCX Manager local en `"https://hcxmanagerIP:9443"` utilizando credenciales de administrador.

> Utilice la contraseña definida durante la implementación de OVA.

4. En la licencia, ingrese la clave copiada del paso 3 y haga clic en **Activar**.

> El conector HCX local debe tener acceso a Internet.

5. En **Ubicación del centro de datos**, proporcione la ubicación más cercana para instalar VMware HCX Manager en las instalaciones. Haga clic en **Continuar**.
6. En **Nombre del sistema**, actualice el nombre y haga clic en **Continuar**.
7. Haga clic en **Sí, continuar**.
8. En **Conectar su vCenter**, proporcione el nombre de dominio completo (FQDN) o la dirección IP de vCenter Server y las credenciales adecuadas y haga clic en **Continuar**.

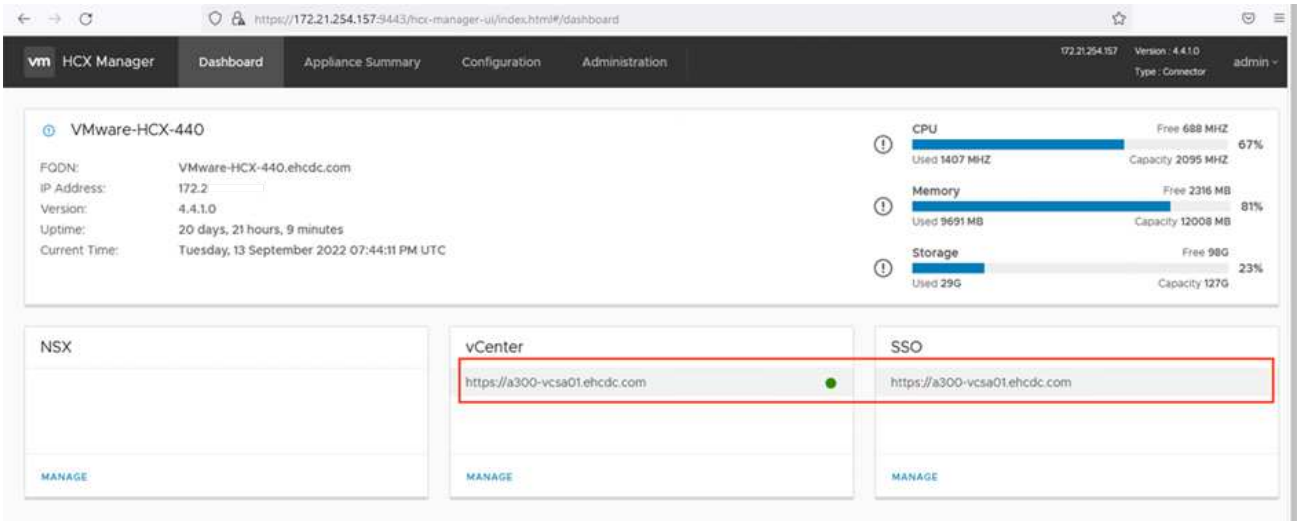
> Utilice el FQDN para evitar problemas de conectividad más adelante.

9. En **Configurar SSO/PSC**, proporcione el FQDN o la dirección IP del controlador de servicios de plataforma y haga clic en **Continuar**.

   Introduzca el FQDN o la dirección IP de VMware vCenter Server.

10. Verifique que la información ingresada sea correcta y haga clic en **Reiniciar**.
11. Después de reiniciar los servicios, vCenter Server se muestra en verde en la página que aparece. Tanto vCenter Server como SSO deben tener los parámetros de configuración adecuados, que deben ser los mismos que en la página anterior.

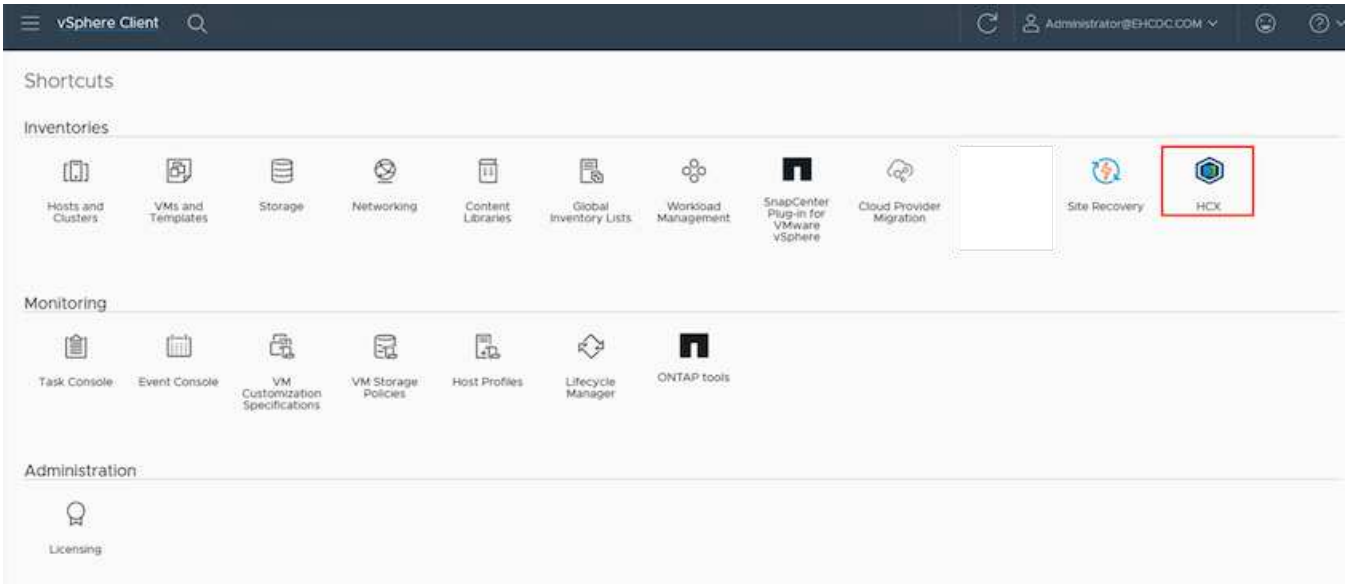
   Este proceso debería tardar aproximadamente entre 10 y 20 minutos para que el complemento se agregue al vCenter Server.



▼ **Paso 4: Vincular VMware HCX Connector local con Azure VMware Solution HCX Cloud Manager**

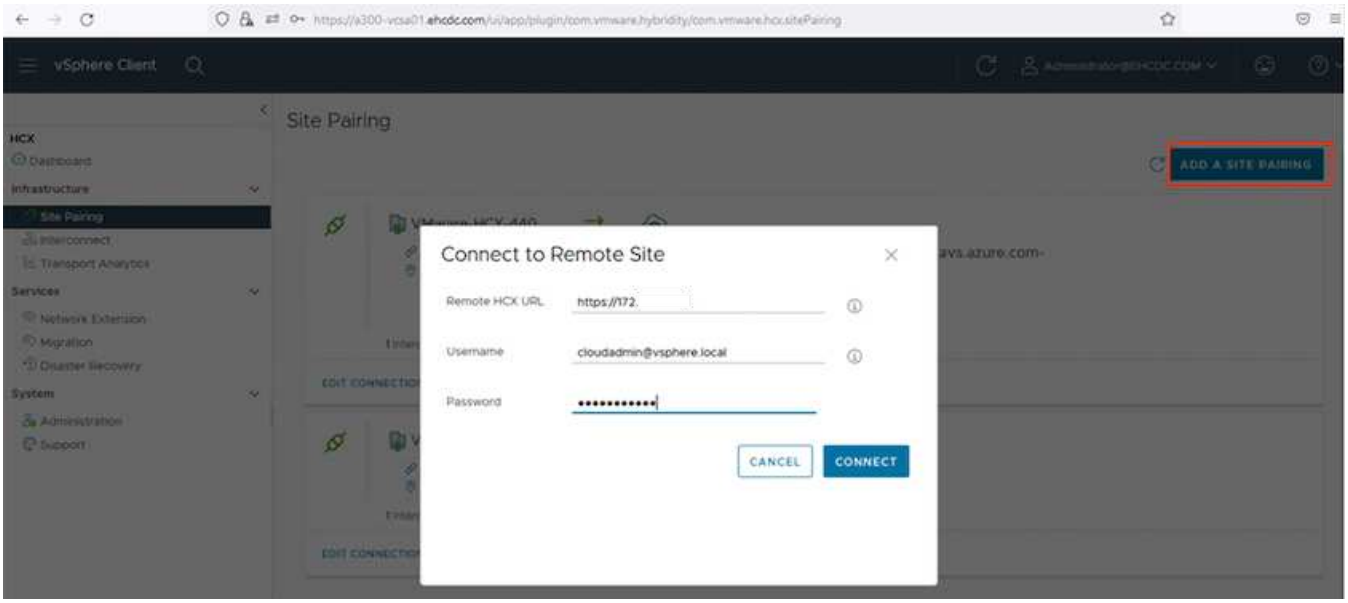
Una vez instalado el conector HCX tanto en la instancia local como en Azure VMware Solution, configure el conector HCX de VMware en la instancia local para la nube privada de Azure VMware Solution agregando el emparejamiento. Para configurar el emparejamiento del sitio, complete los siguientes pasos:

1. Para crear un par de sitios entre el entorno de vCenter local y Azure VMware Solution SDDC, inicie sesión en el servidor vCenter local y acceda al nuevo complemento HCX vSphere Web Client.



1. En Infraestructura, haga clic en **Agregar un emparejamiento de sitios**.

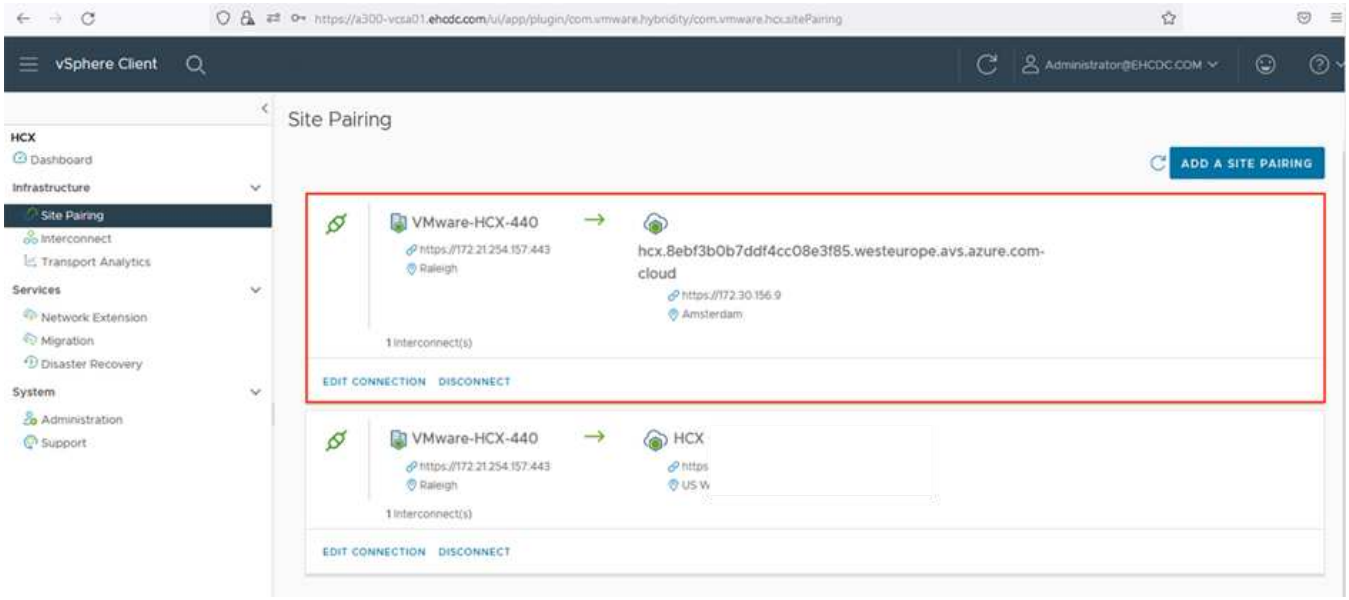
> Ingrese la dirección URL o IP de Azure VMware Solution HCX Cloud Manager y las credenciales para la función CloudAdmin para acceder a la nube privada.



1. Haga clic en **Conectar**.

> VMware HCX Connector debe poder enrutarse a la IP de HCX Cloud Manager a través del puerto 443.

1. Una vez creado el emparejamiento, el emparejamiento del sitio recién configurado estará disponible en el Panel de HCX.

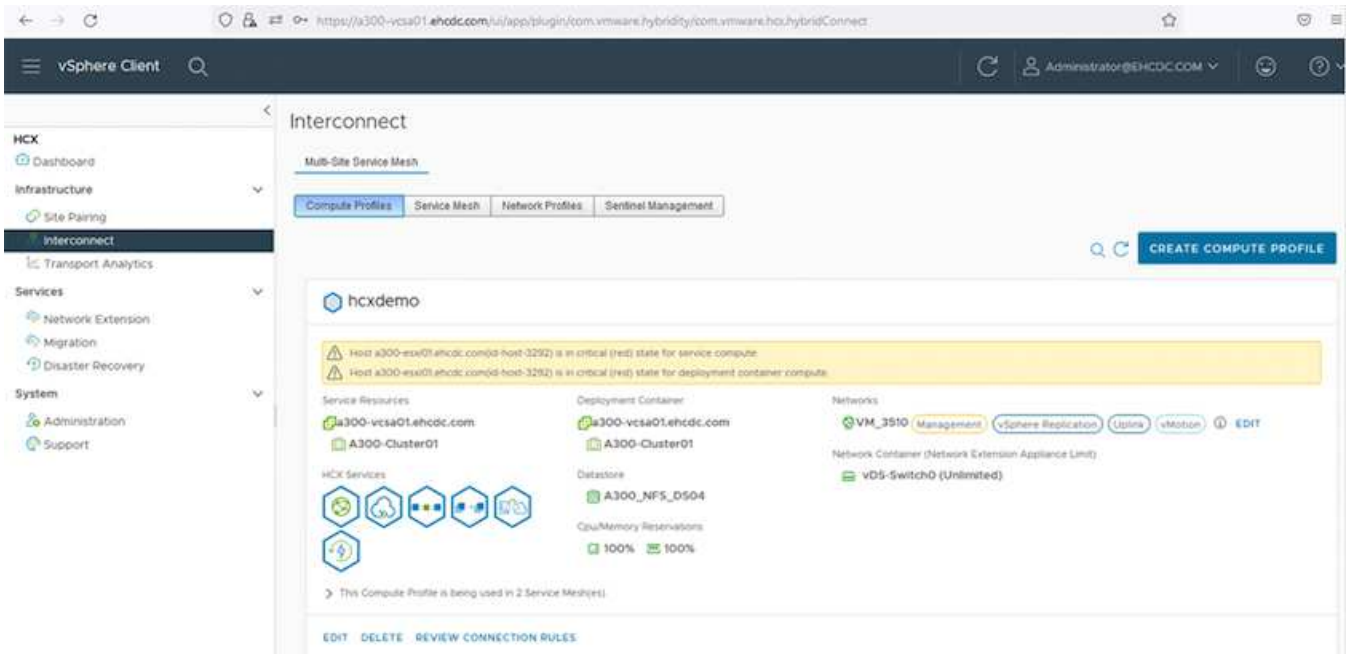


▼ **Paso 5: Configurar el perfil de red, el perfil de cómputo y la malla de servicio**

El dispositivo de servicio VMware HCX Interconnect proporciona capacidades de replicación y migración basadas en vMotion a través de Internet y conexiones privadas al sitio de destino. La interconexión proporciona cifrado, ingeniería de tráfico y movilidad de máquinas virtuales. Para crear un dispositivo de servicio de interconexión, complete los siguientes pasos:

1. En Infraestructura, seleccione **Interconexión > Malla de servicios multisitio > Perfiles de cómputo > Crear perfil de cómputo**.

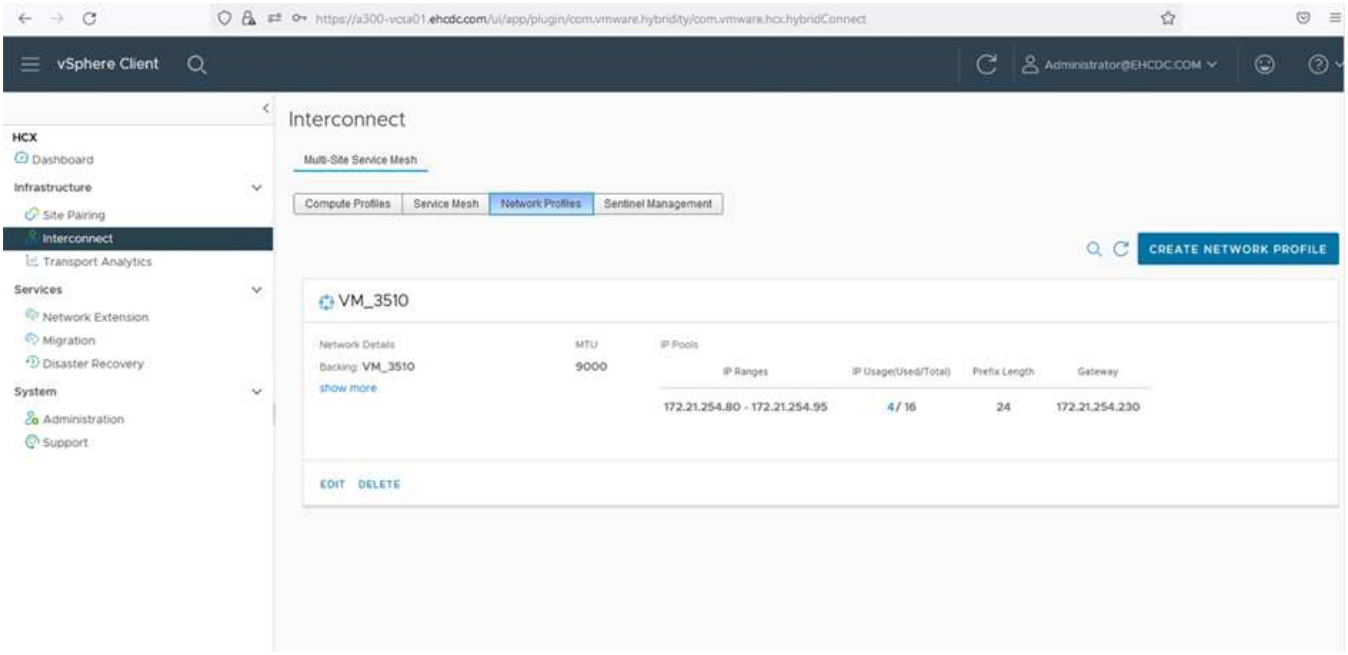
Los perfiles de cómputo definen los parámetros de implementación, incluidos los dispositivos que se implementan y qué parte del centro de datos de VMware es accesible para el servicio HCX.



1. Una vez creado el perfil de cómputo, cree los perfiles de red seleccionando **Multi-Site Service Mesh > Perfiles de red > Crear perfil de red**.

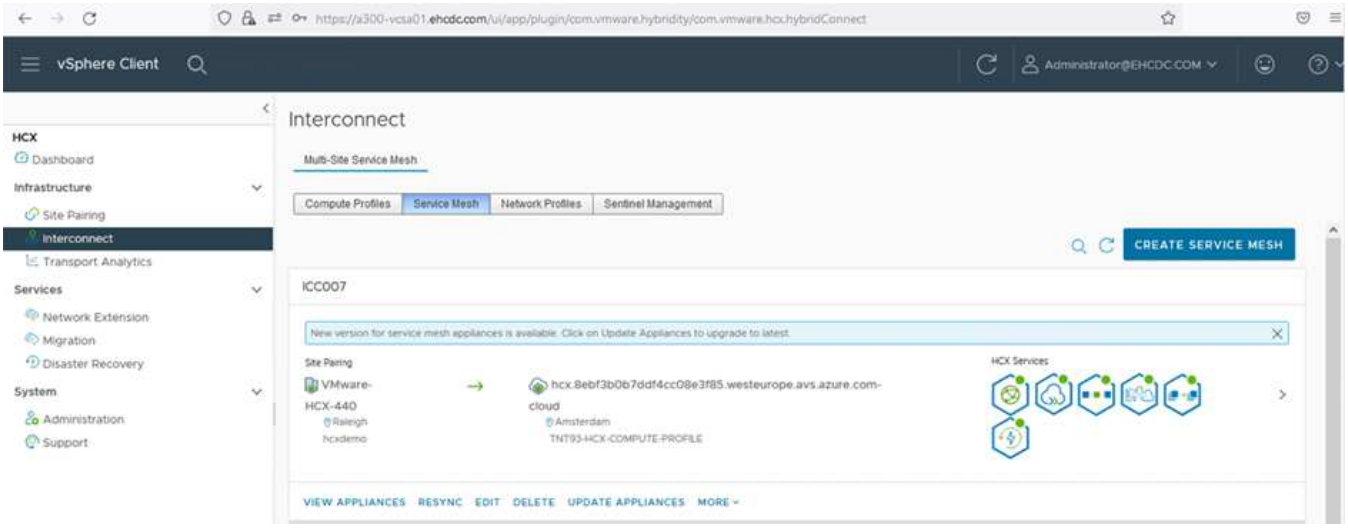
El perfil de red define un rango de direcciones IP y redes que HCX utiliza para sus dispositivos virtuales.

Este paso requiere dos o más direcciones IP. Estas direcciones IP se asignan desde la red de administración a los dispositivos de interconexión.



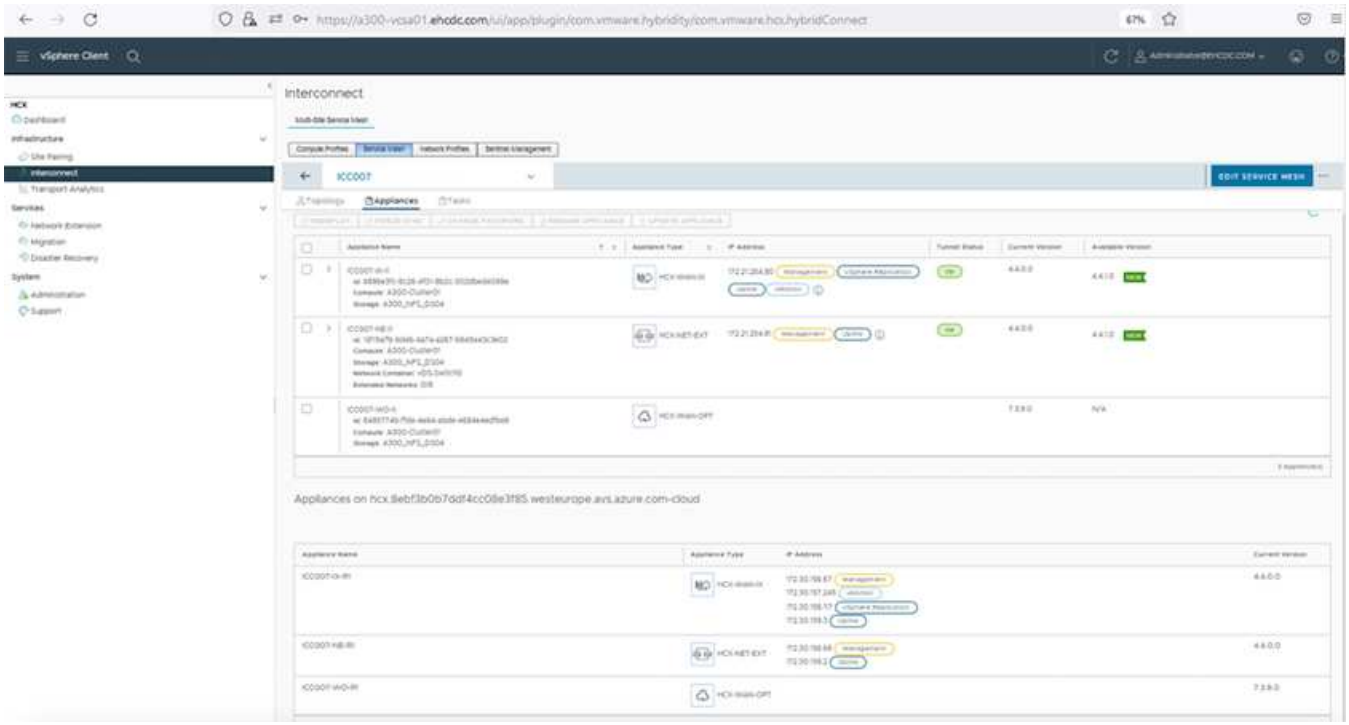
1. En este momento, los perfiles de cómputo y de red se han creado con éxito.
2. Cree Service Mesh seleccionando la pestaña **Service Mesh** dentro de la opción **Interconectar** y seleccione los sitios locales y de Azure SDDC.
3. Service Mesh especifica un par de perfiles de red y cómputo local y remoto.

Como parte de este proceso, los dispositivos HCX se implementan y configuran automáticamente tanto en los sitios de origen como de destino para crear una estructura de transporte segura.



1. Este es el paso final de la configuración. Esto debería tomar cerca de 30 minutos para completar la implementación. Una vez configurada la malla de servicio, el entorno está listo con los túneles IPsec

creados exitosamente para migrar las máquinas virtuales de carga de trabajo.



▼ **Paso 6: Migrar cargas de trabajo**

Las cargas de trabajo se pueden migrar de manera bidireccional entre los SDDC locales y de Azure mediante diversas tecnologías de migración de VMware HCX. Las máquinas virtuales se pueden mover hacia y desde entidades activadas por VMware HCX mediante múltiples tecnologías de migración, como migración masiva de HCX, HCX vMotion, migración en frío de HCX, HCX Replication Assisted vMotion (disponible con la edición HCX Enterprise) y HCX OS Assisted Migration (disponible con la edición HCX Enterprise).

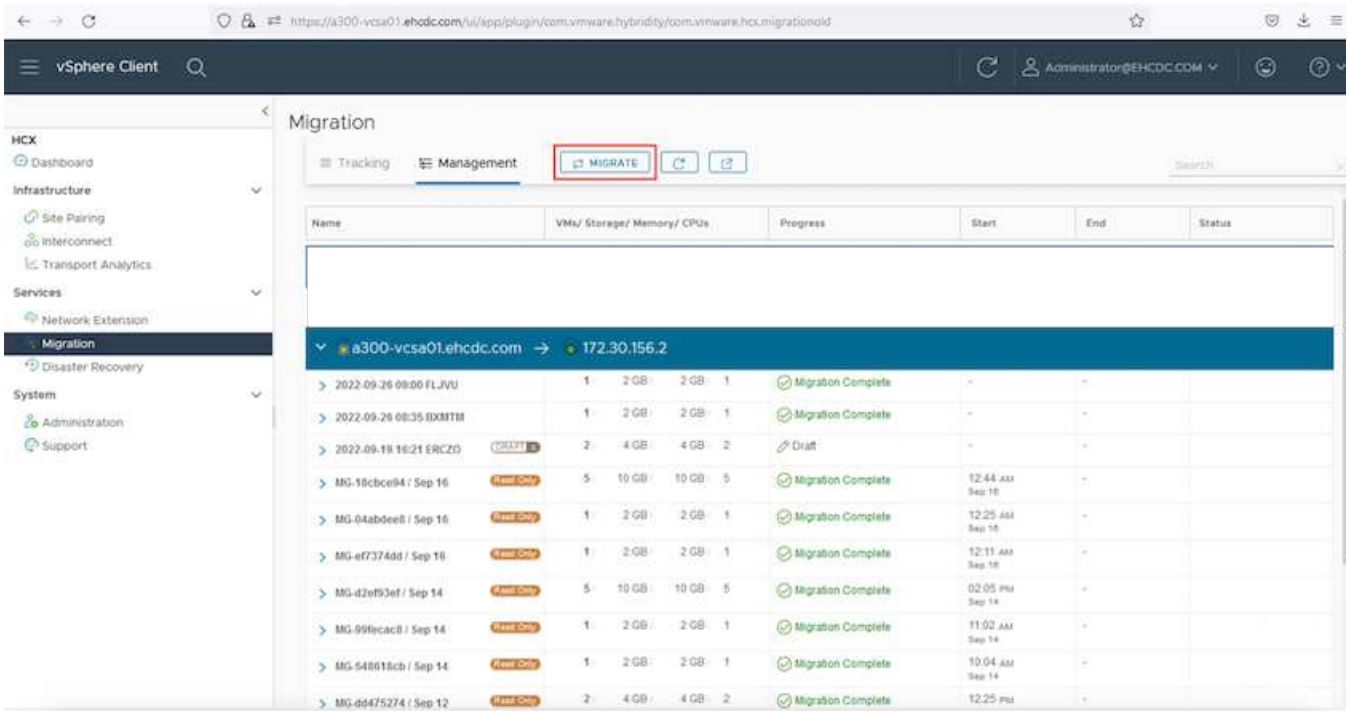
Para obtener más información sobre los distintos mecanismos de migración de HCX, consulte "Tipos de migración de VMware HCX" .

Migración masiva

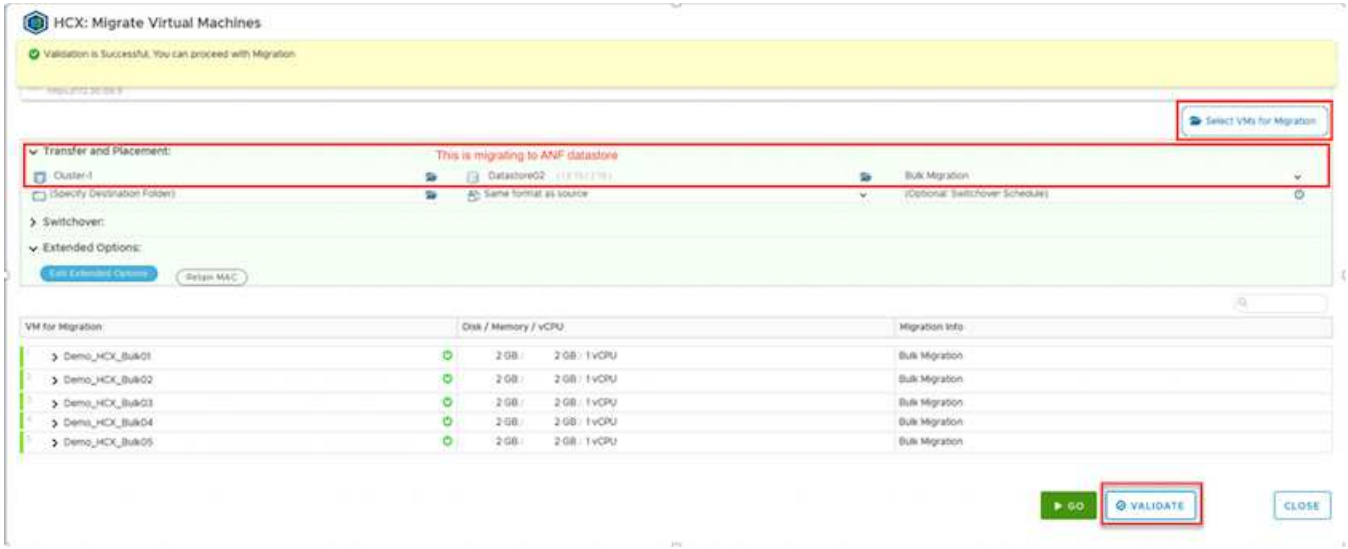
Esta sección detalla el mecanismo de migración masiva. Durante una migración masiva, la capacidad de migración masiva de HCX utiliza vSphere Replication para migrar archivos de disco mientras recrea la VM en la instancia de vSphere HCX de destino.

Para iniciar migraciones masivas de máquinas virtuales, complete los siguientes pasos:

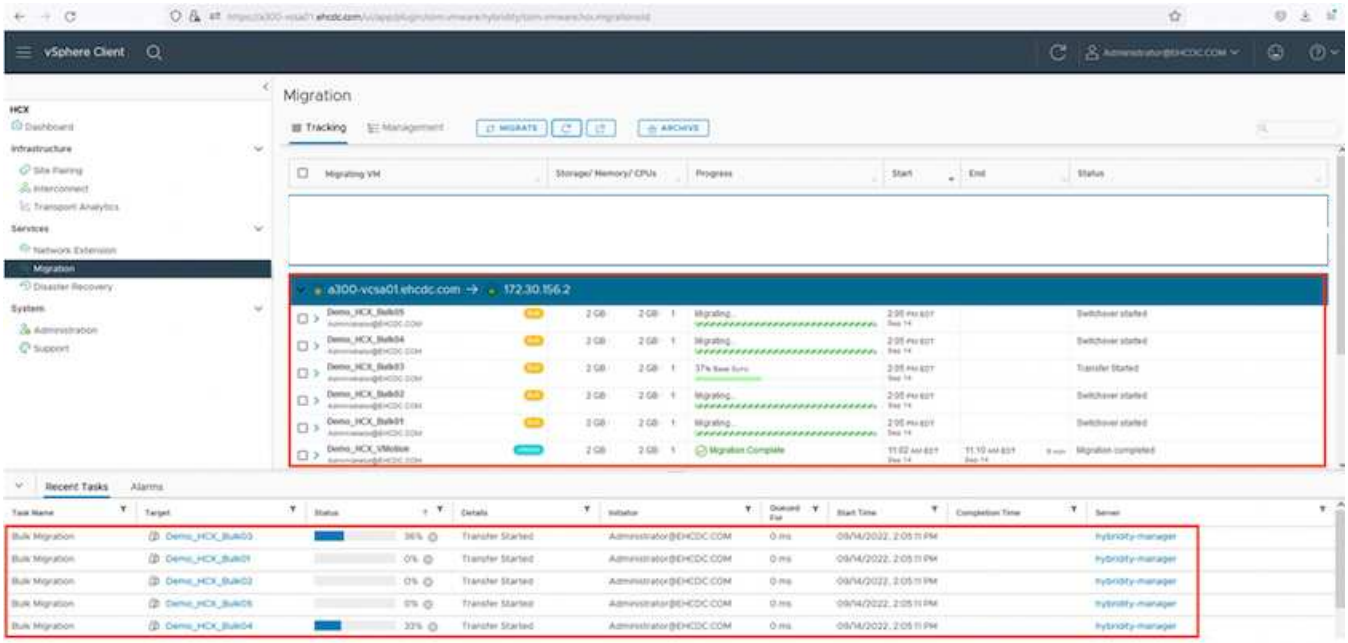
1. Acceda a la pestaña **Migrar** en **Servicios > Migración**.



1. En **Conexión de sitio remoto**, seleccione la conexión del sitio remoto y seleccione el origen y el destino. En este ejemplo, el destino es el punto final HCX de Azure VMware Solution SDDC.
2. Haga clic en **Seleccionar máquinas virtuales para migración**. Esto proporciona una lista de todas las máquinas virtuales locales. Seleccione las máquinas virtuales según la expresión match:value y haga clic en **Agregar**.
3. En la sección **Transferencia y ubicación**, actualice los campos obligatorios (**Clúster**, **Almacenamiento**, **Destino** y **Red**), incluido el perfil de migración, y haga clic en **Validar**.

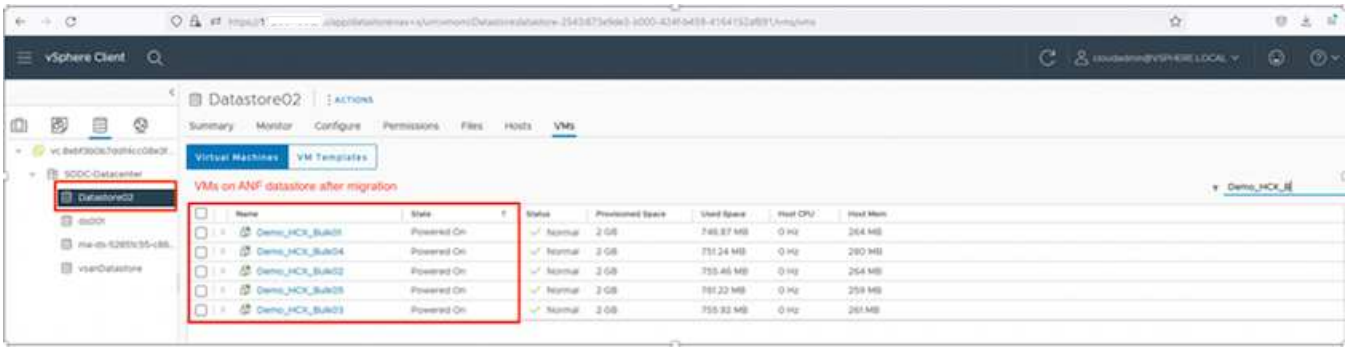


1. Una vez completadas las comprobaciones de validación, haga clic en **Ir** para iniciar la migración.



Durante esta migración, se crea un disco de marcador de posición en el almacén de datos de Azure NetApp Files especificado dentro del vCenter de destino para habilitar la replicación de los datos del disco de la máquina virtual de origen en los discos de marcador de posición. HBR se activa para una sincronización completa con el objetivo y, una vez completada la línea base, se realiza una sincronización incremental según el ciclo del objetivo del punto de recuperación (RPO). Una vez completada la sincronización completa/incremental, el cambio se activa automáticamente a menos que se establezca una programación específica.

1. Una vez completada la migración, valídela accediendo al vCenter del SDDC de destino.

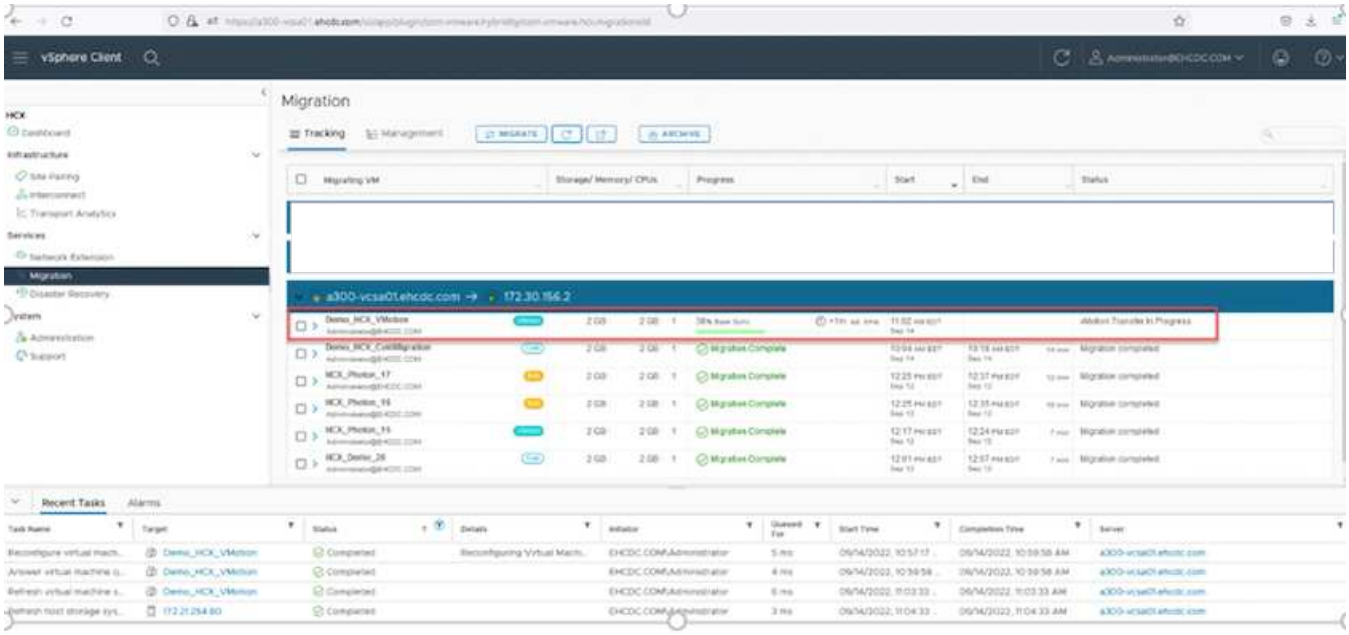


Para obtener información adicional y detallada sobre las distintas opciones de migración y sobre cómo migrar cargas de trabajo desde las instalaciones locales a Azure VMware Solution mediante HCX, consulte "Consideraciones sobre la migración de VMware HCX" .

Para obtener más información sobre este proceso, no dude en ver el siguiente vídeo:

Migración de carga de trabajo mediante HCX

Aquí hay una captura de pantalla de la opción HCX vMotion.



Para obtener más información sobre este proceso, no dude en ver el siguiente vídeo:

HCX vMotion

Asegúrese de que haya suficiente ancho de banda disponible para manejar la migración.

El almacén de datos ANF de destino debe tener suficiente espacio para manejar la migración.

Conclusión

Ya sea que su objetivo sea una nube completa o una nube híbrida y datos que residen en cualquier tipo o proveedor de almacenamiento en las instalaciones, Azure NetApp Files y HCX brindan excelentes opciones para implementar y migrar las cargas de trabajo de las aplicaciones al mismo tiempo que reducen el TCO al hacer que los requisitos de los datos se integren perfectamente con la capa de aplicación. Cualquiera que sea el caso de uso, elija Azure VMware Solution junto con Azure NetApp Files para obtener rápidamente beneficios de la nube, infraestructura y operaciones consistentes en las instalaciones y en múltiples nubes, portabilidad bidireccional de cargas de trabajo y capacidad y rendimiento de nivel empresarial. Es el mismo proceso y los mismos procedimientos familiares que se utilizan para conectar el almacenamiento y migrar máquinas virtuales mediante VMware vSphere Replication, VMware vMotion o incluso la copia de archivos de red (NFC).

Comida para llevar

Los puntos clave de este documento incluyen:

- Ahora puede usar Azure NetApp Files como almacén de datos en Azure VMware Solution SDDC.
- Puede migrar datos fácilmente desde las instalaciones locales al almacén de datos de Azure NetApp Files .
- Puede ampliar y reducir fácilmente el almacén de datos de Azure NetApp Files para cumplir con los requisitos de capacidad y rendimiento durante la actividad de migración.

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes enlaces de sitios web:

- Documentación de Azure VMware Solution

"https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Documentación de Azure NetApp Files

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- Consideraciones sobre la migración de VMware HCX

"https://learn.microsoft.com/en-us/azure/azure-vmware/architecture-migrate"

NetApp para GCP/GCVE

Capacidades de NetApp para Google Cloud Platform GCVE

Obtenga más información sobre las capacidades que NetApp aporta a Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE): desde NetApp como un dispositivo de almacenamiento conectado invitado o un almacén de datos NFS complementario hasta la migración de flujos de trabajo, la extensión/ampliación a la nube, la copia de seguridad/restauración y la recuperación ante desastres.

Salte a la sección del contenido deseado seleccionando entre las siguientes opciones:

- "Configuración de GCVE en GCP"
- "Opciones de almacenamiento de NetApp para GCVE"
- "Soluciones en la nube NetApp /VMware"

Configuración de GCVE en GCP

Al igual que en las instalaciones locales, la planificación de un entorno de virtualización basado en la nube es fundamental para lograr un entorno exitoso listo para producción para la creación de máquinas virtuales y la migración.

Esta sección describe cómo configurar y administrar GCVE y usarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp .

> El almacenamiento en el huésped es el único método compatible para conectar Cloud Volumes ONTAP y Google Cloud NetApp Volumes a GCVE.

El proceso de configuración se puede dividir en los siguientes pasos:

- Implementar y configurar GCVE
- Habilitar el acceso privado a GCVE

Ver el detalle"Pasos de configuración para GCVE" .

Opciones de almacenamiento de NetApp para GCVE

El almacenamiento de NetApp se puede utilizar de varias maneras (ya sea conectado por instancia o como un almacén de datos NFS complementario) dentro de GCP GCVE.

Por favor visite"Opciones de almacenamiento de NetApp compatibles" Para más información.

Google Cloud admite el almacenamiento de NetApp en las siguientes configuraciones:

- Cloud Volumes ONTAP (CVO) como almacenamiento conectado para invitados
- Google Cloud NetApp Volumes (NetApp Volumes) como almacenamiento conectado para invitados
- Google Cloud NetApp Volumes (NetApp Volumes) como almacén de datos NFS complementario

Ver el detalle"Opciones de almacenamiento de conexión de invitados para GCVE" . Ver el detalle"Opciones de almacén de datos NFS suplementarias para GCVE" .

Leer más sobre"Compatibilidad del almacén de datos de Google Cloud NetApp Volumes con Google Cloud VMware Engine (blog de NetApp)" o"Cómo usar Google Cloud NetApp Volumes como almacenes de datos para Google Cloud VMware Engine (blog de Google)"

Casos de uso de soluciones

Con las soluciones de nube de NetApp y VMware, muchos casos de uso son fáciles de implementar en Azure AVS. Estos casos se definen para cada una de las áreas de nube definidas por VMware:

- Proteger (incluye recuperación ante desastres y copia de seguridad/restauración)
- Extender
- Emigrar

"Explora las soluciones de NetApp para Google Cloud GCVE"

Proteger las cargas de trabajo en GCP/GCVE

Recuperación ante desastres consistente con aplicaciones con NetApp SnapCenter y Veeam Replication

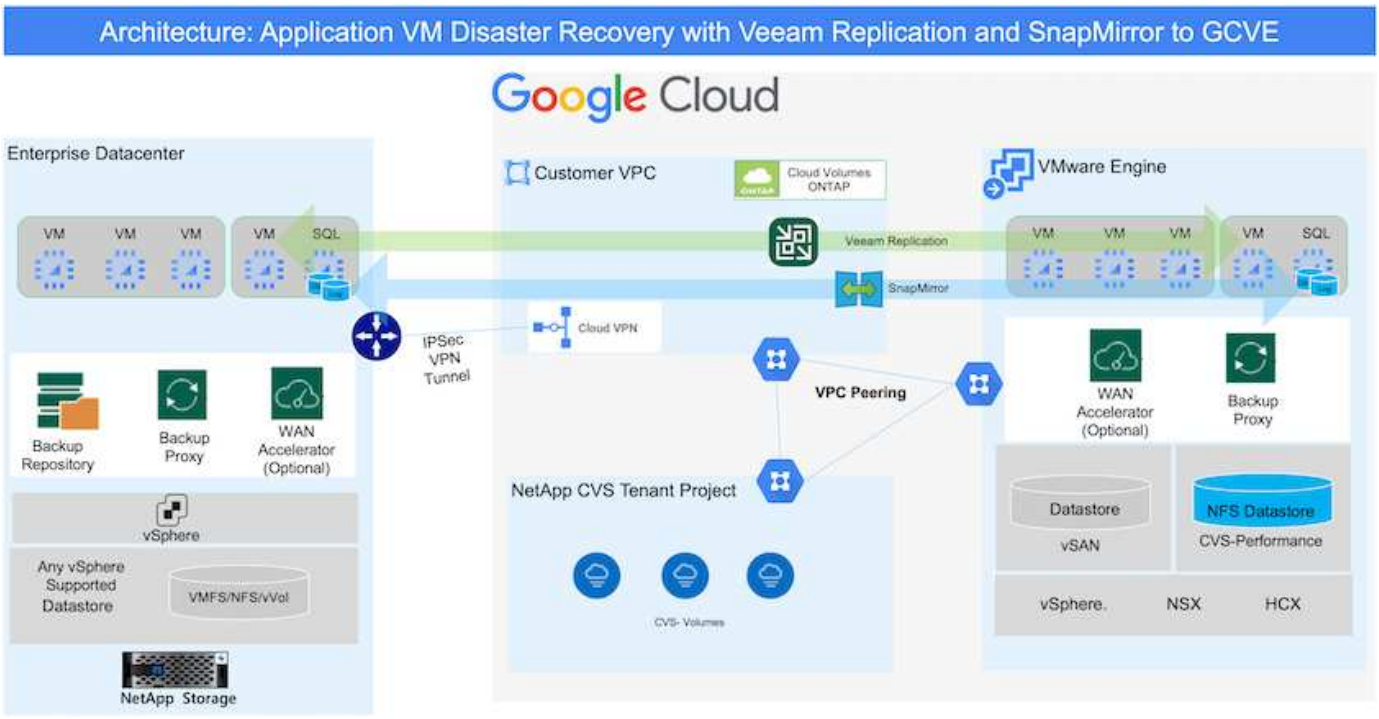
La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos como ransomware. Con NetApp SnapMirror, las cargas de trabajo locales de VMware que usan almacenamiento conectado a invitados se pueden replicar en NetApp Cloud Volumes ONTAP que se ejecuta en Google Cloud.

Descripción general

Muchos clientes buscan una solución de recuperación ante desastres eficaz para sus máquinas virtuales de aplicaciones alojadas en VMware vSphere. Muchos de ellos utilizan su solución de respaldo existente para realizar la recuperación en caso de desastre. Muchas veces esa solución aumenta el RTO y no cumple sus expectativas. Para reducir el RPO y el RTO, la replicación de VM de Veeam se puede utilizar incluso desde las instalaciones locales hasta GCVE siempre que haya conectividad de red y un entorno con los permisos adecuados disponibles. NOTA: Veeam VM Replication no protege los dispositivos de almacenamiento conectados a la máquina virtual invitada, como los montajes iSCSI o NFS, dentro de la máquina virtual invitada. Es necesario protegerlos por separado.

Para lograr una replicación consistente de la aplicación para SQL VM y reducir el RTO, utilizamos SnapCenter para orquestar las operaciones de SnapMirror de los volúmenes de registro y de bases de datos SQL.

Este documento proporciona un enfoque paso a paso para configurar y ejecutar la recuperación ante desastres que utiliza NetApp SnapMirror, Veeam y Google Cloud VMware Engine (GCVE).



Suposiciones

Este documento se centra en el almacenamiento interno de datos de aplicaciones (también conocido como almacenamiento conectado por invitado) y asumimos que el entorno local utiliza SnapCenter para realizar copias de seguridad consistentes con las aplicaciones.

> Este documento se aplica a cualquier solución de copia de seguridad o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las mejores prácticas para crear políticas de respaldo que cumplan con los SLA de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos deben crearse según el diseño de VLAN local.

> Existen múltiples opciones para conectar centros de datos locales a Google Cloud, lo que nos impide delinear un flujo de trabajo específico en este documento. Consulta la documentación de Google Cloud para conocer el método de conectividad local a Google adecuado.

Implementación de la solución de recuperación ante desastres

Descripción general de la implementación de la solución

1. Asegúrese de que los datos de la aplicación estén respaldados mediante SnapCenter con los requisitos de RPO necesarios.
2. Aprovisiona Cloud Volumes ONTAP con el tamaño de instancia correcto mediante NetApp Console dentro de la suscripción y la red virtual adecuadas.

a. Configure SnapMirror para los volúmenes de aplicación relevantes.

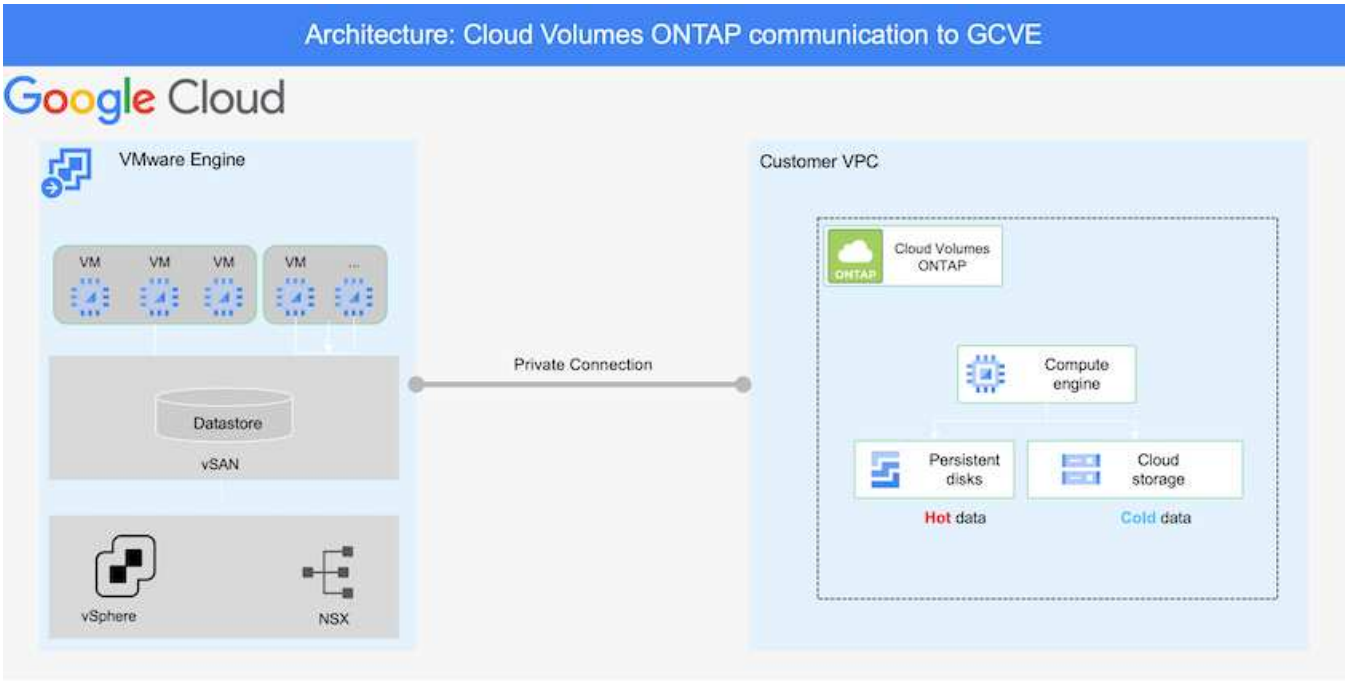
b. Actualice las políticas de respaldo en SnapCenter para activar las actualizaciones de SnapMirror después de los trabajos programados.

3. Instale el software Veeam y comience a replicar máquinas virtuales en la instancia de Google Cloud VMware Engine.
4. Durante un desastre, rompe la relación de SnapMirror mediante NetApp Console y activa la conmutación por error de las máquinas virtuales con Veeam.
   a. Vuelva a conectar los LUN ISCSI y los montajes NFS para las máquinas virtuales de la aplicación.
   b. Abrir aplicaciones en línea.
5. Invoque la conmutación por error al sitio protegido mediante la resincronización inversa de SnapMirror después de que se haya recuperado el sitio principal.

Detalles de la implementación

▼ **Configurar CVO en Google Cloud y replicar volúmenes en CVO**

El primer paso es configurar Cloud Volumes ONTAP en Google Cloud ("CVO") y replique los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retenciones de instantáneas deseadas.



Para obtener instrucciones paso a paso de muestra sobre cómo configurar SnapCenter y replicar los datos, consulte"Configurar la replicación con SnapCenter"

Revisión de la protección de máquinas virtuales SQL con SnapCenter

▼ **Configurar los hosts GCVE y el acceso a los datos CVO**

Dos factores importantes a tener en cuenta al implementar el SDDC son el tamaño del clúster SDDC en la solución GCVE y cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costos operativos generales. El SDDC puede ser tan pequeño como tres hosts, o incluso un clúster de múltiples hosts en una implementación a gran escala.

Los Google Cloud NetApp Volumes para el almacén de datos NFS y Cloud Volumes ONTAP para bases de datos y registros de SQL se pueden implementar en cualquier VPC y GCVE debe tener una conexión privada a esa VPC para montar el almacén de datos NFS y hacer que la máquina virtual se conecte a los LUN iSCSI.

Para configurar GCVE SDDC, consulte"Implementar y configurar el entorno de virtualización en Google Cloud Platform (GCP)" . Como requisito previo, verifique que las máquinas virtuales invitadas que residen en los hosts GCVE puedan consumir datos de Cloud Volumes ONTAP una vez que se haya establecido la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de cargas de trabajo locales a GCVE (máquinas virtuales con VMDK de aplicaciones y máquinas virtuales con almacenamiento invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de volúmenes de aplicaciones a Cloud Volumes ONTAP.

▼ **Instalar componentes de Veeam**

Según el escenario de implementación, el servidor de respaldo de Veeam, el repositorio de respaldo y el proxy de respaldo que deben implementarse. Para este caso de uso, no es necesario implementar un almacén de objetos para Veeam y tampoco es necesario un repositorio de escalabilidad horizontal. "Consulte la documentación de Veeam para conocer el procedimiento de instalación." Para obtener información adicional, consulte"Migración con Veeam Replication"

▼ **Configurar la replicación de máquinas virtuales con Veeam**

Tanto el vCenter local como el vCenter GCVE deben registrarse en Veeam. "Configurar el trabajo de replicación de máquinas virtuales de vSphere" En el paso de Procesamiento de invitados del asistente, seleccione deshabilitar el procesamiento de aplicaciones, ya que utilizaremos SnapCenter para realizar copias de seguridad y recuperación basadas en aplicaciones.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

▼ **Conmutación por error de la máquina virtual de Microsoft SQL Server**

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Beneficios de esta solución

- Utiliza la replicación eficiente y resistente de SnapMirror.
- Se recupera a cualquier punto disponible en el tiempo con retención de instantáneas ONTAP .
- La automatización completa está disponible para todos los pasos necesarios para recuperar cientos a miles de máquinas virtuales, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonación que no modifican el volumen replicado.
  - Esto evita el riesgo de corrupción de datos en volúmenes e instantáneas.
  - Evita interrupciones de replicación durante los flujos de trabajo de prueba de DR.
  - Aprovecha los datos de DR para flujos de trabajo más allá de DR, como desarrollo y prueba, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas de remediación.
- Veeam Replication permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

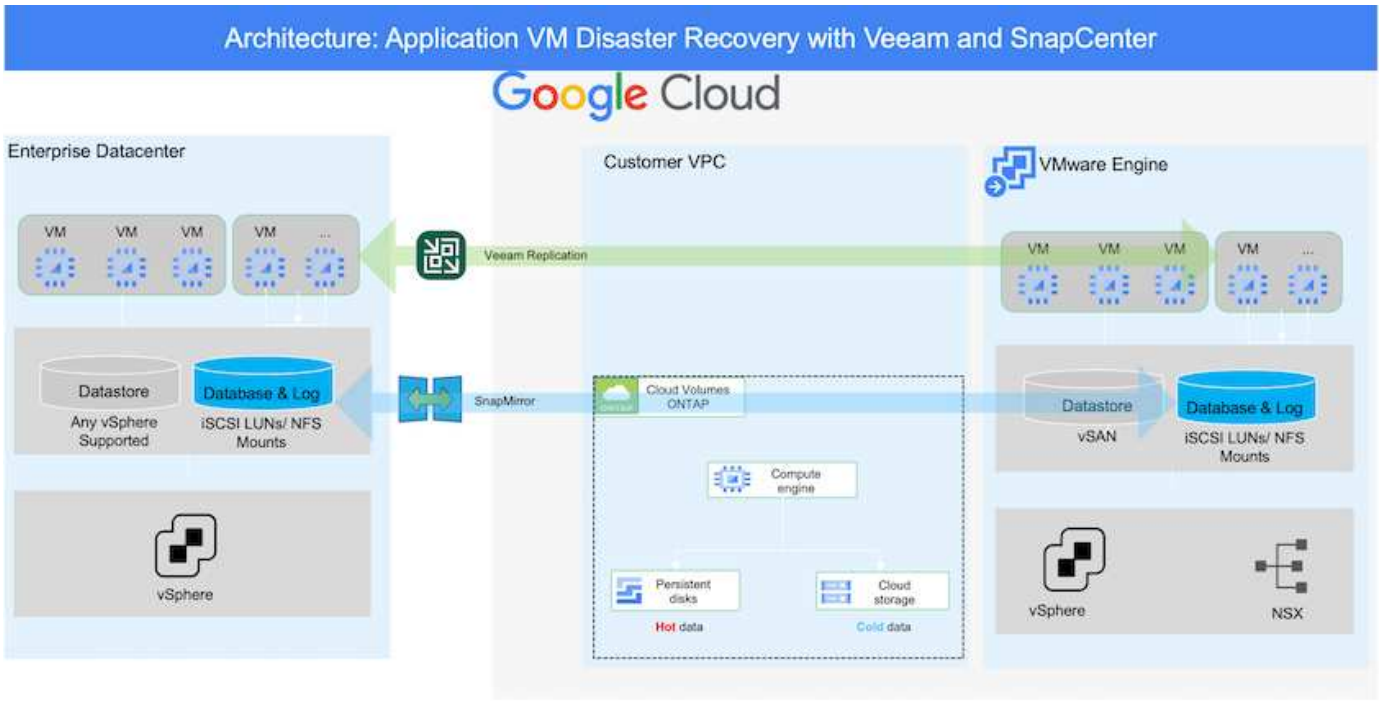
Recuperación ante desastres de aplicaciones con SnapCenter, Cloud Volumes ONTAP y Veeam Replication

La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos como ransomware. Con NetApp SnapMirror, las cargas de trabajo locales de VMware que usan almacenamiento conectado a invitados se pueden replicar en NetApp Cloud Volumes ONTAP que se ejecuta en Google Cloud.

Descripción general

Esto cubre los datos de la aplicación; sin embargo, ¿qué pasa con las máquinas virtuales reales? La recuperación ante desastres debe cubrir todos los componentes dependientes, incluidas máquinas virtuales, VMDK, datos de aplicaciones y más. Para lograr esto, se puede usar SnapMirror junto con Veeam para recuperar sin problemas cargas de trabajo replicadas desde las instalaciones locales a Cloud Volumes ONTAP mientras se usa el almacenamiento vSAN para los VMDK de VM.

Este documento proporciona un enfoque paso a paso para configurar y ejecutar la recuperación ante desastres que utiliza NetApp SnapMirror, Veeam y Google Cloud VMware Engine (GCVE).



Suposiciones

Este documento se centra en el almacenamiento interno de datos de aplicaciones (también conocido como almacenamiento conectado por invitado) y asumimos que el entorno local utiliza SnapCenter para realizar copias de seguridad consistentes con las aplicaciones.

> Este documento se aplica a cualquier solución de copia de seguridad o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las mejores prácticas para crear políticas de respaldo que cumplan con los SLA de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos deben crearse según el diseño de VLAN local.

Existen múltiples opciones para conectar centros de datos locales a Google Cloud, lo que nos impide delinear un flujo de trabajo específico en este documento. Consulta la documentación de Google Cloud para conocer el método de conectividad local a Google adecuado.

Implementación de la solución de recuperación ante desastres

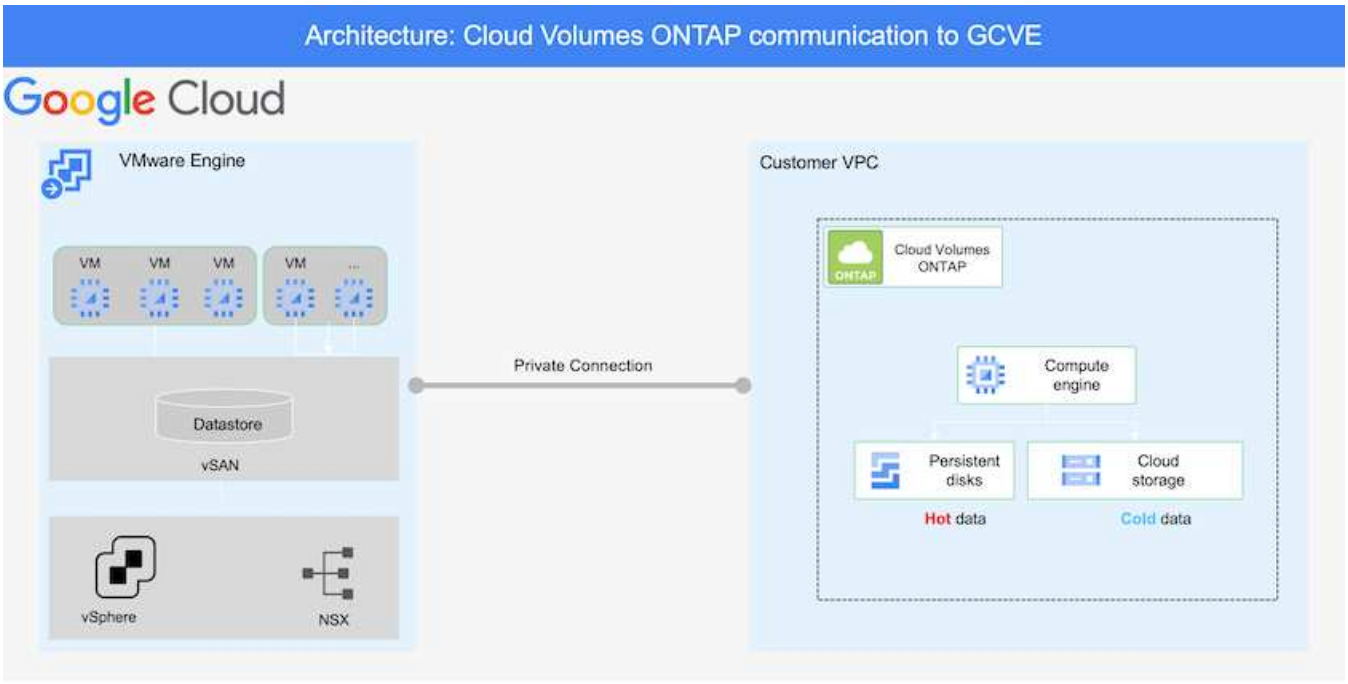
Descripción general de la implementación de la solución

1. Asegúrese de que los datos de la aplicación estén respaldados mediante SnapCenter con los requisitos de RPO necesarios.
2. Aprovisione Cloud Volumes ONTAP con el tamaño de instancia correcto utilizando Cloud Manager dentro de la suscripción y la red virtual adecuadas.
   a. Configure SnapMirror para los volúmenes de aplicación relevantes.
   b. Actualice las políticas de respaldo en SnapCenter para activar las actualizaciones de SnapMirror después de los trabajos programados.
3. Instale el software Veeam y comience a replicar máquinas virtuales en la instancia de Google Cloud VMware Engine.
4. Durante un evento de desastre, rompa la relación de SnapMirror usando Cloud Manager y active la conmutación por error de las máquinas virtuales con Veeam.
   a. Vuelva a conectar los LUN ISCSI y los montajes NFS para las máquinas virtuales de la aplicación.
   b. Abrir aplicaciones en línea.
5. Invoque la conmutación por error al sitio protegido mediante la resincronización inversa de SnapMirror después de que se haya recuperado el sitio principal.

Detalles de la implementación

▼ **Configurar CVO en Google Cloud y replicar volúmenes en CVO**

El primer paso es configurar Cloud Volumes ONTAP en Google Cloud ("CVO") y replique los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retenciones de instantáneas deseadas.



Para obtener instrucciones paso a paso de muestra sobre cómo configurar SnapCenter y replicar los datos, consulte"Configurar la replicación con SnapCenter"

Configurar la replicación con SnapCenter

▼ **Configurar los hosts GCVE y el acceso a los datos CVO**

Dos factores importantes a tener en cuenta al implementar el SDDC son el tamaño del clúster SDDC en la solución GCVE y cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costos operativos generales. El SDDC puede ser tan pequeño como tres hosts, o incluso un clúster de múltiples hosts en una implementación a gran escala.

Cloud Volumes ONTAP se puede implementar en cualquier VPC y GCVE debe tener una conexión privada a esa VPC para que la VM se conecte a los LUN iSCSI.

Para configurar GCVE SDDC, consulte"Implementar y configurar el entorno de virtualización en Google Cloud Platform (GCP)" . Como requisito previo, verifique que las máquinas virtuales invitadas que residen en los hosts GCVE puedan consumir datos de Cloud Volumes ONTAP una vez que se haya establecido la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de cargas de trabajo locales a GCVE (máquinas virtuales con VMDK de aplicaciones y máquinas virtuales con almacenamiento invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de volúmenes de aplicaciones a Cloud Volumes ONTAP.

▼ **Instalar componentes de Veeam**

Según el escenario de implementación, el servidor de respaldo de Veeam, el repositorio de respaldo y el proxy de respaldo que deben implementarse. Para este caso de uso, no es necesario implementar un almacén de objetos para Veeam y tampoco es necesario un repositorio de escalabilidad horizontal.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Consulte la documentación de Veeam para conocer el procedimiento de instalación."]

▼ **Configurar la replicación de máquinas virtuales con Veeam**

Tanto el vCenter local como el vCenter GCVE deben registrarse en Veeam. "Configurar el trabajo de replicación de máquinas virtuales de vSphere" En el paso de Procesamiento de invitados del asistente, seleccione deshabilitar el procesamiento de aplicaciones, ya que utilizaremos SnapCenter para realizar copias de seguridad y recuperación basadas en aplicaciones.

Configurar el trabajo de replicación de máquinas virtuales de vSphere

▼ **Conmutación por error de la máquina virtual de Microsoft SQL Server**

Conmutación por error de la máquina virtual de Microsoft SQL Server

Beneficios de esta solución

- Utiliza la replicación eficiente y resistente de SnapMirror.
- Se recupera a cualquier punto disponible en el tiempo con retención de instantáneas ONTAP .
- La automatización completa está disponible para todos los pasos necesarios para recuperar cientos a miles de máquinas virtuales, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonación que no modifican el volumen replicado.

    - Esto evita el riesgo de corrupción de datos en volúmenes e instantáneas.
    - Evita interrupciones de replicación durante los flujos de trabajo de prueba de DR.
    - Aprovecha los datos de DR para flujos de trabajo más allá de DR, como desarrollo y prueba, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas de remediación.
- Veeam Replication permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

Uso del almacén de datos Veeam Replication y Google Cloud NetApp Volumes para la recuperación ante desastres en Google Cloud VMware Engine

Un plan integral de recuperación ante desastres es fundamental para las empresas en tiempos de crisis. Muchas organizaciones aprovechan la computación en la nube para las operaciones diarias y la recuperación ante desastres. Este enfoque proactivo puede reducir o eliminar interrupciones comerciales costosas.

Este artículo describe cómo usar Veeam Backup & Replication para configurar la recuperación ante desastres de máquinas virtuales VMware locales en Google Cloud VMware Engine (GCVE) con Google Cloud NetApp Volumes (NetApp Volumes).

Descripción general

Google Cloud NetApp Volumes es un servicio de almacenamiento de Google y NetApp que está disponible para Google Cloud. El servicio NetApp Volumes proporciona almacenamiento NFS/SMB de alto rendimiento. El almacenamiento NFS de NetApp Volumes certificado por VMware se puede utilizar como almacén de datos externo para hosts ESXi en GCVE. Los usuarios deben establecer una conexión de peering entre su nube privada GCVE y el proyecto NetApp Volumes. No hay cargos de red como resultado del acceso al almacenamiento dentro de una región. Los usuarios pueden crear volúmenes de NetApp Volumes en la consola de Google Cloud y habilitar la protección contra eliminación antes de montar los volúmenes como almacenes de datos en sus hosts ESXi.

Los almacenes de datos NFS basados en NetApp Volumes se pueden usar para replicar datos desde las instalaciones locales mediante cualquier solución de terceros validada que proporcione capacidad de replicación de máquinas virtuales. Al agregar almacenes de datos de NetApp Volumes, se permite una implementación rentable en lugar de construir un SDDC basado en Google Cloud VMware Engine (GCVE) con una gran cantidad de hosts ESXi para acomodar el almacenamiento. Este enfoque se denomina "grupo de luces piloto". Un clúster de luz piloto es una configuración de host GCVE mínima (3 hosts GCVE ESXi) junto con la capacidad de almacenamiento de datos de NetApp Volumes para permitir un escalamiento independiente para cumplir con los requisitos de capacidad.

El objetivo es mantener una infraestructura rentable con solo los componentes principales para gestionar una conmutación por error. Un grupo de luces piloto puede expandirse y agregar más hosts GCVE en caso de una conmutación por error. Una vez que se resuelve la conmutación por error y se reanudan las operaciones normales, el grupo piloto puede reducir su escala y volver a un modo operativo de bajo costo.

Propósitos de este documento

Este artículo describe cómo usar un almacén de datos de Google Cloud NetApp Volumes con Veeam Backup & Replication para configurar la recuperación ante desastres de máquinas virtuales VMware locales en GCVE mediante la funcionalidad del software de replicación de máquinas virtuales de Veeam.

Veeam Backup & Replication es una aplicación de backup y replicación para entornos virtuales. Cuando se replican máquinas virtuales, Veeam Backup & Replication creará una copia exacta de las máquinas virtuales en el formato nativo de VMware vSphere en el clúster SDDC de GCVE de destino. Veeam Backup &

Replication mantendrá la copia sincronizada con la VM original. La replicación proporciona el mejor objetivo de tiempo de recuperación (RTO) ya que hay una copia montada de una máquina virtual en el sitio de recuperación ante desastres en un estado listo para iniciarse.

Este mecanismo de replicación garantiza que las cargas de trabajo puedan iniciarse rápidamente en GCVE en caso de un desastre. El software Veeam Backup & Replication también optimiza la transmisión de tráfico para la replicación a través de WAN y conexiones lentas. Además, también filtra bloques de datos duplicados, bloques de datos cero, archivos de intercambio y "archivos del sistema operativo invitado de VM excluidos". El software también comprimirá el tráfico de réplicas. Para evitar que los trabajos de replicación consuman todo el ancho de banda de la red, se pueden utilizar aceleradores de WAN y reglas de limitación de red.

El proceso de replicación en Veeam Backup & Replication está impulsado por trabajos, lo que significa que la replicación se realiza mediante la configuración de trabajos de replicación. En el caso de un evento de desastre, se puede activar la conmutación por error para recuperar las máquinas virtuales mediante la conmutación por error a su copia de réplica. Cuando se realiza una conmutación por error, una VM replicada asume el rol de la VM original. La conmutación por error se puede realizar al último estado de una réplica o a cualquiera de sus puntos de restauración conocidos como correctos. Esto permite la recuperación de ransomware o pruebas aisladas según sea necesario. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.

Descripción general de la solución

Esta solución cubre los siguientes pasos de alto nivel:

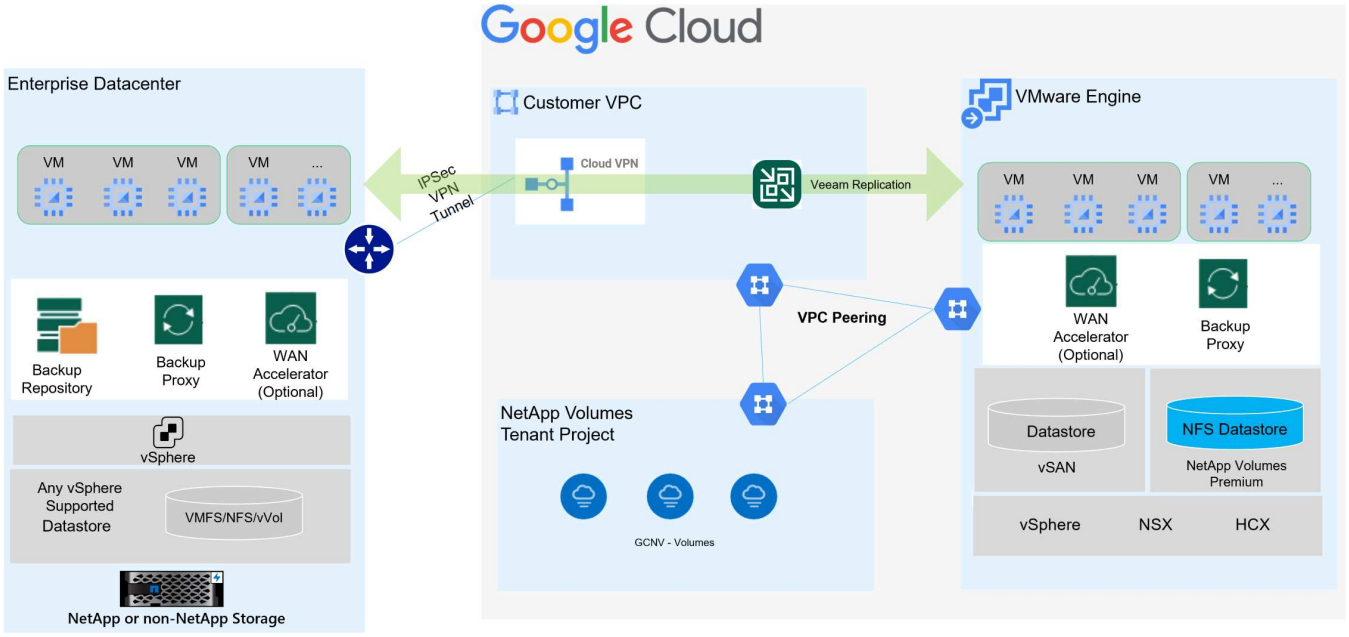
1. Cree un volumen NFS con Google Cloud NetApp Volumes
2. Siga el proceso de GCP para crear un almacén de datos GCVE a partir del volumen NFS de NetApp Volumes.
3. Configure un trabajo de replicación para crear réplicas de máquinas virtuales mediante Veeam Backup & Replication.
4. Cree un plan de conmutación por error y realice la conmutación por error.
5. Vuelva a las máquinas virtuales de producción una vez que se complete el evento de desastre y el sitio principal esté en funcionamiento.

> Al crear un volumen en NetApp Volumes, para usarlo como almacén de datos GCVE, solo se admite NFS v3.

Para obtener más información sobre el uso de volúmenes NFS de NetApp Volumes como almacenes de datos para GCVE, consulte "Uso de un volumen NFS como almacén de datos de vSphere alojado por Google Cloud NetApp Volumes" .

Arquitectura

El siguiente diagrama muestra la arquitectura de la solución presentada en esta documentación. Una práctica recomendada es tener un servidor Veeam Backup & Replication ubicado tanto en el sitio local como en el SDDC de GCVE. La copia de seguridad y la recuperación las realiza y administra el servidor Veeam en las instalaciones, y la replicación la administra el servidor Veeam en el SDDC de GCVE. Esta arquitectura proporciona la máxima disponibilidad cuando ocurre una falla en el centro de datos principal.



Requisitos previos para la replicación de Veeam en almacenes de datos de GCVE y NetApp Volumes

Esta solución requiere los siguientes componentes y configuraciones:

1. NetApp Volumes tiene un grupo de almacenamiento disponible con suficiente capacidad libre para acomodar el volumen NFS que se creará.
2. El software Veeam Backup and Replication se ejecuta en un entorno local con conectividad de red adecuada.
3. Asegúrese de que la máquina virtual de respaldo de Veeam Backup & Replication esté conectada a los clústeres SDDC GCVE de origen y de destino.
4. Asegúrese de que la máquina virtual de respaldo de Veeam Backup & Replication esté conectada a las máquinas virtuales del servidor proxy de Veeam en los clústeres GCVE de origen y de destino.
5. El servidor de respaldo debe poder resolver nombres cortos y conectarse a los vCenter de origen y de destino.

Los usuarios deben realizar una conexión de emparejamiento entre su nube privada GCVE y el proyecto de NetApp Volumes mediante las páginas de emparejamiento de red VPC o conexiones privadas dentro de la interfaz de usuario de la consola de VMware Engine Cloud.

> Veeam requiere una cuenta de usuario de la solución GCVE con privilegios elevados al añadir el servidor vCenter de GCVE al inventario de Veeam Backup and Replication. Para obtener más información consulta la documentación de Google Cloud Platform (GCP), "Elevación de privilegios de VMware Engine".

Para obtener información adicional, consulte "Consideraciones y limitaciones" en la documentación de Veeam Backup & Replication.

Pasos de implementación

Las siguientes secciones describen los pasos de implementación para crear y montar un almacén de datos NFS utilizando Google Cloud NetApp Volumes y usar Veeam Backup and Replication para implementar una solución completa de recuperación ante desastres entre un centro de datos local y Google Cloud VMware

Engine.

Cree un volumen NFS y un almacén de datos de NetApp Volumes para GCVE

Referirse a "Uso de un volumen NFS como almacén de datos de vSphere alojado por Google Cloud NetApp Volumes" para obtener una descripción general de cómo utilizar Google Cloud NetApp Volumes como almacén de datos para GCVE.

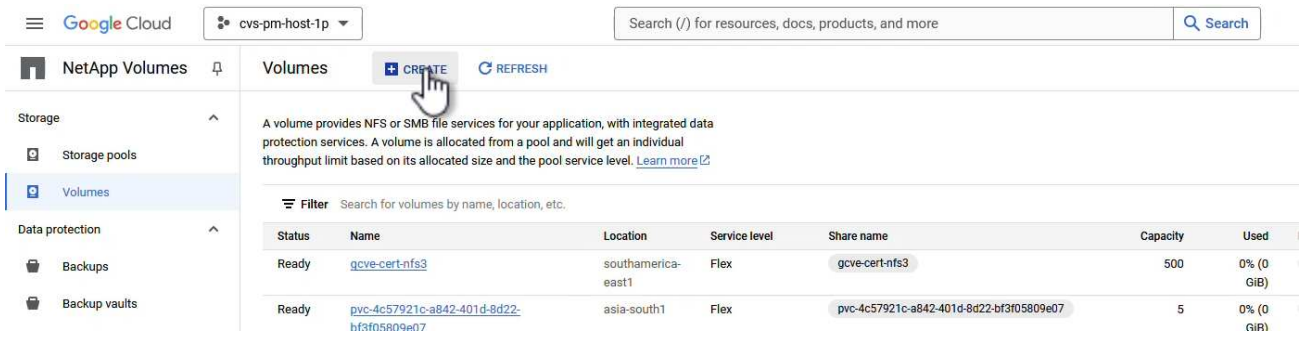
Complete los siguientes pasos para crear y utilizar un almacén de datos NFS para GCVE mediante NetApp Volumes:

▼ **Crear un volumen NFS de NetApp Volumes**

Se accede a Google Cloud NetApp Volumes desde la consola de Google Cloud Platform (GCP).

Referirse a "Crear un volumen" en la documentación de Google Cloud NetApp Volumes para obtener información detallada sobre este paso.

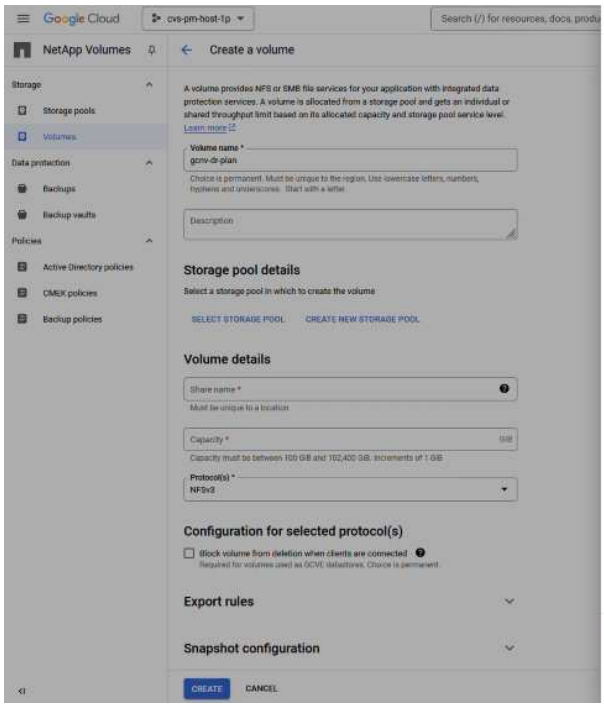
1. En un navegador web, navegue hasta https://console.cloud.google.com/ e inicie sesión en su consola GCP. Busque * NetApp Volumes* para comenzar.
2. En la interfaz de administración de * NetApp Volumes*, haga clic en **Crear** para comenzar a crear un volumen NFS.

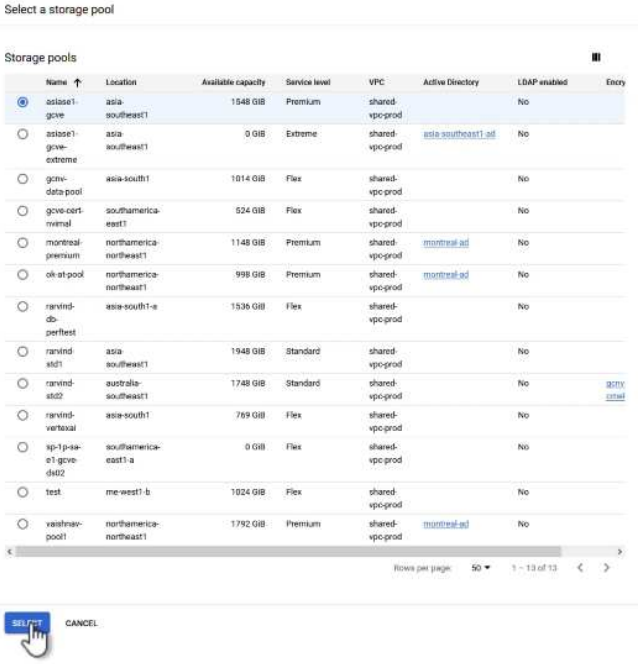


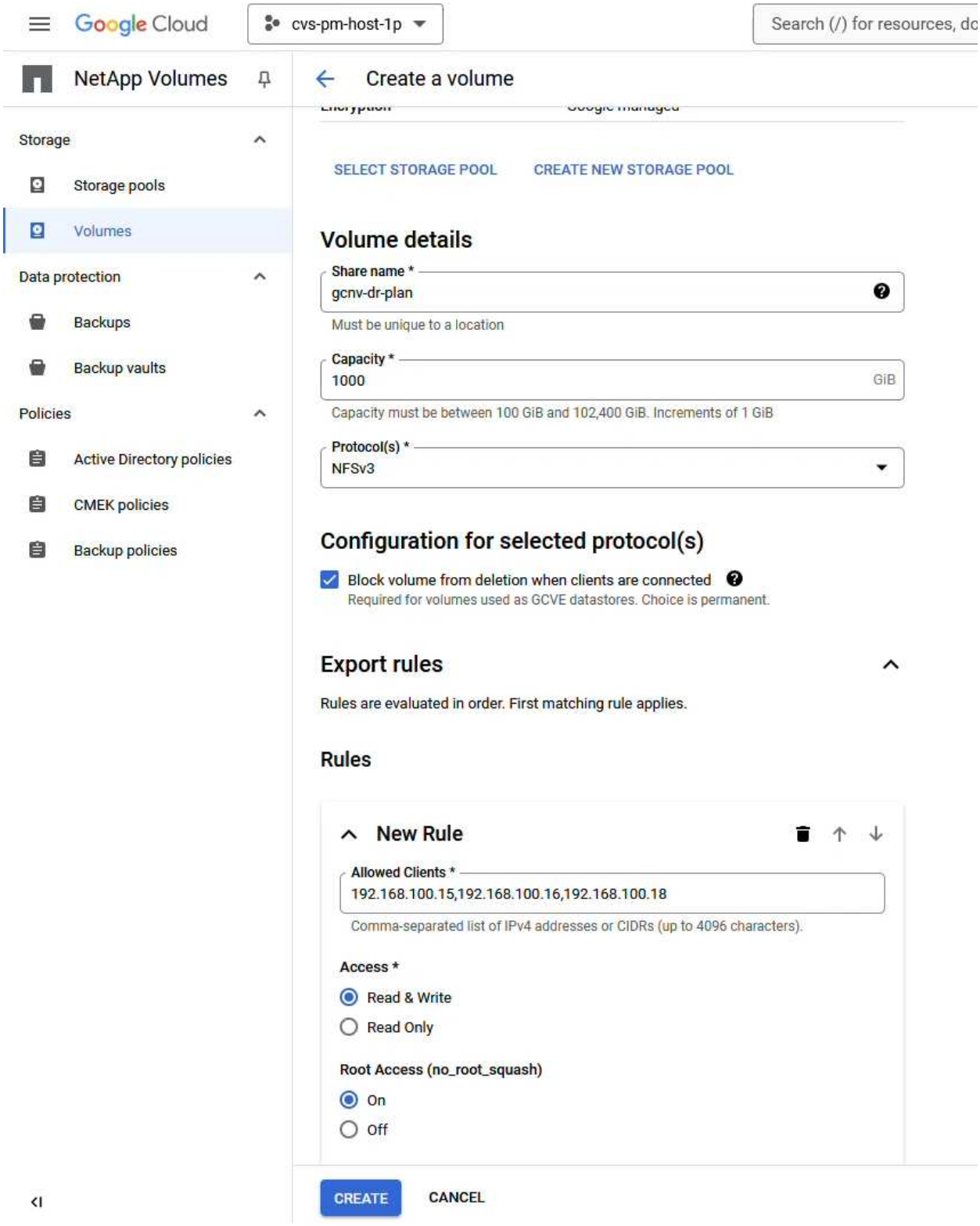
3. En el asistente **Crear un volumen**, complete toda la información requerida:
   - Un nombre para el volumen.
   - El grupo de almacenamiento en el que se creará el volumen.
   - Un nombre de recurso compartido utilizado al montar el volumen NFS.
   - La capacidad del volumen en GiB.
   - El protocolo de almacenamiento que se utilizará.
   - Marque la casilla para **Bloquear el volumen para que no se elimine cuando los clientes estén conectados** (requerido por GCVE cuando se monta como un almacén de datos).
   - Las reglas de exportación para acceder al volumen. Estas son las direcciones IP de los adaptadores ESXi en la red NFS.
   - Una programación de instantáneas utilizada para proteger el volumen mediante instantáneas locales.
   - Opcionalmente, elija hacer una copia de seguridad del volumen y/o crear etiquetas para el volumen.

   Al crear un volumen en NetApp Volumes, para usarlo como almacén de datos GCVE,

solo se admite NFS v3.

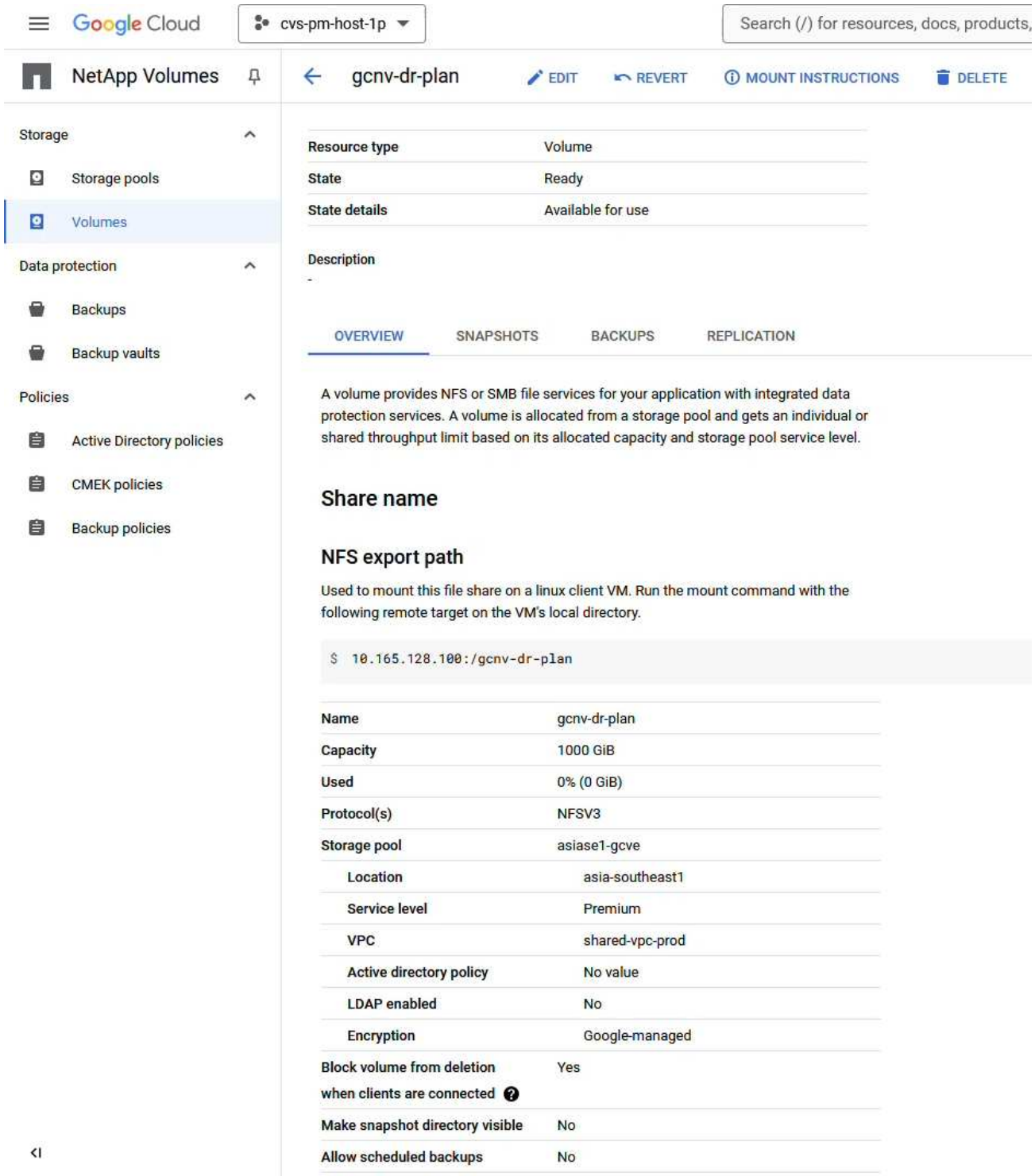






Haga clic en **Crear** para terminar de crear el volumen.

4. Una vez creado el volumen, la ruta de exportación NFS necesaria para montar el volumen se puede ver desde la página de propiedades del volumen.



▼ **Montar el almacén de datos NFS en GCVE**

Al momento de escribir este artículo, el proceso para montar un almacén de datos en GCVE requiere abrir un ticket de soporte de GCP para que el volumen se monte como un almacén de datos NFS.

Referirse a "Uso de un volumen NFS como almacén de datos de vSphere alojado por Google Cloud NetApp Volumes" Para más información.

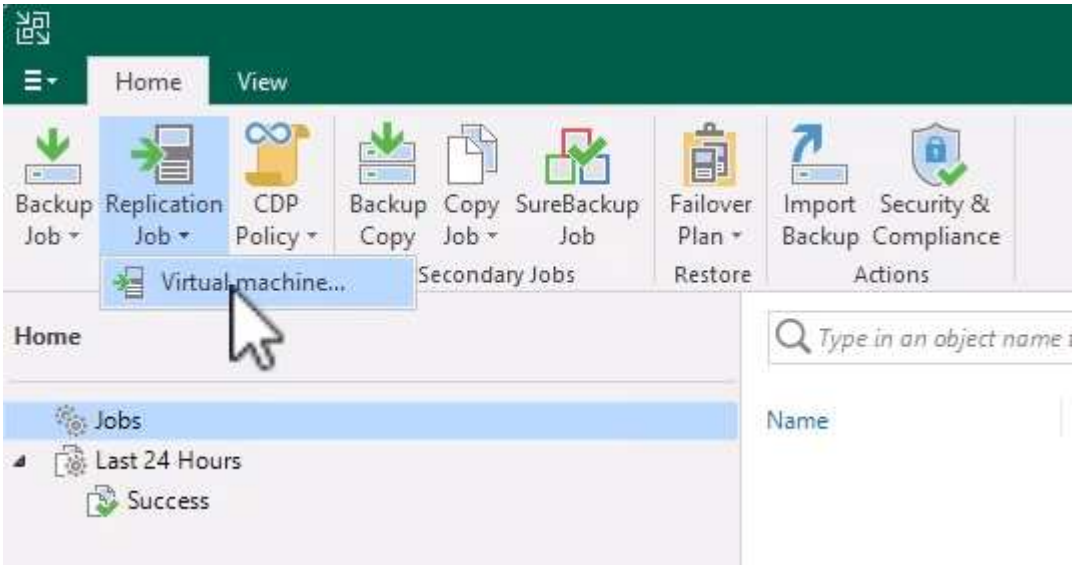
Replicar máquinas virtuales en GCVE y ejecutar un plan de conmutación por error y recuperación

▼ **Replicar máquinas virtuales en un almacén de datos NFS en GCVE**

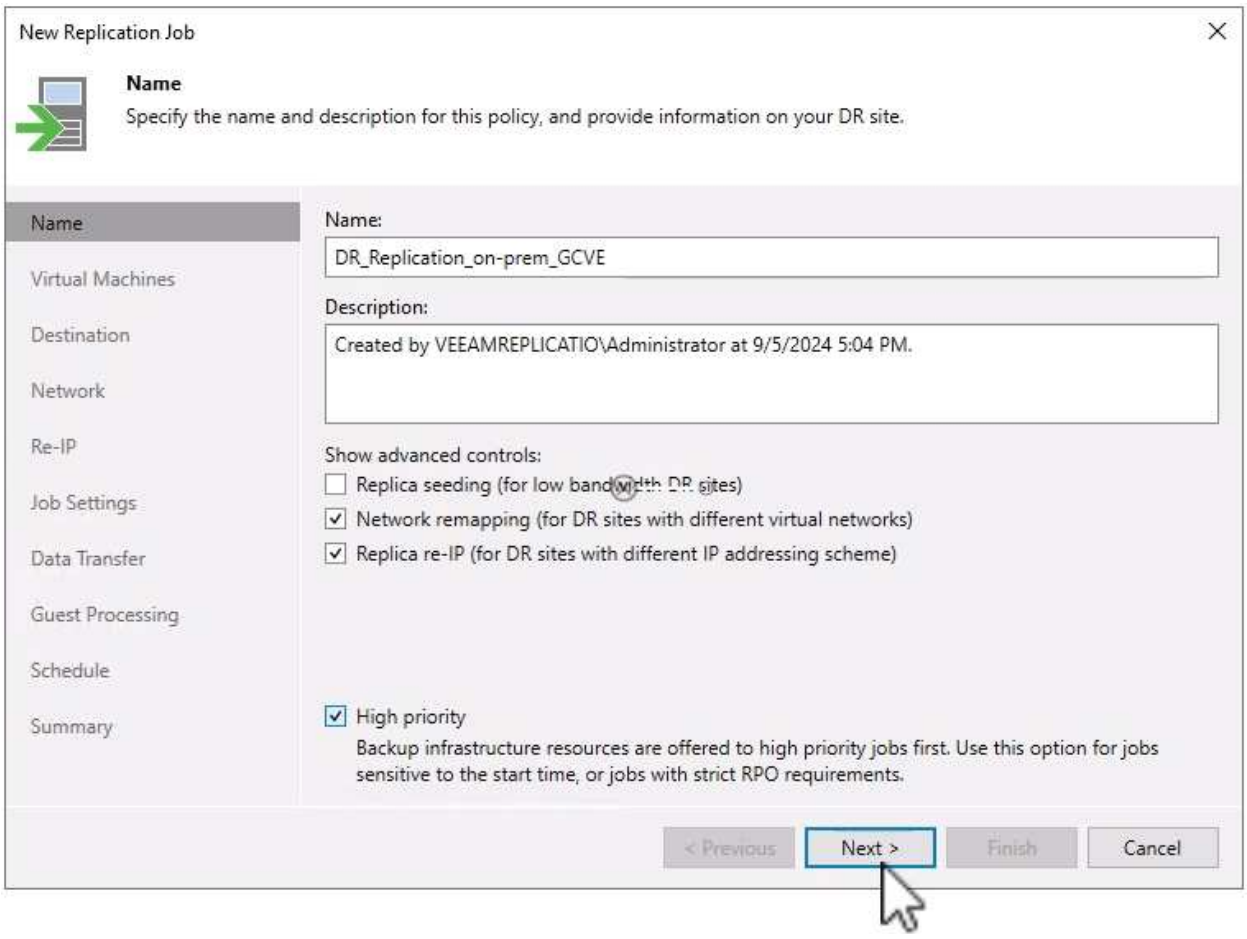
Veeam Backup & Replication aprovecha las capacidades de instantáneas de VMware vSphere. Durante la replicación, Veeam Backup & Replication solicita a VMware vSphere que cree una instantánea de VM. La instantánea de VM es la copia puntual de una VM que incluye discos virtuales, estado del sistema, configuración y metadatos. Veeam Backup & Replication utiliza la instantánea como fuente de datos para la replicación.

Para replicar máquinas virtuales, complete los siguientes pasos:

1. Abra la consola de Veeam Backup & Replication.
2. En la pestaña **Inicio**, haga clic en **Trabajo de replicación > Máquina virtual…**

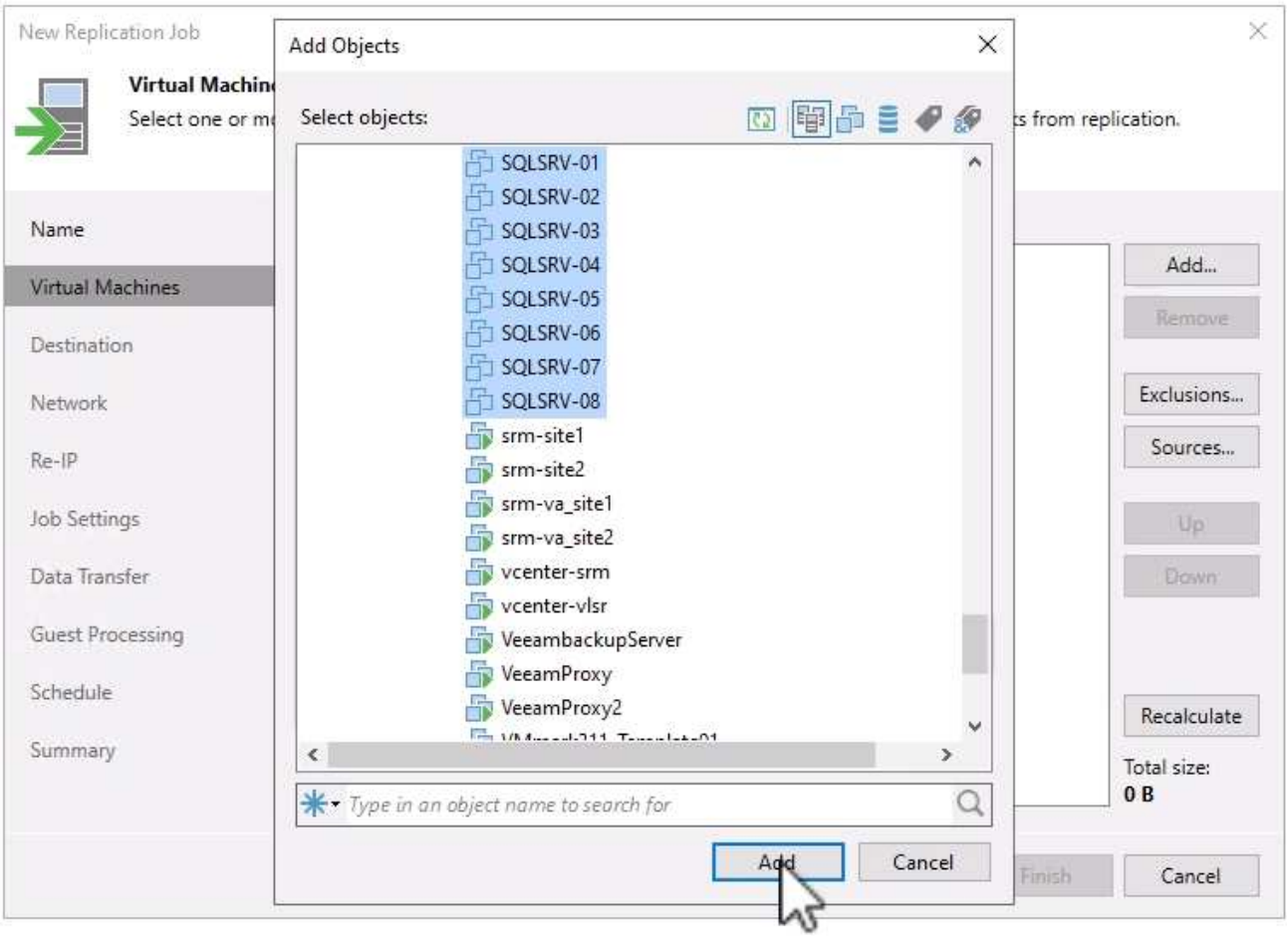


3. En la página **Nombre** del asistente **Nuevo trabajo de replicación**, especifique un nombre de trabajo y seleccione las casillas de verificación de control avanzado adecuadas.
   - Seleccione la casilla de verificación Siembra de réplicas si la conectividad entre las instalaciones locales y GCP tiene un ancho de banda restringido.
   - Seleccione la casilla de verificación Reasignación de red (para sitios SDDC de GCVE con redes diferentes) si los segmentos en el SDDC de GCVE no coinciden con los de las redes del sitio local.
   - Seleccione la casilla de verificación Re-IP de réplica (para sitios DR con esquema de direccionamiento IP diferente) si el esquema de direccionamiento IP en el sitio de producción local difiere del esquema en el sitio GCVE de destino.

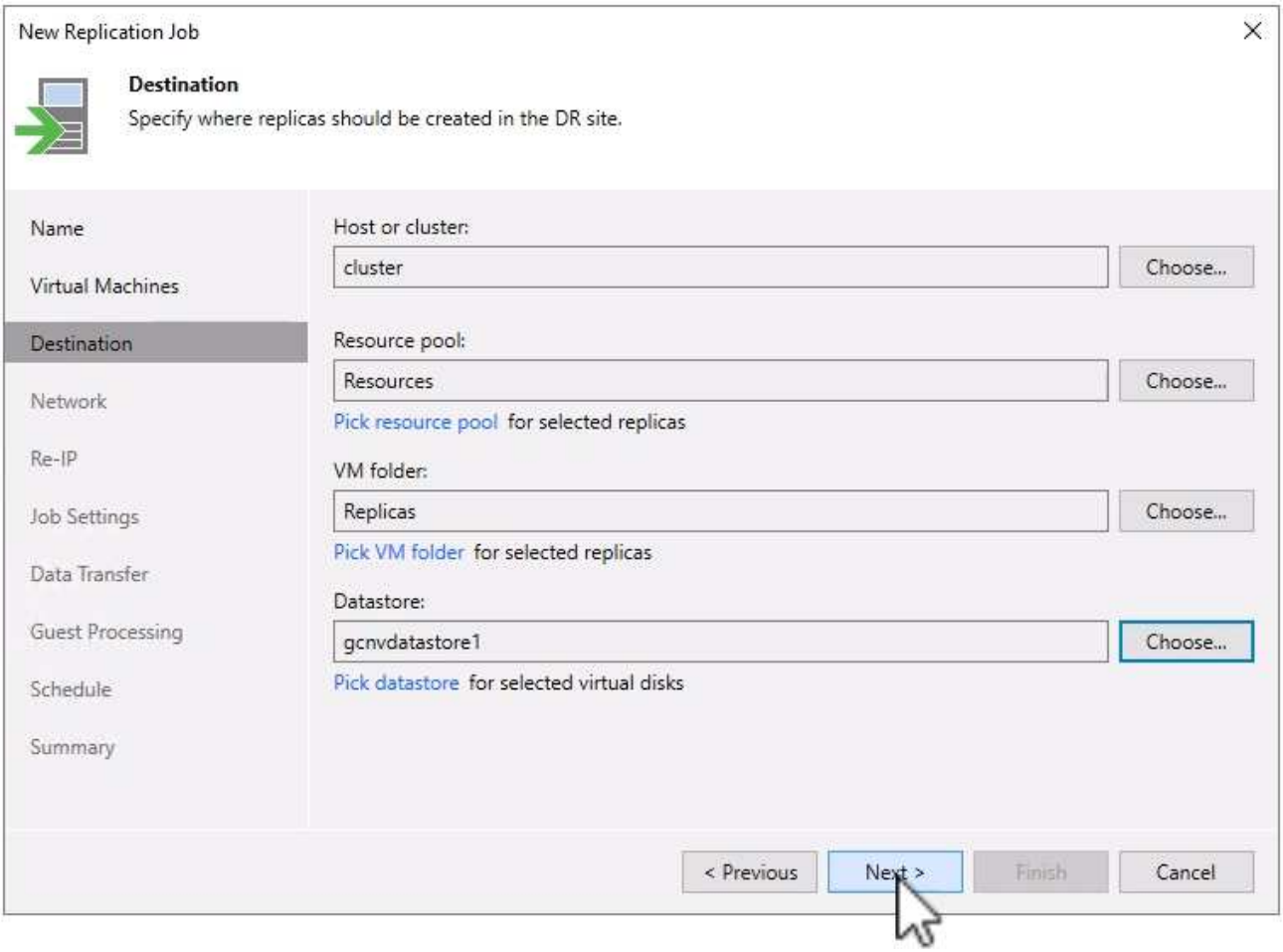


4. En la página **Máquinas virtuales**, seleccione las máquinas virtuales que se replicarán en el almacén de datos de NetApp Volumes conectado a un SDDC de GCVE. Haga clic en **Agregar**, luego en la ventana **Agregar objeto** seleccione las máquinas virtuales o los contenedores de máquinas virtuales necesarios y haga clic en **Agregar**. Haga clic en **Siguiente**.

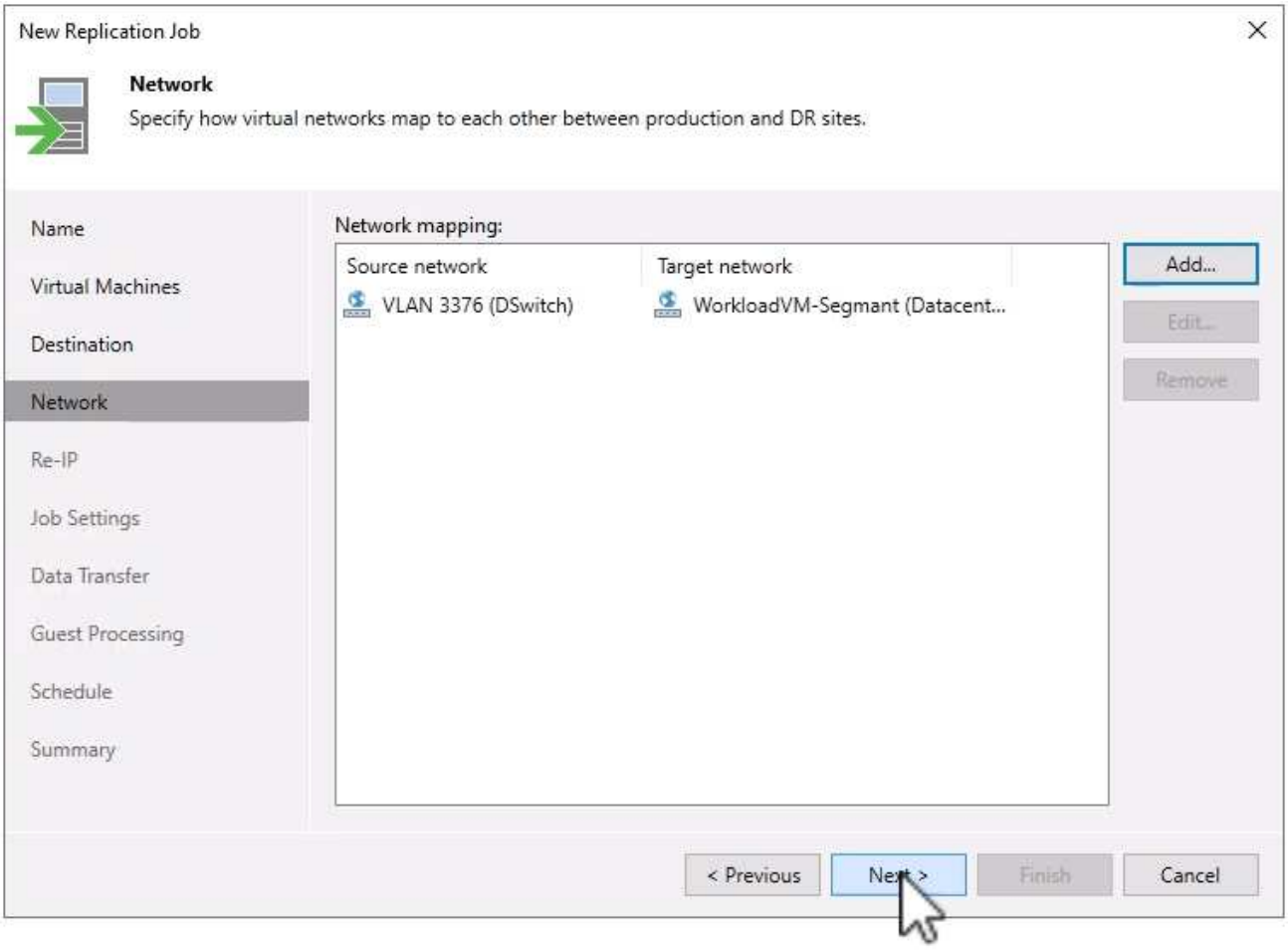
> Las máquinas virtuales se pueden colocar en vSAN para llenar la capacidad del almacén de datos de vSAN disponible. En un clúster piloto, la capacidad utilizable de un clúster vSAN de 3 nodos será limitada. El resto de los datos se pueden colocar fácilmente en los almacenes de datos de Google Cloud NetApp Volumes para que se puedan recuperar las máquinas virtuales y luego se pueda expandir el clúster para cumplir con los requisitos de CPU/memoria.



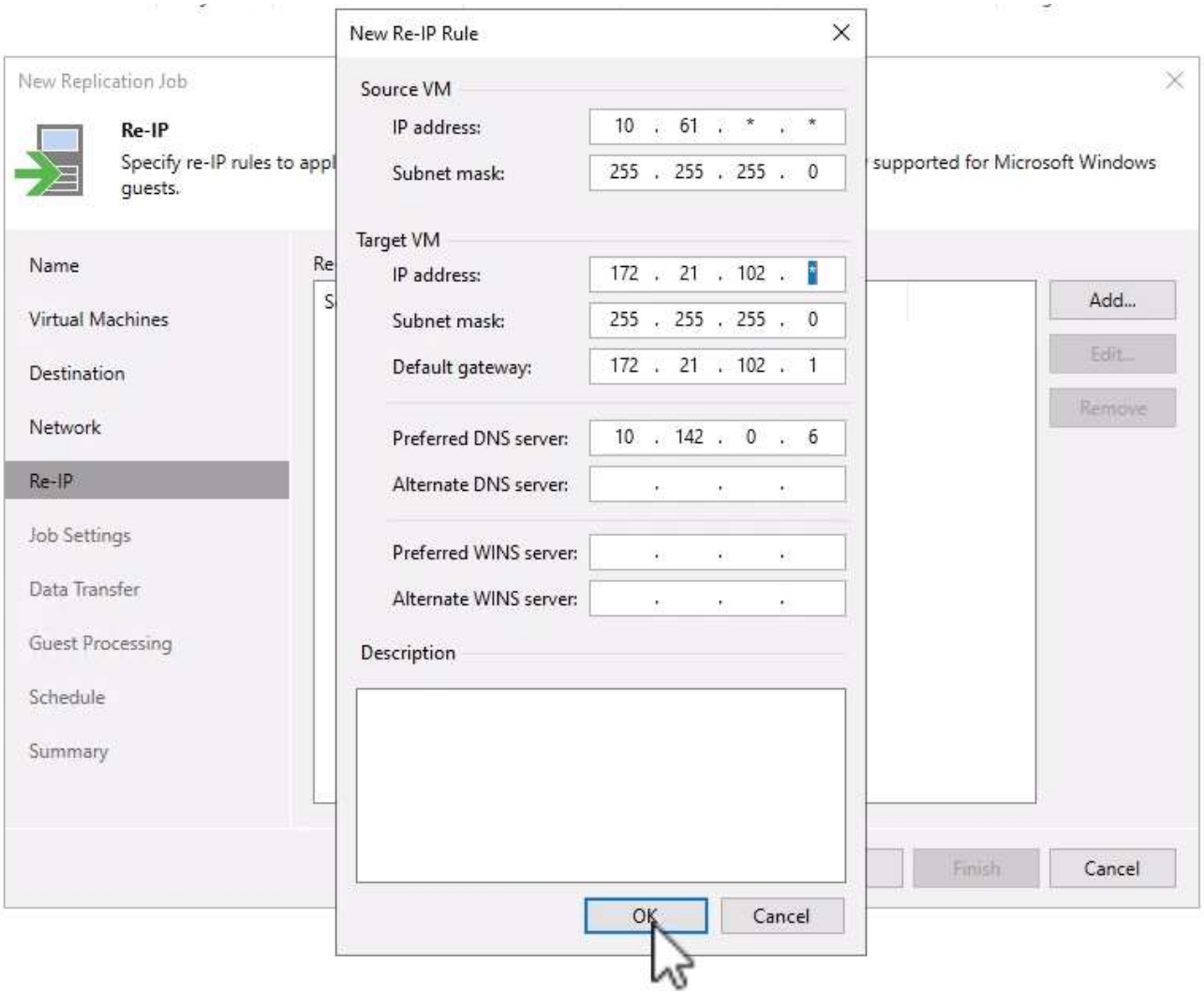
5. En la página **Destino**, seleccione el destino como el clúster/los hosts del SDDC de GCVE y el grupo de recursos, la carpeta de VM y el almacén de datos de NetApp Volumes adecuados para las réplicas de VM. Haga clic en **Siguiente** para continuar.



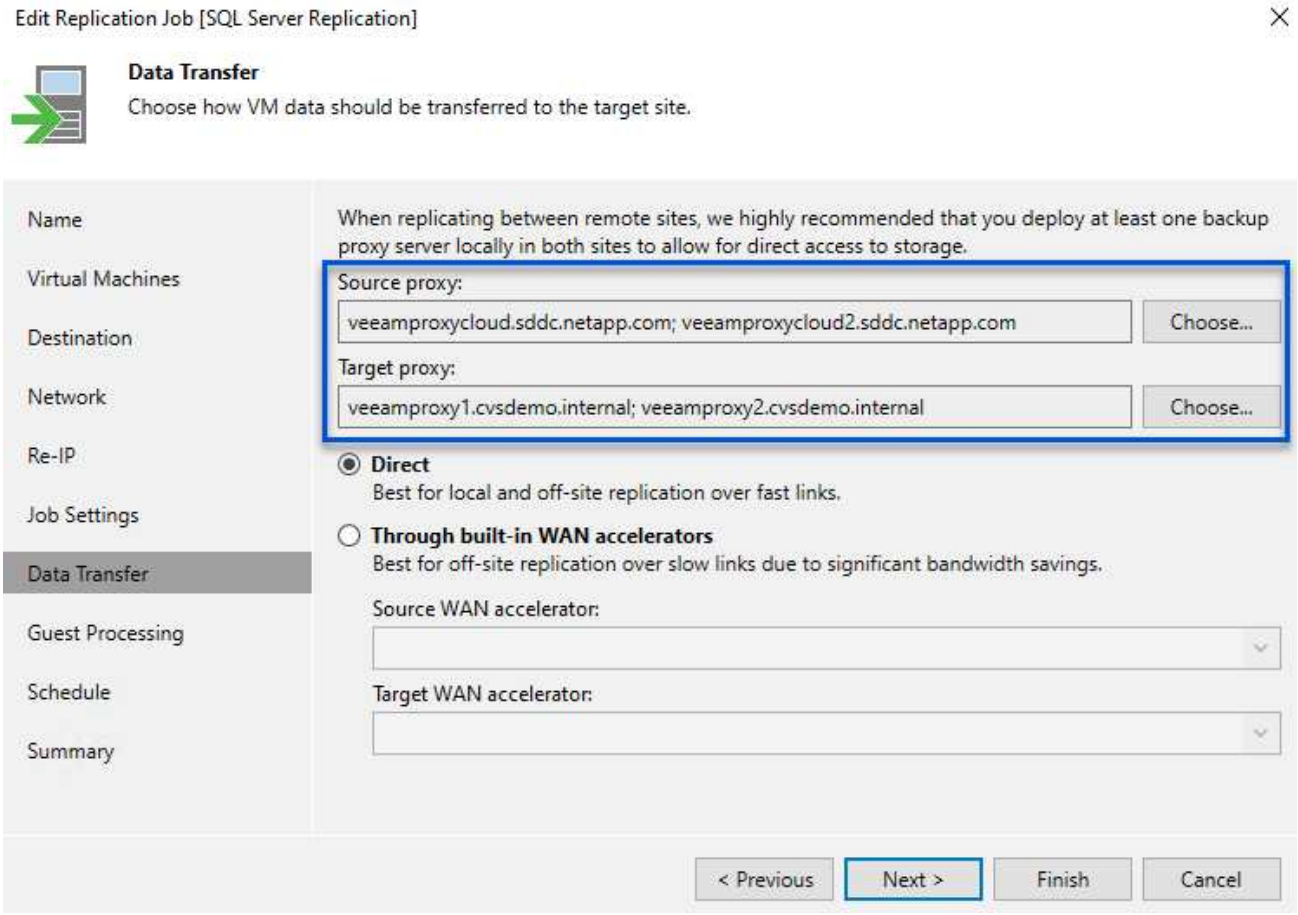
6. En la página **Red**, cree la asignación entre las redes virtuales de origen y de destino según sea necesario. Haga clic en **Siguiente** para continuar.



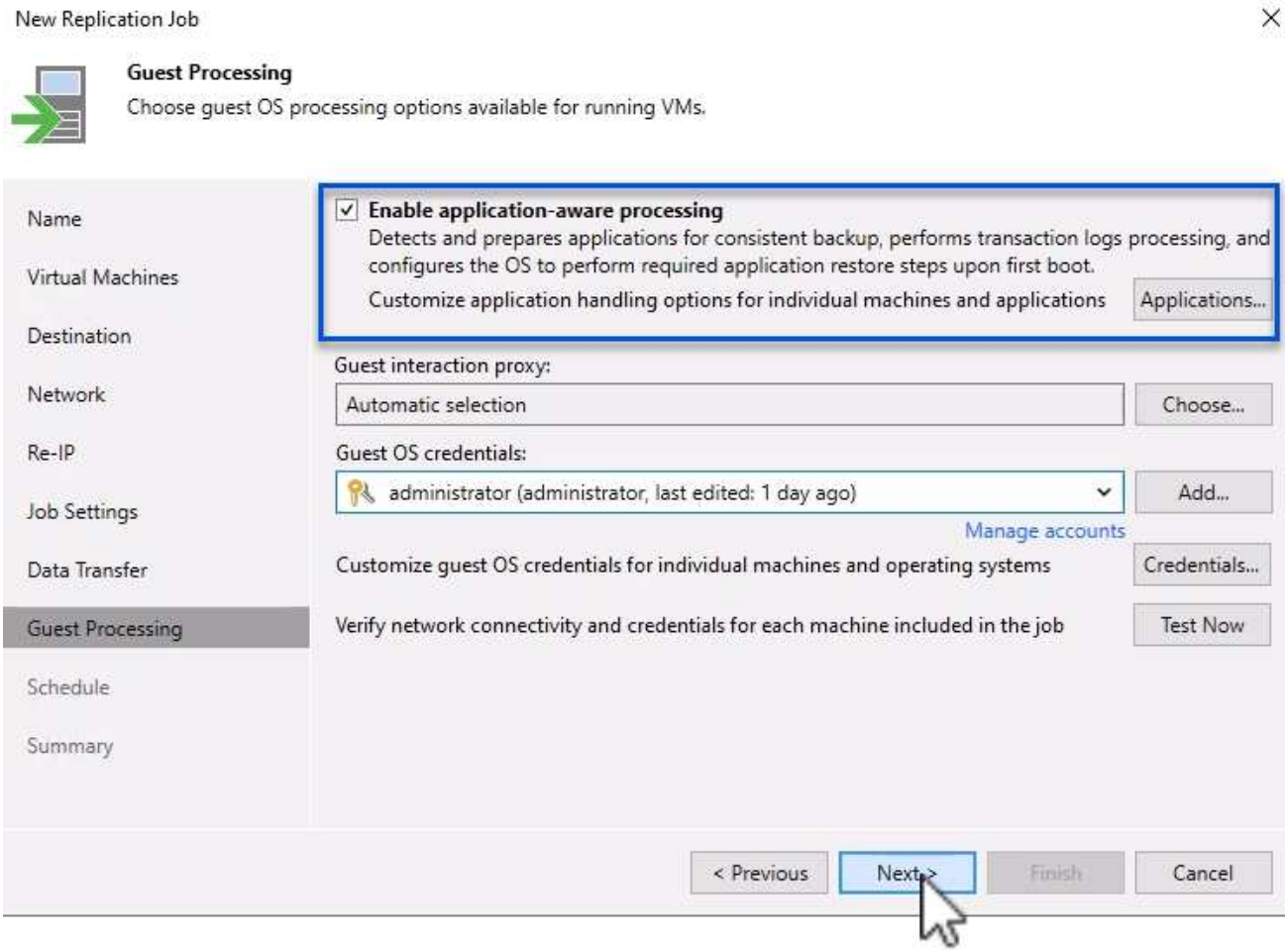
7. En la página **Re-IP**, haga clic en el botón **Agregar…** para agregar una nueva regla de re-IP. Complete los rangos de IP de las máquinas virtuales de origen y destino para especificar la red que se aplicará a las máquinas virtuales de origen en caso de una conmutación por error. Utilice asteriscos para especificar que se indica un rango de direcciones para ese octeto. Haga clic en **Siguiente** para continuar.



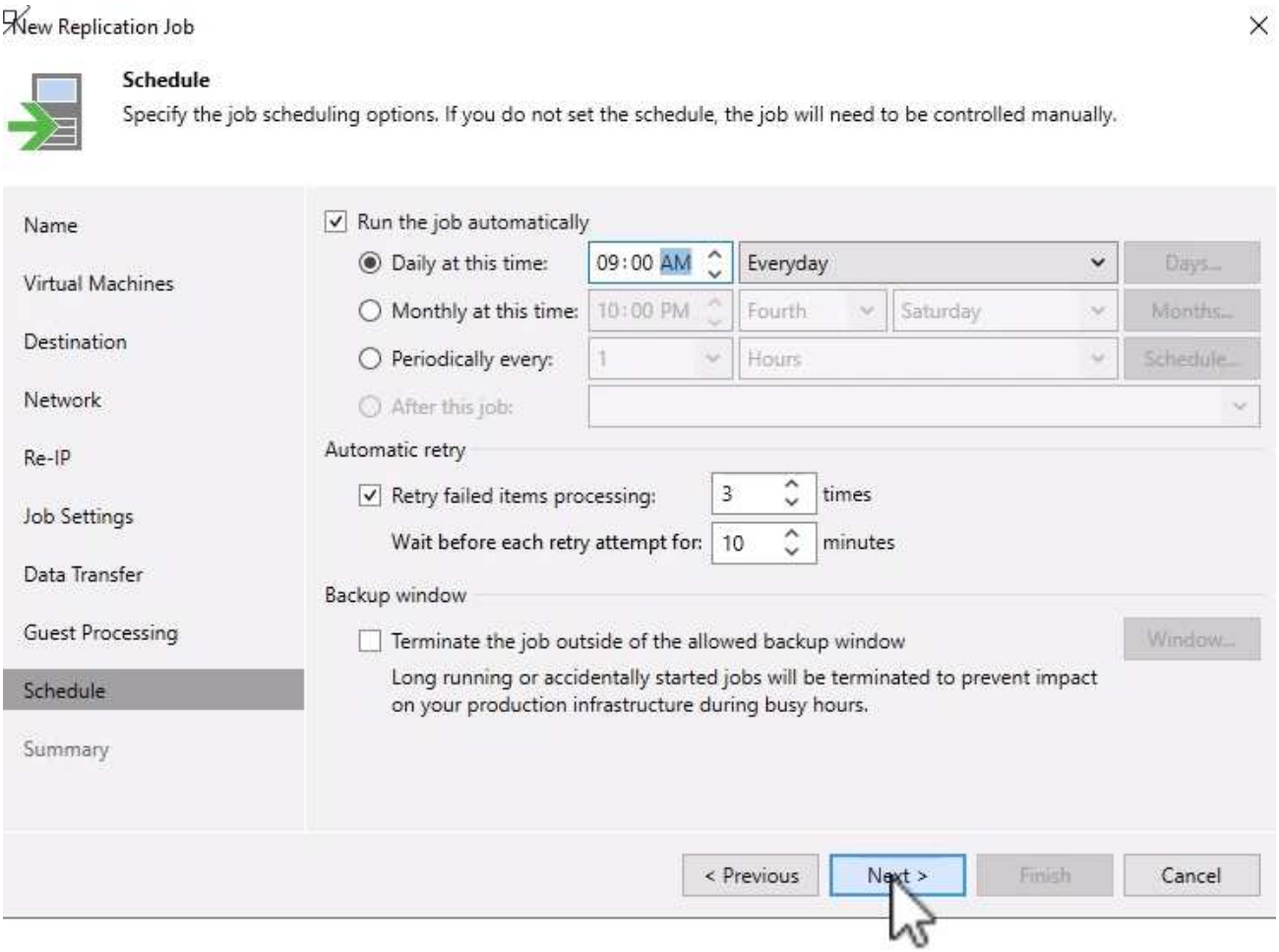
8. En la página **Configuración del trabajo**, especifique el repositorio de respaldo que almacenará metadatos para las réplicas de VM, la política de retención y seleccione el botón en la parte inferior para **Avanzado…** botón en la parte inferior para configuraciones de trabajo adicionales. Haga clic en **Siguiente** para continuar.
9. En **Transferencia de datos**, seleccione los servidores proxy que residen en los sitios de origen y de destino, y mantenga seleccionada la opción Directa. Aquí también se pueden seleccionar aceleradores WAN, si están configurados. Haga clic en **Siguiente** para continuar.



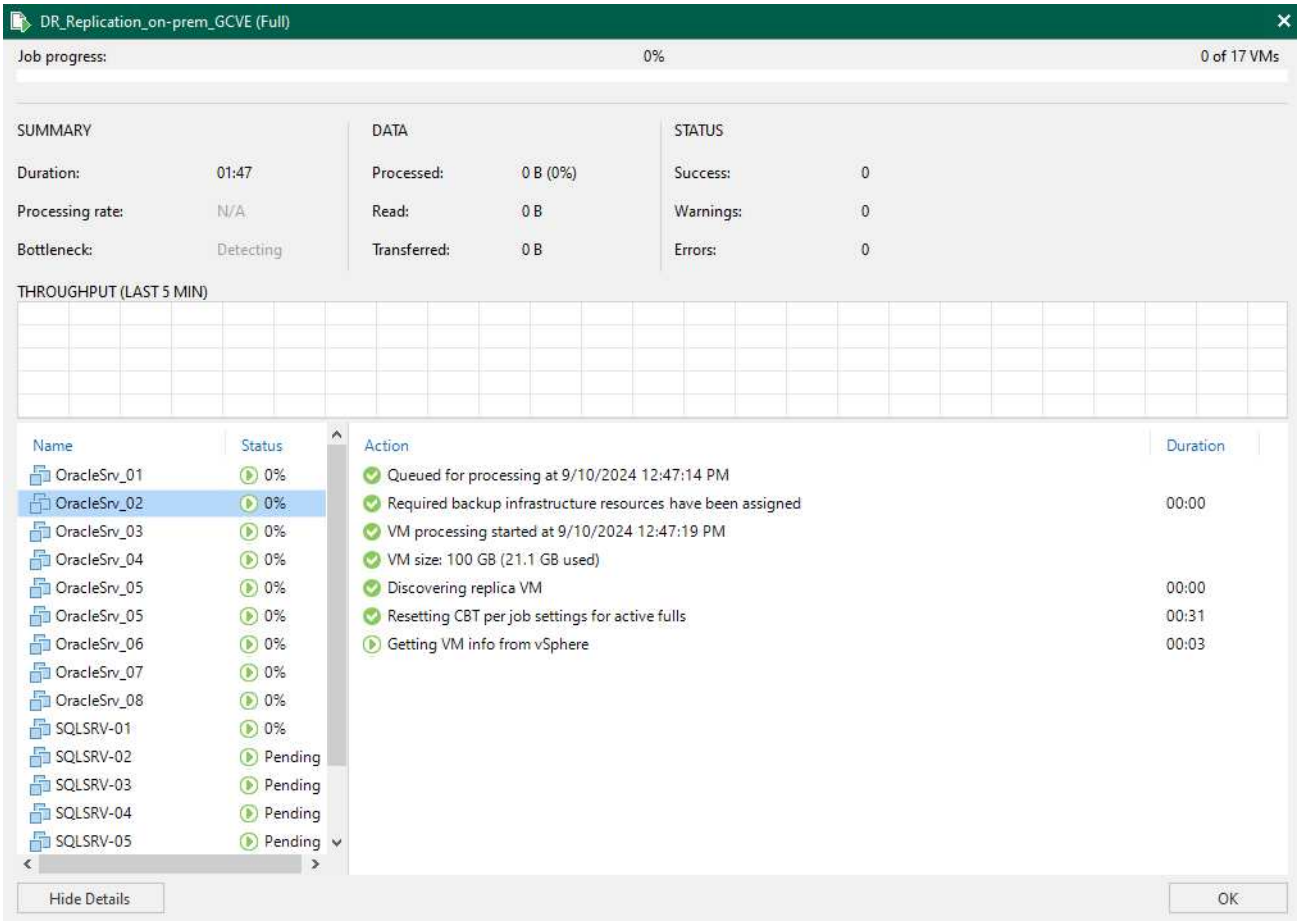
10. En la página **Procesamiento de invitados**, marque la casilla **Habilitar procesamiento consciente de la aplicación** según sea necesario y seleccione las **Credenciales del sistema operativo invitado**. Haga clic en **Siguiente** para continuar.



11. En la página **Programación**, defina los horarios y la frecuencia con que se ejecutará el trabajo de replicación. Haga clic en **Siguiente** para continuar.



12. Por último, revise la configuración del trabajo en la página **Resumen**. Marque la casilla para **Ejecutar el trabajo cuando haga clic en Finalizar** y haga clic en **Finalizar** para completar la creación del trabajo de replicación.
13. Una vez ejecutado, el trabajo de replicación se puede ver en la ventana de estado del trabajo.



Para obtener información adicional sobre la replicación de Veeam, consulte"Cómo funciona la replicación"

▼ **Crear un plan de conmutación por error**

Cuando se complete la replicación o siembra inicial, cree el plan de conmutación por error. El plan de conmutación por error ayuda a realizar la conmutación por error de las máquinas virtuales dependientes una por una o como grupo de manera automática. El plan de conmutación por error es el modelo para el orden en que se procesan las máquinas virtuales, incluidos los retrasos en el arranque. El plan de conmutación por error también ayuda a garantizar que las máquinas virtuales dependientes críticas ya estén en ejecución.

Después de completar la replicación o siembra inicial, cree un plan de conmutación por error. Este plan sirve como modelo estratégico para orquestar la conmutación por error de las máquinas virtuales dependientes, ya sea individualmente o como grupo. Define el orden de procesamiento de las máquinas virtuales, incorpora los retrasos de arranque necesarios y garantiza que las máquinas virtuales dependientes críticas estén operativas antes que otras. Al implementar un plan de conmutación por error bien estructurado, las organizaciones pueden optimizar su proceso de recuperación ante desastres, minimizando el tiempo de inactividad y manteniendo la integridad de los sistemas interdependientes durante un evento de conmutación por error.

Al crear el plan, Veeam Backup & Replication identifica y utiliza automáticamente los puntos de restauración más recientes para iniciar las réplicas de VM.

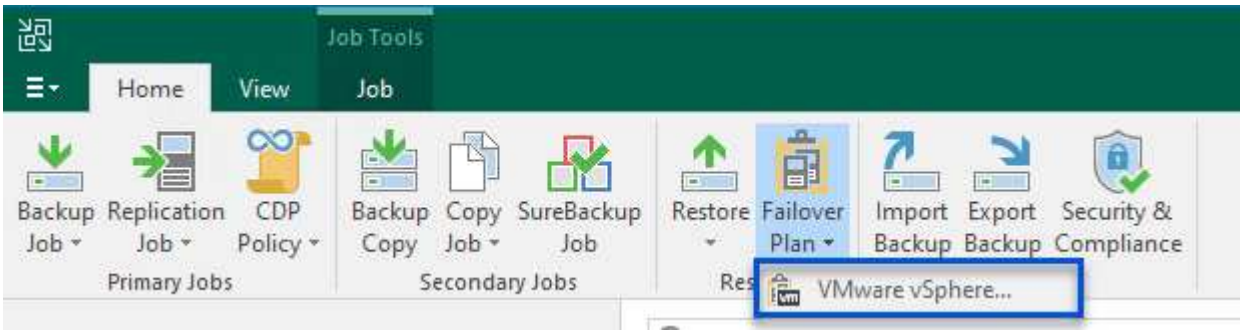
ⓘ El plan de conmutación por error solo se puede crear una vez que se completa la replicación inicial y las réplicas de la máquina virtual están en estado Listo.

La cantidad máxima de máquinas virtuales que se pueden iniciar simultáneamente cuando se ejecuta un plan de conmutación por error es 10.

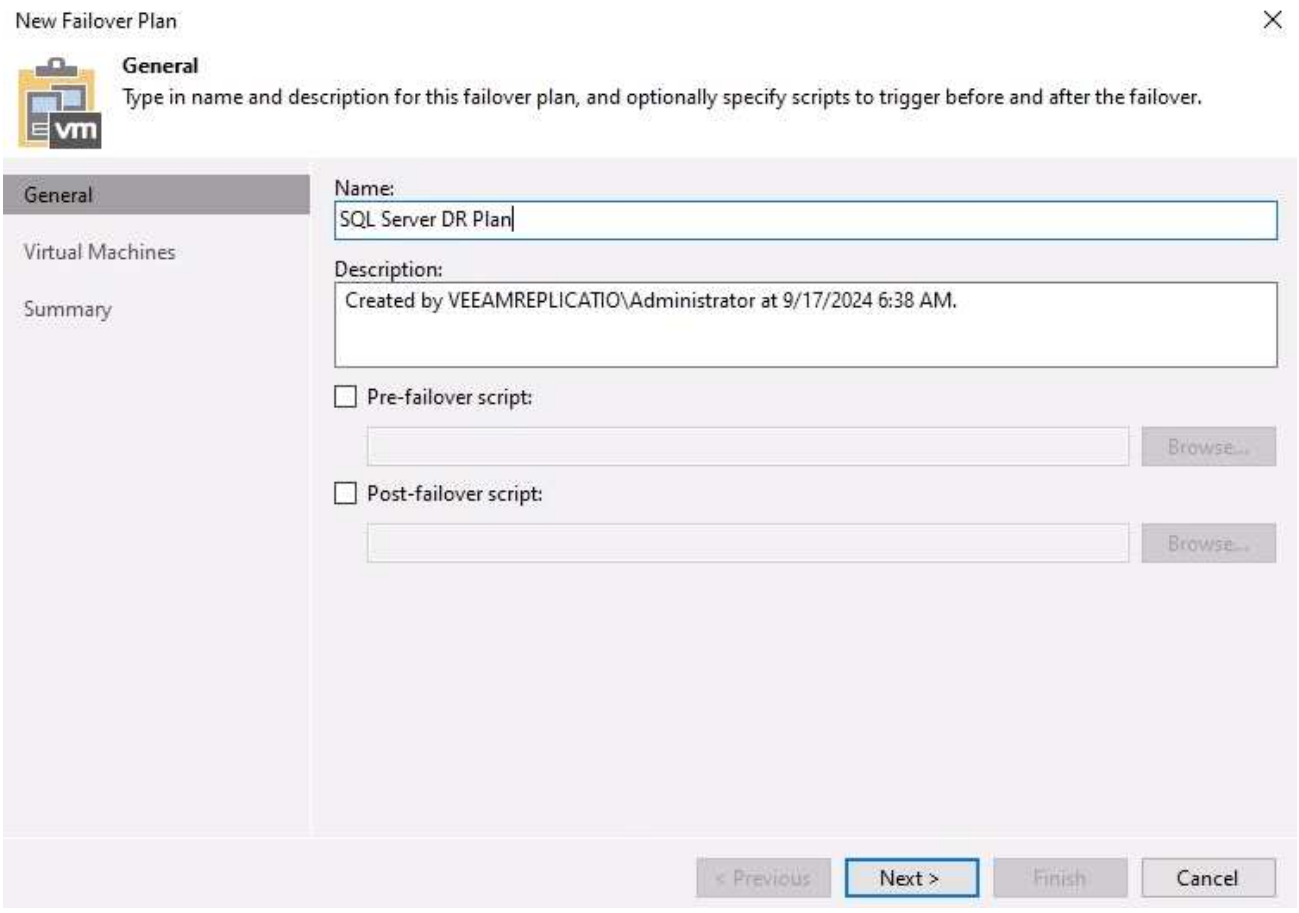
Durante el proceso de conmutación por error, las máquinas virtuales de origen no se apagarán.

Para crear el **Plan de conmutación por error**, complete los siguientes pasos:

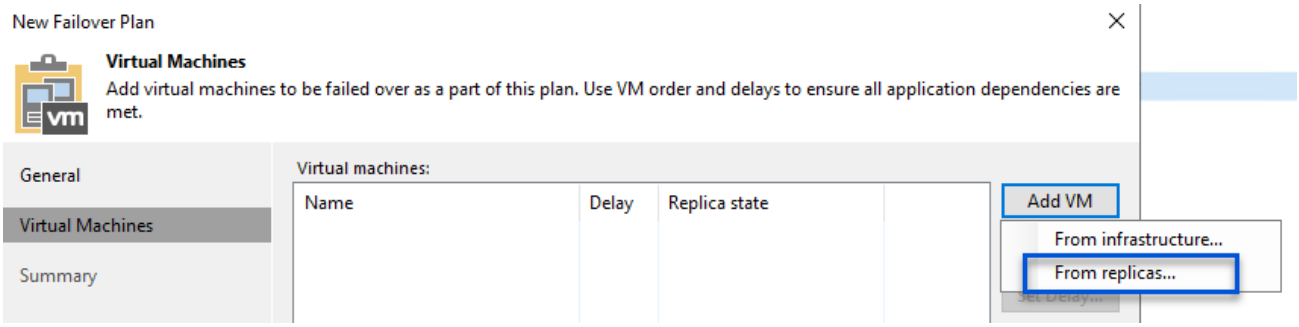
1. En la vista **Inicio**, haga clic en el botón **Plan de conmutación por error** en la sección **Restaurar**. En el menú desplegable, seleccione **VMware vSphere…**

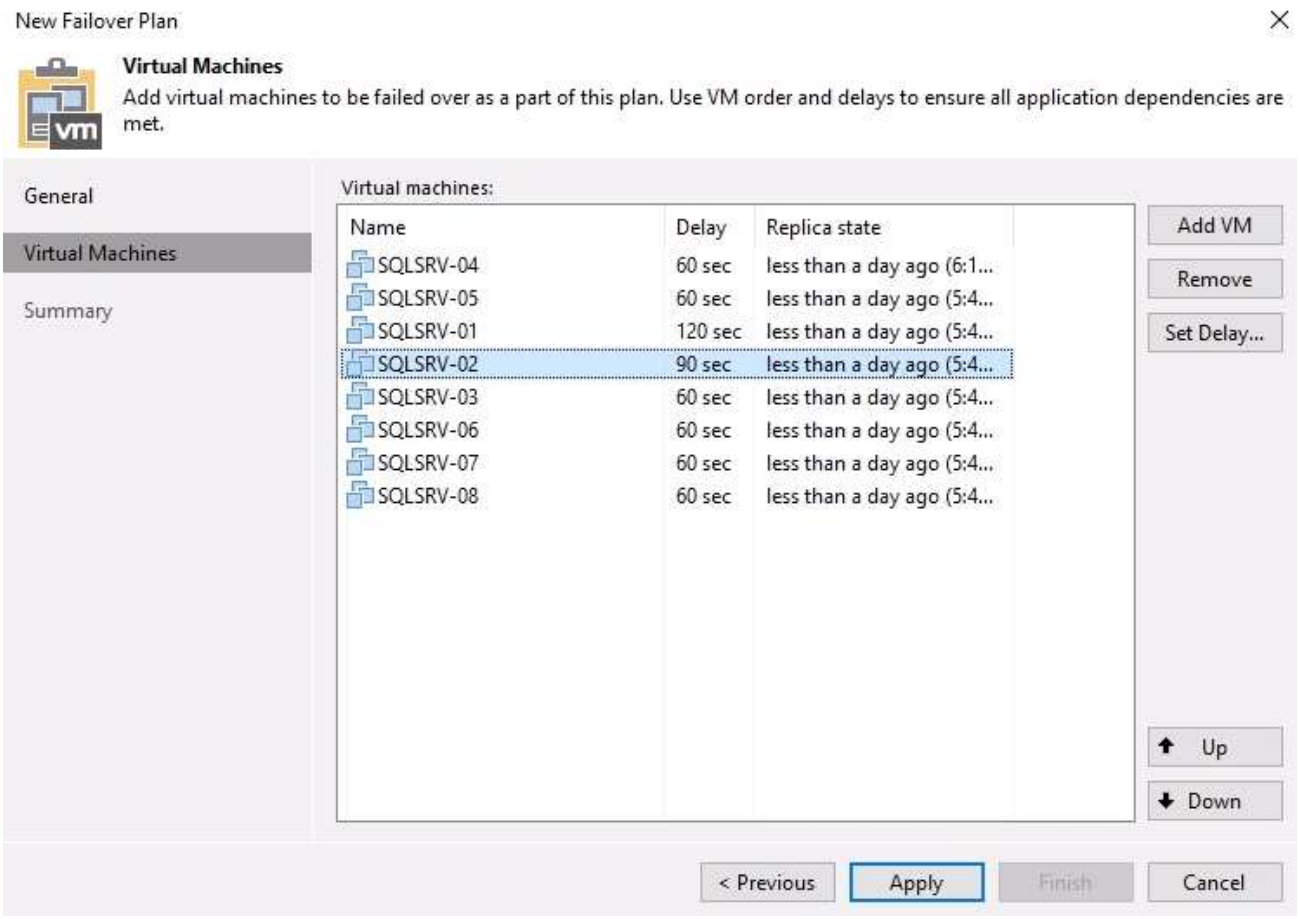


2. En la página **General** del asistente **Nuevo plan de conmutación por error**, proporcione un nombre y una descripción para el plan. Se pueden agregar scripts previos y posteriores a la conmutación por error según sea necesario. Por ejemplo, ejecute un script para apagar las máquinas virtuales antes de iniciar las máquinas virtuales replicadas.



3. En la página **Máquinas virtuales**, haga clic en el botón para **Agregar VM** y seleccione **Desde réplicas…**. Seleccione las máquinas virtuales que formarán parte del plan de conmutación por error y luego modifique el orden de arranque de las máquinas virtuales y los retrasos de arranque necesarios para cumplir con las dependencias de la aplicación.





Haga clic en **Aplicar** para continuar.

4. Finalmente revise todas las configuraciones del plan de conmutación por error y haga clic en **Finalizar** para crear el plan de conmutación por error.

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

▼ **Ejecutar el plan de conmutación por error**

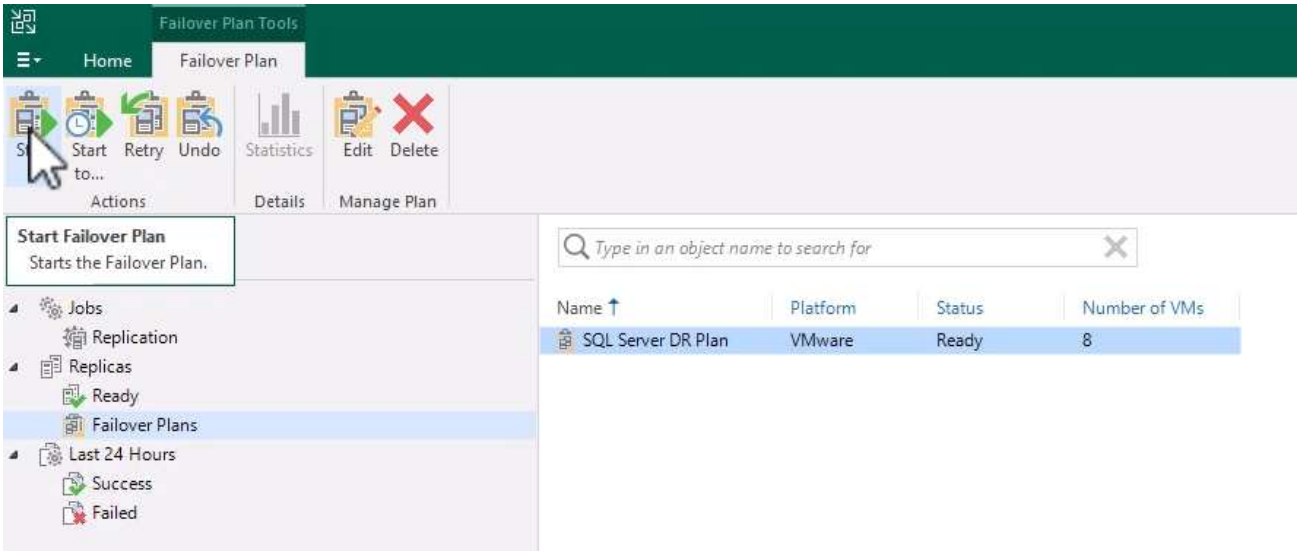
Durante la conmutación por error, la máquina virtual de origen en el sitio de producción cambia a su réplica en el sitio de recuperación ante desastres. Como parte del proceso, Veeam Backup & Replication restaura la réplica de la VM al punto de restauración requerido y transfiere todas las actividades de E/S de la VM de origen a su réplica. Las réplicas no sólo sirven para desastres reales, sino también para simular simulacros de recuperación ante desastres. En la simulación de conmutación por error, la máquina virtual de origen continúa ejecutándose. Una vez completadas las pruebas necesarias, se puede deshacer la conmutación por error y volver las operaciones a la normalidad.

ⓘ Asegúrese de que la segmentación de la red esté implementada para evitar conflictos de IP durante la conmutación por error.

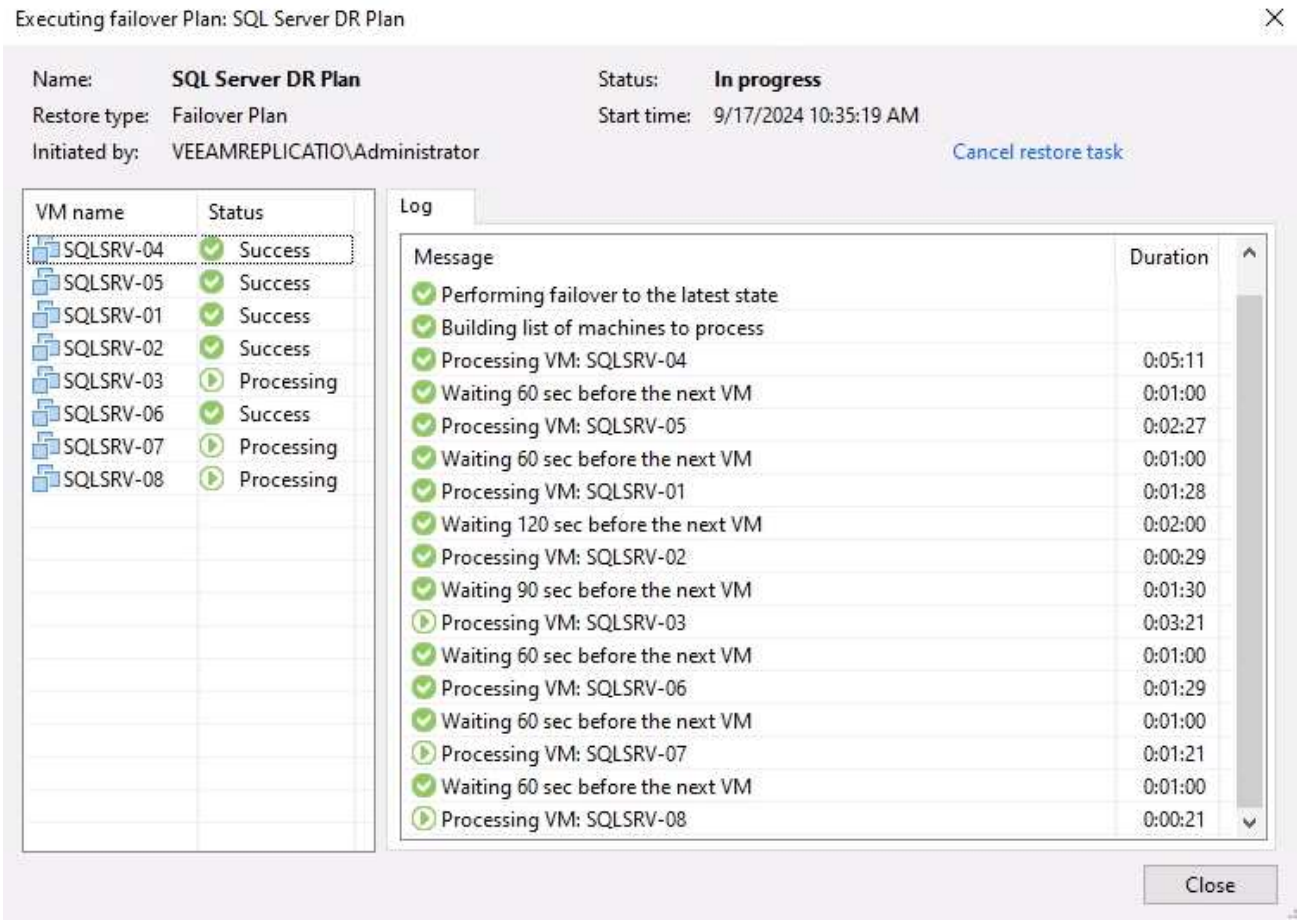
Complete los siguientes pasos para iniciar el plan de conmutación por error:

1. Para comenzar, en la vista **Inicio**, haga clic en **Réplicas > Planes de conmutación por error** en el menú de la izquierda y luego en el botón **Inicio**. Alternativamente, se puede utilizar el botón **Iniciar a…**

para realizar una conmutación por error a un punto de restauración anterior.



2. Supervise el progreso de la conmutación por error en la ventana **Ejecutando plan de conmutación por error**.



Veeam Backup & Replication detiene todas las actividades de replicación de la máquina

virtual de origen hasta que su réplica vuelva al estado Listo.

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

▼ **Retorno al sitio de producción**

La realización de una conmutación por error se considera un paso intermedio y debe finalizarse según el requisito. Las opciones incluyen lo siguiente:

- **Retorno a producción**: vuelve a la máquina virtual original y sincroniza todas las modificaciones realizadas durante el período activo de la réplica con la máquina virtual de origen.

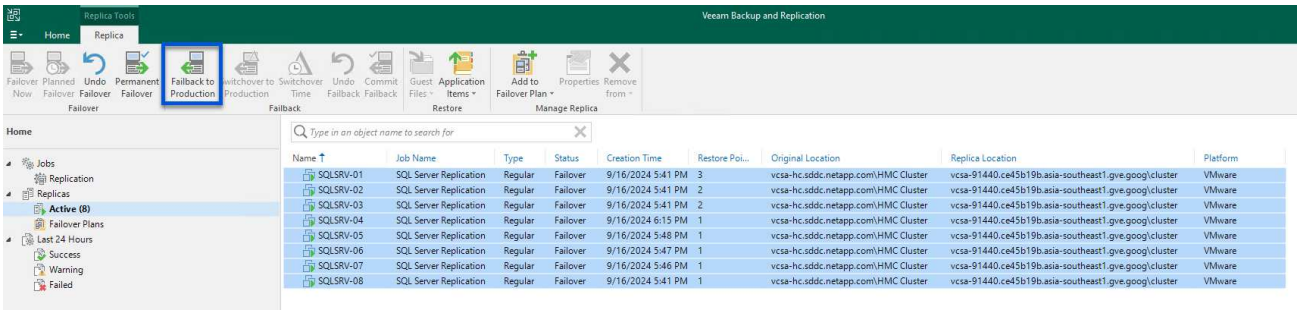
> ⓘ Durante la conmutación por error, los cambios se transfieren pero no se aplican inmediatamente. Seleccione **Confirmar conmutación por error** una vez que se haya verificado la funcionalidad de la máquina virtual original. Como alternativa, elija **Deshacer conmutación por error** para volver a la réplica de la máquina virtual si la máquina virtual original muestra un comportamiento inesperado.

- **Deshacer conmutación por error**: vuelve a la máquina virtual original y descarta todos los cambios realizados en la réplica de la máquina virtual durante su período operativo.
- **Conmutación por error permanente**: cambia de forma permanente de la máquina virtual original a su réplica y establece la réplica como la nueva máquina virtual principal para las operaciones en curso.

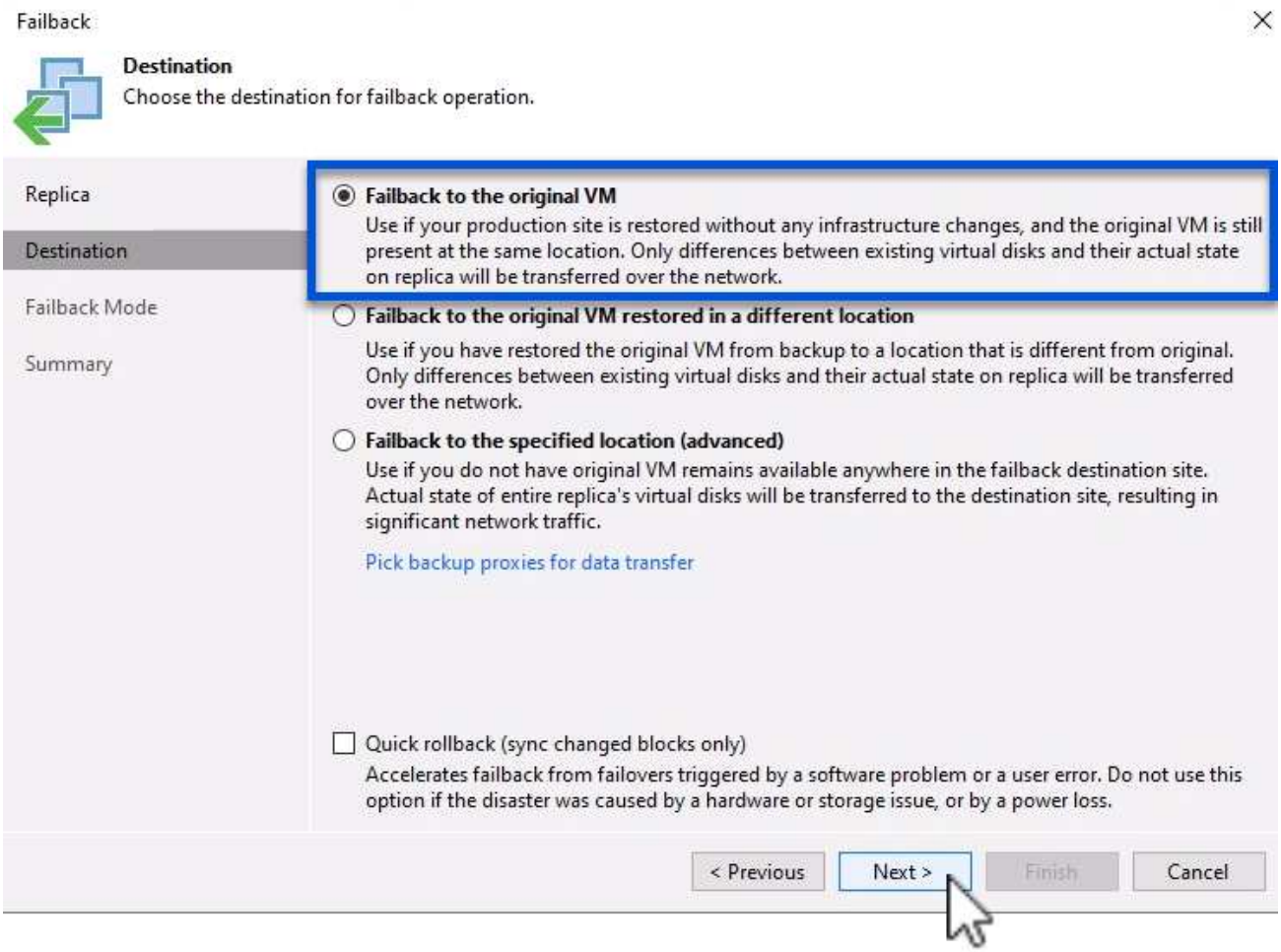
En este escenario, se seleccionó la opción "Retorno a producción".

Complete los siguientes pasos para realizar una conmutación por error al sitio de producción:

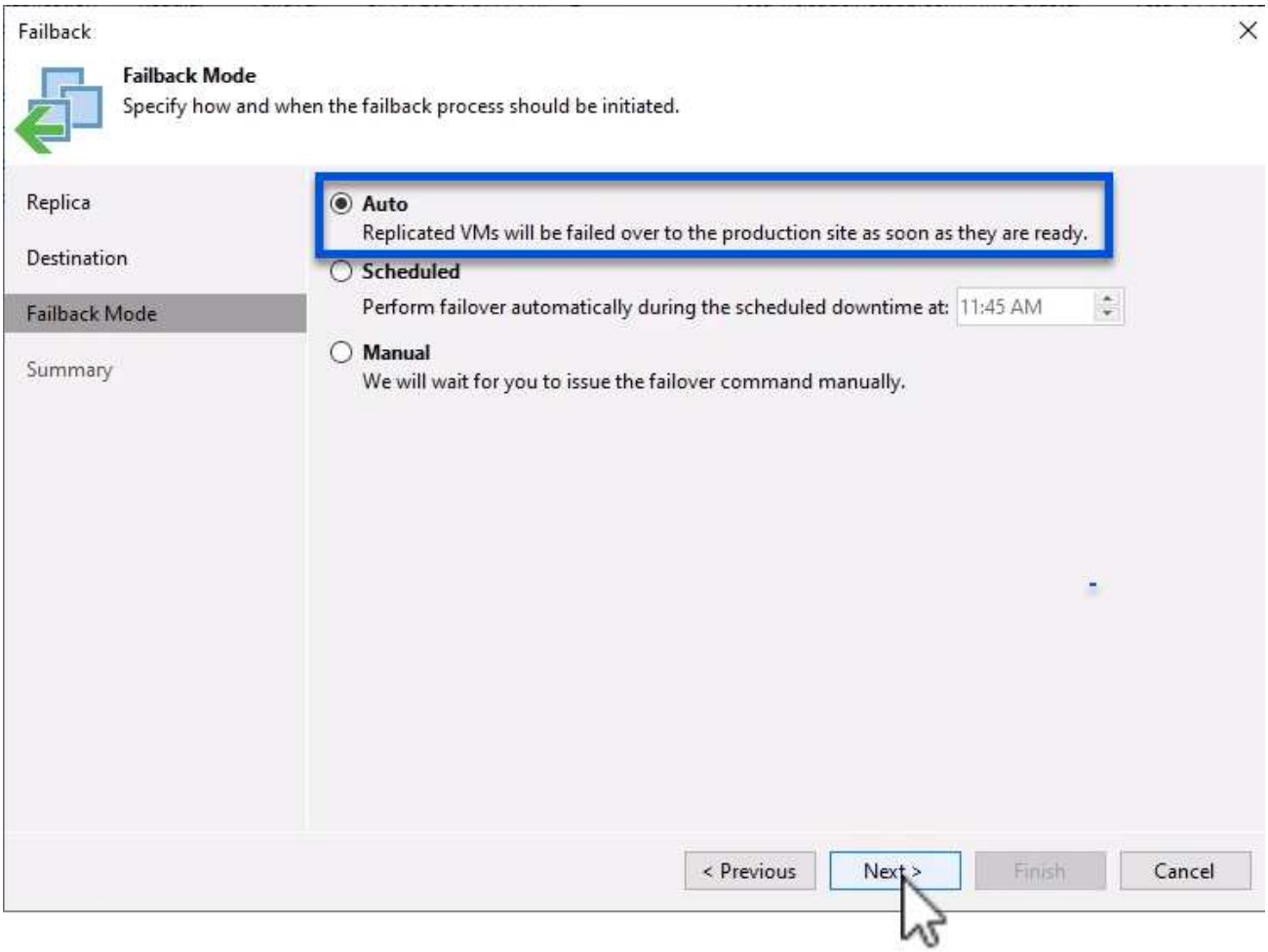
1. Desde la vista **Inicio**, haga clic en **Réplicas > Activas** en el menú de la izquierda. Seleccione las máquinas virtuales que se incluirán y haga clic en el botón **Retorno a producción** en el menú superior.



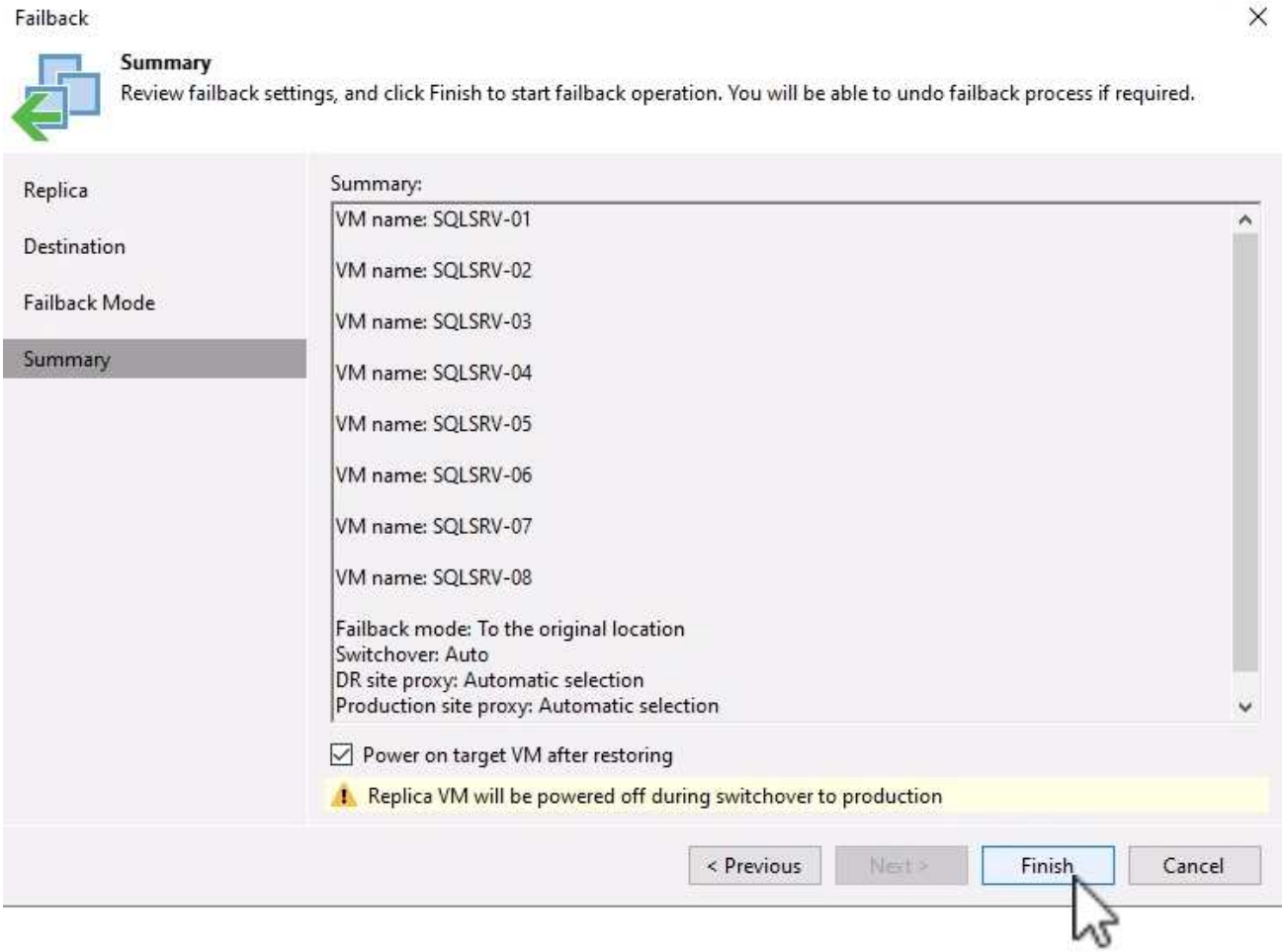
2. En la página **Réplica** del asistente de **Conmutación por recuperación**, seleccione las réplicas que desea incluir en el trabajo de conmutación por recuperación.
3. En la página **Destino**, seleccione **Retorno a la máquina virtual original** y haga clic en **Siguiente** para continuar.



4. En la página **Modo de conmutación por error**, seleccione **Automático** para iniciar la conmutación por error lo antes posible.

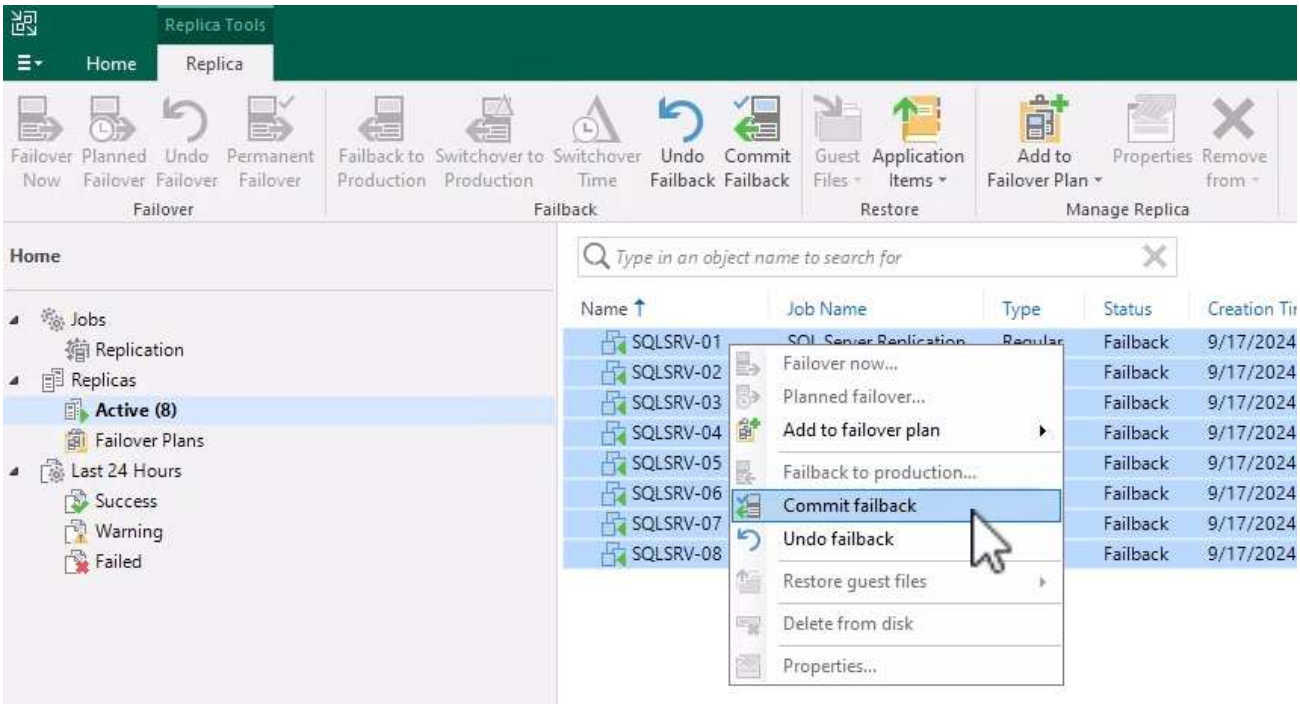


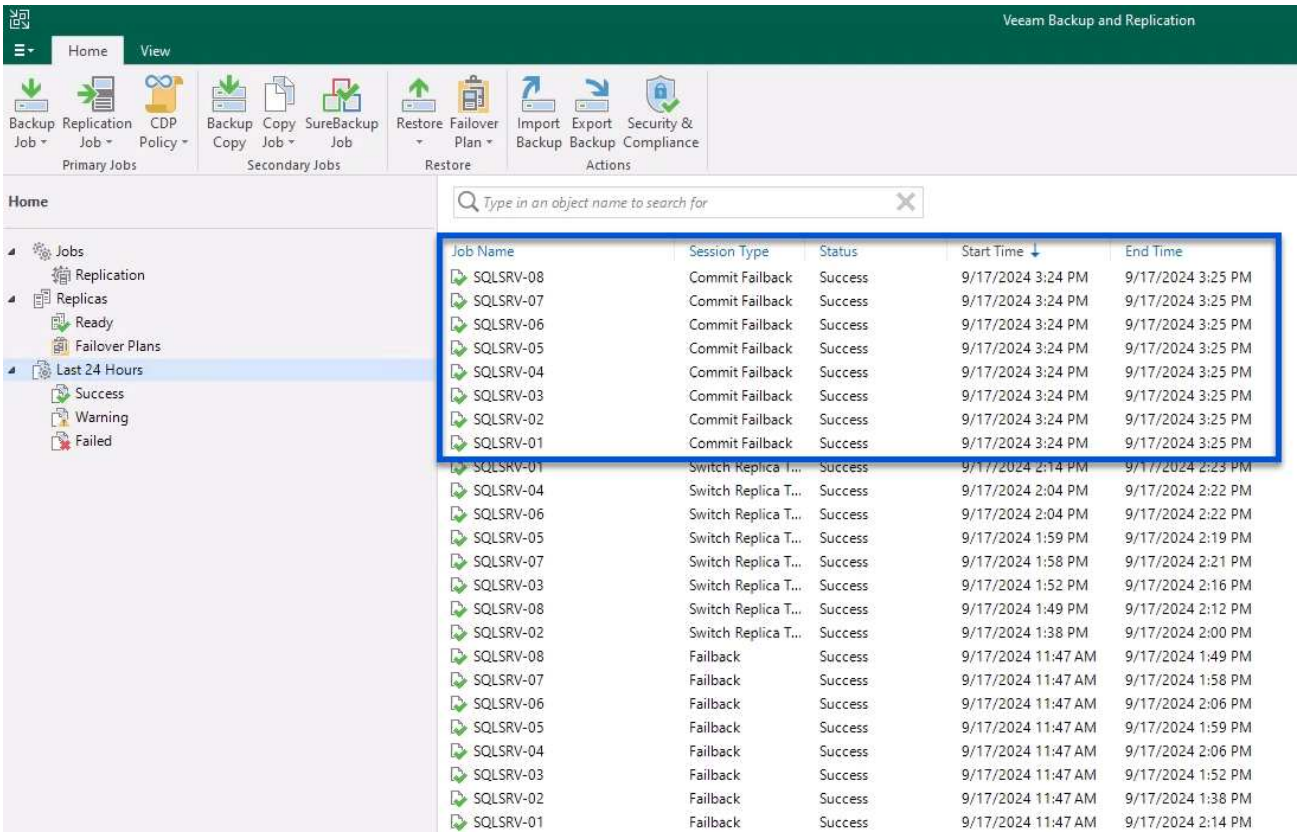
5. En la página **Resumen**, elija si desea **Encender la máquina virtual de destino después de restaurar** y luego haga clic en Finalizar para iniciar el trabajo de conmutación por recuperación.



La confirmación de conmutación por error finaliza la operación de conmutación por error, confirmando la integración exitosa de los cambios en la máquina virtual de producción. Tras la confirmación, Veeam Backup & Replication reanuda las actividades de replicación regulares para la máquina virtual de producción restaurada. Esto cambia el estado de la réplica restaurada de *Failback* a *Ready*.

1. Para confirmar la conmutación por error, navegue a **Réplicas > Activas**, seleccione las máquinas virtuales que se confirmarán, haga clic con el botón derecho y seleccione **Confirmar conmutación por error**.





Una vez que la conmutación por error a producción es exitosa, todas las máquinas virtuales se restauran al sitio de producción original.

Para obtener información detallada sobre el proceso de conmutación por error, consulte la documentación de Veeam."Conmutación por error y recuperación para replicación" .

Conclusión

La funcionalidad del almacén de datos de Google Cloud NetApp Volumes permite a Veeam y otras herramientas de terceros validadas brindar soluciones de recuperación ante desastres (DR) rentables. Al utilizar clústeres Pilot Light en lugar de clústeres grandes y dedicados para réplicas de máquinas virtuales, las organizaciones pueden reducir significativamente los gastos. Este enfoque permite estrategias de recuperación ante desastres personalizadas que aprovechan las soluciones de respaldo internas existentes para la recuperación ante desastres basada en la nube, eliminando la necesidad de centros de datos locales adicionales. En caso de desastre, la conmutación por error se puede iniciar con un solo clic o configurar para que ocurra automáticamente, lo que garantiza la continuidad del negocio con un tiempo de inactividad mínimo.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

Migrar cargas de trabajo en GCP/GCVE

Migrar cargas de trabajo al almacén de datos de Google Cloud NetApp Volumes en Google Cloud VMware Engine mediante VMware HCX: guía de inicio rápido

Uno de los casos de uso más comunes del almacén de datos de Google Cloud VMware Engine y Cloud Volume Service es la migración de cargas de trabajo de VMware. VMware HCX es una opción preferida y proporciona varios mecanismos de migración para mover máquinas virtuales (VM) locales y sus datos a almacenes de datos NFS de Cloud Volume Service.

Descripción general: Migración de máquinas virtuales con VMware HCX, almacenes de datos de Google Cloud NetApp Volumes y Google Cloud VMware Engine (GCVE)

VMware HCX es principalmente una plataforma de migración diseñada para simplificar la migración de aplicaciones, el reequilibrio de la carga de trabajo e incluso la continuidad del negocio en las nubes. Se incluye como parte de Google Cloud VMware Engine Private Cloud y ofrece muchas formas de migrar cargas de trabajo y puede usarse para operaciones de recuperación ante desastres (DR).

Este documento proporciona una guía paso a paso para aprovisionar el almacén de datos de Cloud Volume Service, seguido de la descarga, implementación y configuración de VMware HCX, incluidos todos sus componentes principales en las instalaciones locales y en el lado de VMware Engine de Google Cloud, incluida la interconexión, la extensión de red y la optimización de WAN para habilitar varios mecanismos de migración de VM.

> ⓘ VMware HCX funciona con cualquier tipo de almacén de datos, ya que la migración se realiza a nivel de máquina virtual. Por lo tanto, este documento es aplicable a clientes existentes de NetApp y a clientes que no son de NetApp que planean implementar Cloud Volume Service con Google Cloud VMware Engine para una implementación de nube VMware rentable.

▼ **Pasos de alto nivel**

Esta lista proporciona los pasos de alto nivel necesarios para emparejar y migrar las máquinas virtuales a HCX Cloud Manager en el lado de Google Cloud VMware Engine desde HCX Connector local:

1. Prepare HCX a través del portal Google VMware Engine.
2. Descargue e implemente el instalador de HCX Connector Open Virtualization Appliance (OVA) en el servidor VMware vCenter local.

3. Active HCX con la clave de licencia.
4. Empareje el conector VMware HCX local con Google Cloud VMware Engine HCX Cloud Manager.
5. Configurar el perfil de red, el perfil de cómputo y la malla de servicio.
6. (Opcional) Realice la extensión de la red para evitar la re-IP durante las migraciones.
7. Validar el estado del dispositivo y asegurarse de que la migración sea posible.
8. Migrar las cargas de trabajo de la máquina virtual.

▼ Prerrequisitos

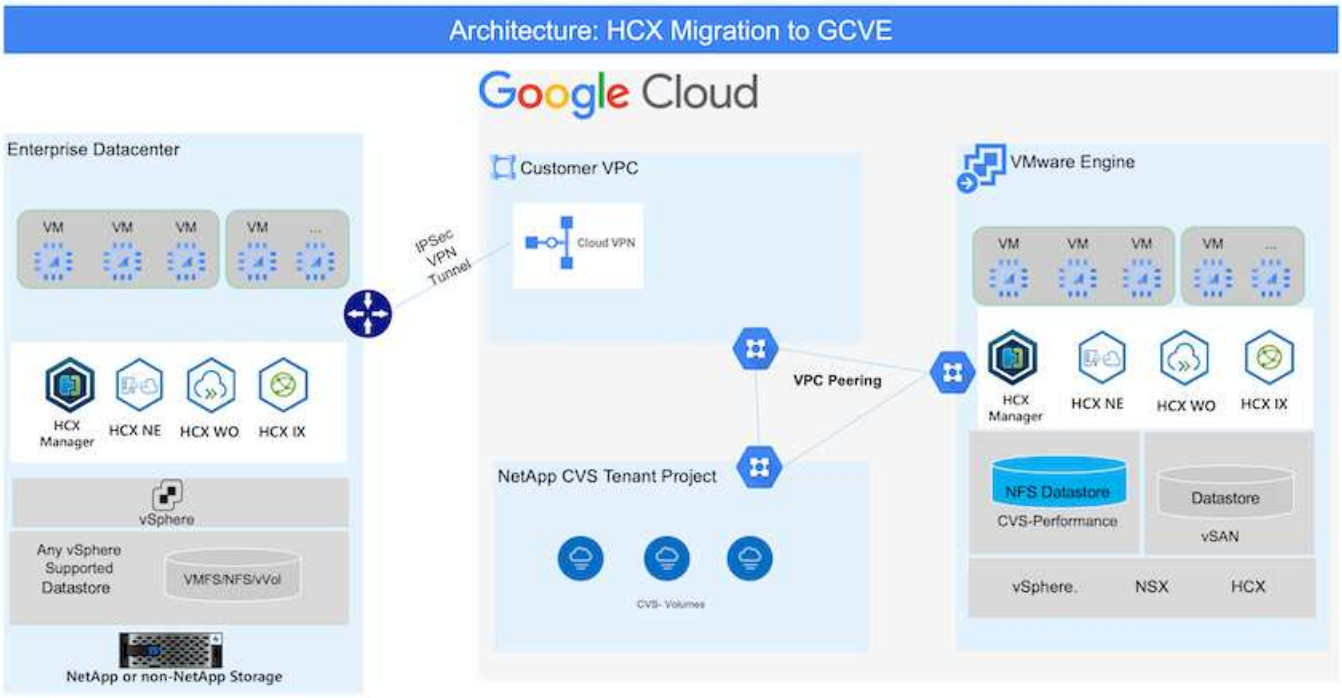
Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte este "enlace" . Una vez cumplidos los requisitos previos, incluida la conectividad, descargue la clave de licencia HCX del portal de Google Cloud VMware Engine. Después de descargar el instalador de OVA, continúe con el proceso de instalación como se describe a continuación.

> ⓘ HCX Advanced es la opción predeterminada y la edición VMware HCX Enterprise también está disponible a través de un ticket de soporte y recibe soporte sin costo adicional. Referirse "este enlace"

- Utilice un centro de datos definido por software (SDDC) de Google Cloud VMware Engine existente o cree una nube privada mediante este"Enlace de NetApp" o esto "Enlace de Google" .
- La migración de máquinas virtuales y datos asociados desde el centro de datos local habilitado para VMware vSphere requiere conectividad de red desde el centro de datos al entorno SDDC. Antes de migrar cargas de trabajo, "Configurar una conexión Cloud VPN o Cloud Interconnect" entre el entorno local y la respectiva nube privada.
- La ruta de red desde el entorno local de VMware vCenter Server a la nube privada de Google Cloud VMware Engine debe admitir la migración de máquinas virtuales mediante vMotion.
- Asegúrese de que se cumplan los requisitos "reglas y puertos de firewall" Se permiten para el tráfico de vMotion entre el servidor vCenter local y el vCenter de SDDC.
- El volumen NFS de Cloud Volume Service debe montarse como un almacén de datos en Google Cloud VMware Engine. Siga los pasos detallados en este "enlace" para conectar almacenes de datos de Cloud Volume Service a los hosts de VMware Engines de Google Cloud.

▼ Arquitectura de alto nivel

Para fines de prueba, el entorno de laboratorio local utilizado para esta validación se conectó a través de una VPN en la nube, lo que permite la conectividad local con Google Cloud VPC.



Para obtener más detalles sobre el uso de VMware HCX con Google, consulte "Enlace de VMware"

Implementación de la solución

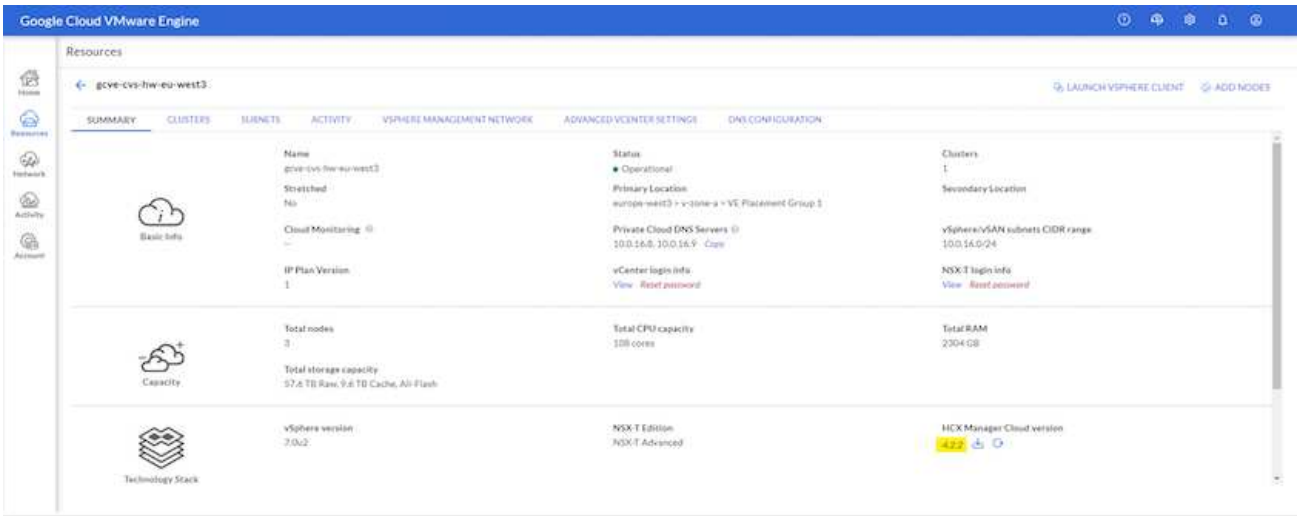
Siga la serie de pasos para completar la implementación de esta solución:

▼ **Paso 1: Prepare HCX a través del portal de Google VMware Engine**

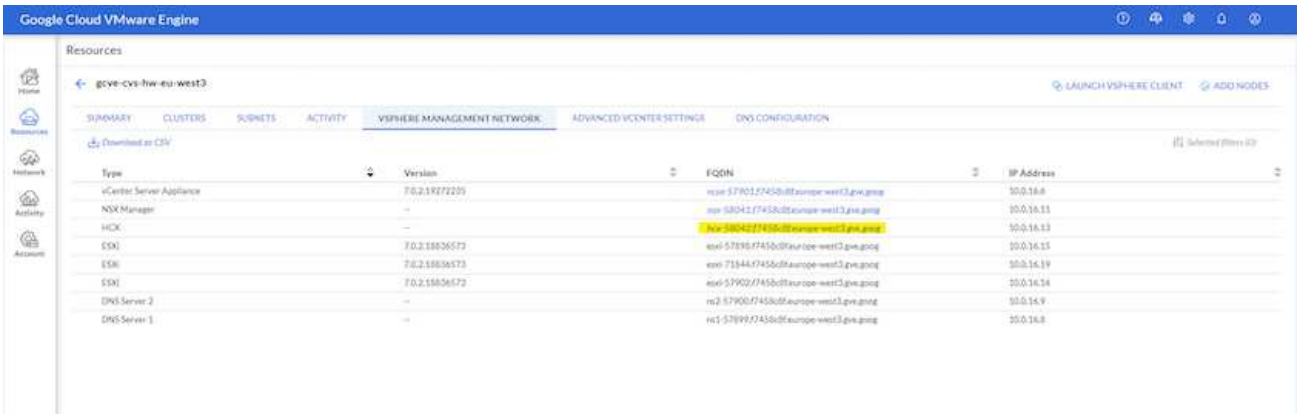
El componente HCX Cloud Manager se instala automáticamente a medida que aprovisiona una nube privada con VMware Engine. Para prepararse para el emparejamiento del sitio, complete los siguientes pasos:

1. Inicie sesión en el portal de Google VMware Engine e inicie sesión en HCX Cloud Manager.

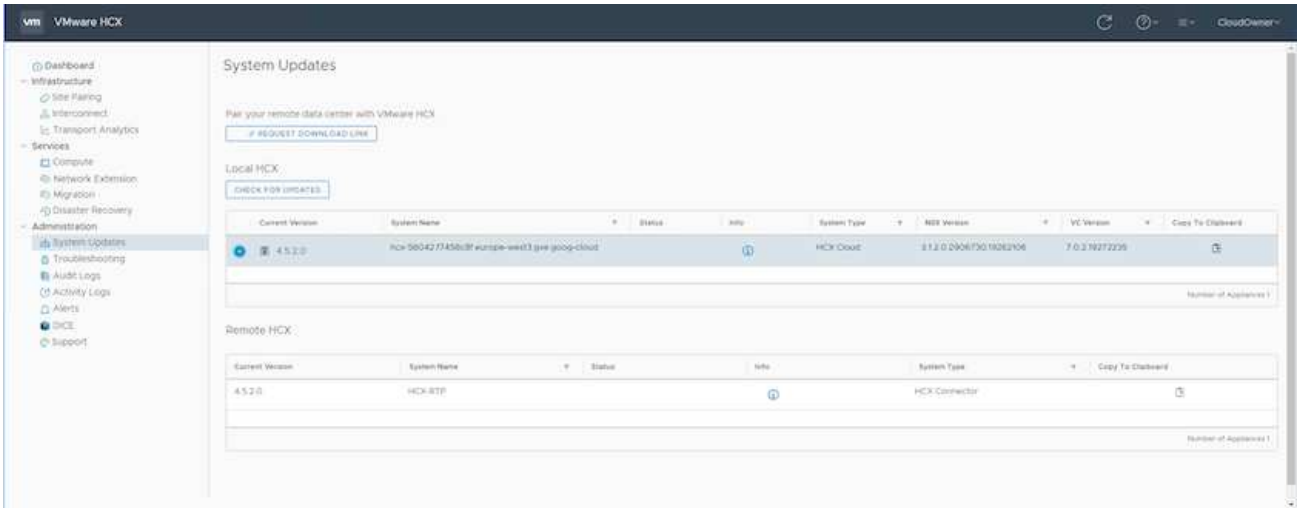
   Puede iniciar sesión en la consola HCX haciendo clic en el enlace de la versión HCX



   o haciendo clic en HCX FQDN en la pestaña Red de administración de vSphere.



2. En HCX Cloud Manager, vaya a **Administración > Actualizaciones del sistema**.
3. Haga clic en **Solicitar enlace de descarga** y descargue el archivo OVA.



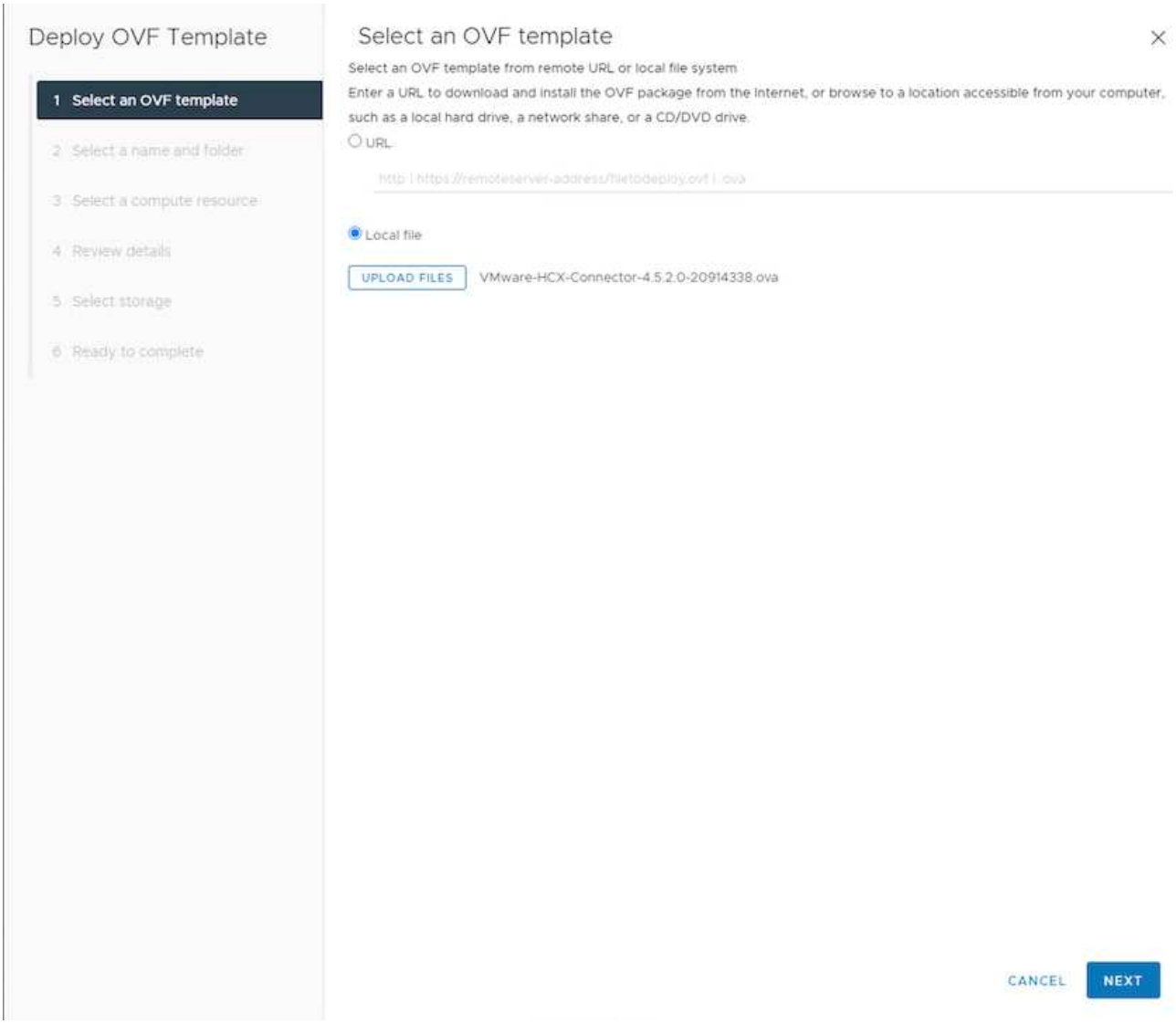
4. Actualice HCX Cloud Manager a la última versión disponible desde la interfaz de usuario de HCX Cloud Manager.

▼ **Paso 2: Implementar el instalador OVA en el servidor vCenter local**

Para que el conector local se conecte al HCX Manager en Google Cloud VMware Engine, asegúrese de que los puertos de firewall adecuados estén abiertos en el entorno local.

Para descargar e instalar HCX Connector en el vCenter Server local, complete los siguientes pasos:

1. Descargue el ova de la consola HCX en Google Cloud VMware Engine como se indica en el paso anterior.
2. Una vez descargado el OVA, impleméntelo en el entorno local de VMware vSphere utilizando la opción **Implementar plantilla OVF**.



3. Ingrese toda la información requerida para la implementación de OVA, haga clic en **Siguiente** y luego haga clic en **Finalizar** para implementar el OVA del conector VMware HCX.

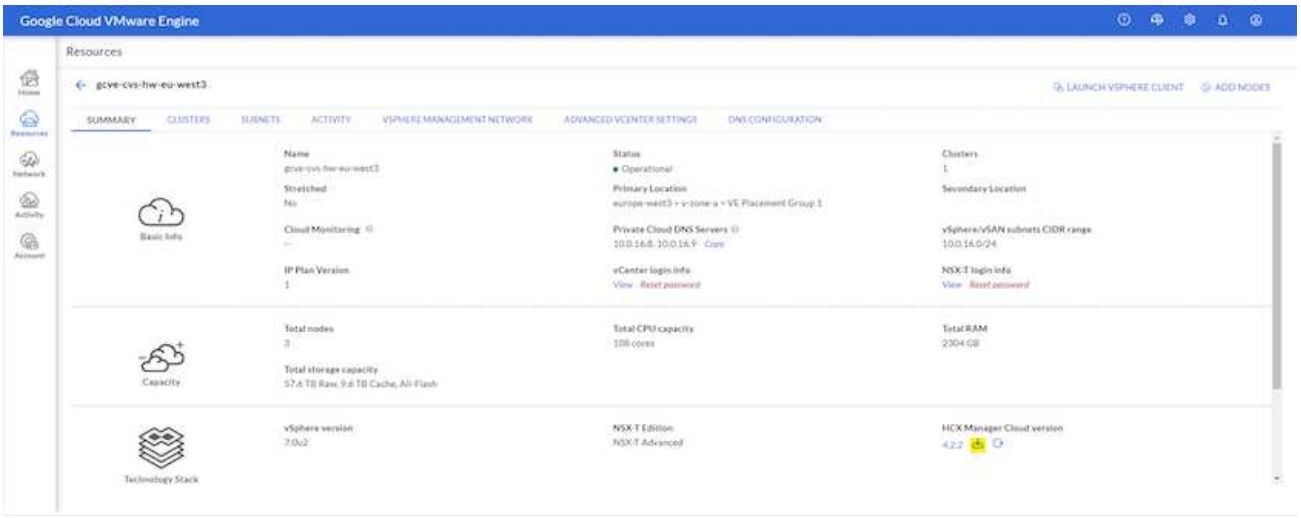
   Encienda el dispositivo virtual manualmente.

Para obtener instrucciones paso a paso, consulte la "Documentación de Google HCX" .

▼ **Paso 3: Activar el conector HCX con la clave de licencia**

Después de implementar VMware HCX Connector OVA en las instalaciones e iniciar el dispositivo, complete los siguientes pasos para activar HCX Connector. Genere la clave de licencia desde el portal de Google Cloud VMware Engine y actívela en VMware HCX Manager.

1. Desde el portal de VMware Engine, haga clic en Recursos, seleccione la nube privada y **haga clic en el ícono de descarga debajo de Versión de HCX Manager Cloud**.



Abra el archivo descargado y copie la cadena de clave de licencia.

2. Inicie sesión en VMware HCX Manager local en `"https://hcxmanagerIP:9443"` utilizando credenciales de administrador.

   Utilice la hcxmanagerIP y la contraseña definidas durante la implementación de OVA.

3. En la licencia, ingrese la clave copiada del paso 3 y haga clic en **Activar**.

   El conector HCX local debe tener acceso a Internet.

4. En **Ubicación del centro de datos**, proporcione la ubicación más cercana para instalar VMware HCX Manager en las instalaciones. Haga clic en **Continuar**.
5. En **Nombre del sistema**, actualice el nombre y haga clic en **Continuar**.
6. Haga clic en **Sí, continuar**.
7. En **Conectar su vCenter**, proporcione el nombre de dominio completo (FQDN) o la dirección IP de vCenter Server y las credenciales adecuadas y haga clic en **Continuar**.

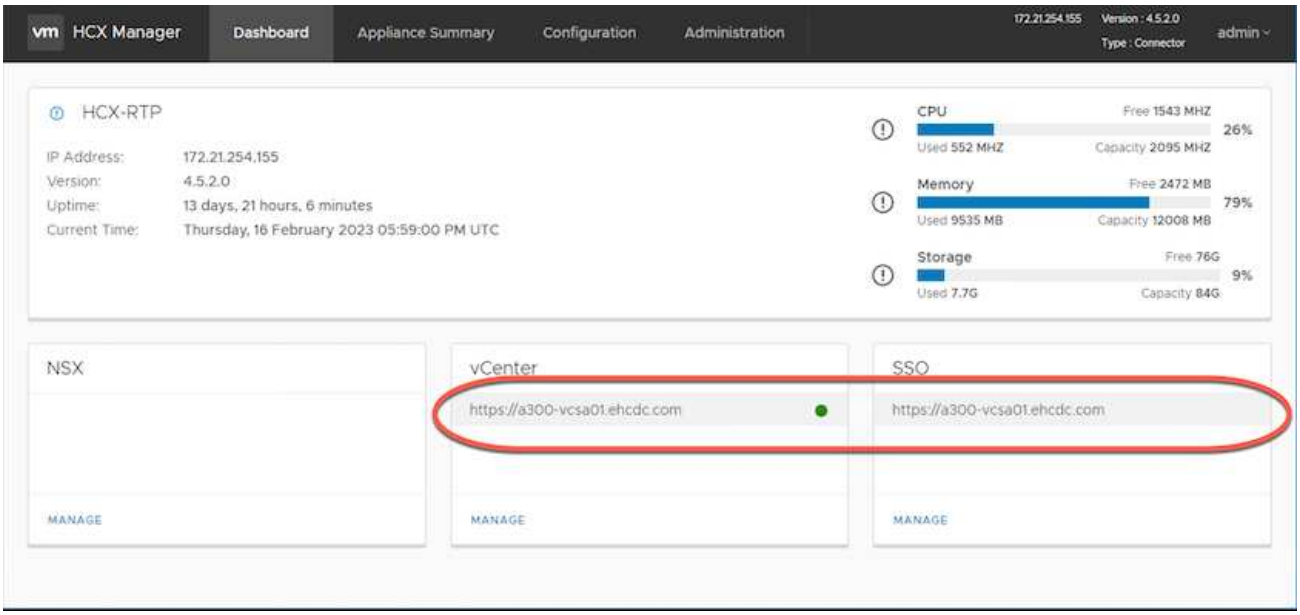
   Utilice el FQDN para evitar problemas de conectividad más adelante.

8. En **Configurar SSO/PSC**, proporcione el FQDN o la dirección IP del Controlador de servicios de plataforma (PSC) y haga clic en **Continuar**.

   Para PSC integrado, ingrese el FQDN o la dirección IP de VMware vCenter Server.

9. Verifique que la información ingresada sea correcta y haga clic en **Reiniciar**.
10. Después de reiniciar los servicios, vCenter Server se muestra en verde en la página que aparece. Tanto vCenter Server como SSO deben tener los parámetros de configuración adecuados, que deben ser los mismos que en la página anterior.

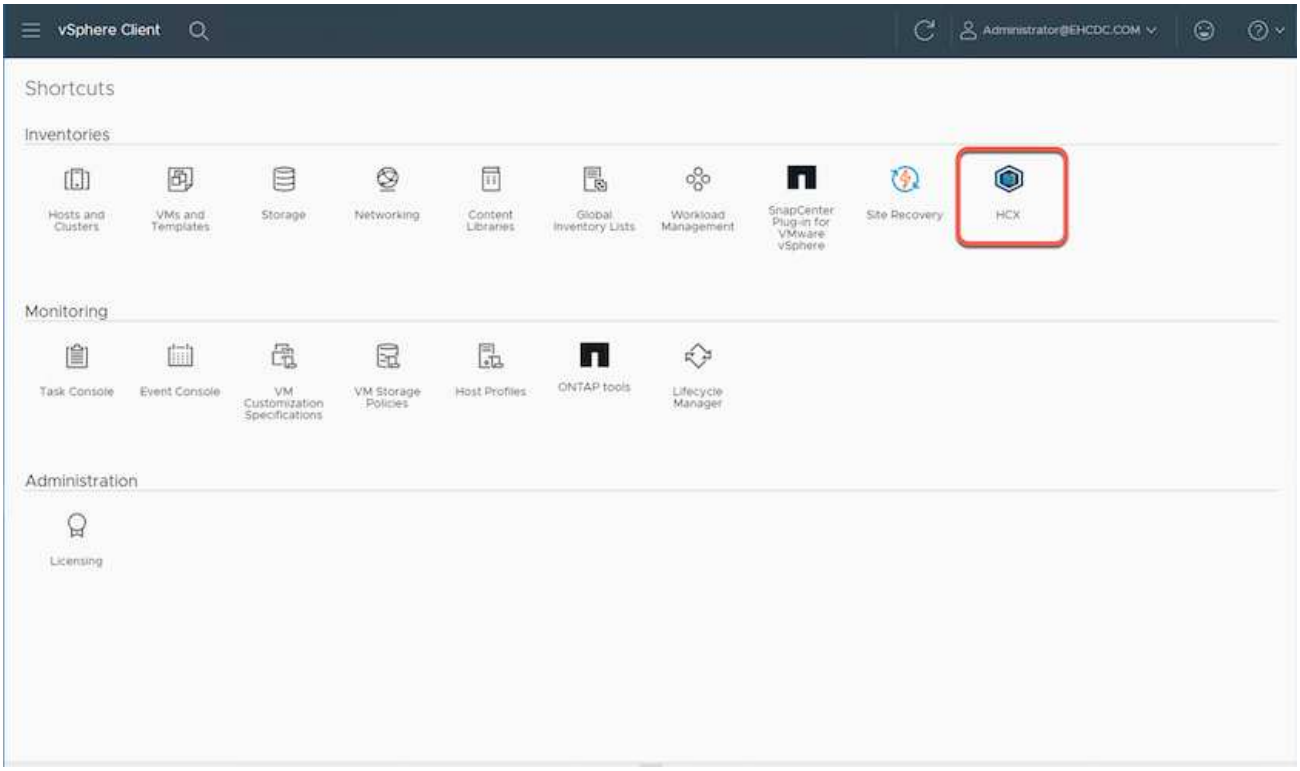
    Este proceso debería tardar aproximadamente entre 10 y 20 minutos para que el complemento se agregue al vCenter Server.



▼ **Paso 4: Vincular VMware HCX Connector local con Google Cloud VMware Engine HCX Cloud Manager**

Una vez implementado y configurado el conector HCX en el vCenter local, establezca la conexión con Cloud Manager agregando el emparejamiento. Para configurar el emparejamiento del sitio, complete los siguientes pasos:

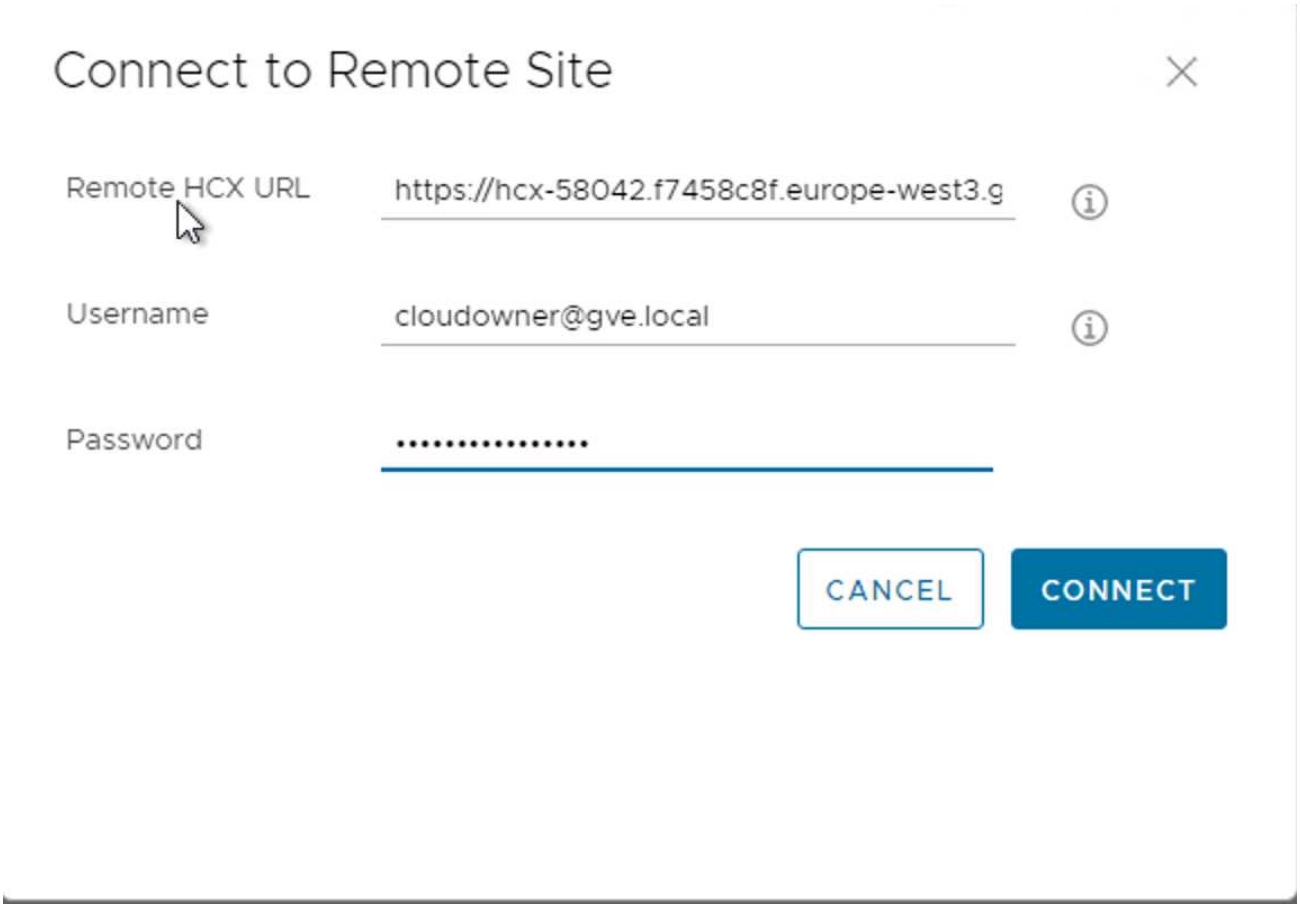
1. Para crear un par de sitios entre el entorno de vCenter local y Google Cloud VMware Engine SDDC, inicie sesión en el servidor vCenter local y acceda al nuevo complemento HCX vSphere Web Client.



2. En Infraestructura, haga clic en **Agregar un emparejamiento de sitios**.

Ingrese la URL o la dirección IP de Google Cloud VMware Engine HCX Cloud Manager y las credenciales del usuario con privilegios de rol de propietario de la nube para acceder

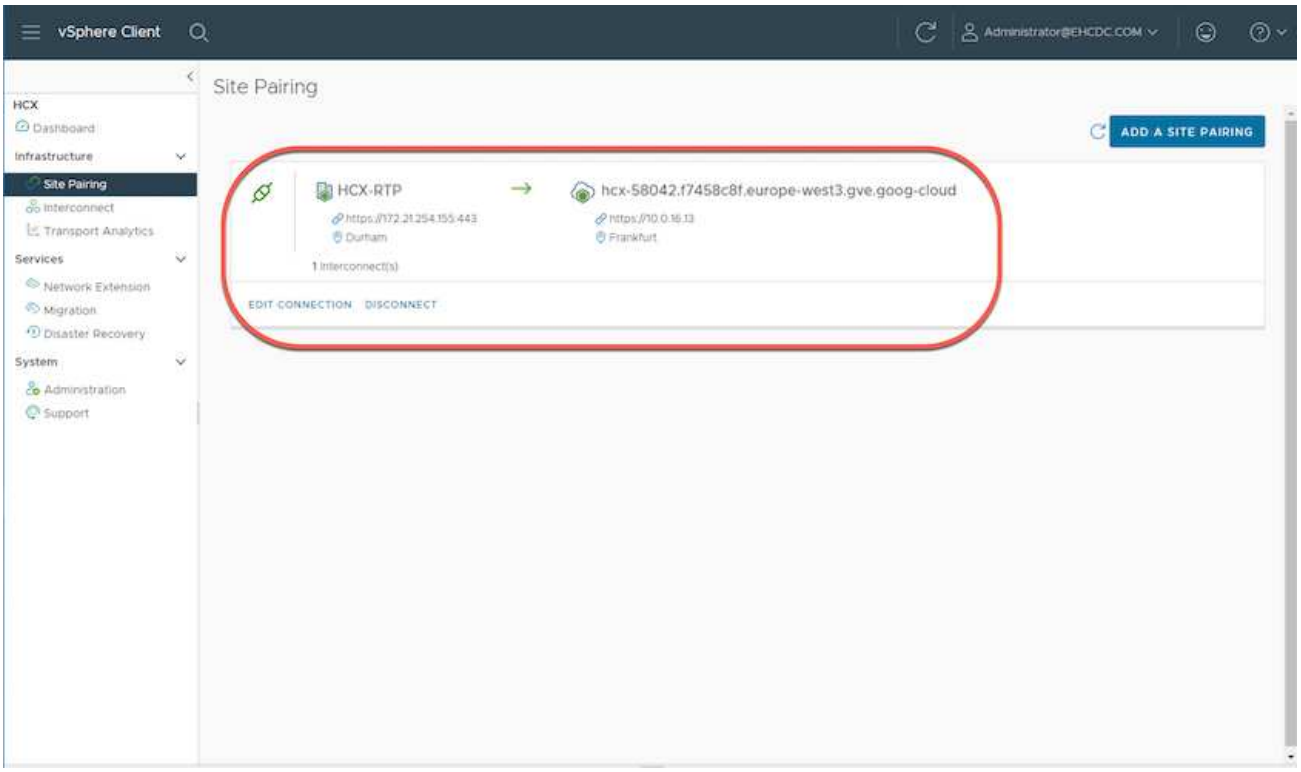
a la nube privada.



3. Haga clic en **Conectar**.

VMware HCX Connector debe poder enrutarse a la IP de HCX Cloud Manager a través del puerto 443.

4. Una vez creado el emparejamiento, el emparejamiento del sitio recién configurado estará disponible en el Panel de HCX.

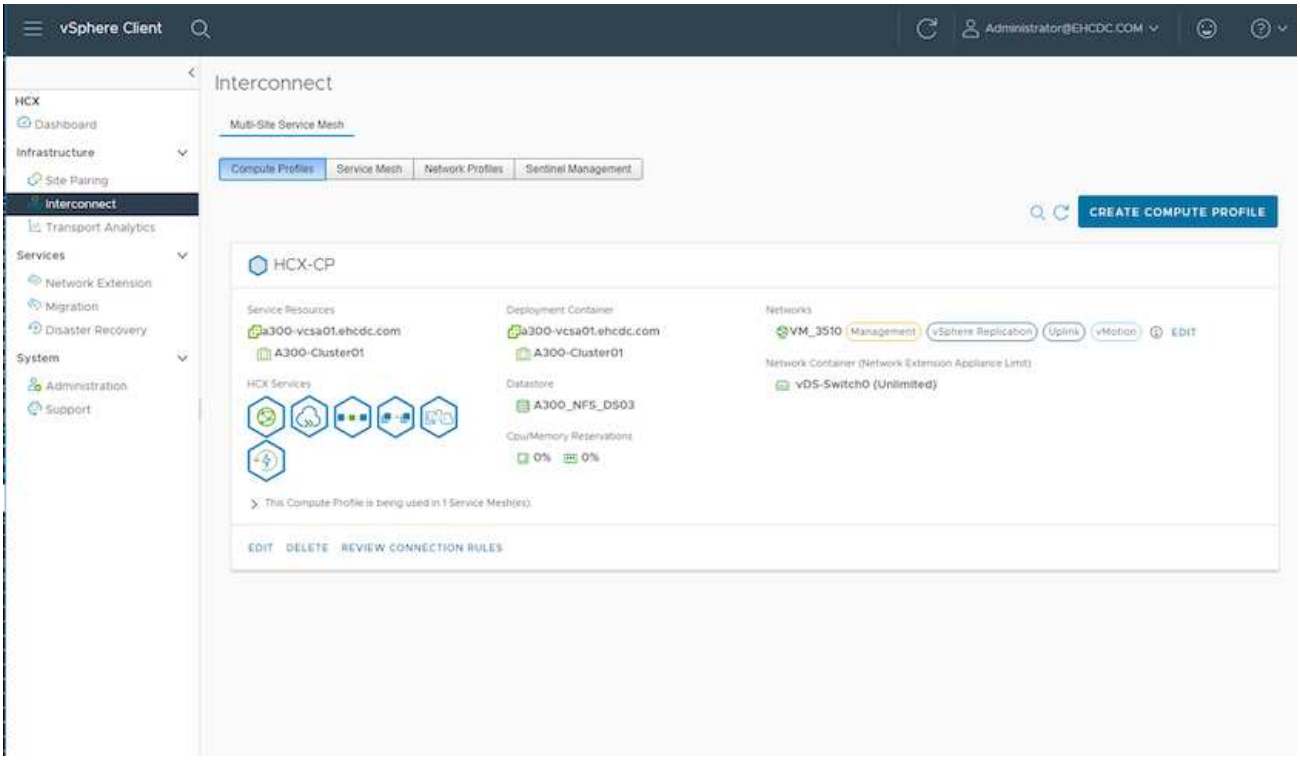


▼ **Paso 5: Configurar el perfil de red, el perfil de cómputo y la malla de servicio**

El dispositivo de servicio VMware HCX Interconnect proporciona capacidades de replicación y migración basadas en vMotion a través de Internet y conexiones privadas al sitio de destino. La interconexión proporciona cifrado, ingeniería de tráfico y movilidad de máquinas virtuales. Para crear un dispositivo de servicio de interconexión, complete los siguientes pasos:

1. En Infraestructura, seleccione **Interconexión > Malla de servicios multisitio > Perfiles de cómputo > Crear perfil de cómputo**.

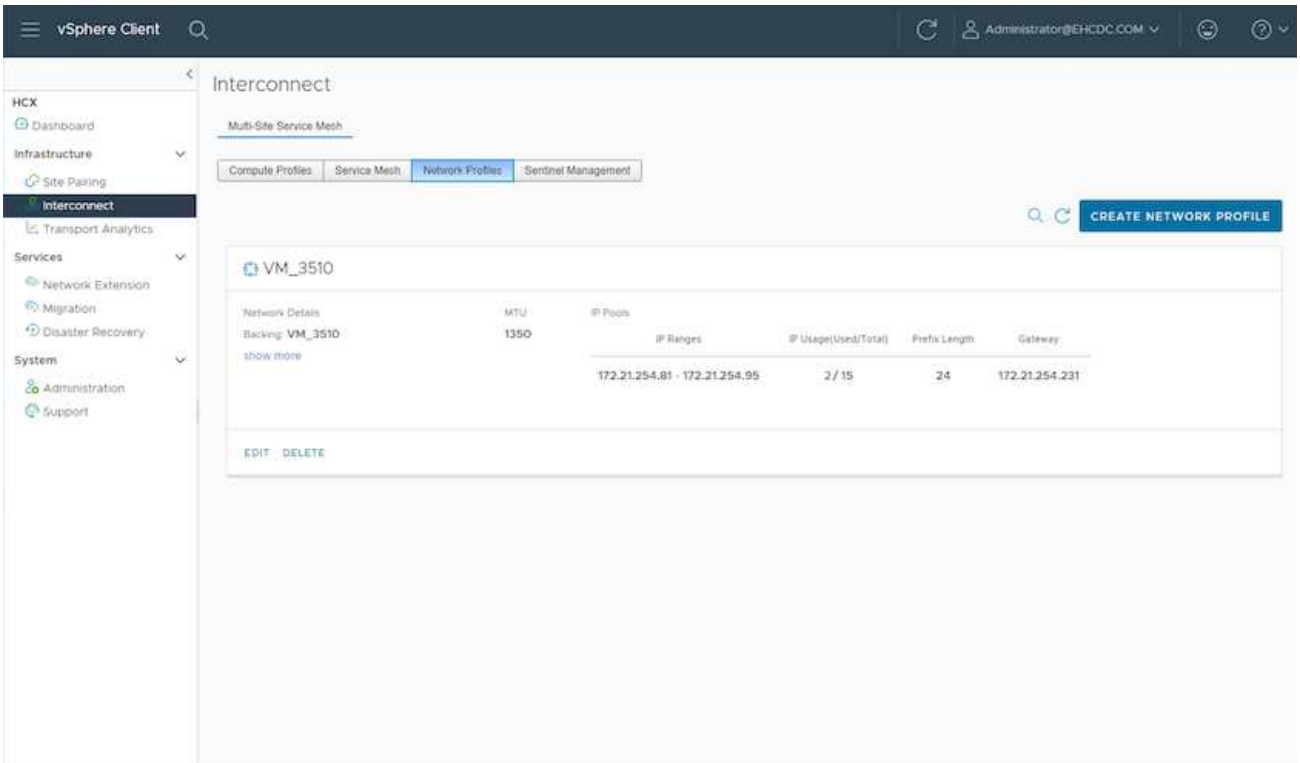
Los perfiles de cómputo definen los parámetros de implementación, incluidos los dispositivos que se implementan y qué parte del centro de datos de VMware es accesible para el servicio HCX.



2. Una vez creado el perfil de cómputo, cree los perfiles de red seleccionando **Multi-Site Service Mesh > Perfiles de red > Crear perfil de red**.

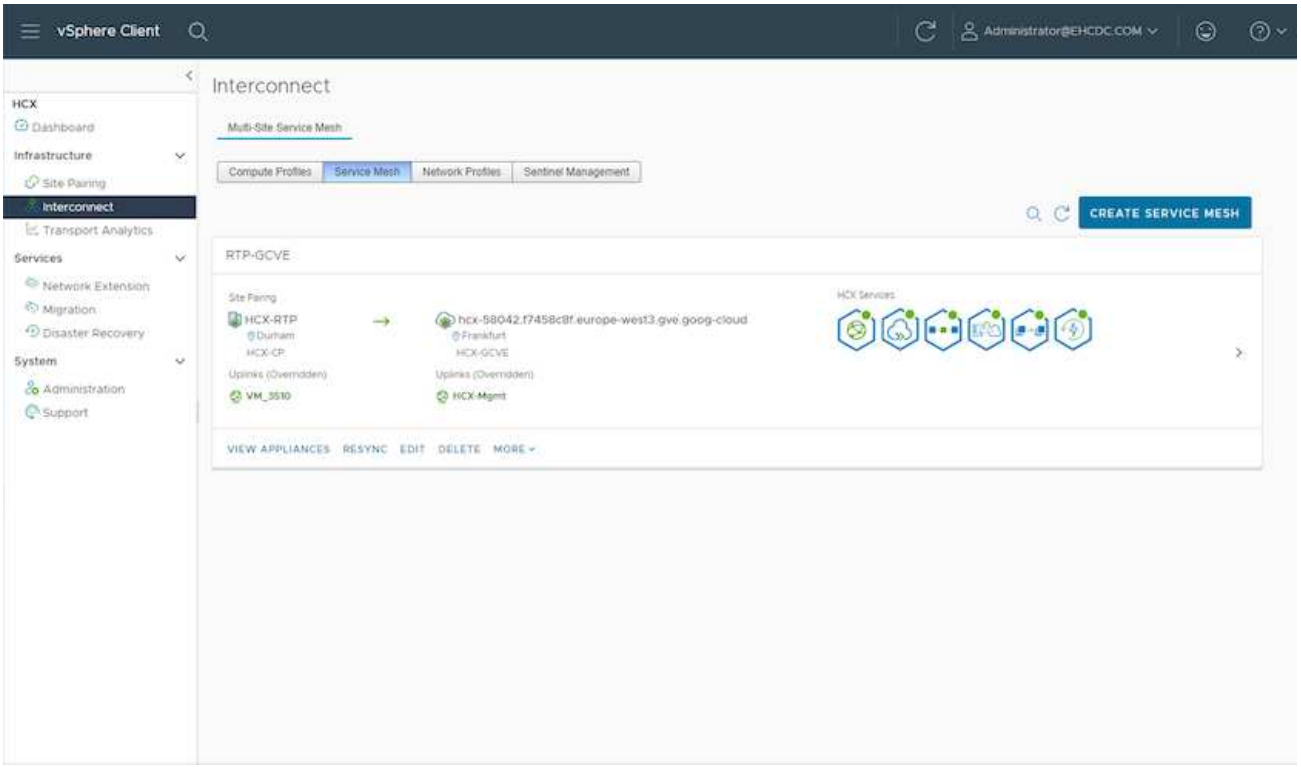
   El perfil de red define un rango de direcciones IP y redes que HCX utiliza para sus dispositivos virtuales.

   > Este paso requiere dos o más direcciones IP. Estas direcciones IP se asignan desde la red de administración a los dispositivos de interconexión.

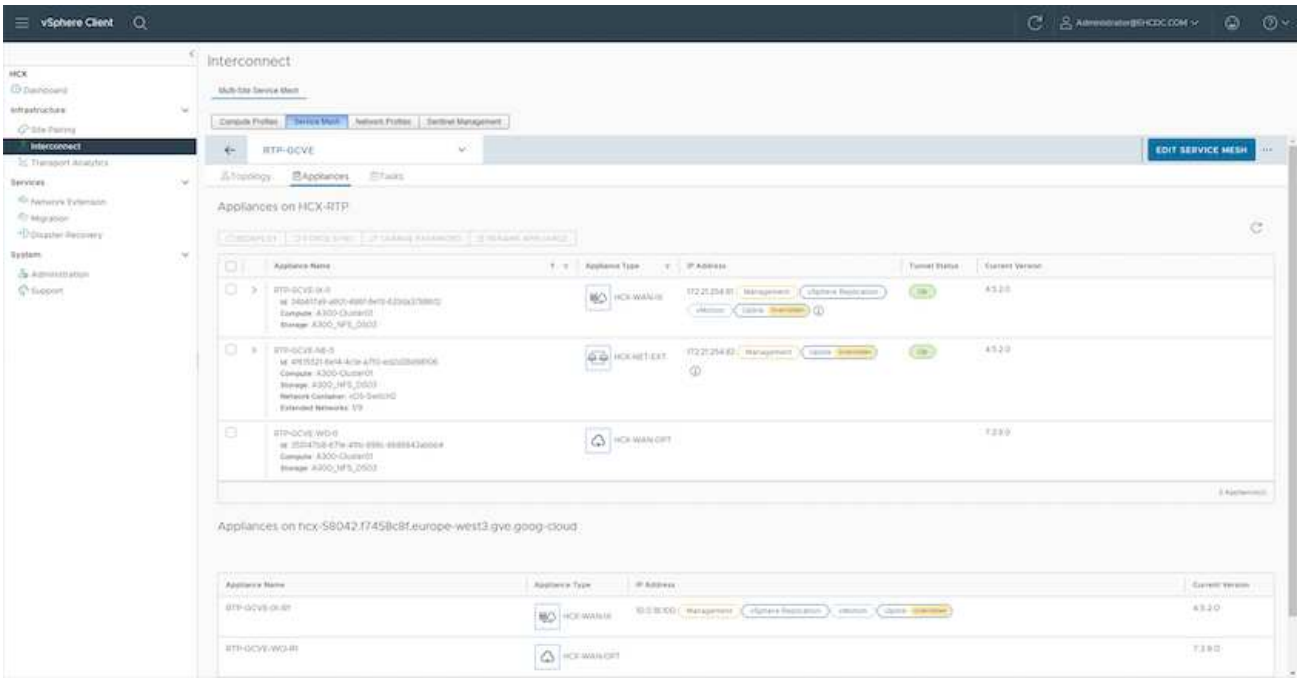


3. En este momento, los perfiles de cómputo y de red se han creado con éxito.
4. Cree la malla de servicio seleccionando la pestaña **Malla de servicio** dentro de la opción **Interconectar** y seleccione los sitios locales y GCVE SDDC.
5. Service Mesh especifica un par de perfiles de red y cómputo local y remoto.

> Como parte de este proceso, los dispositivos HCX se implementan y configuran automáticamente tanto en los sitios de origen como de destino para crear una estructura de transporte segura.



6. Este es el paso final de la configuración. Esto debería tomar cerca de 30 minutos para completar la implementación. Una vez configurada la malla de servicio, el entorno está listo con los túneles IPsec creados exitosamente para migrar las máquinas virtuales de carga de trabajo.



▼ **Paso 6: Migrar cargas de trabajo**

Las cargas de trabajo se pueden migrar de manera bidireccional entre los SDDC locales y de GCVE mediante diversas tecnologías de migración de VMware HCX. Las máquinas virtuales se pueden mover hacia y desde entidades activadas por VMware HCX mediante múltiples tecnologías de migración, como migración masiva de HCX, HCX vMotion, migración en frío de HCX, HCX Replication Assisted vMotion (disponible con la edición HCX Enterprise) y HCX OS Assisted Migration (disponible con la edición HCX Enterprise).

Para obtener más información sobre los distintos mecanismos de migración de HCX, consulte "Migración de máquinas virtuales VMware mediante la documentación de VMware HCX" .

El dispositivo HCX-IX utiliza el servicio Mobility Agent para realizar migraciones de vMotion, Cold y Replication Assisted vMotion (RAV).

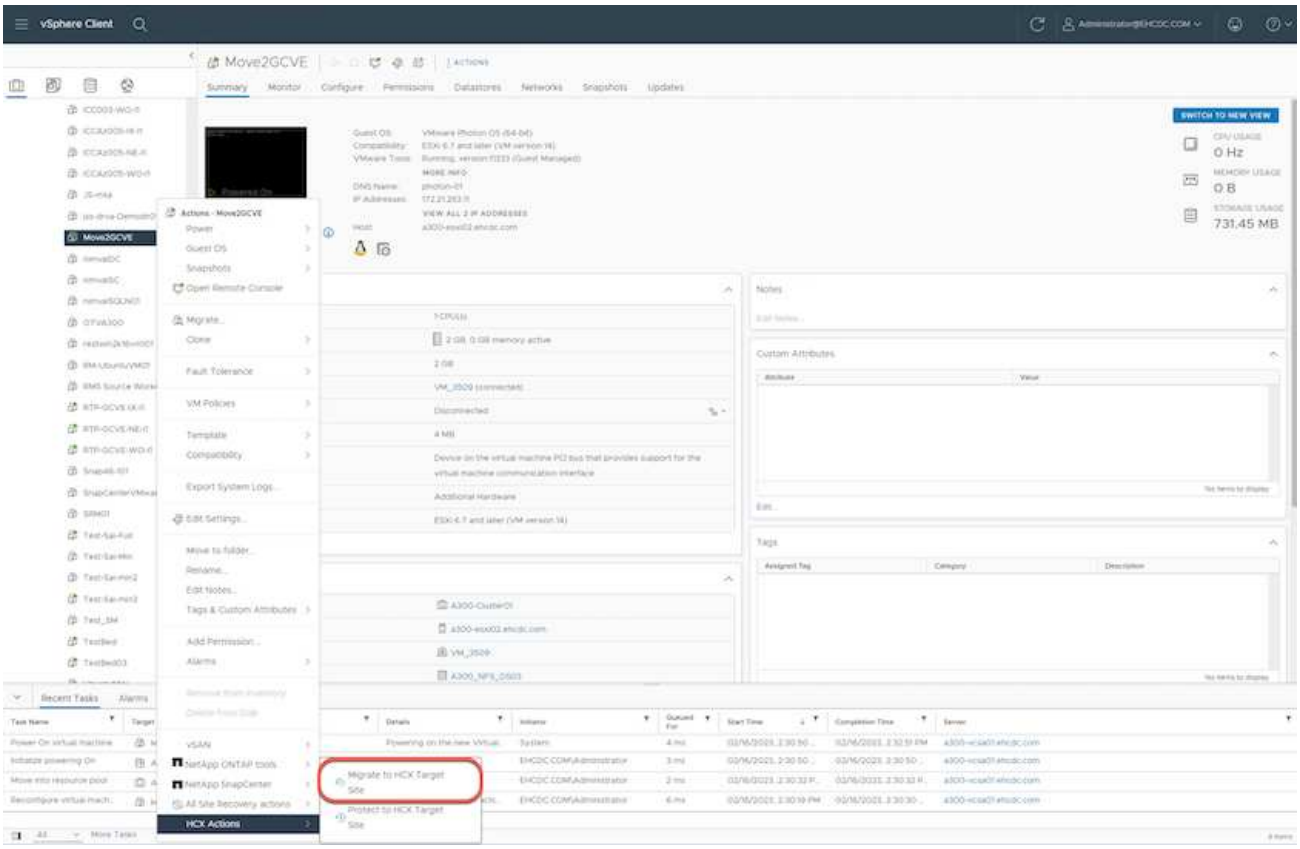
> ⓘ El dispositivo HCX-IX agrega el servicio Mobility Agent como un objeto host en vCenter Server. Los recursos de procesador, memoria, almacenamiento y red que se muestran en este objeto no representan el consumo real en el hipervisor físico que aloja el dispositivo IX.

HCX vMotion

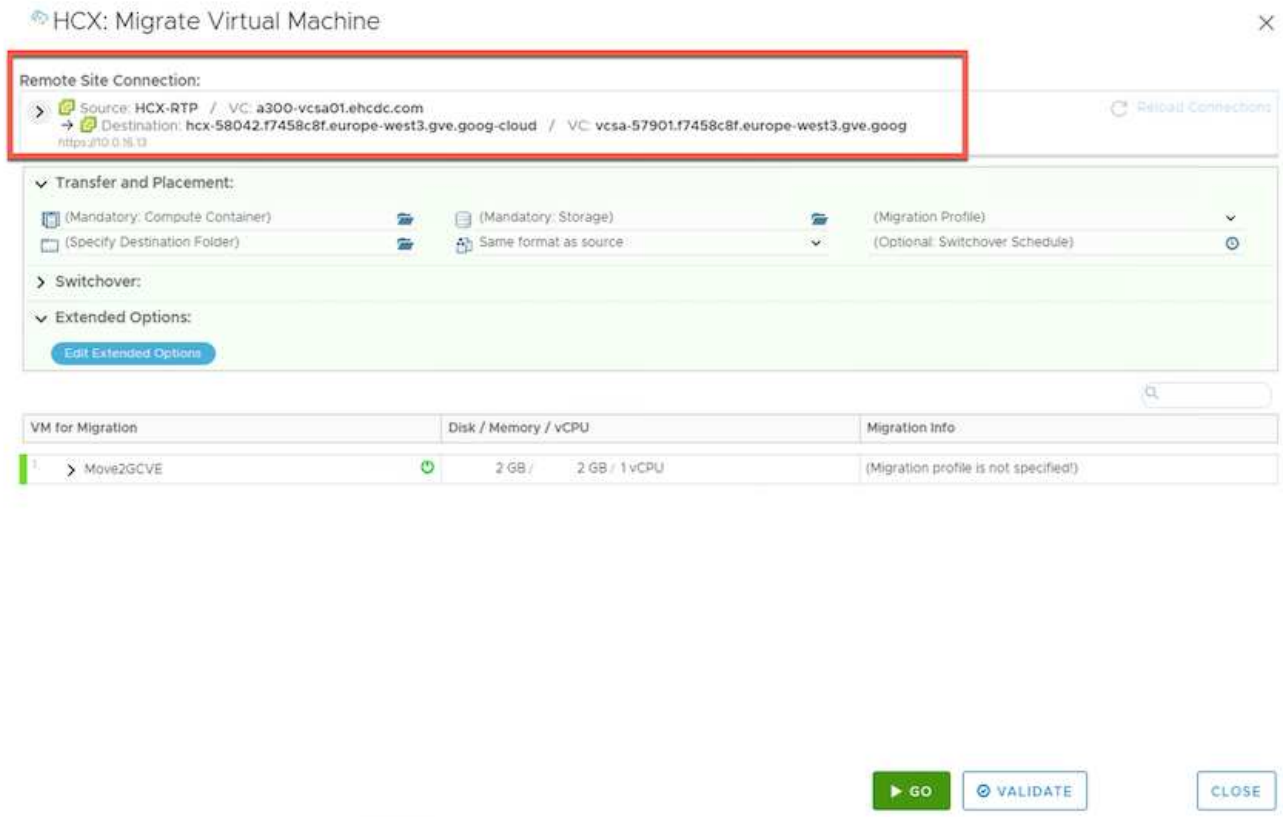
Esta sección describe el mecanismo HCX vMotion. Esta tecnología de migración utiliza el protocolo VMware vMotion para migrar una VM a GCVE. La opción de migración de vMotion se utiliza para migrar el estado de una sola máquina virtual a la vez. No hay interrupción del servicio durante este método de migración.

> ⓘ La extensión de red debe estar en su lugar (para el grupo de puertos en el que está conectada la VM) para poder migrar la VM sin la necesidad de realizar un cambio de dirección IP.

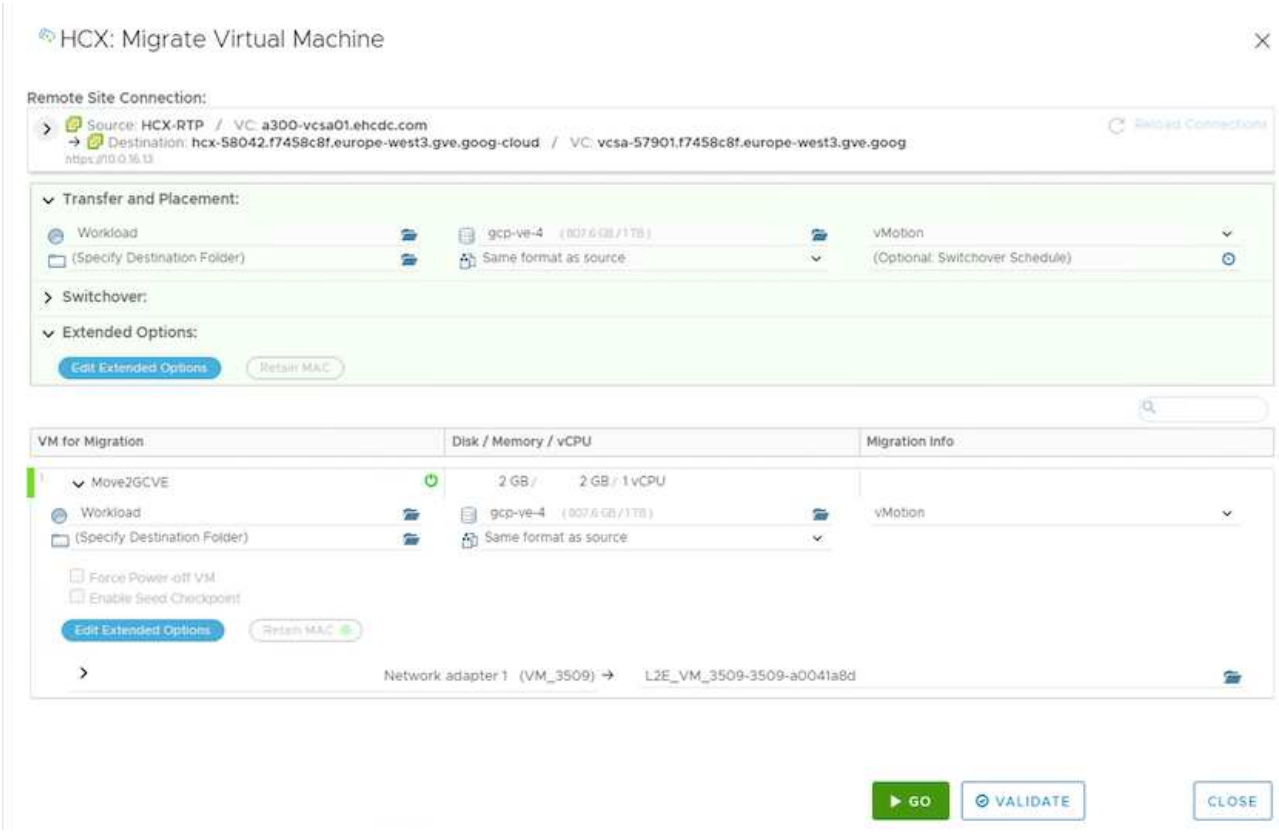
1. Desde el cliente vSphere local, vaya a Inventario, haga clic con el botón derecho en la VM que se migrará y seleccione Acciones HCX > Migrar al sitio de destino HCX.



2. En el asistente Migrar máquina virtual, seleccione la Conexión de sitio remoto (GCVE de destino).



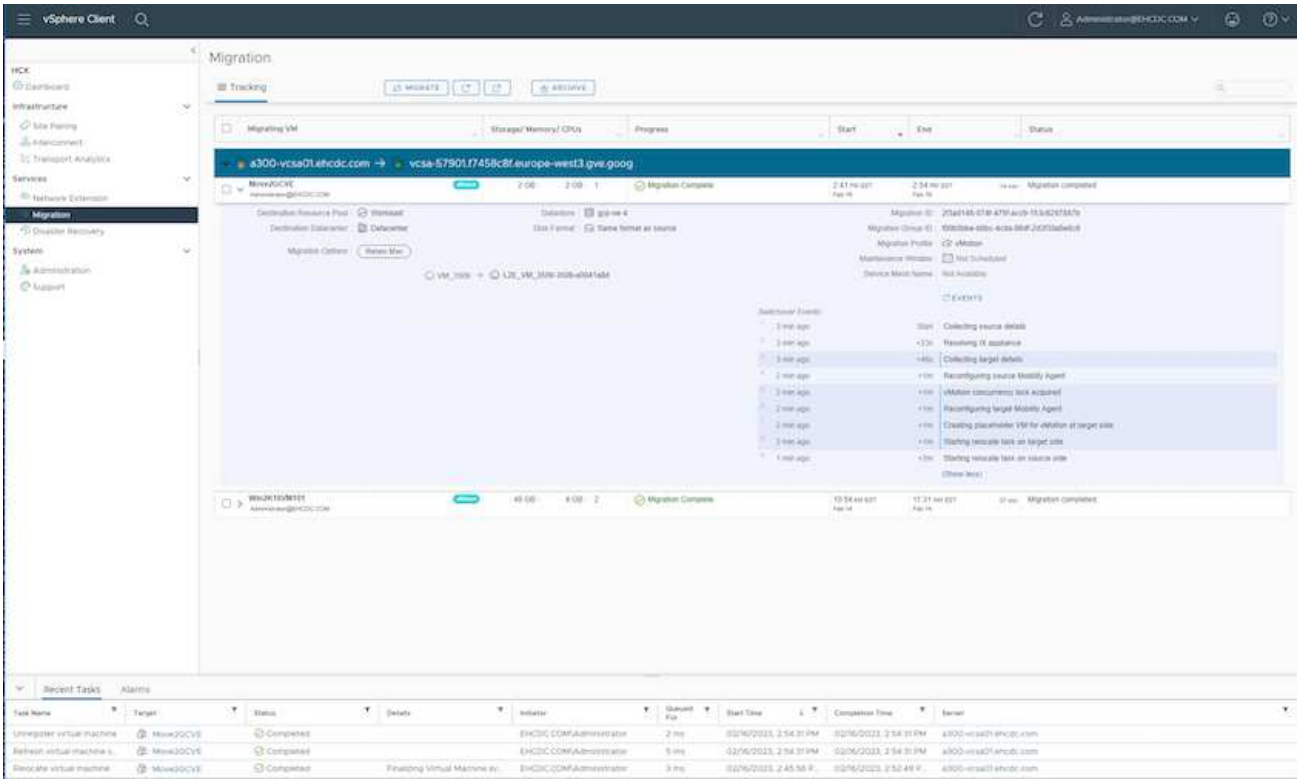
3. Actualice los campos obligatorios (Clúster, Almacenamiento y Red de destino), haga clic en Validar.



4. Una vez completadas las comprobaciones de validación, haga clic en Ir para iniciar la migración.

> La transferencia de vMotion captura la memoria activa de la VM, su estado de ejecución, su dirección IP y su dirección MAC. Para obtener más información sobre los requisitos y limitaciones de HCX vMotion, consulte "Comprensión de VMware HCX vMotion y la migración en frío" .

5. Puede supervisar el progreso y la finalización de vMotion desde el panel de HCX > Migración.



El almacén de datos NFS de destino de Google Cloud NetApp Volumes (NetApp Volumes) debe tener suficiente espacio para manejar la migración.

Conclusión

Ya sea que su objetivo sea una nube completa o una nube híbrida y datos que residen en cualquier tipo/proveedor de almacenamiento en las instalaciones, Cloud Volume Service y HCX brindan excelentes opciones para implementar y migrar las cargas de trabajo de las aplicaciones al mismo tiempo que reducen el TCO al hacer que los requisitos de los datos se integren perfectamente con la capa de aplicación. Cualquiera que sea el caso de uso, elija Google Cloud VMware Engine junto con Cloud Volume Service para obtener rápidamente los beneficios de la nube, una infraestructura y operaciones consistentes en las instalaciones y en múltiples nubes, portabilidad bidireccional de cargas de trabajo y capacidad y rendimiento de nivel empresarial. Es el mismo proceso y los mismos procedimientos familiares que se utilizan para conectar el almacenamiento y migrar máquinas virtuales mediante VMware vSphere Replication, VMware vMotion o incluso la copia de archivos de red (NFC).

Comida para llevar

Los puntos clave de este documento incluyen:

- Ahora puede utilizar Cloud Volume Service como almacén de datos en Google Cloud VMware Engine SDDC.
- Puede migrar datos fácilmente desde las instalaciones locales al almacén de datos de Cloud Volume Service.
- Puede ampliar y reducir fácilmente el almacén de datos de Cloud Volume Service para satisfacer los requisitos de capacidad y rendimiento durante la actividad de migración.

Vídeos de Google y VMware como referencia

▼ **De Google**

- "Implementar el conector HCX con GCVE"
- "Configurar HCX ServiceMesh con GCVE"
- "Migrar VM con HCX a GCVE"

▼ **De VMware**

- "Implementación del conector HCX para GCVE"
- "Configuración de HCX ServiceMesh para GCVE"
- "Migración de la carga de trabajo de HCX a GCVE"

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes enlaces de sitios web:

- Documentación de Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Documentación del servicio de volumen en la nube

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Guía del usuario de VMware HCX

  "https://docs.vmware.com/en/VMware-HCX/index.html"

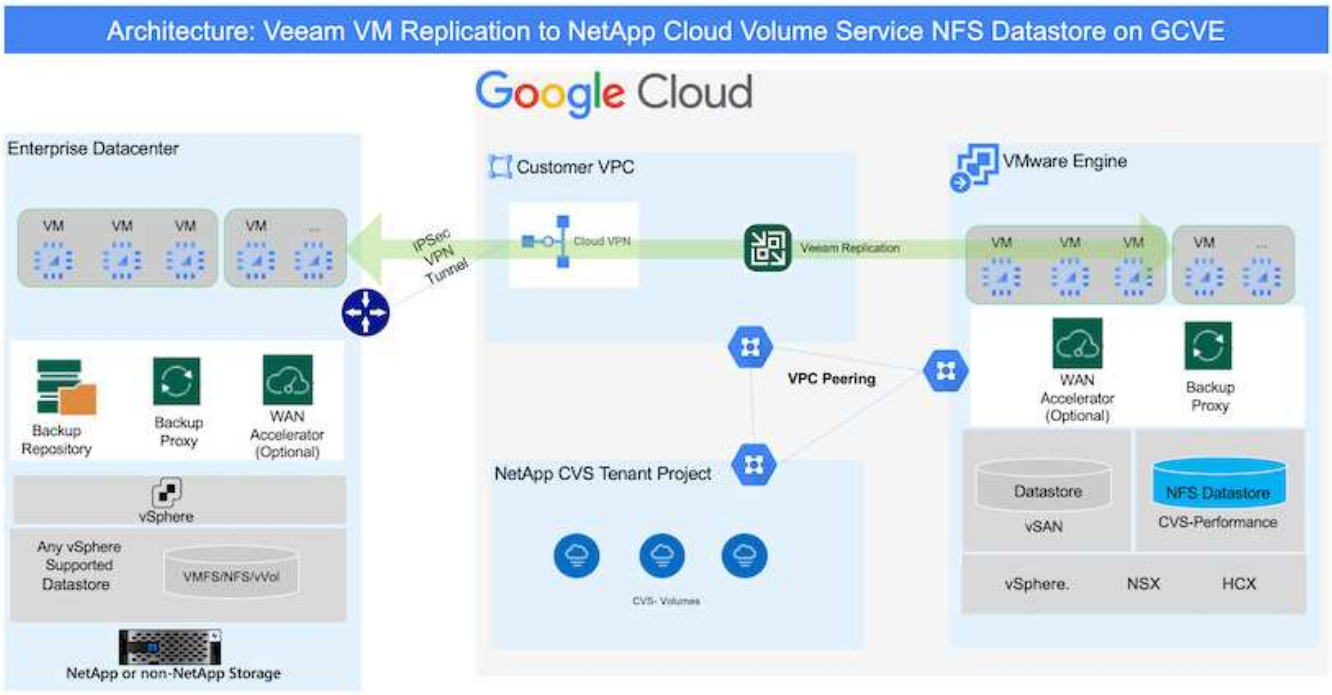
Migración de máquinas virtuales al almacén de datos NFS de Google Cloud NetApp Volumes en Google Cloud VMware Engine mediante la función de replicación de Veeam

Los clientes que actualmente utilizan Veeam para sus necesidades de protección de datos continúan usando esa solución para migrar las cargas de trabajo a GCVE y disfrutar de los beneficios de los almacenes de datos NFS de Google Cloud NetApp Volumes .

Descripción general

Las cargas de trabajo de VM que se ejecutan en VMware vSphere se pueden migrar a Google Cloud VMware Engine (GCVE) mediante la función de replicación de Veeam.

Este documento proporciona un enfoque paso a paso para configurar y realizar la migración de máquinas virtuales que utilizan Google Cloud NetApp Volumes, Veeam y Google Cloud VMware Engine (GCVE).



Suposiciones

Este documento asume que tiene Google Cloud VPN o Cloud Interconnect u otra opción de red establecida para establecer la conectividad de red desde servidores vSphere existentes a Google Cloud VMware Engine.

> Existen múltiples opciones para conectar centros de datos locales a Google Cloud, lo que nos impide delinear un flujo de trabajo específico en este documento. Consulte la"Documentación de Google Cloud" para el método de conectividad local a Google adecuado.

Implementación de la solución de migración

Descripción general de la implementación de la solución

1. Asegúrese de que el almacén de datos NFS de Google Cloud NetApp Volumes esté montado en GCVE vCenter.
2. Asegúrese de que Veeam Backup Recovery esté implementado en el entorno VMware vSphere existente
3. Cree un trabajo de replicación para comenzar a replicar máquinas virtuales en la instancia de Google Cloud VMware Engine.
4. Realizar conmutación por error del trabajo de replicación de Veeam.
5. Realizar conmutación por error permanente en Veeam.

Detalles de la implementación

Asegúrese de que el almacén de datos NFS de Google Cloud NetApp Volumes esté montado en GCVE vCenter

Inicie sesión en GCVE vCenter y asegúrese de que haya disponible un almacén de datos NFS con espacio suficiente. En caso contrario, consulte"Montar volúmenes NetApp como almacén de datos NFS en GCVE"

Asegúrese de que Veeam Backup Recovery esté implementado en el entorno VMware vSphere existente

Por favor refiérase"Componentes de replicación de Veeam" Documentación para instalar los componentes necesarios.

Cree un trabajo de replicación para comenzar a replicar máquinas virtuales en la instancia de Google Cloud VMware Engine.

Tanto el vCenter local como el vCenter GCVE deben registrarse en Veeam. "Configurar el trabajo de replicación de máquinas virtuales de vSphere" Aquí hay un vídeo que explica cómo"Configurar trabajo de replicación" .

> La máquina virtual réplica puede tener una IP diferente a la de la máquina virtual de origen y también puede estar conectada a un grupo de puertos diferente. Para más detalles, consulte el vídeo de arriba.

Realizar conmutación por error del trabajo de replicación de Veeam

Para migrar máquinas virtuales, realice"Realizar conmutación por error"

Realizar conmutación por error permanente en Veeam.

Para tratar a GCVE como su nuevo entorno de origen, realice"Conmutación por error permanente"

Beneficios de esta solución

- La infraestructura de respaldo de Veeam existente se puede utilizar para la migración.
- Veeam Replication permite cambiar las direcciones IP de las máquinas virtuales en el sitio de destino.
- Permite reasignar datos existentes replicados fuera de Veeam (como datos replicados desde el sistema NetApp)
- Tiene la capacidad de especificar diferentes grupos de puertos de red en el sitio de destino.
- Puede especificar el orden en que se encenderán las máquinas virtuales.
- Utiliza VMware Change Block Tracking para minimizar la cantidad de datos que se envían a través de la WAN.
- Capacidad de ejecutar scripts previos y posteriores para la replicación.
- Capacidad de ejecutar scripts previos y posteriores a las instantáneas.

Proteja sus datos con Google Cloud NetApp Volumes en Google Cloud

TR-4918: Descripción general de seguridad - Google Cloud NetApp Volumes en Google Cloud

Oliver Krause, Justin Parisi, NetApp

La seguridad, especialmente en la nube, donde la infraestructura está fuera del control de los administradores de almacenamiento, es fundamental para poder confiar tus datos a los servicios que ofrecen los proveedores de la nube. Este documento ofrece una visión general de las soluciones de seguridad que ofrece "Google Cloud NetApp Volumes se proporciona en Google Cloud".

Público objetivo

El público al que va dirigido este documento incluye, entre otros, los siguientes roles:

- Proveedores de nube
- administradores de almacenamiento
- Arquitectos de almacenamiento
- Recursos de campo
- tomadores de decisiones empresariales

Si tiene preguntas sobre el contenido de este informe técnico, consulte la sección"Contáctanos."

Abreviatura	Definición
Volúmenes NetApp -SW	Google Cloud NetApp Volumes, tipo de servicio Volúmenes NetApp
Volúmenes NetApp - Rendimiento	Servicio de volumen en la nube, tipo de servicio NetApp Volumes-Rendimiento
Anuncio de servicio público	

Cómo Google Cloud NetApp Volumes en Google Cloud protege tus datos

Google Cloud NetApp Volumes en Google Cloud ofrece una multitud de formas de proteger sus datos de forma nativa.

Arquitectura segura y modelo de arrendamiento

Google Cloud NetApp Volumes proporciona una arquitectura segura en Google Cloud al segmentar la administración de servicios (plano de control) y el acceso a los datos (plano de datos) en diferentes puntos finales para que ninguno pueda afectar al otro (consulte la sección"Arquitectura de Google Cloud NetApp Volumes"). Utiliza Google "acceso a servicios privados" (PSA) marco para proporcionar el servicio. Este marco distingue entre el productor de servicios, que es proporcionado y operado por NetApp, y el consumidor de servicios, que es una nube privada virtual (VPC) en un proyecto de cliente, que aloja a los clientes que desean acceder a los recursos compartidos de archivos de Google Cloud NetApp Volumes .

En esta arquitectura, los inquilinos (ver la sección"Modelo de arrendamiento") se definen como proyectos de Google Cloud que están completamente aislados entre sí a menos que el usuario los conecte explícitamente. Los inquilinos permiten el aislamiento completo de los volúmenes de datos, los servicios de nombres externos y otras piezas esenciales de la solución de otros inquilinos mediante la plataforma de volúmenes Google Cloud NetApp Volumes . Debido a que la plataforma Google Cloud NetApp Volumes está conectada a través del emparejamiento de VPC, ese aislamiento también se aplica a ella. Puede habilitar el uso compartido de volúmenes de Google Cloud NetApp Volumes entre varios proyectos mediante una VPC compartida (consulte la sección"VPC compartidas"). Puede aplicar controles de acceso a recursos compartidos SMB y exportaciones NFS para limitar quién o qué puede ver o modificar conjuntos de datos.

Gestión de identidad sólida para el plano de control

En el plano de control donde se lleva a cabo la configuración de Google Cloud NetApp Volumes , la administración de identidades se realiza mediante "Gestión de acceso a la identidad (IAM)" . IAM es un servicio estándar que le permite controlar la autenticación (inicios de sesión) y la autorización (permisos) para las instancias de proyectos de Google Cloud. Toda la configuración se realiza con las API de Google Cloud NetApp Volumes a través de un transporte HTTPS seguro utilizando cifrado TLS 1.2, y la autenticación se

realiza mediante tokens JWT para mayor seguridad. La interfaz de usuario de la consola de Google para Google Cloud NetApp Volumes traduce la entrada del usuario en llamadas a la API de Google Cloud NetApp Volumes .

Fortalecimiento de la seguridad: limitación de las superficies de ataque

Parte de una seguridad eficaz es limitar la cantidad de superficies de ataque disponibles en un servicio. Las superficies de ataque pueden incluir una variedad de cosas, incluidos datos en reposo, transferencias en vuelo, inicios de sesión y los conjuntos de datos en sí.

Un servicio administrado elimina algunas de las superficies de ataque inherentes a su diseño. Gestión de infraestructura, tal y como se describe en la sección"Operación de servicio," es manejado por un equipo dedicado y está automatizado para reducir la cantidad de veces que un humano toca las configuraciones, lo que ayuda a reducir la cantidad de errores intencionales y no intencionales. La red está protegida para que sólo los servicios necesarios puedan acceder entre sí. El cifrado está integrado en el almacenamiento de datos y solo el plano de datos necesita atención de seguridad por parte de los administradores de Google Cloud NetApp Volumes . Al ocultar la mayor parte de la gestión detrás de una interfaz API, se logra seguridad limitando las superficies de ataque.

Modelo de confianza cero

Históricamente, la filosofía de seguridad de TI ha sido confiar pero verificar, y se ha manifestado en confiar únicamente en mecanismos externos (como firewalls y sistemas de detección de intrusiones) para mitigar las amenazas. Sin embargo, los ataques y las brechas han evolucionado para eludir la verificación en entornos a través de phishing, ingeniería social, amenazas internas y otros métodos que proporcionan la verificación para ingresar a las redes y causar estragos.

Zero Trust se ha convertido en una nueva metodología en seguridad, cuyo mantra actual es "no confiar en nada y al mismo tiempo verificarlo todo". Por lo tanto, no se permite el acceso a nada por defecto. Este mantra se aplica de diversas maneras, incluidos los firewalls estándar y los sistemas de detección de intrusiones (IDS) y también con los siguientes métodos:

- Métodos de autenticación fuertes (como tokens JWT o Kerberos cifrados con AES)
- Fuentes únicas y sólidas de identidades (como Windows Active Directory, Protocolo ligero de acceso a directorios (LDAP) y Google IAM)
- Segmentación de red y multitenencia segura (solo los inquilinos tienen acceso permitido de forma predeterminada)
- Controles de acceso granulares con políticas de acceso con privilegios mínimos
- Pequeñas listas exclusivas de administradores dedicados y confiables con auditoría digital y registros en papel

Los Google Cloud NetApp Volumes que se ejecutan en Google Cloud se adhieren al modelo Zero Trust al implementar la postura de "no confiar en nada, verificar todo".

Cifrado

Cifrar datos en reposo (ver la sección"Cifrado de datos en reposo") mediante cifrados XTS-AES-256 con NetApp Volume Encryption (NVE) y en tránsito con"Cifrado SMB" o soporte NFS Kerberos 5p. Quédese tranquilo sabiendo que las transferencias de replicación entre regiones están protegidas por encriptación TLS 1.2 (consulte el enlace de la sección:gcp-gcnv-security-considerations.html#Detección, prevención y mitigación de ransomware, malware y virus#cross-region-replication["Replicación entre regiones"]). Además, la red de Google también proporciona comunicaciones cifradas (consulte la sección"Cifrado de datos en tránsito") para una capa adicional de protección contra ataques. Para obtener más información sobre el cifrado de

transporte, consulte la sección"Red de Google Cloud" .

Protección de datos y copias de seguridad

La seguridad no se trata sólo de la prevención de ataques. También se trata de cómo nos recuperamos de los ataques si ocurren. Esta estrategia incluye protección de datos y copias de seguridad. Google Cloud NetApp Volumes proporciona métodos para replicar a otras regiones en caso de interrupciones (consulte la sección"Replicación entre regiones") o si un conjunto de datos se ve afectado por un ataque de ransomware. También puede realizar copias de seguridad asincrónicas de datos en ubicaciones fuera de la instancia de Google Cloud NetApp Volumes mediante"Copia de seguridad de Google Cloud NetApp Volumes" . Con copias de seguridad periódicas, la mitigación de eventos de seguridad puede llevar menos tiempo y ahorrar dinero y angustia a los administradores.

Mitigación rápida de ransomware con copias Snapshot líderes en la industria

Además de la protección de datos y las copias de seguridad, Google Cloud NetApp Volumes proporciona soporte para copias Snapshot inmutables (consulte la sección"Copias de instantáneas inmutables") de volúmenes que permiten la recuperación de ataques de ransomware (consulte la sección"Operación del servicio") en cuestión de segundos después de descubrir el problema y con una interrupción mínima. El tiempo de recuperación y los efectos dependen de la programación de la instantánea, pero puede crear copias de instantáneas que proporcionen deltas de tan solo una hora en ataques de ransomware. Las copias instantáneas tienen un efecto insignificante en el rendimiento y el uso de la capacidad y son un enfoque de bajo riesgo y alta recompensa para proteger sus conjuntos de datos.

Consideraciones de seguridad y superficies de ataque

El primer paso para comprender cómo proteger sus datos es identificar los riesgos y las posibles superficies de ataque.

Estos incluyen (pero no se limitan a) lo siguiente:

- Administración e inicios de sesión
- Datos en reposo
- Datos en vuelo
- Redes y cortafuegos
- Ransomware, malware y virus

Comprender las superficies de ataque puede ayudarle a proteger mejor sus entornos. Google Cloud NetApp Volumes en Google Cloud ya considera muchos de estos temas e implementa la funcionalidad de seguridad de forma predeterminada, sin ninguna interacción administrativa.

Garantizar inicios de sesión seguros

Al proteger los componentes de su infraestructura crítica, es fundamental asegurarse de que solo los usuarios aprobados puedan iniciar sesión y administrar sus entornos. Si los actores maliciosos violan sus credenciales administrativas, entonces tienen las llaves del castillo y pueden hacer lo que quieran: cambiar configuraciones, eliminar volúmenes y copias de seguridad, crear puertas traseras o deshabilitar las programaciones de instantáneas.

Google Cloud NetApp Volumes para Google Cloud brinda protección contra inicios de sesión administrativos no autorizados a través de la ofuscación del almacenamiento como servicio (StaaS). El proveedor de la nube mantiene completamente Google Cloud NetApp Volumes, sin posibilidad de iniciar sesión externamente. Todas las operaciones de instalación y configuración están completamente automatizadas, por lo que un

administrador humano nunca tiene que interactuar con los sistemas excepto en circunstancias muy raras.

Si se requiere iniciar sesión, Google Cloud NetApp Volumes en Google Cloud protege los inicios de sesión al mantener una lista muy corta de administradores confiables que tienen acceso para iniciar sesión en los sistemas. Este control ayuda a reducir la cantidad de posibles actores maliciosos con acceso. Además, la red de Google Cloud oculta los sistemas detrás de capas de seguridad de red y expone solo lo necesario al mundo exterior. Para obtener información sobre la arquitectura de Google Cloud, Google Cloud NetApp Volumes , consulte la sección"Arquitectura de Google Cloud NetApp Volumes ."

Administración y actualizaciones de clústeres

Dos áreas con posibles riesgos de seguridad incluyen la administración del clúster (qué sucede si un actor malicioso tiene acceso de administrador) y las actualizaciones (qué sucede si se compromete una imagen de software).

Protección de la administración del almacenamiento

El almacenamiento proporcionado como servicio elimina el riesgo adicional de exposición para los administradores al quitar ese acceso a los usuarios finales fuera del centro de datos en la nube. En cambio, la única configuración realizada es la del plano de acceso a datos por parte de los clientes. Cada inquilino administra sus propios volúmenes y ningún inquilino puede acceder a otras instancias de Google Cloud NetApp Volumes . El servicio se gestiona de forma automatizada, con una lista muy pequeña de administradores de confianza a los que se les da acceso a los sistemas a través de los procesos cubiertos en la sección"Operación del servicio."

El tipo de servicio NetApp Volumes-Performance ofrece replicación entre regiones como una opción para brindar protección de datos a una región diferente en caso de una falla en una región. En esos casos, es posible conmutar los Google Cloud NetApp Volumes a la región no afectada para mantener el acceso a los datos.

Actualizaciones de servicio

Las actualizaciones ayudan a proteger los sistemas vulnerables. Cada actualización proporciona mejoras de seguridad y correcciones de errores que minimizan las superficies de ataque. Las actualizaciones de software se descargan desde repositorios centralizados y se validan antes de permitir las actualizaciones para verificar que se utilicen imágenes oficiales y que las actualizaciones no estén comprometidas por actores maliciosos.

Con Google Cloud NetApp Volumes, las actualizaciones son manejadas por los equipos del proveedor de la nube, lo que elimina la exposición al riesgo para los equipos de administradores al proporcionar expertos con experiencia en configuración y actualizaciones que han automatizado y probado completamente el proceso. Las actualizaciones no generan interrupciones y Google Cloud NetApp Volumes mantiene las últimas actualizaciones para obtener mejores resultados generales.

Para obtener información sobre el equipo de administradores que realiza estas actualizaciones de servicio, consulte la sección"Operación del servicio."

Protección de datos en reposo

El cifrado de datos en reposo es importante para proteger datos confidenciales en caso de que un disco sea robado, devuelto o reutilizado. Los datos en Google Cloud NetApp Volumes están protegidos en reposo mediante cifrado basado en software.

- Las claves generadas por Google se utilizan para NetApp Volumes-SW.
- Para NetApp Volumes-Performance, las claves por volumen se almacenan en un administrador de claves

integrado en Google Cloud NetApp Volumes, que utiliza NetApp ONTAP CryptoMod para generar claves de cifrado AES-256. CryptoMod figura en la lista de módulos validados FIPS 140-2 CMVP. Ver "Certificado FIPS 140-2 n.° 4144" .

A partir de noviembre de 2021, la versión preliminar de la funcionalidad de cifrado administrado por el cliente (CMEK) estuvo disponible para NetApp Volumes-Performance. Esta funcionalidad le permite cifrar las claves por volumen con claves maestras por proyecto y por región alojadas en Google Key Management Service (KMS). KMS le permite conectar administradores de claves externos.

Para obtener más información sobre cómo configurar KMS para NetApp Volumes-Performance, consulta "Consulte la documentación de Google Cloud NetApp Volumes".

Para más información sobre arquitectura, consulte la sección"Arquitectura de Google Cloud NetApp Volumes ."

Protección de datos durante el vuelo

Además de proteger los datos en reposo, también debe poder proteger los datos cuando están en tránsito entre la instancia de Google Cloud NetApp Volumes y un cliente o destino de replicación. Google Cloud NetApp Volumes proporciona cifrado para datos en tránsito a través de protocolos NAS mediante métodos de cifrado como el cifrado SMB con Kerberos, la firma/sellado de paquetes y NFS Kerberos 5p para el cifrado de extremo a extremo de las transferencias de datos.

La replicación de volúmenes de Google Cloud NetApp Volumes utiliza TLS 1.2, que aprovecha los métodos de cifrado AES-GCM.

La mayoría de los protocolos en vuelo inseguros, como Telnet, NDMP, etc., están deshabilitados de forma predeterminada. Sin embargo, el DNS no está cifrado por Google Cloud NetApp Volumes (no es compatible con DNS Sec) y debe cifrarse mediante cifrado de red externa cuando sea posible. Ver la sección"Cifrado de datos en tránsito" para obtener más información sobre cómo proteger los datos durante el vuelo.

Para obtener información sobre el cifrado del protocolo NAS, consulte la sección"Protocolos NAS."

Usuarios y grupos para permisos NAS

Parte de la seguridad de sus datos en la nube implica una autenticación adecuada de usuarios y grupos, donde los usuarios que acceden a los datos se verifican como usuarios reales en el entorno y los grupos contienen usuarios válidos. Estos usuarios y grupos proporcionan acceso inicial para compartir y exportar, así como validación de permisos para archivos y carpetas en el sistema de almacenamiento.

Google Cloud NetApp Volumes utiliza autenticación de usuarios y grupos de Windows basada en Active Directory estándar para recursos compartidos SMB y permisos de estilo Windows. El servicio también puede aprovechar proveedores de identidad UNIX como LDAP para usuarios y grupos UNIX para exportaciones NFS, validación de ID NFSv4, autenticación Kerberos y ACL NFSv4.



Actualmente, solo Active Directory LDAP es compatible con Google Cloud NetApp Volumes para la funcionalidad LDAP.

Detección, prevención y mitigación de ransomware, malware y virus

El ransomware, el malware y los virus son una amenaza persistente para los administradores, y la detección, prevención y mitigación de esas amenazas siempre son una prioridad para las organizaciones empresariales. Un solo evento de ransomware en un conjunto de datos crítico puede costar potencialmente millones de dólares, por lo que es beneficioso hacer lo que pueda para minimizar el riesgo.

Aunque Google Cloud NetApp Volumes actualmente no incluye medidas nativas de detección o prevención, como protección antivirus o "detección automática de ransomware", hay formas de recuperarte rápidamente de un ataque de ransomware al habilitar programaciones periódicas de Snapshot. Las copias de Snapshot son punteros inmutables y de solo lectura a los bloques modificados del sistema de archivos, son casi instantáneas, tienen un impacto mínimo en el rendimiento y solo ocupan espacio cuando los datos se modifican o eliminan. Puedes establecer programaciones para las copias de Snapshot que se ajusten a tu objetivo de punto de recuperación (RPO) y objetivo de tiempo de recuperación (RTO) aceptables, y puedes conservar hasta 1,024 copias de Snapshot por volumen.

El soporte de instantáneas se incluye sin costo adicional (más allá de los cargos de almacenamiento de datos por bloques modificados/datos retenidos por copias de instantáneas) con Google Cloud NetApp Volumes y, en el caso de un ataque de ransomware, se puede usar para volver a una copia de instantánea anterior a que ocurriera el ataque. Las restauraciones de instantáneas demoran solo unos segundos en completarse y luego puede volver a servir datos de manera normal. Para obtener más información, consulte "La solución de NetApp para ransomware" .

Para evitar que el ransomware afecte a su empresa se necesita un enfoque de varios niveles que incluya uno o más de los siguientes:

- Protección de puntos finales
- Protección contra amenazas externas mediante firewalls de red
- Detección de anomalías en los datos
- Múltiples copias de seguridad (en el sitio y fuera del sitio) de conjuntos de datos críticos
- Pruebas de restauración periódicas de las copias de seguridad
- Copias de Snapshot de NetApp inmutables de solo lectura
- Autenticación multifactor para infraestructura crítica
- Auditorías de seguridad de los inicios de sesión del sistema

Esta lista está lejos de ser exhaustiva, pero es un buen modelo a seguir cuando se enfrenta el riesgo de ataques de ransomware. Los Google Cloud NetApp Volumes en Google Cloud ofrecen varias formas de protegerse contra eventos de ransomware y reducir sus efectos.

Copias de instantáneas inmutables

Google Cloud NetApp Volumes proporciona de forma nativa copias instantáneas de solo lectura inmutables que se toman según un cronograma personalizable para una rápida recuperación en un momento determinado en caso de eliminación de datos o si un volumen completo ha sido víctima de un ataque de ransomware. Las restauraciones de instantáneas a copias de instantáneas anteriores en buen estado son rápidas y minimizan la pérdida de datos según el período de retención de sus programas de instantáneas y RTO/RPO. El efecto sobre el rendimiento con la tecnología Snapshot es insignificante.

Debido a que las copias instantáneas en los Google Cloud NetApp Volumes son de solo lectura, no pueden infectarse con ransomware a menos que este haya proliferado en el conjunto de datos sin que nadie se dé cuenta y se hayan tomado copias instantáneas de los datos infectados por ransomware. Es por esto que también debes considerar la detección de ransomware basada en anomalías de datos. Google Cloud NetApp Volumes actualmente no proporciona detección de forma nativa, pero puedes usar un software de monitoreo externo.

Copias de seguridad y restauraciones

Google Cloud NetApp Volumes proporciona capacidades de respaldo de cliente NAS estándar (como

respaldos mediante NFS o SMB).

- NetApp Volumes-Performance ofrece replicación de volúmenes entre regiones a otros volúmenes de NetApp Volumes-Performance. Para obtener más información, consulta "replicación de volumen" en la documentación de Google Cloud NetApp Volumes.
- NetApp Volumes-SW ofrece funciones de copia de seguridad y restauración de volúmenes integradas en el servicio. Para obtener más información, consulta "copia de seguridad en la nube" en la documentación de Google Cloud NetApp Volumes.

La replicación de volumen proporciona una copia exacta del volumen de origen para una conmutación por error rápida en caso de desastre, incluidos eventos de ransomware.

Replicación entre regiones

NetApp Volumes-Performance le permite replicar volúmenes de forma segura en las regiones de Google Cloud para casos de uso de archivo y protección de datos mediante el uso de cifrado TLS1.2 AES 256 GCM en una red de servicio de backend controlada por NetApp mediante interfaces específicas utilizadas para la replicación que se ejecuta en la red de Google. Un volumen primario (de origen) contiene los datos de producción activos y se replica en un volumen secundario (de destino) para proporcionar una réplica exacta del conjunto de datos primario.

La replicación inicial transfiere todos los bloques, pero las actualizaciones solo transmiten los bloques modificados en un volumen primario. Por ejemplo, si una base de datos de 1 TB que reside en un volumen principal se replica al volumen secundario, se transfiere 1 TB de espacio en la replicación inicial. Si esa base de datos tiene unos cientos de filas (hipotéticamente, unos pocos MB) que cambian entre la inicialización y la siguiente actualización, solo los bloques con las filas modificadas se replican en la secundaria (unos pocos MB). Esto ayuda a garantizar que los tiempos de transferencia se mantengan bajos y mantiene bajos los costos de replicación.

Todos los permisos sobre archivos y carpetas se replican en el volumen secundario, pero los permisos de acceso a recursos compartidos (como políticas y reglas de exportación o recursos compartidos SMB y ACL de recursos compartidos) se deben gestionar por separado. En el caso de una conmutación por error del sitio, el sitio de destino debe aprovechar los mismos servicios de nombre y conexiones de dominio de Active Directory para proporcionar un manejo consistente de las identidades y permisos de usuarios y grupos. Puede utilizar un volumen secundario como destino de conmutación por error en caso de desastre rompiendo la relación de replicación, lo que convierte el volumen secundario en lectura y escritura.

Las réplicas de volumen son de solo lectura, lo que proporciona una copia inmutable de los datos fuera del sitio para una rápida recuperación de datos en casos en los que un virus ha infectado los datos o un ransomware ha cifrado el conjunto de datos principal. Los datos de solo lectura no se cifrarán, pero, si el volumen principal se ve afectado y se produce una replicación, los bloques infectados también se replican. Puede usar copias de Snapshot más antiguas, no afectadas, para recuperarse, pero los SLA pueden quedar fuera del alcance del RTO/RPO prometido dependiendo de qué tan rápido se detecte un ataque.

Además, puedes evitar acciones administrativas malintencionadas, como la eliminación de volúmenes, la eliminación de Snapshot o los cambios en la planificación de SnapVault, mediante la gestión de la replicación entre regiones (CRR) en Google Cloud. Esto se hace creando roles personalizados que separan a los administradores de volúmenes, que pueden eliminar volúmenes de origen pero no romper las réplicas espejo y, por lo tanto, no pueden eliminar volúmenes de destino, de los administradores de CRR, que no pueden realizar ninguna operación de volumen. Consulta "Consideraciones de seguridad" en la documentación de Google Cloud NetApp Volumes los permisos permitidos para cada grupo de administradores.

Copia de seguridad de Google Cloud NetApp Volumes

Si bien Google Cloud NetApp Volumes proporciona una alta durabilidad de los datos, los eventos externos pueden provocar la pérdida de datos. En el caso de un evento de seguridad, como un virus o ransomware, las copias de seguridad y las restauraciones se vuelven fundamentales para reanudar el acceso a los datos de manera oportuna. Un administrador podría eliminar accidentalmente un volumen de Google Cloud NetApp Volumes . O bien los usuarios simplemente desean conservar versiones de respaldo de sus datos durante muchos meses y mantener el espacio de copia Snapshot adicional dentro del volumen se convierte en un desafío económico. Si bien las copias instantáneas deberían ser la forma preferida de conservar versiones de respaldo de las últimas semanas para restaurar los datos perdidos, estas permanecen dentro del volumen y se pierden si este desaparece.

Por todas estas razones, Google Cloud NetApp Volumes ofrece servicios de copia de seguridad a través de "Copia de seguridad de Google Cloud NetApp Volumes".

La copia de seguridad de Google Cloud NetApp Volumes genera una copia del volumen en Google Cloud Storage (GCS). Solo realiza una copia de seguridad de los datos reales almacenados dentro del volumen, no del espacio libre. Funciona de forma incremental para siempre, lo que significa que transfiere el contenido del volumen una vez y desde allí continúa realizando copias de seguridad únicamente de los datos modificados. En comparación con los conceptos de copia de seguridad clásicos con múltiples copias de seguridad completas, ahorra grandes cantidades de almacenamiento de copia de seguridad, lo que reduce los costos. Debido a que el precio mensual del espacio de respaldo es menor en comparación con un volumen, es un lugar ideal para mantener versiones de respaldo por más tiempo.

Los usuarios pueden usar una copia de seguridad de Google Cloud NetApp Volumes para restaurar cualquier versión de copia de seguridad en el mismo volumen o en uno diferente dentro de la misma región. Si se elimina el volumen de origen, los datos de respaldo se conservan y deben administrarse (por ejemplo, eliminarse) de forma independiente.

Google Cloud NetApp Volumes backup está integrado en Google Cloud NetApp Volumes como opción. Puedes decidir qué volúmenes proteger activando Google Cloud NetApp Volumes backup para cada volumen. Consulta la "Documentación de copia de seguridad de Google Cloud NetApp Volumes" para obtener información sobre las copias de seguridad, la "Número máximo de versiones de copia de seguridad admitidas", la programación y "precios".

Todos los datos de respaldo de un proyecto se almacenan dentro de un depósito GCS, que es administrado por el servicio y no es visible para el usuario. Cada proyecto utiliza un contenedor diferente. Actualmente, los depósitos están en la misma región que los volúmenes de Google Cloud NetApp Volumes , pero se están discutiendo más opciones. Consulte la documentación para conocer el estado más reciente.

El transporte de datos desde un depósito de Google Cloud NetApp Volumes a GCS utiliza redes internas del servicio de Google con HTTPS y TLS1.2. Los datos se cifran en reposo con claves administradas por Google.

Para gestionar las copias de seguridad de Google Cloud NetApp Volumes (crear, eliminar y restaurar copias de seguridad), debes tener el rol de "roles/netapp.admin".

Descripción general

Parte de confiar en una solución en la nube es comprender la arquitectura y cómo está protegida. En esta sección se destacan diferentes aspectos de la arquitectura de Google Cloud NetApp Volumes en Google para ayudar a aliviar posibles inquietudes sobre cómo se protegen los datos, así como también para señalar áreas en las que podrían requerirse pasos de configuración adicionales para obtener la implementación más segura.

La arquitectura general de Google Cloud NetApp Volumes se puede dividir en dos componentes principales: el plano de control y el plano de datos.

Plano de control

El plano de control en Google Cloud NetApp Volumes es la infraestructura de backend administrada por los administradores de Google Cloud NetApp Volumes y el software de automatización nativo de NetApp . Este plano es completamente transparente para los usuarios finales e incluye redes, hardware de almacenamiento, actualizaciones de software, etc., para ayudar a brindar valor a una solución residente en la nube como Google Cloud NetApp Volumes.

Plano de datos

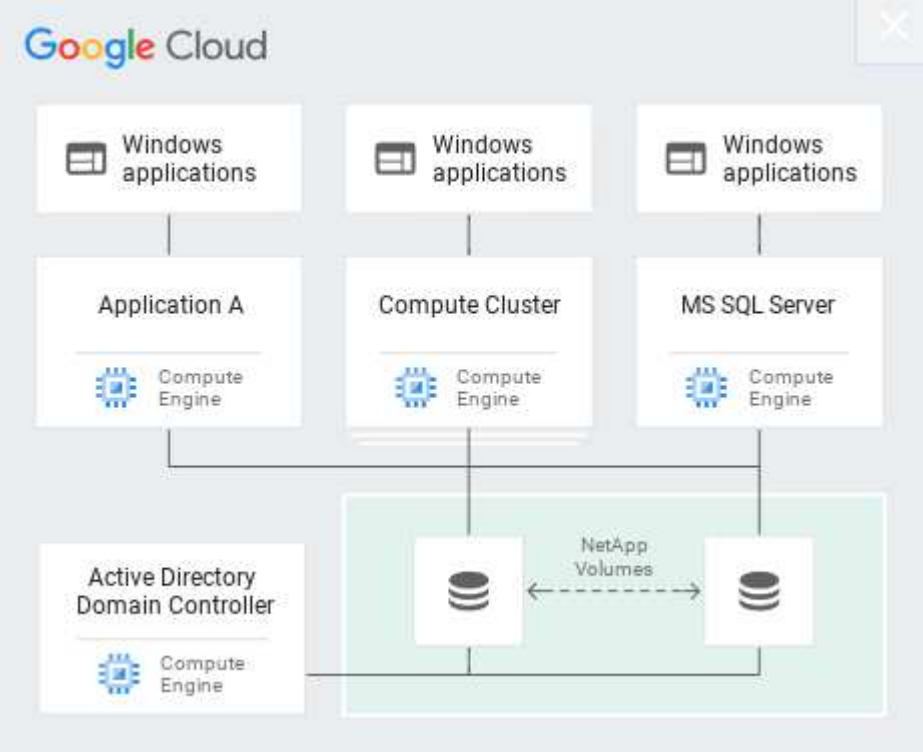
El plano de datos en Google Cloud NetApp Volumes incluye los volúmenes de datos reales y la configuración general de Google Cloud NetApp Volumes (como control de acceso, autenticación Kerberos, etc.). El plano de datos está completamente bajo el control de los usuarios finales y los consumidores de la plataforma Google Cloud NetApp Volumes .

Existen claras diferencias en cómo se protege y gestiona cada avión. Las siguientes secciones cubren estas diferencias, comenzando con una descripción general de la arquitectura de Google Cloud NetApp Volumes .

Arquitectura de Google Cloud NetApp Volumes

De manera similar a otros servicios nativos de Google Cloud, como CloudSQL, Google Cloud VMware Engine (GCVE) y FileStore, Google Cloud NetApp Volumes utiliza "Anuncio de servicio público de Google" para prestar el servicio. En PSA, los servicios se construyen dentro de un proyecto de productor de servicios, que utiliza "Intercambio de redes VPC" para conectarse con el consumidor del servicio. El productor de servicios es proporcionado y operado por NetApp, y el consumidor de servicios es una VPC en un proyecto de cliente, que aloja a los clientes que desean acceder a los recursos compartidos de archivos de Google Cloud NetApp Volumes .

La siguiente figura, referenciada desde el "Google Cloud NetApp Volumes documentación", repasa una vista a grandes rasgos.



La parte sobre la línea punteada muestra el plano de control del servicio, que controla el ciclo de vida del volumen. La parte debajo de la línea punteada muestra el plano de datos. El cuadro azul de la izquierda representa el VPC del usuario (consumidor de servicios), el cuadro azul de la derecha es el productor de servicios proporcionado por NetApp. Ambos están conectados a través del peering VPC.

Modelo de arrendamiento

En Google Cloud NetApp Volumes, los proyectos individuales se consideran inquilinos únicos. Esto significa que la manipulación de volúmenes, copias instantáneas, etc., se realizan proyecto por proyecto. En otras palabras, todos los volúmenes son propiedad del proyecto en el que fueron creados y solo ese proyecto puede administrar y acceder a los datos dentro de ellos de forma predeterminada. Esta se considera la vista del plano de control del servicio.

VPC compartidas

En la vista del plano de datos, Google Cloud NetApp Volumes puede conectarse a una VPC compartida. Puede crear volúmenes en el proyecto de alojamiento o en uno de los proyectos de servicio conectados a la VPC compartida. Todos los proyectos (host o servicio) conectados a esa VPC compartida pueden alcanzar los volúmenes en la capa de red (TCP/IP). Debido a que todos los clientes con conectividad de red en la VPC compartida pueden acceder potencialmente a los datos a través de protocolos NAS, se debe usar el control de acceso en el volumen individual (como listas de control de acceso de usuarios/grupos (ACL) y nombres de host/direcciones IP para exportaciones NFS) para controlar quién puede acceder a los datos.

Puede conectar Google Cloud NetApp Volumes a hasta cinco VPC por proyecto de cliente. En el plano de control, el proyecto le permite administrar todos los volúmenes creados, sin importar a qué VPC estén conectados. En el plano de datos, las VPC están aisladas entre sí y cada volumen solo se puede conectar a una VPC.

El acceso a los volúmenes individuales está controlado por mecanismos de control de acceso específicos del protocolo (NFS/SMB).

En otras palabras, en la capa de red, todos los proyectos conectados a la VPC compartida pueden ver el

volumen, mientras que, en el lado de administración, el plano de control solo permite que el proyecto propietario vea el volumen.

Controles de servicio de VPC

Los controles de servicio de VPC establecen un perímetro de control de acceso alrededor de los servicios de Google Cloud que están conectados a Internet y son accesibles en todo el mundo. Estos servicios proporcionan control de acceso a través de las identidades de los usuarios, pero no pueden restringir desde qué ubicación de red se originan las solicitudes. Los controles de servicio de VPC cierran esa brecha al introducir la capacidad de restringir el acceso a redes definidas.

El plano de datos de Google Cloud NetApp Volumes no está conectado a Internet externo, sino a VPC privadas con límites de red bien definidos (perímetros). Dentro de esa red, cada volumen utiliza un control de acceso específico del protocolo. Cualquier conectividad de red externa es creada explícitamente por los administradores de proyectos de Google Cloud. Sin embargo, el plano de control no proporciona las mismas protecciones que el plano de datos y cualquier persona puede acceder a él desde cualquier lugar con credenciales válidas ("Tokens JWT").

En resumen, el plano de datos de Google Cloud NetApp Volumes proporciona la capacidad de control de acceso a la red, sin el requisito de admitir controles de servicio de VPC y no los utiliza explícitamente.

Consideraciones sobre rastreo y detección de paquetes

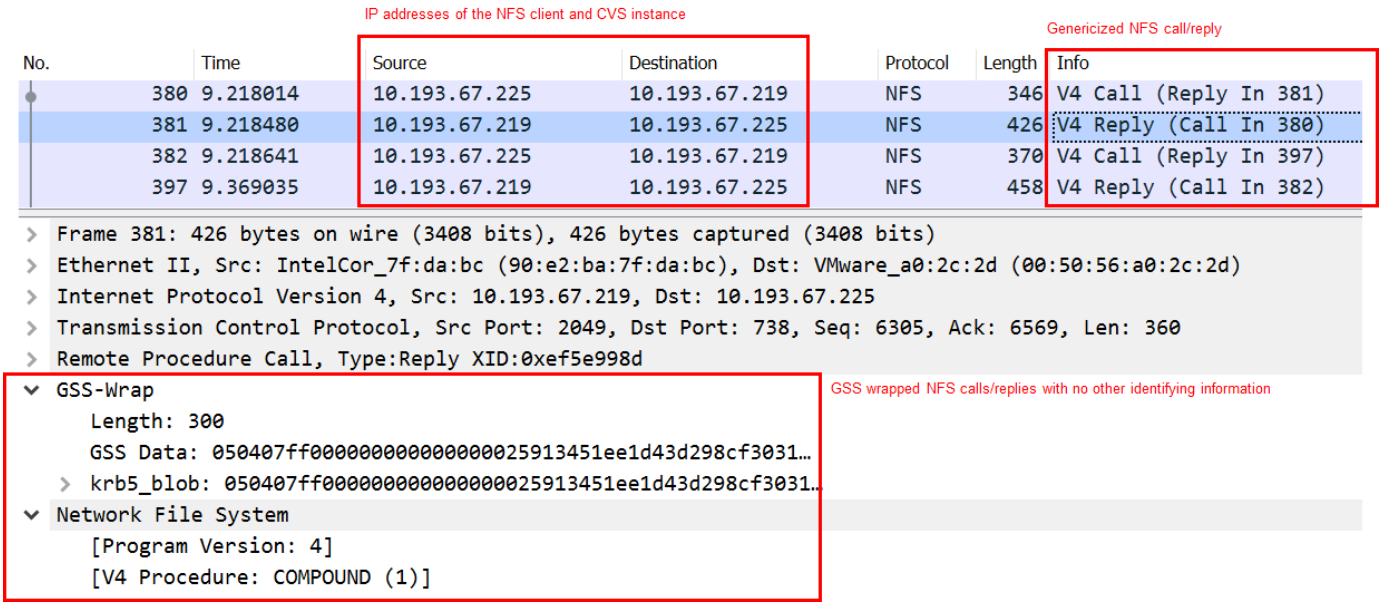
Las capturas de paquetes pueden ser útiles para solucionar problemas de red u otros problemas (como permisos NAS, conectividad LDAP, etc.), pero también pueden usarse de forma maliciosa para obtener información sobre direcciones IP de red, direcciones MAC, nombres de usuarios y grupos, y qué nivel de seguridad se está utilizando en los puntos finales. Debido a la forma en que se configuran las redes, las VPC y las reglas de firewall de Google Cloud, debería ser difícil obtener acceso no deseado a los paquetes de red sin credenciales de inicio de sesión del usuario o"Tokens JWT" en las instancias de la nube. Las capturas de paquetes solo son posibles en puntos finales (como máquinas virtuales [VM]) y solo son posibles en puntos finales internos a la VPC, a menos que se utilice una VPC compartida o un túnel de red externo/reenvío de IP para permitir explícitamente el tráfico externo a los puntos finales. No hay forma de rastrear el tráfico fuera de los clientes.

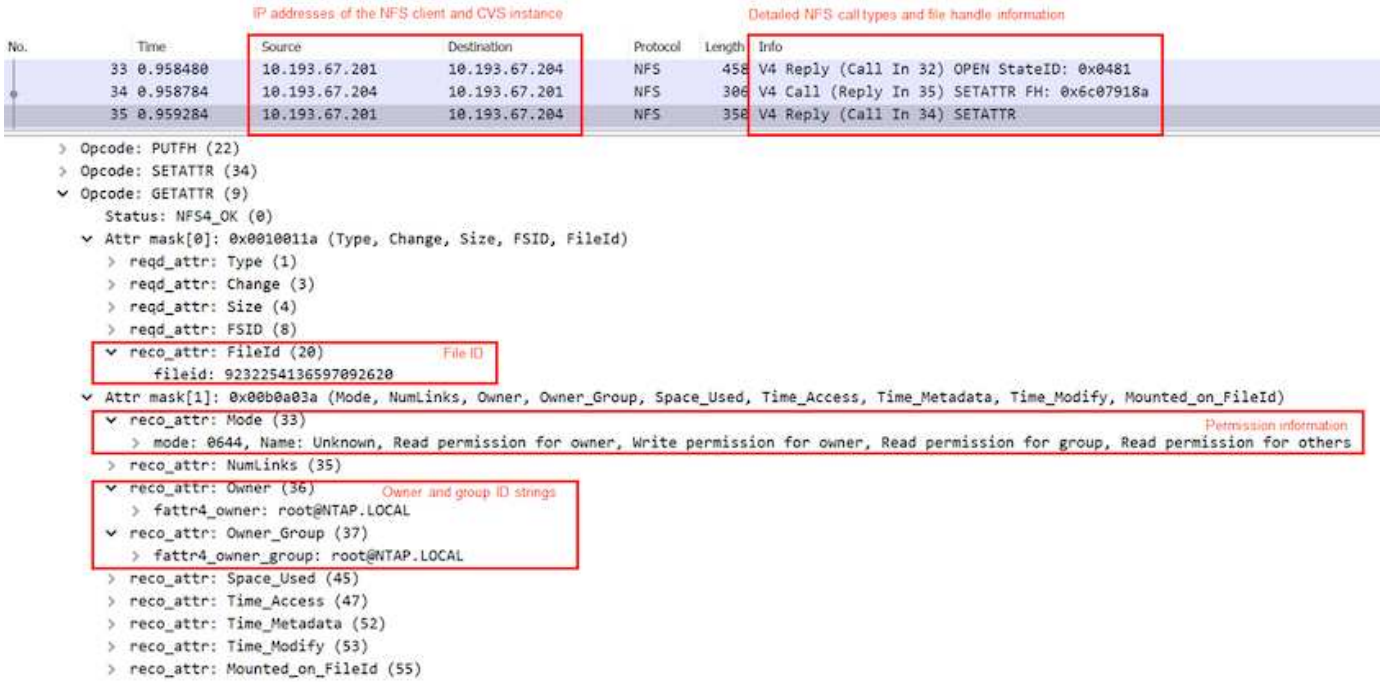
Cuando se utilizan VPC compartidas, el cifrado en tránsito con NFS Kerberos y/o"Cifrado SMB" Puede enmascarar gran parte de la información obtenida de los rastros. Sin embargo, parte del tráfico todavía se envía en texto sin formato, como"DNS" y"Consultas LDAP" . La siguiente figura muestra una captura de paquetes de una consulta LDAP de texto sin formato que se origina en Google Cloud NetApp Volumes y la posible información de identificación que está expuesta. Las consultas LDAP en Google Cloud NetApp Volumes actualmente no admiten cifrado ni LDAP sobre SSL. Soporte de NetApp Volumes-Performance para firma LDAP, si Active Directory lo solicita. NetApp Volumes-SW no admite la firma LDAP.



unixUserPassword es consultado por LDAP y no se envía en texto simple sino en un hash salado. De forma predeterminada, Windows LDAP no rellena los campos unixUserPassword. Este campo solo es necesario si necesita aprovechar Windows LDAP para inicios de sesión interactivos a través de LDAP para los clientes. Google Cloud NetApp Volumes no admite inicios de sesión LDAP interactivos en las instancias.

La siguiente figura muestra una captura de paquetes de una conversación NFS Kerberos junto a una captura de NFS sobre AUTH_SYS. Observe cómo la información disponible en un seguimiento difiere entre los dos y cómo habilitar el cifrado en vuelo ofrece una mayor seguridad general para el tráfico NAS.





Interfaces de red de VM

Un truco que los atacantes podrían intentar es agregar una nueva tarjeta de interfaz de red (NIC) a una máquina virtual en "modo promiscuo" (duplicación de puertos) o habilitar el modo promiscuo en una NIC existente para rastrear todo el tráfico. En Google Cloud, agregar una nueva NIC requiere que una máquina virtual se apague por completo, lo que genera alertas para que los atacantes no puedan hacerlo sin ser detectados.

Además, las NIC no se pueden configurar en modo promiscuo y activarán alertas en Google Cloud.

Arquitectura del plano de control

Todas las acciones de gestión de Google Cloud NetApp Volumes se realizan a través de API. La administración de Google Cloud NetApp Volumes integrada en GCP Cloud Console también utiliza la API de Google Cloud NetApp Volumes .

Gestión de identidad y acceso

Gestión de identidad y acceso("SOY") es un servicio estándar que le permite controlar la autenticación (inicios de sesión) y la autorización (permisos) para las instancias del proyecto de Google Cloud. Google IAM proporciona un registro de auditoría completo de la autorización y eliminación de permisos. Actualmente, Google Cloud NetApp Volumes no proporciona auditoría del plano de control.

Descripción general de autorización/permiso

IAM ofrece permisos integrados y granulares para Google Cloud NetApp Volumes. Puedes encontrar una "Lista completa de permisos granulares aquí".

IAM también ofrece dos roles predefinidos llamados `netappcloudvolumes.admin` y `netappcloudvolumes.viewer` . Estos roles se pueden asignar a usuarios o cuentas de servicio específicos.

Asigne roles y permisos adecuados para permitir que los usuarios de IAM administren Google Cloud NetApp

Volumes.

Algunos ejemplos de uso de permisos granulares incluyen los siguientes:

- Cree un rol personalizado con solo permisos de obtención, enumeración, creación y actualización para que los usuarios no puedan eliminar volúmenes.
- Utilice un rol personalizado con solo `snapshot.*` permisos para crear una cuenta de servicio que se utiliza para crear una integración de instantáneas consistente con la aplicación.
- Crea un rol personalizado para delegar `volumereplication.*` a usuarios específicos.

Cuentas de servicio

Para realizar llamadas a la API de Google Cloud NetApp Volumes a través de scripts o "Terraformar" , debe crear una cuenta de servicio con el `roles/netappcloudvolumes.admin` role. Puede usar esta cuenta de servicio para generar los tokens JWT necesarios para autenticar las solicitudes de API de Google Cloud NetApp Volumes de dos maneras diferentes:

- Genere una clave JSON y utilice las API de Google para derivar un token JWT a partir de ella. Este es el enfoque más simple, pero implica la gestión manual de secretos (la clave JSON).
- Usar "Suplantación de cuenta de servicio" con `roles/iam.serviceAccountTokenCreator` . El código (script, Terraform, etc.) se ejecuta con "Credenciales predeterminadas de la aplicación" y se hace pasar por la cuenta de servicio para obtener sus permisos. Este enfoque refleja las mejores prácticas de seguridad de Google.

Consulta "Creando su cuenta de servicio y clave privada" en la documentación de Google cloud para obtener más información.

API de Google Cloud NetApp Volumes

La API de Google Cloud NetApp Volumes utiliza una API basada en REST que usa HTTPS (TLSv1.2) como transporte de red subyacente. Puedes consultar la definición más reciente de la API e información sobre cómo usarla en "API de Cloud Volumes en la documentación de Google Cloud".

El punto final de API es operado y protegido por NetApp mediante la funcionalidad HTTPS (TLSv1.2) estándar.

Tokens JWT

La autenticación a la API se realiza con tokens portadores JWT("RFC-7519"). Los tokens JWT válidos deben obtenerse mediante la autenticación IAM de Google Cloud. Esto debe hacerse obteniendo un token de IAM proporcionando una clave JSON de cuenta de servicio.

Registro de auditoría

Actualmente, no hay disponibles registros de auditoría del plano de control accesibles para el usuario.

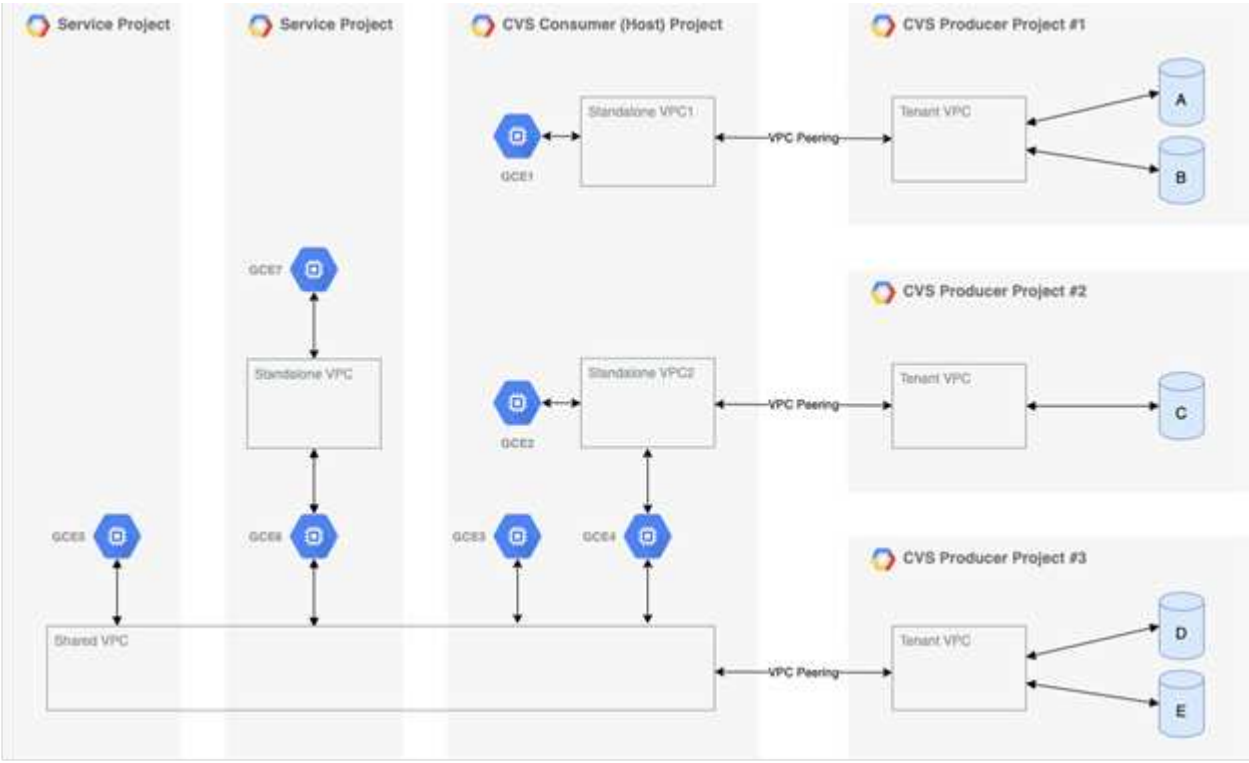
Arquitectura del plano de datos

Google Cloud NetApp Volumes para Google Cloud aprovecha Google Cloud "acceso a servicios privados" estructura. En este marco, los usuarios pueden conectarse a Google Cloud NetApp Volumes. Este marco utiliza redes de servicios y estructuras de peering de VPC como otros servicios de Google Cloud, lo que garantiza un aislamiento completo

entre inquilinos.

Para obtener una descripción general de la arquitectura de Google Cloud NetApp Volumes para Google Cloud, consulta "Arquitectura para Google Cloud NetApp Volumes".

Las VPC de usuario (independientes o compartidas) se conectan a las VPC dentro de los proyectos de inquilinos administrados Google Cloud NetApp Volumes , que alojan los volúmenes.



La figura anterior muestra un proyecto (el proyecto de consumidor de NetApp Volumes en el medio) con tres redes de VPC conectadas a Google Cloud NetApp Volumes y varias máquinas virtuales de Compute Engine (GCE1-7) que comparten volúmenes:

- VPC1 permite que GCE1 acceda a los volúmenes A y B.
- VPC2 permite que GCE2 y GCE4 accedan al volumen C.
- La tercera red VPC es una VPC compartida, compartida con dos proyectos de servicio. Permite que GCE3, GCE4, GCE5 y GCE6 accedan a los volúmenes D y E. Las redes VPC compartidas solo son compatibles con volúmenes del tipo de servicio NetApp Volumes-Performance.

GCE7 no puede acceder a ningún volumen.

Los datos se pueden cifrar tanto en tránsito (mediante cifrado Kerberos o SMB) como en reposo en Google Cloud NetApp Volumes.

Cifrado de datos en tránsito

Los datos en tránsito se pueden cifrar en la capa de protocolo NAS, y la propia red de Google Cloud está cifrada, como se describe en las siguientes secciones.

Red de Google Cloud

Google Cloud cifra el tráfico a nivel de red como se describe en "Cifrado en tránsito" en la documentación de Google. Como se menciona en la sección "Arquitectura de Google Cloud NetApp Volumes ", Google Cloud NetApp Volumes se entrega desde un proyecto de producción de PSA controlado por NetApp.

En el caso de NetApp Volumes-SW, el inquilino productor ejecuta máquinas virtuales de Google para brindar el servicio. Google cifra automáticamente el tráfico entre las máquinas virtuales de los usuarios y las máquinas virtuales de Google Cloud NetApp Volumes .

Aunque la ruta de datos de NetApp Volumes-Performance no está completamente cifrada en la capa de red, NetApp y Google utilizan una combinación "de cifrado IEEE 802.1AE (MACSec)" , "encapsulación" (cifrado de datos) y redes físicamente restringidas para proteger los datos en tránsito entre el tipo de servicio NetApp Google Cloud NetApp Volumes NetApp Volumes y Google Cloud.

Protocolos NAS

Los protocolos NAS NFS y SMB proporcionan cifrado de transporte opcional en la capa de protocolo.

Cifrado SMB

"Cifrado SMB"Proporciona cifrado de extremo a extremo de datos SMB y protege los datos contra escuchas clandestinas en redes no confiables. Puede habilitar el cifrado tanto para la conexión de datos del cliente/servidor (solo disponible para clientes compatibles con SMB3.x) como para la autenticación del controlador de servidor/dominio.

Cuando el cifrado SMB está habilitado, los clientes que no admiten el cifrado no pueden acceder al recurso compartido.

Google Cloud NetApp Volumes admite los cifrados de seguridad RC4-HMAC, AES-128-CTS-HMAC-SHA1 y AES-256-CTS-HMAC-SHA1 para el cifrado SMB. SMB negocia el tipo de cifrado más alto admitido por el servidor.

NFSv4.1 Kerberos

Para NFSv4.1, NetApp Volumes-Performance ofrece autenticación Kerberos como se describe en "RFC7530" Puede habilitar Kerberos por volumen.

El tipo de cifrado más fuerte disponible actualmente para Kerberos es AES-256-CTS-HMAC-SHA1. Google Cloud NetApp Volumes admite AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 y DES para NFS. También admite ARCFOUR-HMAC (RC4) para tráfico CIFS/SMB, pero no para NFS.

Kerberos proporciona tres niveles de seguridad diferentes para montajes NFS que ofrecen opciones sobre qué tan fuerte debe ser la seguridad de Kerberos.

Según Red Hat "Opciones de montaje comunes" documentación:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
```

```
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

Como regla general, cuanto más interviene el nivel de seguridad de Kerberos, peor es el rendimiento, ya que el cliente y el servidor dedican tiempo a cifrar y descifrar operaciones NFS para cada paquete enviado. Muchos clientes y servidores NFS brindan soporte para la descarga de AES-NI a las CPU para una mejor experiencia general, pero el impacto en el rendimiento de Kerberos 5p (cifrado completo de extremo a extremo) es significativamente mayor que el impacto de Kerberos 5 (autenticación de usuario).

La siguiente tabla muestra las diferencias en lo que hace cada nivel por la seguridad y el rendimiento.

Nivel de seguridad	Seguridad	Actuación
NFSv3—sys	• Menos seguro; texto simple con identificadores de usuario/grupo numéricos • Capaz de ver UID, GID, direcciones IP de cliente, rutas de exportación, nombres de archivos, permisos en capturas de paquetes	• Mejor para la mayoría de los casos
NFSv4.x—sys	• Más seguro que NFSv3 (ID de cliente, coincidencia de cadena de nombre/cadena de dominio) pero aún texto simple • Capaz de ver UID, GID, direcciones IP de cliente, cadenas de nombres, ID de dominio, rutas de exportación, nombres de archivos y permisos en capturas de paquetes	• Ideal para cargas de trabajo secuenciales (como máquinas virtuales, bases de datos y archivos grandes). • Malo con gran cantidad de archivos/altos metadatos (30-50 % peor)

Nivel de seguridad	Seguridad	Actuación
NFS—krb5	• Cifrado Kerberos para credenciales en cada paquete NFS: envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita acceso al montaje necesita un ticket Kerberos válido (ya sea a través de nombre de usuario/contraseña o intercambio manual de pestañas de claves); el ticket vence después de un período de tiempo específico y el usuario debe volver a autenticarse para acceder. • Sin cifrado para operaciones NFS o protocolos auxiliares como mount/portmapper/nlm (se pueden ver rutas de exportación, direcciones IP, controladores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes)	• Mejor en la mayoría de los casos para Kerberos; peor que AUTH_SYS

Nivel de seguridad	Seguridad	Actuación
NFS—krb5i	• Cifrado Kerberos para credenciales en cada paquete NFS: envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita acceso al montaje necesita un ticket Kerberos válido (ya sea mediante nombre de usuario/contraseña o intercambio manual de pestañas de claves); el ticket vence después de un período de tiempo específico y el usuario debe volver a autenticarse para acceder. • Sin cifrado para operaciones NFS o protocolos auxiliares como mount/portmapper/nlm (se pueden ver rutas de exportación, direcciones IP, controladores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes) • Se agrega la suma de comprobación GSS de Kerberos a cada paquete para garantizar que nada intercepte los paquetes. Si las sumas de comprobación coinciden, se permite la conversación.	• Mejor que krb5p porque la carga útil NFS no está cifrada; la única sobrecarga adicional en comparación con krb5 es la suma de comprobación de integridad. El rendimiento de krb5i no será mucho peor que el de krb5, pero experimentará cierta degradación.

Nivel de seguridad	Seguridad	Actuación
NFS – krb5p	• Cifrado Kerberos para credenciales en cada paquete NFS: envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita acceso al montaje necesita un ticket Kerberos válido (ya sea mediante nombre de usuario/contraseña o intercambio manual de claves); el ticket vence después de un período de tiempo específico y el usuario debe volver a autenticarse para acceder. • Todas las cargas útiles de paquetes NFS están cifradas con el contenedor GSS (no se pueden ver los controladores de archivos, permisos, nombres de archivos ni atime/mtime en las capturas de paquetes). • Incluye verificación de integridad. • El tipo de operación NFS es visible (FSINFO, ACCESS, GETATTR, etc.). • Los protocolos auxiliares (mount, portmap, nlm, etc.) no están cifrados (se pueden ver rutas de exportación y direcciones IP).	• Peor rendimiento de los niveles de seguridad; krb5p tiene que cifrar/descifrar más. • Mejor rendimiento que krb5p con NFSv4.x para cargas de trabajo con gran cantidad de archivos.

En Google Cloud NetApp Volumes, se utiliza un servidor Active Directory configurado como servidor Kerberos y servidor LDAP (para buscar identidades de usuario a partir de un esquema compatible con RFC2307). No se admiten otros servidores Kerberos o LDAP. NetApp recomienda encarecidamente que utilice LDAP para la gestión de identidades en Google Cloud NetApp Volumes. Para obtener información sobre cómo se muestra NFS Kerberos en las capturas de paquetes, consulte la sección enlace:gcp-gcnv-arch-detail.html#Consideraciones sobre rastreo/detección de paquetes["Consideraciones sobre rastreo/detección de paquetes."]

Cifrado de datos en reposo

Todos los volúmenes de Google Cloud NetApp Volumes están cifrados en reposo mediante cifrado AES-256, lo que significa que todos los datos del usuario escritos en los medios están cifrados y solo se pueden descifrar con una clave por volumen.

- Para NetApp Volumes-SW, se utilizan claves generadas por Google.

- Para NetApp Volumes-Performance, las claves por volumen se almacenan en un administrador de claves integrado en Google Cloud NetApp Volumes.

A partir de noviembre de 2021, estuvo disponible la vista previa de la funcionalidad de claves de cifrado administradas por el cliente (CMEK). Esto le permite cifrar las claves por volumen con una clave maestra por proyecto y por región alojada en "Servicio de administración de claves de Google (KMS)." KMS le permite conectar administradores de claves externos.

Para obtener información sobre cómo configurar KMS para NetApp Volumes-Performance, consulta "Configuración de claves de cifrado administradas por el cliente".

Cortafuegos

Google Cloud NetApp Volumes expone múltiples puertos TCP para servir recursos compartidos NFS y SMB:

- "Puertos necesarios para el acceso NFS"
- "Puertos necesarios para el acceso SMB"

Además, SMB, NFS con LDAP, incluido Kerberos, y las configuraciones de doble protocolo requieren acceso a un dominio de Windows Active Directory. Las conexiones de Active Directory deben "configurado" para cada región. Los controladores de dominio (DC) de Active Directory se identifican mediante "Descubrimiento de DC basado en DNS" utilizando los servidores DNS especificados. Se utiliza cualquiera de los DC devueltos. La lista de DC elegibles se puede limitar especificando un sitio de Active Directory.

Google Cloud NetApp Volumes se conecta mediante direcciones IP del rango CIDR asignado con el comando `gcloud compute address` mientras "Incorporación de Google Cloud NetApp Volumes". Puedes utilizar este rango CIDR como direcciones de origen para configurar los cortafuegos de entrada de tus controladores de dominio de Active Directory.

Los controladores de dominio de Active Directory deben "Exponer puertos a los CIDR de Google Cloud NetApp Volumes como se menciona aquí".

Descripción general de los protocolos NAS

Los protocolos NAS incluyen NFS (v3 y v4.1) y SMB/CIFS (2.x y 3.x). Estos protocolos son la forma en que NetApp Volumes permite el acceso compartido a los datos entre múltiples clientes NAS. Además, Google Cloud NetApp Volumes puede proporcionar acceso a clientes NFS y SMB/CIFS simultáneamente (protocolo dual) al tiempo que respeta todas las configuraciones de identidad y permisos de los archivos y carpetas en los recursos compartidos NAS. Para mantener la mayor seguridad posible en la transferencia de datos, Google Cloud NetApp Volumes admite el cifrado de protocolo en tránsito mediante cifrado SMB y NFS Kerberos 5p.



El protocolo dual solo está disponible con NetApp Volumes-Performance.

Conceptos básicos de los protocolos NAS

Los protocolos NAS son formas para que varios clientes de una red accedan a los mismos datos en un sistema de almacenamiento, como Google Cloud NetApp Volumes en GCP. NFS y SMB son los protocolos NAS definidos y funcionan sobre una base

cliente/servidor, donde Google Cloud NetApp Volumes actúa como servidor. Los clientes envían solicitudes de acceso, lectura y escritura al servidor, y el servidor es responsable de coordinar los mecanismos de bloqueo de archivos, almacenar permisos y gestionar las solicitudes de identidad y autenticación.

Por ejemplo, se sigue el siguiente proceso general si un cliente NAS desea crear un nuevo archivo en una carpeta.

1. El cliente solicita al servidor información sobre el directorio (permisos, propietario, grupo, ID de archivo, espacio disponible, etc.); el servidor responde con la información si el cliente y el usuario solicitantes tienen los permisos necesarios en la carpeta principal.
2. Si los permisos del directorio permiten el acceso, el cliente pregunta al servidor si el nombre del archivo que se está creando ya existe en el sistema de archivos. Si el nombre del archivo ya está en uso, la creación falla. Si el nombre del archivo no existe, el servidor le informa al cliente que puede continuar.
3. El cliente emite una llamada al servidor para crear el archivo con el identificador de directorio y el nombre del archivo y establece los tiempos de acceso y modificación. El servidor emite un ID de archivo único para el archivo para asegurarse de que no se creen otros archivos con el mismo ID de archivo.
4. El cliente envía una llamada para verificar los atributos del archivo antes de la operación ESCRIBIR. Si los permisos lo permiten, el cliente escribe el nuevo archivo. Si el protocolo o la aplicación utilizan el bloqueo, el cliente solicita al servidor un bloqueo para evitar que otros clientes accedan al archivo mientras está bloqueado para evitar la corrupción de datos.

Sistema Nacional de Archivos

NFS es un protocolo de sistema de archivos distribuido que es un estándar IETF abierto definido en una Solicitud de comentarios (RFC) que permite a cualquiera implementar el protocolo.

Los volúmenes en Google Cloud NetApp Volumes se comparten entre los clientes NFS exportando una ruta a la que puede acceder un cliente o un conjunto de clientes. Los permisos para montar estas exportaciones están definidos por políticas y reglas de exportación, que pueden configurar los administradores de Google Cloud NetApp Volumes .

La implementación de NFS de NetApp se considera un estándar de oro para el protocolo y se utiliza en innumerables entornos NAS empresariales. Las siguientes secciones cubren NFS y las funciones de seguridad específicas disponibles en Google Cloud NetApp Volumes y cómo se implementan.

Usuarios y grupos locales predeterminados de UNIX

Google Cloud NetApp Volumes contiene varios usuarios y grupos de UNIX predeterminados para diversas funcionalidades básicas. Estos usuarios y grupos no se pueden modificar ni eliminar actualmente. Actualmente no es posible agregar nuevos usuarios y grupos locales a Google Cloud NetApp Volumes. Los usuarios y grupos de UNIX fuera de los usuarios y grupos predeterminados deben ser proporcionados por un servicio de nombres LDAP externo.

La siguiente tabla muestra los usuarios y grupos predeterminados y sus ID numéricos correspondientes. NetApp recomienda no crear nuevos usuarios o grupos en LDAP o en los clientes locales que reutilizan estos identificadores numéricos.

Usuarios predeterminados: ID numéricos	Grupos predeterminados: identificadores numéricos
• raíz:0 • usuario:65534 • nadie:65535	• raíz:0 • demonio:1 • usuario:65534 • nadie:65535

Al utilizar NFSv4.1, el usuario root puede aparecer como nadie al ejecutar comandos de listado de directorios en clientes NFS. Esto se debe a la configuración de mapeo del dominio de ID del cliente. Vea la sección llamadaNFSv4.1 y el usuario/grupo nobody para obtener detalles sobre este problema y cómo resolverlo.

El usuario root

En Linux, la cuenta raíz tiene acceso a todos los comandos, archivos y carpetas en un sistema de archivos basado en Linux. Debido al poder de esta cuenta, las mejores prácticas de seguridad a menudo requieren que el usuario root esté deshabilitado o restringido de alguna manera. En las exportaciones de NFS, el poder que tiene un usuario raíz sobre los archivos y las carpetas se puede controlar en Google Cloud NetApp Volumes a través de políticas y reglas de exportación y un concepto conocido como squash de raíz.

El aplastamiento de raíz garantiza que el usuario raíz que accede a un montaje NFS se aplaste al usuario numérico anónimo 65534 (consulte la sección "El usuario anónimo ") y actualmente solo está disponible cuando se utiliza NetApp Volumes-Performance seleccionando Desactivado para el acceso raíz durante la creación de la regla de política de exportación. Si el usuario root se reduce al usuario anónimo, ya no tiene acceso para ejecutar chown o "Comandos setuid/setgid (la parte persistente)" en archivos o carpetas en el montaje NFS, y los archivos o carpetas creados por el usuario raíz muestran el UID anónimo como propietario/grupo. Además, el usuario root no puede modificar las ACL de NFSv4. Sin embargo, el usuario root todavía tiene acceso a chmod y a los archivos eliminados para los que no tiene permisos explícitos. Si desea limitar el acceso a los permisos de archivos y carpetas de un usuario raíz, considere usar un volumen con ACL NTFS y crear un usuario de Windows llamado `root` , y aplicar los permisos deseados a los archivos o carpetas.

El usuario anónimo

El ID de usuario anónimo (anon) especifica un ID de usuario o nombre de usuario de UNIX que se asigna a las solicitudes de cliente que llegan sin credenciales NFS válidas. Esto puede incluir al usuario root cuando se utiliza el aplastamiento de raíz. El usuario anónimo en Google Cloud NetApp Volumes es 65534.

Este UID normalmente está asociado con el nombre de usuario `nobody` o `nfsnobody` en entornos Linux. Google Cloud NetApp Volumes también usa 65534 como el usuario local de UNIX `pcuser` (consulte la sección "Usuarios y grupos locales predeterminados de UNIX "), que también es el usuario de respaldo predeterminado para las asignaciones de nombres de Windows a UNIX cuando no se puede encontrar un usuario UNIX coincidente válido en LDAP.

Debido a las diferencias en los nombres de usuario en Linux y Google Cloud NetApp Volumes para el UID 65534, la cadena de nombre de los usuarios asignados a 65534 podría no coincidir al usar NFSv4.1. Como resultado, es posible que veas `nobody` como usuario en algunos archivos y carpetas. Ver la sección "NFSv4.1 y el usuario/grupo nobody " para obtener información sobre este problema y cómo resolverlo.

Control de acceso/exportaciones

El acceso inicial a la exportación/uso compartido de montajes NFS se controla a través de reglas de política de exportación basadas en host contenidas dentro de una política de exportación. Se define una IP de host, un nombre de host, una subred, un grupo de redes o un dominio para permitir el acceso para montar el recurso compartido NFS y el nivel de acceso permitido al host. Las opciones de configuración de reglas de política de exportación dependen del nivel de Google Cloud NetApp Volumes .

Para NetApp Volumes-SW, las siguientes opciones están disponibles para la configuración de la política de exportación:

- **Emparejamiento de clientes.** Lista separada por comas de direcciones IP, lista separada por comas de nombres de host, subredes, grupos de redes y nombres de dominio.
- **Reglas de acceso RO/RW.** Seleccione lectura/escritura o solo lectura para controlar el nivel de acceso a la exportación. NetApp Volumes-Performance ofrece las siguientes opciones:
- **Emparejamiento de clientes.** Lista separada por comas de direcciones IP, lista separada por comas de nombres de host, subredes, grupos de redes y nombres de dominio.
- **Reglas de acceso RO/RW.** Seleccione lectura/escritura o solo lectura para controlar el nivel de acceso para exportar.
- **Acceso root (activado/desactivado).** Configura el squash raíz (ver la sección "El usuario root " para más detalles).
- **Tipo de protocolo.** Esto limita el acceso al montaje NFS a una versión de protocolo específica. Al especificar NFSv3 y NFSv4.1 para el volumen, deje ambos en blanco o marque ambas casillas.
- **Nivel de seguridad Kerberos (cuando está seleccionado Habilitar Kerberos).** Proporciona las opciones de krb5, krb5i y/o krb5p para acceso de solo lectura o de lectura y escritura.

Cambiar la propiedad (chown) y cambiar el grupo (chgrp)

NFS en Google Cloud NetApp Volumes solo permite que el usuario root ejecute chown/chgrp en archivos y carpetas. Otros usuarios ven un `Operation not permitted` error, incluso en archivos de su propiedad. Si utiliza calabaza de raíz (como se explica en la sección "El usuario root "), la raíz se reduce a un usuario no root y no se le permite el acceso a chown y chgrp. Actualmente no existen soluciones alternativas en Google Cloud NetApp Volumes para permitir chown y chgrp para usuarios que no sean root. Si se requieren cambios de propiedad, considere usar volúmenes de protocolo dual y configure el estilo de seguridad en NTFS para controlar los permisos desde el lado de Windows.

Gestión de permisos

Google Cloud NetApp Volumes admite bits de modo (como 644, 777, etc. para rwx) y ACL NFSv4.1 para controlar los permisos en clientes NFS para volúmenes que usan el estilo de seguridad UNIX. Para estos se utiliza la gestión de permisos estándar (como chmod, chown o nfs4_setfacl) y funcionan con cualquier cliente Linux que los admita.

Además, al utilizar volúmenes de protocolo dual configurados en NTFS, los clientes NFS pueden aprovechar la asignación de nombres de Google Cloud NetApp Volumes a los usuarios de Windows, que luego se utilizan para resolver los permisos NTFS. Esto requiere una conexión LDAP a Google Cloud NetApp Volumes para proporcionar traducciones de ID numérico a nombre de usuario porque Google Cloud NetApp Volumes requiere un nombre de usuario de UNIX válido para asignarse correctamente a un nombre de usuario de Windows.

Proporcionar ACL granulares para NFSv3

Los permisos de bit de modo cubren solo al propietario, al grupo y a todos los demás en la semántica, lo que significa que no hay controles de acceso de usuario granulares establecidos para NFSv3 básico. Google Cloud NetApp Volumes no admite ACL POSIX ni atributos extendidos (como chattr), por lo que las ACL granulares solo son posibles en los siguientes escenarios con NFSv3:

- Volúmenes de estilo de seguridad NTFS (se requiere servidor CIFS) con asignaciones de usuarios válidas de UNIX a Windows.
- ACL de NFSv4.1 aplicadas mediante un cliente administrador que monta NFSv4.1 para aplicar ACL.

Ambos métodos requieren una conexión LDAP para la administración de identidad de UNIX y un usuario UNIX válido y información de grupo completada (consulte la sección"LDAP") y solo están disponibles con instancias de NetApp Volumes-Performance. Para utilizar volúmenes de estilo de seguridad NTFS con NFS, debe utilizar protocolo dual (SMB y NFSv3) o protocolo dual (SMB y NFSv4.1), incluso si no se realizan conexiones SMB. Para utilizar ACL NFSv4.1 con montajes NFSv3, debe seleccionar `Both (NFSv3/NFSv4.1)` como el tipo de protocolo.

Los bits del modo UNIX normal no proporcionan el mismo nivel de granularidad en permisos que proporcionan las ACL NTFS o NFSv4.x. La siguiente tabla compara la granularidad de permisos entre los bits del modo NFSv3 y las ACL NFSv4.1. Para obtener información sobre las ACL de NFSv4.1, consulte "nfs4_acl - Listas de control de acceso NFSv4" .

Bits de modo NFSv3	Listas de control de acceso (ACL) de NFSv4.1
• Establecer ID de usuario al ejecutar • Establecer ID de grupo al ejecutar • Guardar texto intercambiado (no definido en POSIX) • Permiso de lectura para el propietario • Permiso de escritura para el propietario • Permiso de ejecución para el propietario de un archivo; o buscar permiso para el propietario en el directorio • Permiso de lectura para el grupo • Permiso de escritura para el grupo • Permiso de ejecución para un grupo en un archivo; o buscar permiso para un grupo en un directorio • Permiso de lectura para otros • Permiso de escritura para otros • Obtener permiso de ejecución para otros en un archivo; o buscar permiso para otros en un directorio	Tipos de entrada de control de acceso (ACE) (Permitir/Denegar/Auditar) * Indicadores de herencia * herencia de directorio * herencia de archivo * herencia de no propagación * herencia de solo herencia Permisos * leer-datos (archivos) / lista-directorio (directorios) * escribir-datos (archivos) / crear-archivo (directorios) * añadir-datos (archivos) / crear-subdirectorio (directorios) * ejecutar (archivos) / cambiar-directorio (directorios) * eliminar * eliminar-hijo * leer-atributos * escribir-atributos * leer-atributos-nombrados * escribir-atributos-nombrados * leer-ACL * escribir-ACL * escribir-propietario * Sincronizar

Finalmente, la membresía del grupo NFS (tanto en NFSv3 como en NFSV4.x) está limitada a un máximo predeterminado de 16 para AUTH_SYS según los límites de paquetes RPC. NFS Kerberos proporciona hasta 32 grupos y las ACL de NFSv4 eliminan la limitación mediante ACL granulares de usuarios y grupos (hasta 1024 entradas por ACE).

Además, Google Cloud NetApp Volumes ofrece compatibilidad ampliada con grupos para aumentar el máximo de grupos admitidos hasta 32. Para ello, necesitas una conexión LDAP a un servidor LDAP que contenga identidades válidas de usuarios y grupos de UNIX. Para obtener más información sobre cómo configurar esto, consulta "Creación y gestión de volúmenes NFS" en la documentación de Google.

ID de usuarios y grupos de NFSv3

Los identificadores de usuarios y grupos de NFSv3 llegan a la red como identificadores numéricos en lugar de nombres. Google Cloud NetApp Volumes no realiza resolución de nombre de usuario para estos identificadores numéricos con NFSv3, y los volúmenes de estilo de seguridad UNIX utilizan solo bits de modo. Cuando hay ACL de NFSv4.1, se necesita una búsqueda de ID numérico o de cadena de nombre para resolver la ACL correctamente, incluso cuando se usa NFSv3. Con volúmenes de estilo de seguridad NTFS, Google Cloud NetApp Volumes debe resolver una identificación numérica para un usuario de UNIX válido y luego asignarla a un usuario de Windows válido para negociar los derechos de acceso.

Limitaciones de seguridad de los identificadores de usuarios y grupos de NFSv3

Con NFSv3, el cliente y el servidor nunca tienen que confirmar que el usuario que intenta leer o escribir con una identificación numérica es un usuario válido; simplemente se confía implícitamente en él. Esto abre el sistema de archivos a posibles violaciones simplemente falsificando cualquier identificación numérica. Para evitar agujeros de seguridad como este, hay algunas opciones disponibles para Google Cloud NetApp Volumes.

- La implementación de Kerberos para NFS obliga a los usuarios a autenticarse con un nombre de usuario y una contraseña o un archivo de claves para obtener un ticket Kerberos que les permita acceder a un montaje. Kerberos está disponible con instancias de NetApp Volumes-Performance y solo con NFSv4.1.
- Limitar la lista de hosts en las reglas de su política de exportación limita qué clientes NFSv3 tienen acceso al volumen de Google Cloud NetApp Volumes .
- El uso de volúmenes de protocolo dual y la aplicación de ACL NTFS al volumen obliga a los clientes NFSv3 a resolver identificaciones numéricas en nombres de usuario UNIX válidos para autenticarse correctamente y acceder a los montajes. Esto requiere habilitar LDAP y configurar las identidades de usuarios y grupos de UNIX.
- Aplastar al usuario root limita el daño que un usuario root puede causar a un montaje NFS, pero no elimina por completo el riesgo. Para obtener más información, consulte la sección "El usuario root . "

En última instancia, la seguridad de NFS está limitada a lo que ofrece la versión del protocolo que estás utilizando. NFSv3, si bien tiene mejor rendimiento en general que NFSv4.1, no proporciona el mismo nivel de seguridad.

NFSv4.1

NFSv4.1 proporciona mayor seguridad y confiabilidad en comparación con NFSv3, por las siguientes razones:

- Bloqueo integrado mediante un mecanismo basado en arrendamiento
- Sesiones con estado
- Toda la funcionalidad NFS en un solo puerto (2049)
- Sólo TCP
- Mapeo de dominios de identificación
- Integración de Kerberos (NFSv3 puede usar Kerberos, pero solo para NFS, no para protocolos auxiliares como NLM)

Dependencias de NFSv4.1

Debido a las características de seguridad adicionales en NFSv4.1, hay algunas dependencias externas involucradas que no eran necesarias para usar NFSv3 (similar a cómo SMB requiere dependencias como Active Directory).

Listas de control de acceso (ACL) de NFSv4.1

Google Cloud NetApp Volumes ofrece compatibilidad con ACL NFSv4.x, que ofrecen ventajas distintivas sobre los permisos de estilo POSIX normales, como las siguientes:

- Control granular del acceso de los usuarios a archivos y directorios
- Mejor seguridad de NFS
- Interoperabilidad mejorada con CIFS/SMB
- Eliminación de la limitación de NFS de 16 grupos por usuario con seguridad AUTH_SYS
- Las ACL evitan la necesidad de resolución de ID de grupo (GID), lo que elimina efectivamente el límite de GID. Las ACL de NFSv4.1 se controlan desde clientes NFS, no desde Google Cloud NetApp Volumes. Para utilizar las ACL de NFSv4.1, asegúrese de que la versión del software de su cliente las admita y que las utilidades NFS adecuadas estén instaladas.

Compatibilidad entre las ACL de NFSv4.1 y los clientes SMB

Las ACL de NFSv4 son diferentes de las ACL de nivel de archivo de Windows (ACL de NTFS) pero tienen una funcionalidad similar. Sin embargo, en entornos NAS multiprotocolo, si hay ACL NFSv4.1 y está usando acceso de protocolo dual (NFS y SMB en los mismos conjuntos de datos), los clientes que usen SMB2.0 y versiones posteriores no podrán ver ni administrar las ACL desde las pestañas de seguridad de Windows.

Cómo funcionan las ACL de NFSv4.1

Como referencia, se definen los siguientes términos:

- **Lista de control de acceso (ACL).** Una lista de entradas de permisos.
- **Entrada de control de acceso (ACE).** Una entrada de permiso en la lista.

Cuando un cliente establece una ACL NFSv4.1 en un archivo durante una operación SETATTR, Google Cloud NetApp Volumes establece esa ACL en el objeto y reemplaza cualquier ACL existente. Si no hay ninguna ACL en un archivo, los permisos de modo en el archivo se calculan a partir de PROPIETARIO@, GRUPO@ y TODOS@. Si hay bits SUID/SGID/STICKY existentes en el archivo, no se verán afectados.

Cuando un cliente obtiene una ACL NFSv4.1 en un archivo durante el curso de una operación GETATTR, Google Cloud NetApp Volumes lee la ACL NFSv4.1 asociada con el objeto, crea una lista de ACE y devuelve la lista al cliente. Si el archivo tiene una ACL NT o bits de modo, entonces se construye una ACL a partir de bits de modo y se devuelve al cliente.

Se deniega el acceso si hay un DENY ACE en la ACL; se concede el acceso si existe un ALLOW ACE. Sin embargo, el acceso también se niega si ninguna de las ACE está presente en la ACL.

Un descriptor de seguridad consta de una ACL de seguridad (SACL) y una ACL discrecional (DACL). Cuando NFSv4.1 interopera con CIFS/SMB, la DACL se asigna uno a uno con NFSv4 y CIFS. La DACL consta de los ACE ALLOW y DENY.

Si un básico `chmod` se ejecuta en un archivo o carpeta con ACL NFSv4.1 establecidas, se conservan las ACL de usuario y grupo existentes, pero se modifican las ACL predeterminadas OWNER@, GROUP@ y

EVERYONE@.

Un cliente que utiliza ACL NFSv4.1 puede configurar y ver ACL para archivos y directorios en el sistema. Cuando se crea un nuevo archivo o subdirectorio en un directorio que tiene una ACL, ese objeto hereda todas las ACE en la ACL que se han etiquetado con la etiqueta apropiada. "indicadores de herencia" .

Si un archivo o directorio tiene una ACL NFSv4.1, esa ACL se utiliza para controlar el acceso sin importar qué protocolo se utilice para acceder al archivo o directorio.

Los archivos y directorios heredan las ACE de las ACL NFSv4 en los directorios principales (posiblemente con las modificaciones apropiadas) siempre que las ACE se hayan etiquetado con los indicadores de herencia correctos.

Cuando se crea un archivo o directorio como resultado de una solicitud NFSv4, la ACL del archivo o directorio resultante depende de si la solicitud de creación de archivo incluye una ACL o solo permisos de acceso a archivos UNIX estándar. La ACL también depende de si el directorio principal tiene una ACL.

- Si la solicitud incluye una ACL, se utiliza esa ACL.
- Si la solicitud incluye solo permisos de acceso a archivos estándar de UNIX y el directorio principal no tiene una ACL, se utiliza el modo de archivo del cliente para establecer permisos de acceso a archivos estándar de UNIX.
- Si la solicitud incluye solo permisos de acceso a archivos estándar de UNIX y el directorio principal tiene una ACL no heredable, se establece una ACL predeterminada basada en los bits de modo pasados a la solicitud en el nuevo objeto.
- Si la solicitud incluye solo permisos de acceso a archivos estándar de UNIX, pero el directorio principal tiene una ACL, las ACE en la ACL del directorio principal son heredadas por el nuevo archivo o directorio siempre que las ACE hayan sido etiquetadas con los indicadores de herencia adecuados.

Permisos de ACE

Los permisos de ACL de NFSv4.1 utilizan una serie de valores de letras mayúsculas y minúsculas (como `rxtncy`) para controlar el acceso. Para obtener más información sobre los valores de estas letras, consulte "CÓMO: Usar ACL de NFSv4" .

Comportamiento de ACL de NFSv4.1 con umask y herencia de ACL

"Las ACL de NFSv4 brindan la capacidad de ofrecer herencia de ACL" . La herencia de ACL significa que los archivos o carpetas creados debajo de objetos con ACL NFSv4.1 configuradas pueden heredar las ACL según la configuración de la "Indicador de herencia de ACL" .

"Máscara de usuario"Se utiliza para controlar el nivel de permiso con el que se crean archivos y carpetas en un directorio sin interacción del administrador. De forma predeterminada, Google Cloud NetApp Volumes permite que umask anule las ACL heredadas, lo cual es el comportamiento esperado según "RFC 5661" .

Formato ACL

Las ACL de NFSv4.1 tienen un formato específico. El siguiente ejemplo es un conjunto ACE en un archivo:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

El ejemplo anterior sigue las pautas de formato ACL de:

```
type:flags:principal:permissions
```

Un tipo de `A` significa "permitir". En este caso, las banderas de herencia no se establecen porque el principal no es un grupo y no incluye herencia. Además, debido a que ACE no es una entrada de AUDITORÍA, no es necesario configurar los indicadores de auditoría. Para obtener más información sobre las ACL de NFSv4.1, consulte "http://linux.die.net/man/5/nfs4_acl" .

Si la ACL de NFSv4.1 no está configurada correctamente (o el cliente y el servidor no pueden resolver una cadena de nombre), la ACL podría no comportarse como se espera o el cambio de ACL podría no aplicarse y generar un error.

Algunos ejemplos de errores incluyen:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

DENEGAR explícitamente

Los permisos de NFSv4.1 pueden incluir atributos DENY explícitos para PROPIETARIO, GRUPO y TODOS. Esto se debe a que las ACL de NFSv4.1 son de denegación predeterminada, lo que significa que si una ACE no concede explícitamente una ACL, entonces se deniega. Los atributos DENY explícitos anulan cualquier ACE de ACCESS, explícito o no.

Los ACE DENY se configuran con una etiqueta de atributo de `D` .

En el siguiente ejemplo, a GROUP@ se le permiten todos los permisos de lectura y ejecución, pero se le niega todo acceso de escritura.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

Se deben evitar las ACL DENY siempre que sea posible porque pueden ser confusas y complicadas; las ACL ALLOW que no están definidas explícitamente se niegan implícitamente. Cuando se configuran DENY ACE, es posible que se les niegue el acceso a los usuarios cuando esperan que se les conceda.

El conjunto anterior de ACE es equivalente a 755 bits de modo, lo que significa:

- El propietario tiene plenos derechos.
- Los grupos sólo tienen permiso de lectura.
- Otros sólo han leído.

Sin embargo, incluso si los permisos se ajustan al equivalente de 775, el acceso puede ser denegado debido al DENY explícito establecido en TODOS.

Dependencias de mapeo de dominios de ID de NFSv4.1

NFSv4.1 aprovecha la lógica de mapeo de dominios de ID como una capa de seguridad para ayudar a verificar que un usuario que intenta acceder a un montaje NFSv4.1 es realmente quien dice ser. En estos casos, el nombre de usuario y el nombre del grupo que provienen del cliente NFSv4.1 agregan una cadena de nombre y la envían a la instancia de Google Cloud NetApp Volumes . Si esa combinación de nombre de usuario/nombre de grupo y cadena de identificación no coincide, entonces el usuario y/o grupo se reduce al usuario predeterminado "nadie" especificado en el `/etc/idmapd.conf` archivo en el cliente.

Esta cadena de identificación es un requisito para el cumplimiento adecuado de los permisos, especialmente cuando se utilizan ACL NFSv4.1 y/o Kerberos. Como resultado, las dependencias del servidor de servicios de nombres, como los servidores LDAP, son necesarias para garantizar la coherencia entre los clientes y Google Cloud NetApp Volumes para la resolución adecuada de la identidad de los nombres de usuarios y grupos.

Google Cloud NetApp Volumes utiliza un valor de nombre de dominio de ID predeterminado estático de `defaultv4iddomain.com` . Los clientes NFS usan de manera predeterminada el nombre de dominio DNS para su configuración de nombre de dominio de ID, pero puede ajustar manualmente el nombre de dominio de ID en `/etc/idmapd.conf` .

Si LDAP está habilitado en Google Cloud NetApp Volumes, entonces Google Cloud NetApp Volumes automatiza el dominio de ID de NFS para cambiar a lo que está configurado para el dominio de búsqueda en DNS y los clientes no necesitarán modificarse a menos que usen nombres de búsqueda de dominio DNS diferentes.

Cuando Google Cloud NetApp Volumes puede resolver un nombre de usuario o un nombre de grupo en archivos locales o LDAP, se utiliza la cadena de dominio y los ID de dominio que no coinciden se reducen a nadie. Si Google Cloud NetApp Volumes no puede encontrar un nombre de usuario o un nombre de grupo en archivos locales o LDAP, se utiliza el valor de identificación numérica y el cliente NFS resuelve el nombre correctamente (esto es similar al comportamiento de NFSv3).

Sin cambiar el dominio de identificación NFSv4.1 del cliente para que coincida con el que usa el volumen de Google Cloud NetApp Volumes , verá el siguiente comportamiento:

- Los usuarios y grupos de UNIX con entradas locales en Google Cloud NetApp Volumes (como root, tal como se define en usuarios y grupos de UNIX locales) se reducen al valor nobody.
- Los usuarios y grupos de UNIX con entradas en LDAP (si Google Cloud NetApp Volumes está configurado para usar LDAP) se reducen a nadie si los dominios DNS son diferentes entre los clientes NFS y Google Cloud NetApp Volumes.
- Los usuarios y grupos de UNIX sin entradas locales o entradas LDAP utilizan el valor de identificación numérica y se resuelven en el nombre especificado en el cliente NFS. Si no existe ningún nombre en el cliente, solo se muestra el ID numérico.

A continuación se muestran los resultados del escenario anterior:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
```

```
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Cuando los dominios de identificación del cliente y del servidor coinciden, así es como se ve el mismo listado de archivos:

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Para obtener más información sobre este problema y cómo resolverlo, consulte la sección "NFSv4.1 y el usuario/grupo nobody . "

Dependencias de Kerberos

Si planea usar Kerberos con NFS, debe tener lo siguiente con Google Cloud NetApp Volumes:

- Dominio de Active Directory para los servicios del Centro de distribución Kerberos (KDC)
- Dominio de Active Directory con atributos de usuario y grupo rellenados con información de UNIX para la funcionalidad LDAP (NFS Kerberos en Google Cloud NetApp Volumes requiere una asignación de SPN de usuario a usuario de UNIX para una funcionalidad adecuada).
- LDAP habilitado en la instancia de Google Cloud NetApp Volumes
- Dominio de Active Directory para servicios DNS

NFSv4.1 y el usuario/grupo nobody

Uno de los problemas más comunes que se observan con una configuración NFSv4.1 es cuando un archivo o carpeta se muestra en una lista usando `ls` como propiedad de la `user:group` combinación de `nobody:nobody` .

Por ejemplo:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

Y el ID numérico es `99` .

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

En algunos casos, el archivo puede mostrar el propietario correcto, pero `nobody` como el grupo.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

¿Quién no es nadie?

El `nobody` El usuario en NFSv4.1 es diferente del `nfsnobody` usuario. Puede ver cómo un cliente NFS ve a cada usuario ejecutando el comando `id` dominio:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Con NFSv4.1, el `nobody` El usuario es el usuario predeterminado definido por el `idmapd.conf` archivo y se puede definir como cualquier usuario que desee utilizar.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

¿Por qué sucede esto?

Debido a que la seguridad a través del mapeo de cadenas de nombres es un principio clave de las operaciones de NFSv4.1, el comportamiento predeterminado cuando una cadena de nombres no coincide adecuadamente es convertir a ese usuario en uno que normalmente no tendrá acceso a los archivos y carpetas propiedad de usuarios y grupos.

Cuando veas `nobody` Para el usuario y/o grupo en las listas de archivos, esto generalmente significa que algo en NFSv4.1 está mal configurado. Aquí puede entrar en juego la distinción entre mayúsculas y minúsculas.

Por ejemplo, si user1@CVSDEMO.LOCAL (uid 1234, gid 1234) accede a una exportación, entonces Google Cloud NetApp Volumes debe poder encontrar user1@CVSDEMO.LOCAL (uid 1234, gid 1234). Si el usuario en Google Cloud NetApp Volumes es USER1@CVSDEMO.LOCAL, entonces no coincidirá (USER1 en mayúsculas versus usuario1 en minúsculas). En muchos casos, puede ver lo siguiente en el archivo de mensajes del cliente:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

Tanto el cliente como el servidor deben estar de acuerdo en que un usuario es realmente quien dice ser, por lo que debe verificar lo siguiente para asegurarse de que el usuario que ve el cliente tenga la misma información que el usuario que ve Google Cloud NetApp Volumes .

- **Dominio de identificación NFSv4.x.** Cliente: `idmapd.conf` archivo; Google Cloud NetApp Volumes utiliza `defaultv4iddomain.com` y no se puede cambiar manualmente. Si se usa LDAP con NFSv4.1, Google Cloud NetApp Volumes cambia el dominio de ID al que usa el dominio de búsqueda de DNS, que es el mismo que el dominio de AD.
- **Nombre de usuario e identificaciones numéricas.** Esto determina dónde el cliente busca nombres de usuario y aprovecha la configuración del conmutador de servicio de nombres: cliente: `nsswitch.conf` y/o archivos de grupo y contraseña locales; Google Cloud NetApp Volumes no permite modificaciones a esto, pero agrega automáticamente LDAP a la configuración cuando está habilitado.
- **Nombre del grupo e identificaciones numéricas.** Esto determina dónde el cliente busca nombres de grupos y aprovecha la configuración del conmutador de servicio de nombres: cliente: `nsswitch.conf` y/o archivos de grupo y contraseña locales; Google Cloud NetApp Volumes no permite modificaciones a esto, pero agrega automáticamente LDAP a la configuración cuando está habilitado.

En casi todos los casos, si ves `nobody` En las listas de usuarios y grupos de los clientes, el problema es la traducción del ID de dominio del nombre de usuario o grupo entre Google Cloud NetApp Volumes y el cliente NFS. Para evitar este escenario, utilice LDAP para resolver la información de usuarios y grupos entre clientes y Google Cloud NetApp Volumes.

Visualización de cadenas de identificación de nombre para NFSv4.1 en clientes

Si está utilizando NFSv4.1, hay una asignación de cadena de nombre que se lleva a cabo durante las operaciones de NFS, como se describió anteriormente.

Además de utilizar `/var/log/messages` Para encontrar un problema con los ID de NFSv4, puede utilizar el "nfsidmap -l" Comando en el cliente NFS para ver qué nombres de usuario se han asignado correctamente al dominio NFSv4.

Por ejemplo, este es el resultado del comando después de que un usuario que puede ser encontrado por el cliente y Google Cloud NetApp Volumes accede a un montaje NFSv4.x:

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Cuando un usuario no se asigna correctamente al dominio de ID NFSv4.1 (en este caso, `netapp-user`) intenta acceder al mismo montaje y toca un archivo, se les asigna `nobody:nobody` , como se esperaba.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
```

```
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

El `nfsidmap -l` La salida muestra al usuario `pcuser` en la pantalla pero no `netapp-user` ; este es el usuario anónimo en nuestra regla de política de exportación(`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" es un protocolo de red para compartir archivos desarrollado por Microsoft que ofrece autenticación centralizada de usuarios y grupos, permisos, bloqueo y uso compartido de archivos a múltiples clientes SMB a través de una red Ethernet. Los archivos y carpetas se presentan a los clientes mediante recursos compartidos, que pueden configurarse con diversas propiedades de uso compartido y ofrecen control de acceso mediante permisos de nivel de recurso compartido. SMB puede presentarse a cualquier cliente que admita el protocolo, incluidos los clientes de Windows, Apple y Linux.

Google Cloud NetApp Volumes proporciona compatibilidad con las versiones SMB 2.1 y 3.x del protocolo.

Control de acceso/recursos compartidos SMB

- Cuando un nombre de usuario de Windows solicita acceso al volumen de Google Cloud NetApp Volumes , Google Cloud NetApp Volumes busca un nombre de usuario de UNIX utilizando los métodos configurados por los administradores de Google Cloud NetApp Volumes .
- Si se configura un proveedor de identidad UNIX externo (LDAP) y los nombres de usuario de Windows/UNIX son idénticos, los nombres de usuario de Windows se asignarán 1:1 a los nombres de usuario de UNIX sin necesidad de ninguna configuración adicional. Cuando LDAP está habilitado, se utiliza Active Directory para alojar esos atributos UNIX para objetos de usuario y grupo.
- Si los nombres de Windows y los nombres de UNIX no coinciden de forma idéntica, se debe configurar LDAP para permitir que Google Cloud NetApp Volumes use la configuración de asignación de nombres LDAP (consulte la sección"Uso de LDAP para la asignación asimétrica de nombres").
- Si no se utiliza LDAP, los usuarios de SMB de Windows se asignan a un usuario UNIX local predeterminado llamado `pcuser` en Google Cloud NetApp Volumes. Esto significa archivos escritos en Windows por usuarios que se asignan a la `pcuser` mostrar la propiedad de UNIX como `pcuser` en

entornos NAS multiprotocolo. `pcuser` Aquí está efectivamente el `nobody` usuario en entornos Linux (UID 65534).

En implementaciones con solo SMB, el `pcuser` La asignación aún se realiza, pero no importará, porque la propiedad de los usuarios y grupos de Windows se muestra correctamente y no se permite el acceso NFS al volumen de solo SMB. Además, los volúmenes exclusivos de SMB no admiten la conversión a volúmenes NFS o de protocolo dual después de su creación.

Windows aprovecha Kerberos para la autenticación de nombre de usuario con los controladores de dominio de Active Directory, lo que requiere un intercambio de nombre de usuario y contraseña con los controladores de dominio de AD, que es externo a la instancia de Google Cloud NetApp Volumes . La autenticación Kerberos se utiliza cuando `\\SERVERNAME` Los clientes SMB utilizan la ruta UNC y se cumple lo siguiente:

- Existe una entrada DNS A/AAAA para SERVERNAME
- Existe un SPN válido para acceso SMB/CIFS para SERVERNAME

Cuando se crea un volumen SMB de Google Cloud NetApp Volumes , el nombre de la cuenta de la máquina se crea tal como se define en la sección"Cómo aparecen los Google Cloud NetApp Volumes en Active Directory." Ese nombre de cuenta de máquina también se convierte en la ruta de acceso al recurso compartido SMB porque Google Cloud NetApp Volumes aprovecha el DNS dinámico (DDNS) para crear las entradas A/AAAA y PTR necesarias en DNS y las entradas SPN necesarias en el principal de la cuenta de máquina.

> Para que se creen entradas PTR, la zona de búsqueda inversa de la dirección IP de la instancia de Google Cloud NetApp Volumes debe existir en el servidor DNS.

Por ejemplo, este volumen de Google Cloud NetApp Volumes utiliza la siguiente ruta de recurso compartido UNC: `\\cvs-east- 433d.cvsdemo.local` .

En Active Directory, estas son las entradas SPN generadas por Google Cloud NetApp Volumes:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Este es el resultado de la búsqueda directa/inversa de DNS:

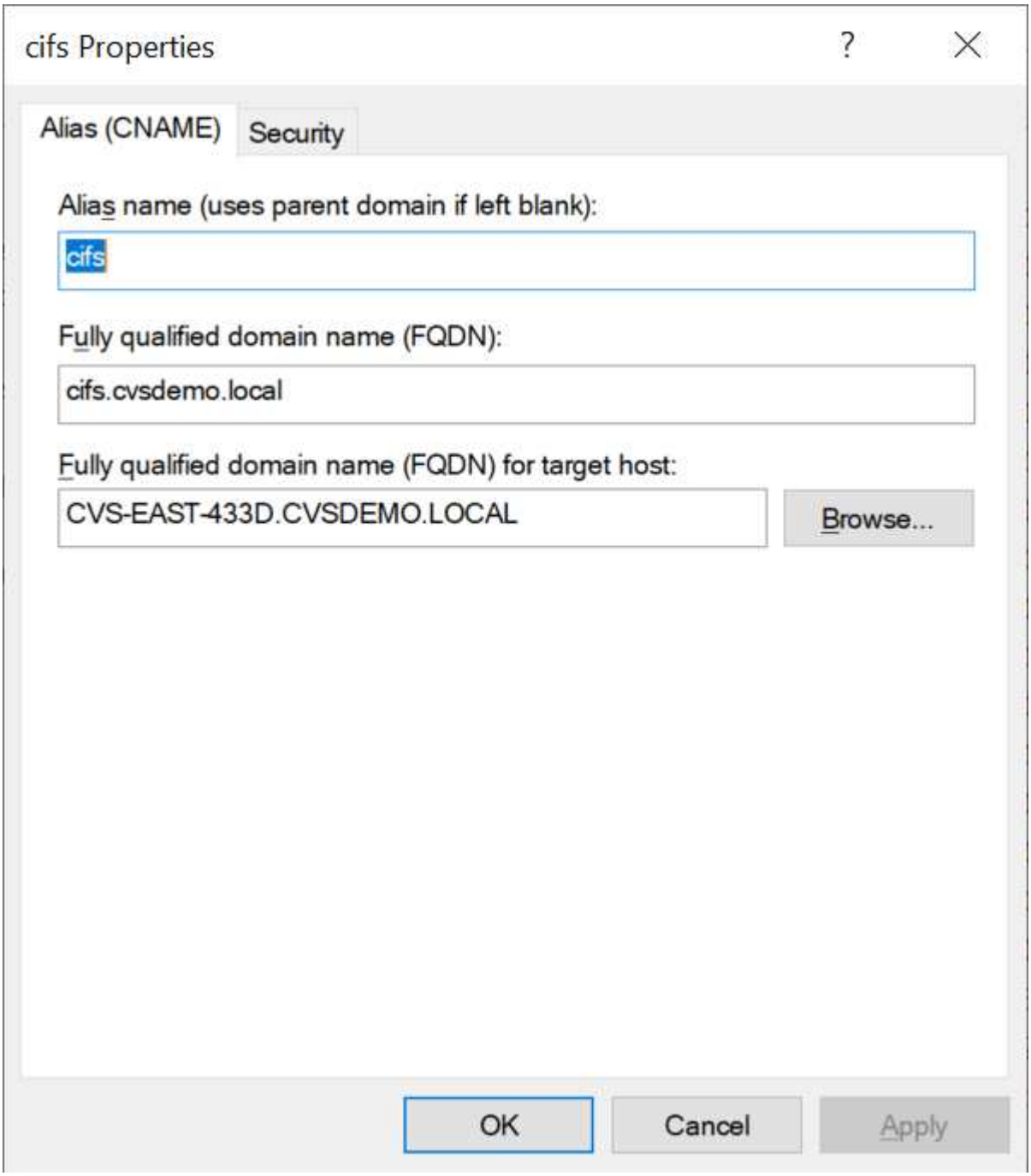
```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

De manera opcional, se puede aplicar un mayor control de acceso habilitando o requiriendo el cifrado SMB para los recursos compartidos SMB en Google Cloud NetApp Volumes. Si uno de los puntos finales no admite el cifrado SMB, no se permitirá el acceso.

Uso de alias de nombre SMB

En algunos casos, puede ser un problema de seguridad para los usuarios finales conocer el nombre de la cuenta de la máquina en uso para Google Cloud NetApp Volumes. En otros casos, es posible que simplemente desee proporcionar una ruta de acceso más sencilla a sus usuarios finales. En esos casos, puedes crear alias SMB.

Si desea crear alias para la ruta compartida SMB, puede aprovechar lo que se conoce como registro CNAME en DNS. Por ejemplo, si desea utilizar el nombre `\\CIFS` para acceder a acciones en lugar de `\\cvs-east-433d.cvsdemo.local` , pero aún desea utilizar la autenticación Kerberos, un CNAME en DNS que apunta al registro A/AAAA existente y un SPN adicional agregado a la cuenta de máquina existente proporciona acceso a Kerberos.



Este es el resultado de la búsqueda directa de DNS resultante después de agregar un CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Esta es la consulta SPN resultante después de agregar nuevos SPN:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

En una captura de paquetes, podemos ver la solicitud de configuración de sesión utilizando el SPN vinculado al CNAME.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

Dialectos de autenticación SMB

Google Cloud NetApp Volumes admite lo siguiente "dialectos" para la autenticación SMB:

- LM
- NTLM
- NTLMv2
- Kerberos

La autenticación Kerberos para el acceso a recursos compartidos SMB es el nivel de autenticación más seguro que puede utilizar. Con el cifrado AES y SMB habilitado, el nivel de seguridad aumenta aún más.

Google Cloud NetApp Volumes también admite compatibilidad con versiones anteriores para la autenticación LM y NTLM. Cuando Kerberos está mal configurado (por ejemplo al crear alias SMB), el acceso compartido recurre a métodos de autenticación más débiles (como NTLMv2). Debido a que estos mecanismos son menos seguros, están deshabilitados en algunos entornos de Active Directory. Si se deshabilitan los métodos de autenticación más débiles y Kerberos no está configurado correctamente, el acceso compartido falla porque

no hay un método de autenticación válido al cual recurrir.

Para obtener información sobre cómo configurar o visualizar los niveles de autenticación admitidos en Active Directory, consulte "Seguridad de la red: nivel de autenticación de LAN Manager" .

Modelos de permisos

Permisos de archivos/NTFS

Los permisos NTFS son los permisos que se aplican a los archivos y carpetas en los sistemas de archivos que adhieren a la lógica NTFS. Puede aplicar permisos NTFS en `Basic` o `Advanced` y se puede configurar para `Allow` o `Deny` para control de acceso.

Los permisos básicos incluyen lo siguiente:

- Control total
- Modificar
- Leer y ejecutar
- Leer
- Escribir

Cuando se establecen permisos para un usuario o grupo, denominado ACE, estos residen en una ACL. Los permisos NTFS utilizan los mismos conceptos básicos de lectura/escritura/ejecución que los bits del modo UNIX, pero también pueden extenderse a controles de acceso más granulares y extendidos (también conocidos como permisos especiales), como tomar propiedad, crear carpetas/agregar datos, escribir atributos y más.

Los bits del modo UNIX estándar no proporcionan el mismo nivel de granularidad que los permisos NTFS (como poder establecer permisos para usuarios individuales y objetos de grupo en una ACL o establecer atributos extendidos). Sin embargo, las ACL de NFSv4.1 proporcionan la misma funcionalidad que las ACL de NTFS.

Los permisos NTFS son más específicos que los permisos para compartir y se pueden utilizar junto con ellos. Con las estructuras de permisos NTFS, se aplica la opción más restrictiva. Como tal, las negaciones explícitas a un usuario o grupo anulan incluso el Control total al definir los derechos de acceso.

Los permisos NTFS se controlan desde los clientes SMB de Windows.

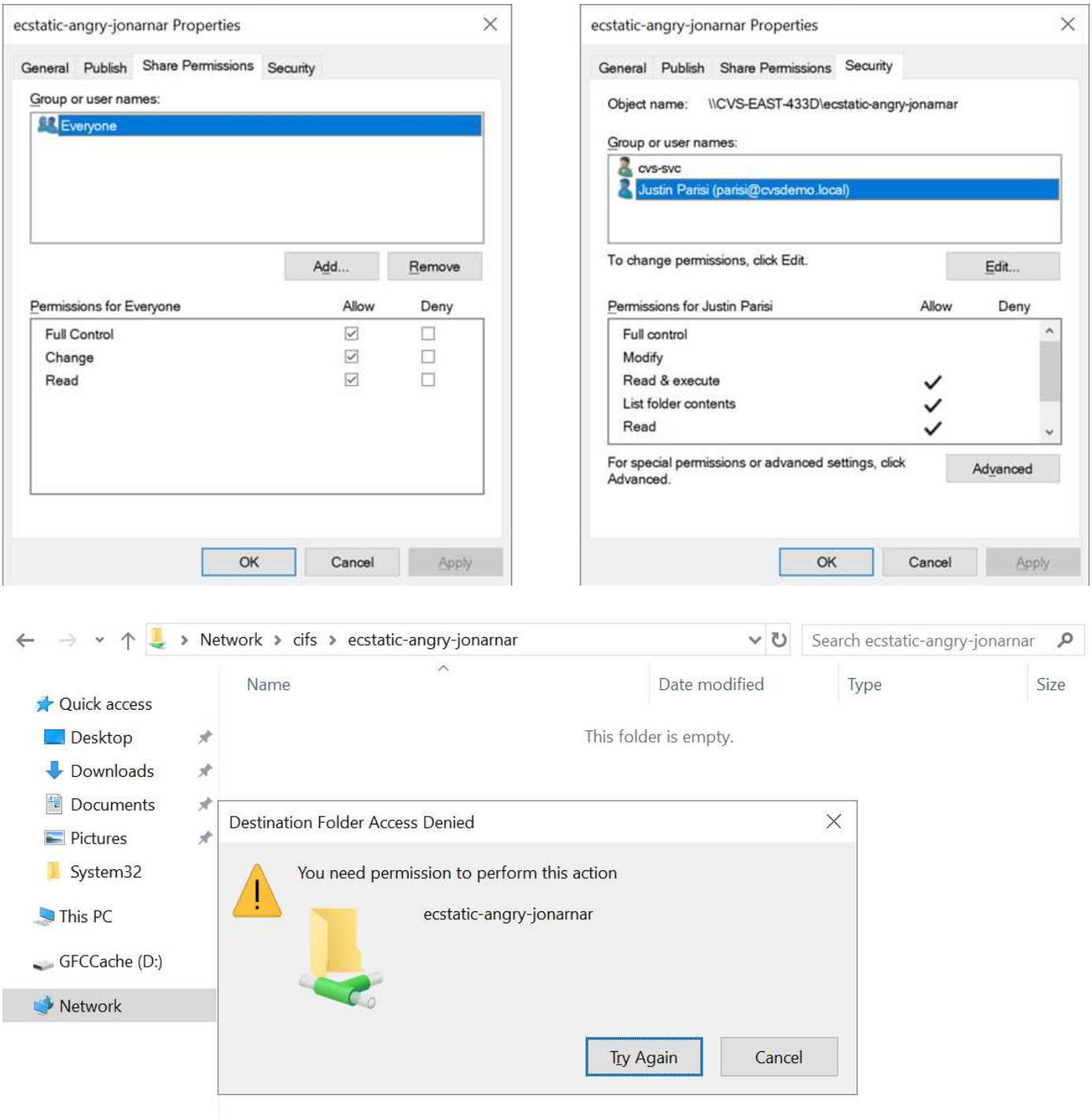
Permisos para compartir

Los permisos para compartir son más generales que los permisos NTFS (solo lectura/modificación/control total) y controlan la entrada inicial a un recurso compartido SMB, de forma similar a cómo funcionan las reglas de política de exportación de NFS.

Aunque las reglas de política de exportación de NFS controlan el acceso a través de información basada en host, como direcciones IP o nombres de host, los permisos de recursos compartidos SMB pueden controlar el acceso mediante el uso de ACE de usuario y grupo en una ACL de recursos compartidos. Puede configurar ACL de uso compartido desde el cliente de Windows o desde la interfaz de administración de Google Cloud NetApp Volumes .

De forma predeterminada, las ACL compartidas y las ACL de volumen inicial incluyen Todos con control total. Las ACL de archivo se deben cambiar, pero los permisos de uso compartido se ven anulados por los permisos de archivo de los objetos en el recurso compartido.

Por ejemplo, si a un usuario solo se le permite acceso de lectura a la ACL del archivo de volumen de Google Cloud NetApp Volumes , se le niega el acceso para crear archivos y carpetas incluso aunque la ACL del recurso compartido esté configurada en Todos con control total, como se muestra en la siguiente figura.



Para obtener mejores resultados de seguridad, haga lo siguiente:

- Eliminar a Todos de las listas de control de acceso (ACL) de archivos y recursos compartidos y, en su lugar, establecer el acceso a recursos compartidos para usuarios o grupos.
- Utilice grupos para el control de acceso en lugar de usuarios individuales para facilitar la administración y acelerar la eliminación o incorporación de usuarios para compartir ACL a través de la administración de grupos.

- Permitir un acceso compartido menos restrictivo y más general a las ACE en los permisos de uso compartido y bloquear el acceso a usuarios y grupos con permisos de archivo para un control de acceso más granular.
- Evite el uso general de ACL de denegación explícita, ya que anulan las ACL de autorización. Limite el uso de ACL de denegación explícita para usuarios o grupos a los que se les debe restringir el acceso a un sistema de archivos rápidamente.
- Asegúrese de prestar atención a la "Herencia de ACL" configuraciones al modificar permisos; configurar el indicador de herencia en el nivel superior de un directorio o volumen con una gran cantidad de archivos significa que cada archivo debajo de ese directorio o volumen tiene permisos heredados agregados a él, lo que puede crear un comportamiento no deseado, como acceso/denegación no deseados y una larga rotación de modificaciones de permisos a medida que se ajusta cada archivo.

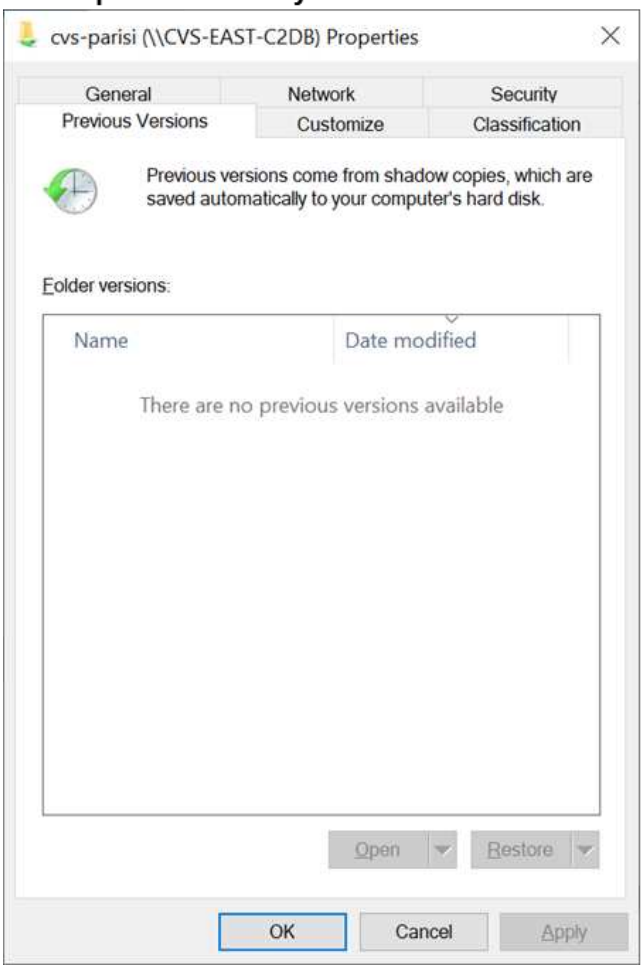
Funciones de seguridad para compartir SMB

Cuando crea por primera vez un volumen con acceso SMB en Google Cloud NetApp Volumes, se le presentan una serie de opciones para proteger ese volumen.

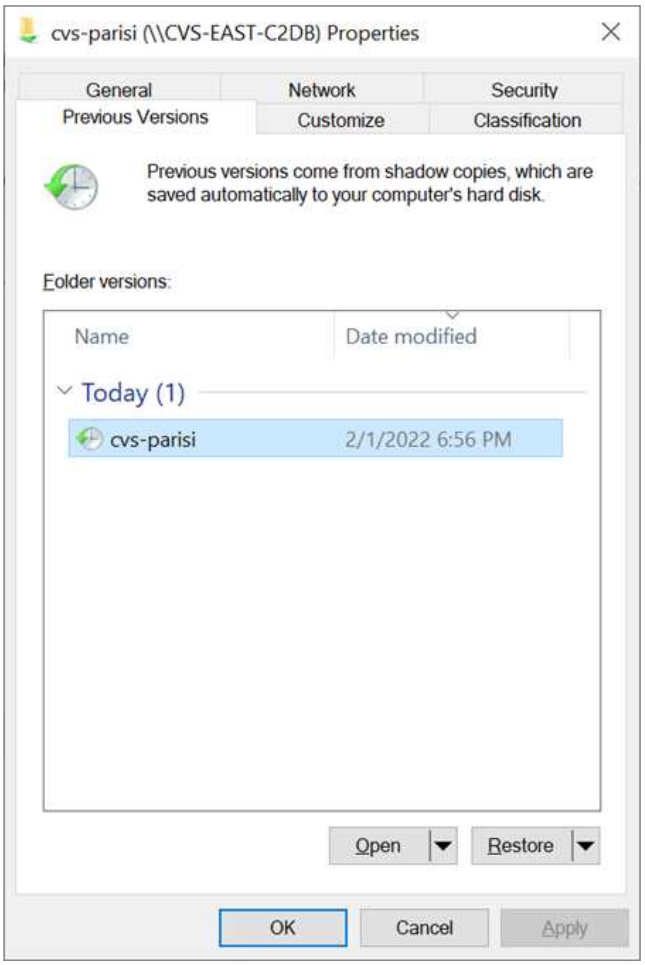
Algunas de estas opciones dependen del nivel de Google Cloud NetApp Volumes (Rendimiento o Software) y las opciones incluyen:

- **Hacer visible el directorio de instantáneas (disponible tanto para NetApp Volumes-Performance como para NetApp Volumes-SW).** Esta opción controla si los clientes SMB pueden acceder o no al directorio Snapshot en un recurso compartido SMB(`\\server\share\~snapshot` y/o pestaña Versiones Anteriores). La configuración predeterminada es No marcada, lo que significa que el volumen está predeterminado a ocultar y no permitir el acceso al mismo. `~snapshot` directorio y no aparecen copias de instantáneas en la pestaña Versiones anteriores para el volumen.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Es posible que sea conveniente ocultar copias instantáneas a los usuarios finales por razones de seguridad, de rendimiento (ocultar estas carpetas de los análisis de AV) o por preferencia. Las instantáneas de Google Cloud NetApp Volumes son de solo lectura, por lo que incluso si estas instantáneas son visibles, los usuarios finales no pueden eliminar ni modificar archivos en el directorio de instantáneas. Se aplican los permisos de archivo sobre los archivos o carpetas en el momento en que se tomó la copia instantánea. Si los permisos de un archivo o carpeta cambian entre copias de Instantánea, los cambios también se aplican a los archivos o carpetas en el directorio de Instantánea. Los usuarios y grupos pueden obtener acceso a estos archivos o carpetas según los permisos. Si bien no es posible eliminar ni modificar archivos en el directorio Snapshot, es posible copiar archivos o carpetas fuera de dicho directorio.

- **Habilitar el cifrado SMB (disponible tanto para NetApp Volumes-Performance como para NetApp Volumes-SW).** El cifrado SMB está deshabilitado en el recurso compartido SMB de manera predeterminada (sin marcar). Al marcar la casilla se habilita el cifrado SMB, lo que significa que el tráfico entre el cliente y el servidor SMB se cifra en tránsito con los niveles de cifrado admitidos más altos negociados. Google Cloud NetApp Volumes admite cifrado de hasta AES-256 para SMB. Habilitar el cifrado SMB implica una pérdida de rendimiento que puede o no ser perceptible para sus clientes SMB (aproximadamente del 10 al 20 %). NetApp recomienda encarecidamente realizar pruebas para ver si esa penalización de rendimiento es aceptable.
- **Ocultar recurso compartido SMB (disponible tanto para NetApp Volumes-Performance como para NetApp Volumes-SW).** Si configura esta opción, oculta la ruta compartida SMB de la navegación normal. Esto significa que los clientes que no conocen la ruta compartida no pueden ver los recursos compartidos cuando acceden a la ruta UNC predeterminada (como `\\NetApp Volumes-SMB`). Cuando se selecciona la casilla de verificación, solo los clientes que conocen explícitamente la ruta compartida de SMB o tienen la ruta compartida definida por un objeto de política de grupo pueden acceder a ella (seguridad mediante

ofuscación).

- **Habilitar enumeración basada en acceso (ABE) (solo NetApp Volumes-SW).** Esto es similar a ocultar el recurso compartido SMB, excepto que los recursos compartidos o archivos solo se ocultan para los usuarios o grupos que no tienen permisos para acceder a los objetos. Por ejemplo, si el usuario de Windows `joe` No se permite al menos el acceso de lectura a través de los permisos, entonces el usuario de Windows `joe` No puedo ver el recurso compartido SMB ni los archivos en absoluto. Esta opción está desactivada de forma predeterminada, pero puedes activarla seleccionando la casilla de verificación. Para obtener más información sobre ABE, consulte el artículo de la base de conocimientos de NetApp "¿Cómo funciona la enumeración basada en acceso (ABE)?"
- **Habilitar soporte para recursos compartidos de disponibilidad continua (CA) (solo NetApp Volumes-Performance).** "Acciones SMB disponibles continuamente" Proporcionar una manera de minimizar las interrupciones de las aplicaciones durante eventos de conmutación por error al replicar estados de bloqueo en todos los nodos del sistema back-end de Google Cloud NetApp Volumes . Esta no es una característica de seguridad, pero ofrece una mejor resistencia general. Actualmente, solo las aplicaciones SQL Server y FSLogix son compatibles con esta funcionalidad.

Acciones ocultas predeterminadas

Cuando se crea un servidor SMB en Google Cloud NetApp Volumes, hay "recursos compartidos administrativos ocultos" (utilizando la convención de nombres $) que se crean además del recurso compartido SMB del volumen de datos. Estos incluyen C$ (acceso a espacios de nombres) e IPC$ (canalizaciones con nombre compartido para la comunicación entre programas, como las llamadas a procedimientos remotos (RPC) utilizadas para el acceso a Microsoft Management Console (MMC)).

El recurso compartido IPC$ no contiene ACL de recursos compartidos y no se puede modificar; se utiliza estrictamente para llamadas RPC y "Windows no permite el acceso anónimo a estos recursos compartidos de forma predeterminada" .

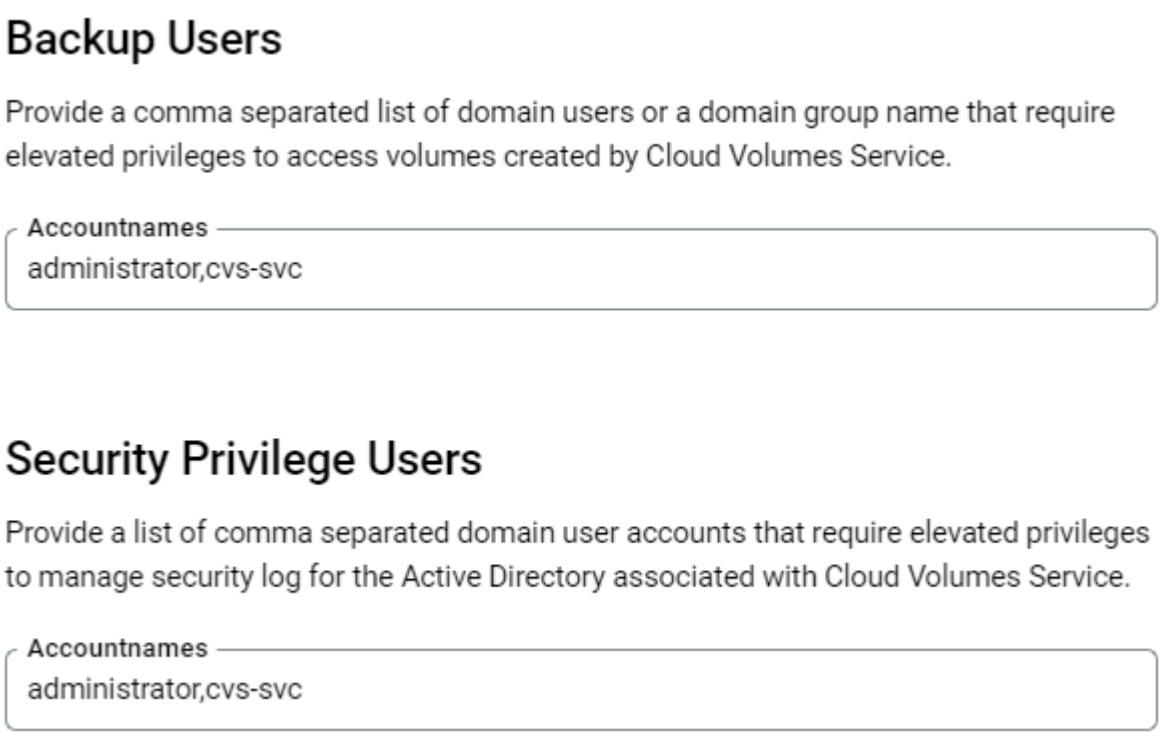
El recurso compartido C$ permite el acceso de BUILTIN/Administradores de manera predeterminada, pero la automatización de Google Cloud NetApp Volumes elimina la ACL del recurso compartido y no permite el acceso a nadie porque el acceso al recurso compartido C$ permite la visibilidad de todos los volúmenes montados en los sistemas de archivos de Google Cloud NetApp Volumes . Como resultado, los intentos de navegar hacia `\\SERVER\C$` fallar.

Cuentas con derechos de administrador/copia de seguridad locales/BUILTIN

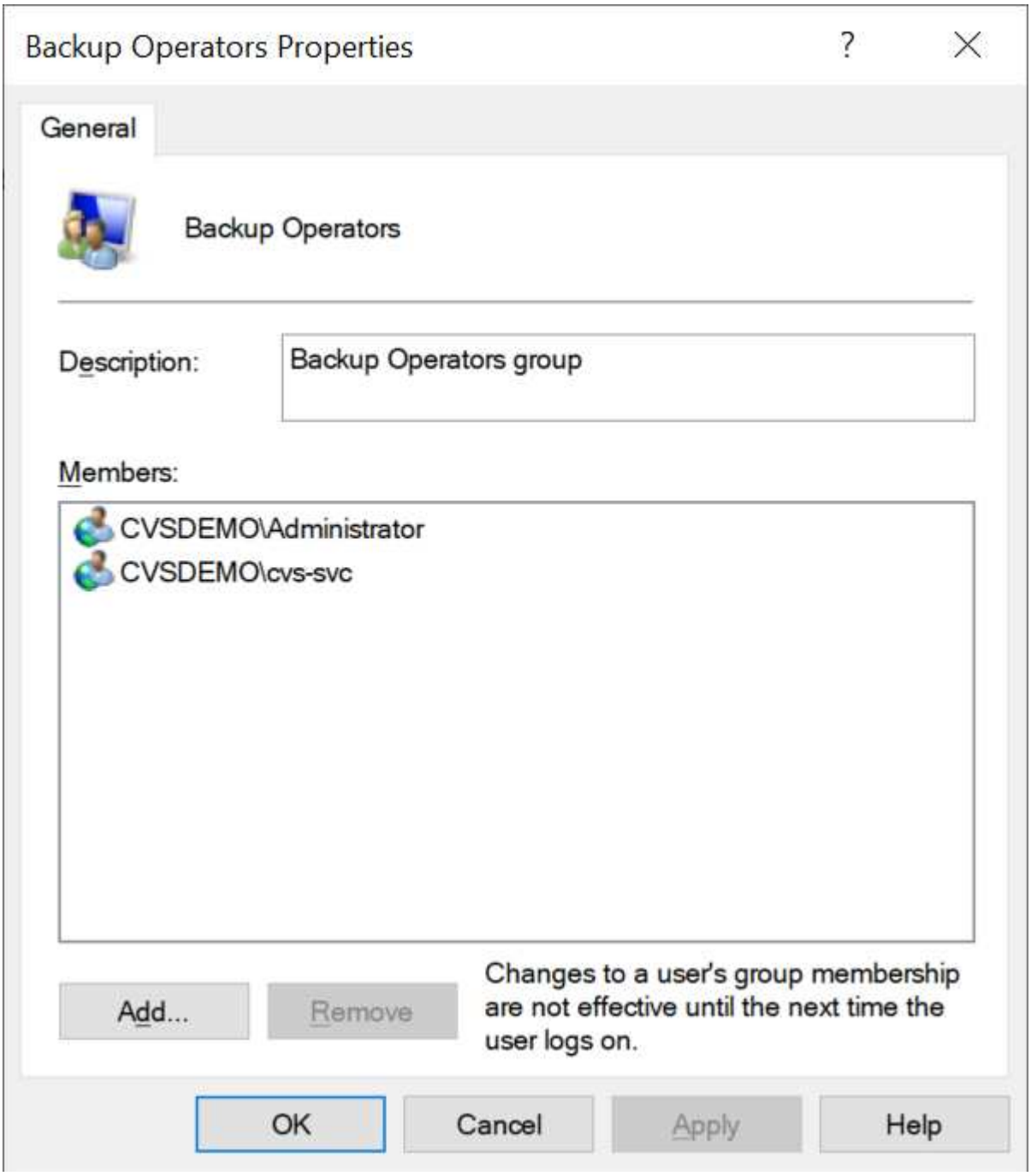
Los servidores SMB de Google Cloud NetApp Volumes mantienen una funcionalidad similar a la de los servidores SMB de Windows normales, ya que hay grupos locales (como BUILTIN\Administrators) que aplican derechos de acceso a usuarios y grupos de dominio seleccionados.

Cuando especifica que se agregará un usuario a Usuarios de respaldo, el usuario se agrega al grupo BUILTIN\Operadores de respaldo en la instancia de Google Cloud NetApp Volumes que usa esa conexión de Active Directory, que luego obtiene la "SeBackupPrivilege y SeRestorePrivilege" .

Cuando agrega un usuario a Usuarios con privilegios de seguridad, se le otorga al usuario el SeSecurityPrivilege, que es útil en algunos casos de uso de aplicaciones, como "SQL Server en recursos compartidos SMB" .



Puede ver las membresías del grupo local de Google Cloud NetApp Volumes a través de MMC con los privilegios adecuados. La siguiente figura muestra los usuarios que se agregaron mediante la consola de Google Cloud NetApp Volumes .

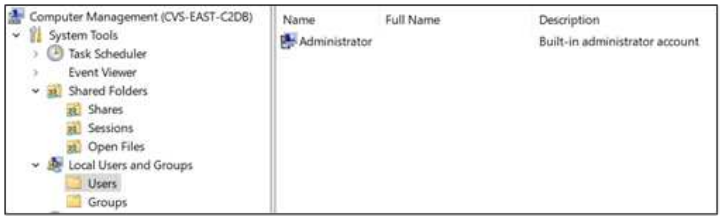


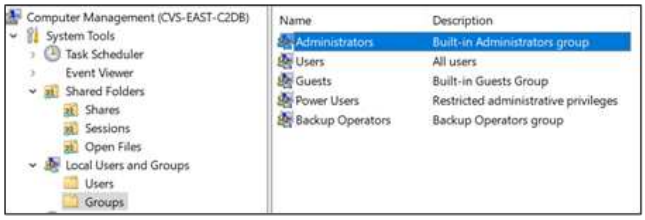
La siguiente tabla muestra la lista de grupos BUILTIN predeterminados y qué usuarios/grupos se agregan de forma predeterminada.

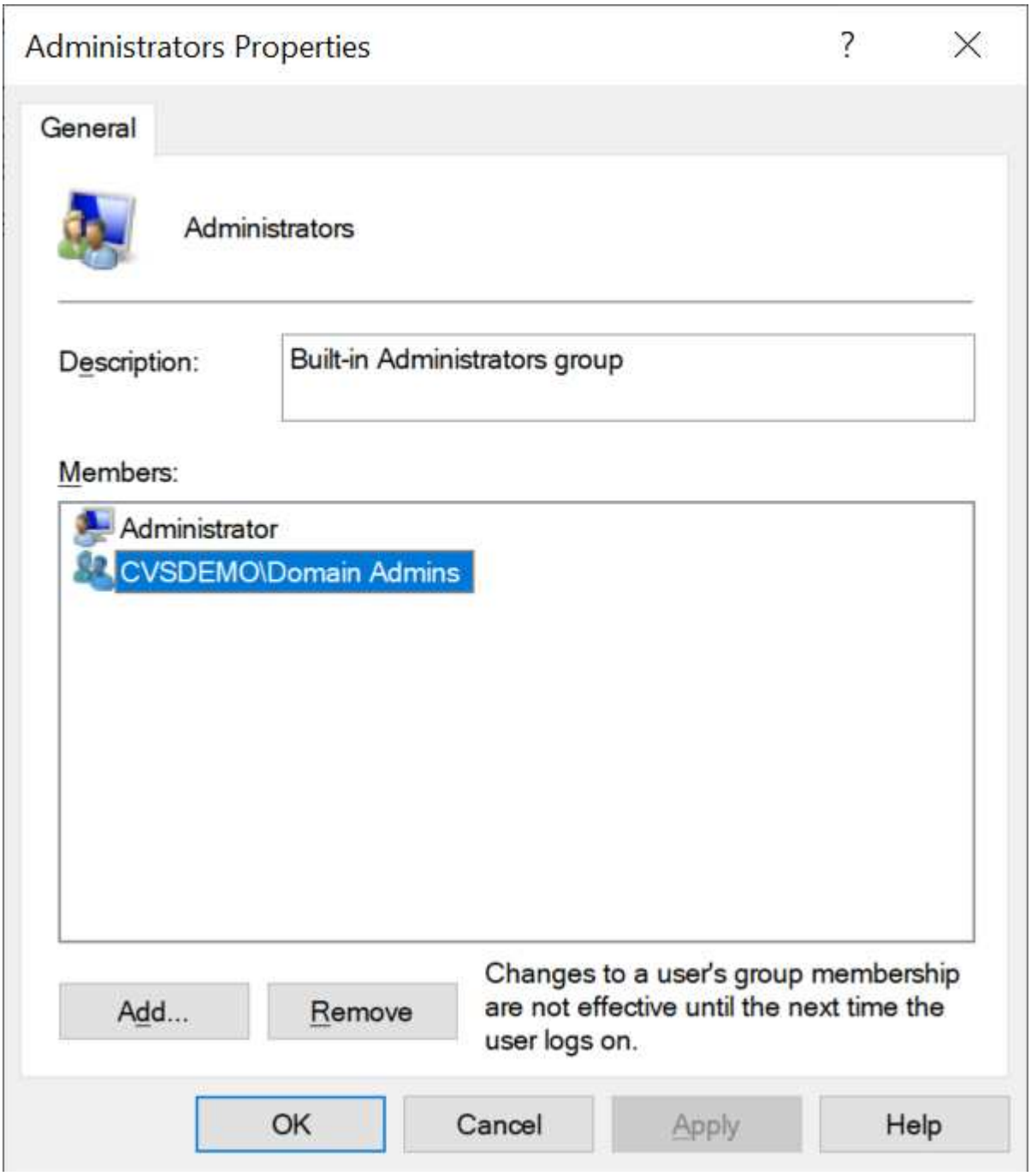
Grupo local/BUILTIN	Miembros predeterminados
BUILTIN\Administradores*	DOMINIO\Administradores del dominio
BUILTIN\Operadores de respaldo*	Ninguno
BUILTIN\Invitados	DOMINIO\Invitados del dominio
BUILTIN\Usuarios avanzados	Ninguno
Usuarios del dominio BUILTIN	DOMINIO\Usuarios del dominio

*Membresía de grupo controlada en la configuración de conexión de Active Directory de Google Cloud NetApp Volumes .

Puede ver usuarios y grupos locales (y miembros del grupo) en la ventana MMC, pero no puede agregar ni eliminar objetos ni cambiar membresías de grupos desde esta consola. De forma predeterminada, solo el grupo Administradores de dominio y el Administrador se agregan al grupo BUILTIN\Administrators en Google Cloud NetApp Volumes. Actualmente no puedes modificar esto.







Acceso a MMC/Administración de equipos

El acceso SMB en Google Cloud NetApp Volumes proporciona conectividad a la MMC de administración de equipos, lo que le permite ver recursos compartidos, administrar ACL de recursos compartidos, ver y administrar sesiones SMB y abrir archivos.

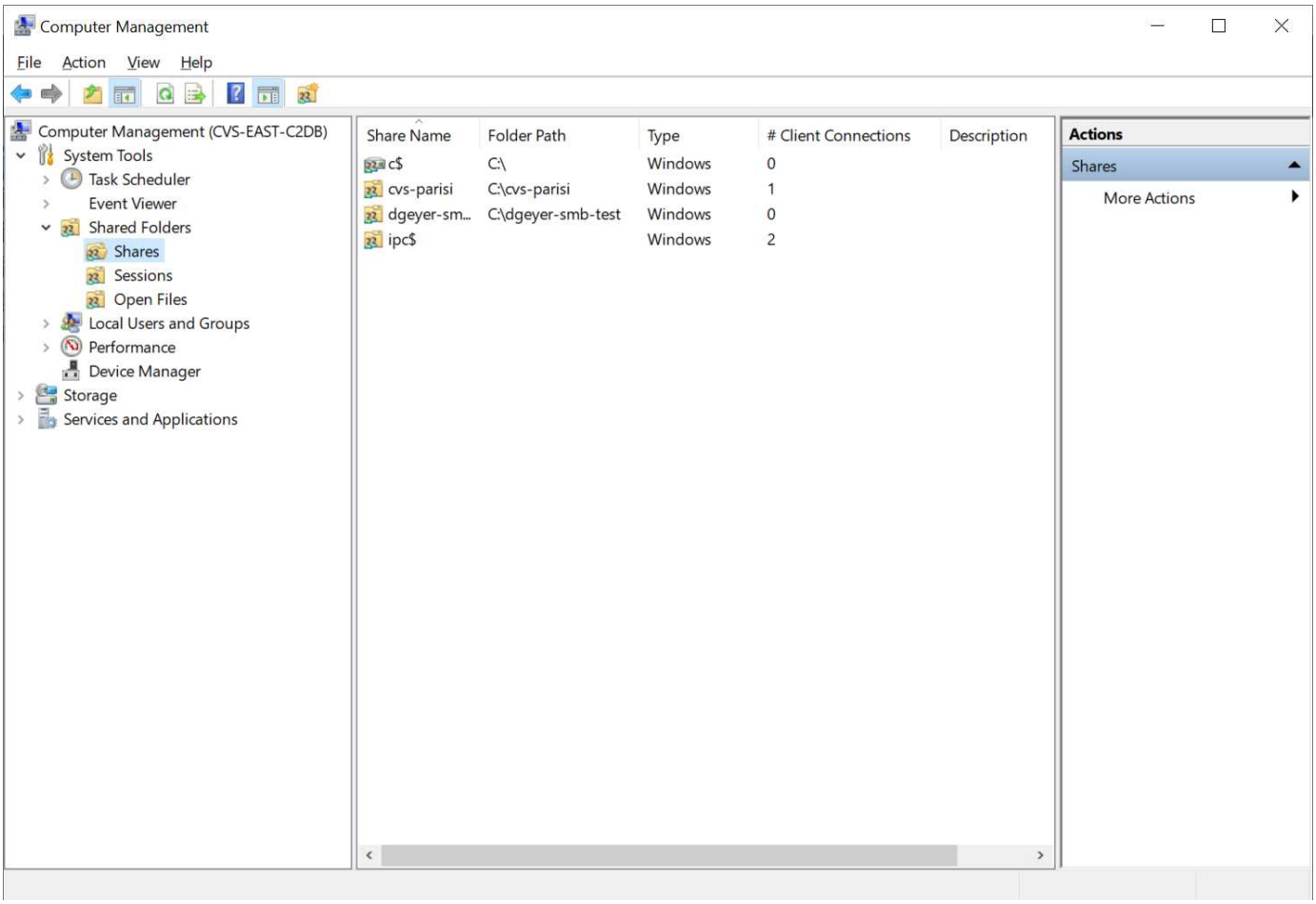
Para usar MMC para ver sesiones y recursos compartidos de SMB en Google Cloud NetApp Volumes, el usuario que inició sesión actualmente debe ser administrador de dominio. A otros usuarios se les permite acceder para ver o administrar el servidor SMB desde MMC y reciben un cuadro de diálogo No tiene permisos cuando intentan ver recursos compartidos o sesiones en la instancia SMB de Google Cloud NetApp Volumes .

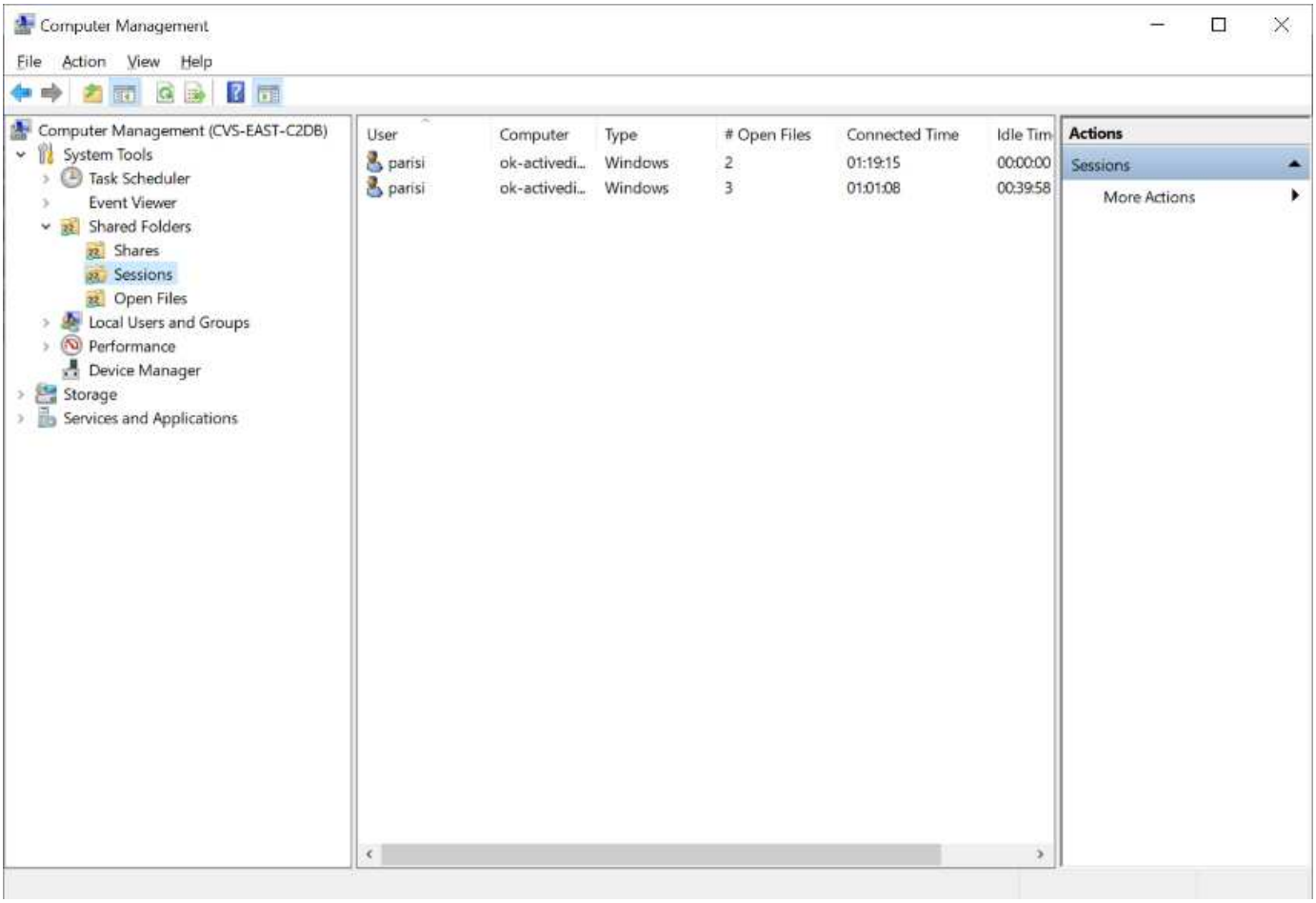
Para conectarse al servidor SMB, abra Administración de equipos, haga clic con el botón derecho en Administración de equipos y luego seleccione Conectarse a otro equipo. Esto abre el cuadro de diálogo Seleccionar computadora donde puede ingresar el nombre del servidor SMB (que se encuentra en la

información del volumen de Google Cloud NetApp Volumes).

Cuando visualiza recursos compartidos de SMB con los permisos adecuados, verá todos los recursos compartidos disponibles en la instancia de Google Cloud NetApp Volumes que comparten la conexión de Active Directory. Para controlar este comportamiento, configure la opción Ocultar recursos compartidos de SMB en la instancia de volumen de Google Cloud NetApp Volumes .

Recuerde que solo se permite una conexión de Active Directory por región.





La siguiente tabla muestra una lista de funcionalidades admitidas y no admitidas para MMC.

Funciones compatibles	Funciones no compatibles
• Ver acciones • Ver sesiones SMB activas • Ver archivos abiertos • Ver usuarios y grupos locales • Ver membresías de grupos locales • Enumerar la lista de sesiones, archivos y conexiones de árbol en el sistema • Cerrar archivos abiertos en el sistema • Cerrar sesiones abiertas • Crear/administrar recursos compartidos	• Creación de nuevos usuarios/grupos locales • Administrar/visualizar usuarios/grupos locales existentes • Ver eventos o registros de rendimiento • Administrar el almacenamiento • Gestión de servicios y aplicaciones

Información de seguridad del servidor SMB

El servidor SMB en Google Cloud NetApp Volumes utiliza una serie de opciones que definen políticas de seguridad para las conexiones SMB, incluidas cosas como el desfase del reloj de Kerberos, la antigüedad de los tickets, el cifrado y más.

La siguiente tabla contiene una lista de esas opciones, lo que hacen, las configuraciones predeterminadas y si

se pueden modificar con Google Cloud NetApp Volumes. Algunas opciones no se aplican a Google Cloud NetApp Volumes.

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Desfase máximo del reloj Kerberos (minutos)	Desfase temporal máximo entre los Google Cloud NetApp Volumes y los controladores de dominio. Si el desfase horario supera los 5 minutos, la autenticación Kerberos falla. Esto se establece en el valor predeterminado de Active Directory.	5	No
Duración del ticket Kerberos (horas)	Tiempo máximo que un ticket Kerberos permanece válido antes de requerir una renovación. Si no se produce la renovación antes de las 10 horas, deberá obtener un nuevo billete. Google Cloud NetApp Volumes realiza estas renovaciones automáticamente. 10 horas es el valor predeterminado de Active Directory.	10	No
Renovación máxima de tickets Kerberos (días)	Número máximo de días que se puede renovar un ticket Kerberos antes de que sea necesaria una nueva solicitud de autorización. Google Cloud NetApp Volumes renueva automáticamente los tickets para conexiones SMB. Siete días es el valor predeterminado de Active Directory.	7	No
Tiempo de espera de conexión de Kerberos KDC (segundos)	La cantidad de segundos que deben transcurrir antes de que se agote el tiempo de conexión de un KDC.	3	No

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Requerir firma para tráfico SMB entrante	Configuración para requerir firma para tráfico SMB. Si se establece como verdadero, los clientes que no admiten la firma no podrán conectarse.	FALSO	
Requerir complejidad de contraseña para cuentas de usuario locales	Se utiliza para contraseñas de usuarios SMB locales. Google Cloud NetApp Volumes no admite la creación de usuarios locales, por lo que esta opción no se aplica a Google Cloud NetApp Volumes.	Verdadero	No
Utilice start_tls para conexiones LDAP de Active Directory	Se utiliza para habilitar el inicio de conexiones TLS para Active Directory LDAP. Google Cloud NetApp Volumes actualmente no permite habilitar esta función.	FALSO	No
¿Está habilitado el cifrado AES-128 y AES-256 para Kerberos?	Esto controla si se utiliza el cifrado AES para las conexiones de Active Directory y se controla con la opción Habilitar cifrado AES para la autenticación de Active Directory al crear o modificar la conexión de Active Directory.	FALSO	Sí
Nivel de compatibilidad de LM	Nivel de dialectos de autenticación admitidos para conexiones de Active Directory. Ver la sección "Dialectos de autenticación SMB " para obtener más información.	ntlmv2-krb	No

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Requerir cifrado SMB para el tráfico CIFS entrante	Requiere cifrado SMB para todos los recursos compartidos. Google Cloud NetApp Volumes no utiliza esto; en su lugar, configure el cifrado por volumen (consulte la sección "Funciones de seguridad para compartir SMB ").	FALSO	No
Seguridad de la sesión del cliente	Establece la firma y/o sellado para la comunicación LDAP. Esto no está configurado actualmente en Google Cloud NetApp Volumes, pero podría ser necesario en futuras versiones para solucionar este problema. La solución para los problemas de autenticación LDAP debido al parche de Windows se cubre en la sección"Vinculación de canal LDAP." .	Ninguno	No
Habilitación de SMB2 para conexiones de CC	Utiliza SMB2 para conexiones de CC. Habilitado por defecto.	Valor predeterminado del sistema	No
Búsqueda de referencias LDAP	Al utilizar varios servidores LDAP, la búsqueda de referencias permite que el cliente haga referencia a otros servidores LDAP de la lista cuando no se encuentra una entrada en el primer servidor. Esto actualmente no es compatible con Google Cloud NetApp Volumes.	FALSO	No
Utilice LDAPS para conexiones seguras de Active Directory	Permite el uso de LDAP sobre SSL. Actualmente no es compatible con Google Cloud NetApp Volumes.	FALSO	No

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Se requiere cifrado para la conexión DC	Requiere cifrado para conexiones DC exitosas. Deshabilitado de forma predeterminada en Google Cloud NetApp Volumes.	FALSO	No

Protocolo dual/multiprotocolo

Google Cloud NetApp Volumes ofrece la posibilidad de compartir los mismos conjuntos de datos tanto con clientes SMB como NFS, manteniendo al mismo tiempo los permisos de acceso adecuados ("protocolo dual"). Esto se consigue coordinando la asignación de identidades entre los protocolos y utilizando un servidor LDAP centralizado para proporcionar las identidades UNIX a Google Cloud NetApp Volumes. Puedes usar Windows Active Directory para proporcionar tanto usuarios de Windows como de UNIX y así facilitar su uso.

Control de acceso

- **Compartir controles de acceso.** Determinar qué clientes y/o usuarios y grupos pueden acceder a un recurso compartido NAS. Para NFS, las políticas y reglas de exportación controlan el acceso de los clientes a las exportaciones. Las exportaciones de NFS se administran desde la instancia de Google Cloud NetApp Volumes . SMB utiliza recursos compartidos CIFS/SMB y ACL compartidos para brindar un control más granular a nivel de usuario y grupo. Solo puede configurar ACL de nivel de recurso compartido desde clientes SMB mediante https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html [MMC/Administración de equipos^] con una cuenta que tenga derechos de administrador en la instancia de Google Cloud NetApp Volumes (consulte el enlace de la sección: gcp-gcnv-smb.html#Cuentas con derechos de administrador/copia de seguridad locales/BUILTIN["Cuentas con derechos de administrador/copia de seguridad locales/BUILTIN."]).
- **Controles de acceso a archivos.** Los permisos se controlan a nivel de archivo o carpeta y siempre se administran desde el cliente NAS. Los clientes NFS pueden utilizar bits de modo tradicional (rwx) o ACL NFSv4. Los clientes SMB aprovechan los permisos NTFS.

El control de acceso a los volúmenes que sirven datos tanto a NFS como a SMB depende del protocolo en uso. Para obtener información sobre los permisos con protocolo dual, consulte la sección "Modelo de permiso ."

Mapeo de usuarios

Cuando un cliente accede a un volumen, Google Cloud NetApp Volumes intenta asignar el usuario entrante a un usuario válido en la dirección opuesta. Esto es necesario para determinar el acceso adecuado en todos los protocolos y para garantizar que el usuario que solicita acceso es realmente quien dice ser.

Por ejemplo, si un usuario de Windows llamado `joe` intenta acceder a un volumen con permisos UNIX a través de SMB, luego Google Cloud NetApp Volumes realiza una búsqueda para encontrar un usuario UNIX correspondiente llamado `joe` . Si existe, entonces los archivos que se escriben en un recurso compartido SMB como usuario de Windows `joe` aparece como usuario UNIX `joe` de clientes NFS.

Alternativamente, si un usuario de UNIX llamado `joe` intenta acceder a un volumen de Google Cloud NetApp Volumes con permisos de Windows, entonces el usuario de UNIX debe poder asignarse a un usuario de

Windows válido. De lo contrario, se deniega el acceso al volumen.

Actualmente, solo se admite Active Directory para la gestión externa de identidades UNIX con LDAP. Para obtener más información sobre cómo configurar el acceso a este servicio, consulta "Creación de una conexión AD".

Modelo de permiso

Al utilizar configuraciones de protocolo dual, Google Cloud NetApp Volumes utiliza estilos de seguridad para volúmenes para determinar el tipo de ACL. Estos estilos de seguridad se configuran según el protocolo NAS especificado o, en el caso de un protocolo dual, es una elección que se realiza al momento de crear el volumen de Google Cloud NetApp Volumes .

- Si solo usa NFS, los volúmenes de Google Cloud NetApp Volumes usan permisos UNIX.
- Si solo usa SMB, los volúmenes de Google Cloud NetApp Volumes usan permisos NTFS.

Si está creando un volumen de protocolo dual, puede elegir el estilo de ACL al crear el volumen. Esta decisión debe tomarse en función de la gestión de permisos deseada. Si sus usuarios administran permisos desde clientes Windows/SMB, seleccione NTFS. Si sus usuarios prefieren utilizar clientes NFS y chmod/chown, utilice estilos de seguridad UNIX.

Consideraciones para crear conexiones de Active Directory

Google Cloud NetApp Volumes brinda la posibilidad de conectar su instancia de Google Cloud NetApp Volumes a un servidor externo de Active Directory para la administración de identidades para usuarios de SMB y UNIX. Es necesario crear una conexión de Active Directory para usar SMB en Google Cloud NetApp Volumes.

La configuración para esto proporciona varias opciones que requieren cierta consideración por motivos de seguridad. El servidor externo de Active Directory puede ser una instancia local o nativa de la nube. Si está utilizando un servidor Active Directory local, no exponga el dominio a la red externa (por ejemplo, con una DMZ o una dirección IP externa). En su lugar, utilice túneles privados seguros o VPN, confianzas de bosque unidireccionales o conexiones de red dedicadas a las redes locales con "Acceso privado a Google" . Consulte la documentación de Google Cloud para obtener más información sobre "Mejores prácticas para usar Active Directory en Google Cloud" .

> NetApp Volumes-SW requiere que los servidores de Active Directory estén ubicados en la misma región. Si se intenta una conexión DC en NetApp Volumes-SW a otra región, el intento falla. Al utilizar NetApp Volumes-SW, asegúrese de crear sitios de Active Directory que incluyan los DC de Active Directory y luego especifique los sitios en Google Cloud NetApp Volumes para evitar intentos de conexión de DC entre regiones.

Credenciales de Active Directory

Cuando SMB o LDAP para NFS está habilitado, Google Cloud NetApp Volumes interactúa con los controladores de Active Directory para crear un objeto de cuenta de máquina para usar en la autenticación. Esto no es diferente de cómo un cliente SMB de Windows se une a un dominio y requiere los mismos derechos de acceso a las unidades organizativas (OU) en Active Directory.

En muchos casos, los grupos de seguridad no permiten el uso de una cuenta de administrador de Windows en servidores externos como Google Cloud NetApp Volumes. En algunos casos, el usuario Administrador de Windows se deshabilita por completo como práctica recomendada de seguridad.

Permisos necesarios para crear cuentas de máquinas SMB

Para agregar objetos de máquina de Google Cloud NetApp Volumes a un Active Directory, se necesita una cuenta que tenga derechos administrativos en el dominio o "permisos delegados para crear y modificar objetos de cuenta de máquina" Se requiere una OU específica. Puede hacer esto con el Asistente para delegación de control en Active Directory creando una tarea personalizada que proporcione a un usuario acceso para la creación o eliminación de objetos de computadora con los siguientes permisos de acceso proporcionados:

- Leer/Escribir
- Crear/eliminar todos los objetos secundarios
- Leer/escribir todas las propiedades
- Cambiar/Restablecer contraseña

Al hacer esto, se agrega automáticamente una ACL de seguridad para el usuario definido a la OU en Active Directory y se minimiza el acceso al entorno de Active Directory. Una vez delegado un usuario, ese nombre de usuario y contraseña se pueden proporcionar como credenciales de Active Directory en esta ventana.



El nombre de usuario y la contraseña que se pasan al dominio de Active Directory aprovechan el cifrado Kerberos durante la consulta y creación de objetos de la cuenta de la máquina para mayor seguridad.

Detalles de la conexión de Active Directory

El "Detalles de la conexión de Active Directory" proporciona orientación para que los administradores den información específica del esquema de Active Directory para la colocación de cuentas de máquina, como la siguiente:

- **Tipo de conexión de Active Directory.** Se utiliza para especificar si la conexión de Active Directory en una región se utiliza para volúmenes de tipo de servicio Google Cloud NetApp Volumes o NetApp Volumes-Performance. Si esta configuración se configura incorrectamente en una conexión existente, es posible que no funcione correctamente al usarla o editarla.
- **Dominio.** El nombre de dominio de Active Directory.
- **Sitio.** Limita los servidores de Active Directory a un sitio específico por seguridad y rendimiento "Consideraciones". Esto es necesario cuando varios servidores de Active Directory abarcan regiones porque Google Cloud NetApp Volumes no admite actualmente permitir solicitudes de autenticación de Active Directory a servidores de Active Directory en una región diferente a la instancia de Google Cloud NetApp Volumes. (Por ejemplo, el controlador de dominio de Active Directory está en una región que solo NetApp Volumes-Performance admite, pero quieres un recurso compartido SMB en una instancia de NetApp Volumes-SW.)
- **Servidores DNS.** Servidores DNS para utilizar en búsquedas de nombres.
- **Nombre NetBIOS (opcional).** Si lo desea, el nombre NetBIOS del servidor. Esto es lo que se utiliza cuando se crean nuevas cuentas de máquina mediante la conexión de Active Directory. Por ejemplo, si el nombre NetBIOS se establece en NetApp Volumes-EAST, los nombres de las cuentas de la máquina serán NetApp Volumes-EAST-{1234}. Ver la sección"Cómo aparecen los Google Cloud NetApp Volumes en Active Directory" Para más información.
- **Unidad organizativa (OU).** La unidad organizativa específica para crear la cuenta de computadora. Esto es útil si está delegando el control a un usuario para cuentas de máquina en una unidad organizativa específica.
- **Cifrado AES.** También puede marcar o desmarcar la casilla de verificación Habilitar cifrado AES para

autenticación de AD. Habilitar el cifrado AES para la autenticación de Active Directory proporciona seguridad adicional para la comunicación de Google Cloud NetApp Volumes con Active Directory durante las búsquedas de usuarios y grupos. Antes de habilitar esta opción, consulte con su administrador de dominio para confirmar que los controladores de dominio de Active Directory admiten la autenticación AES.

> De forma predeterminada, la mayoría de los servidores Windows no deshabilitan cifrados más débiles (como DES o RC4-HMAC), pero si elige deshabilitar cifrados más débiles, confirme que la conexión de Active Directory de Google Cloud NetApp Volumes se haya configurado para habilitar AES. De lo contrario, se producen fallos de autenticación. Habilitar el cifrado AES no deshabilita los cifrados más débiles, sino que agrega compatibilidad con cifrados AES a la cuenta de máquina SMB de Google Cloud NetApp Volumes .

Detalles del dominio Kerberos

Esta opción no se aplica a servidores SMB. Más bien, se utiliza al configurar NFS Kerberos para el sistema Google Cloud NetApp Volumes . Cuando se completan estos detalles, se configura el dominio NFS Kerberos (similar a un archivo krb5.conf en Linux) y se utiliza cuando se especifica NFS Kerberos en la creación del volumen de Google Cloud NetApp Volumes , ya que la conexión de Active Directory actúa como Centro de distribución NFS Kerberos (KDC).

> Actualmente, los KDC que no son de Windows no son compatibles con Google Cloud NetApp Volumes.

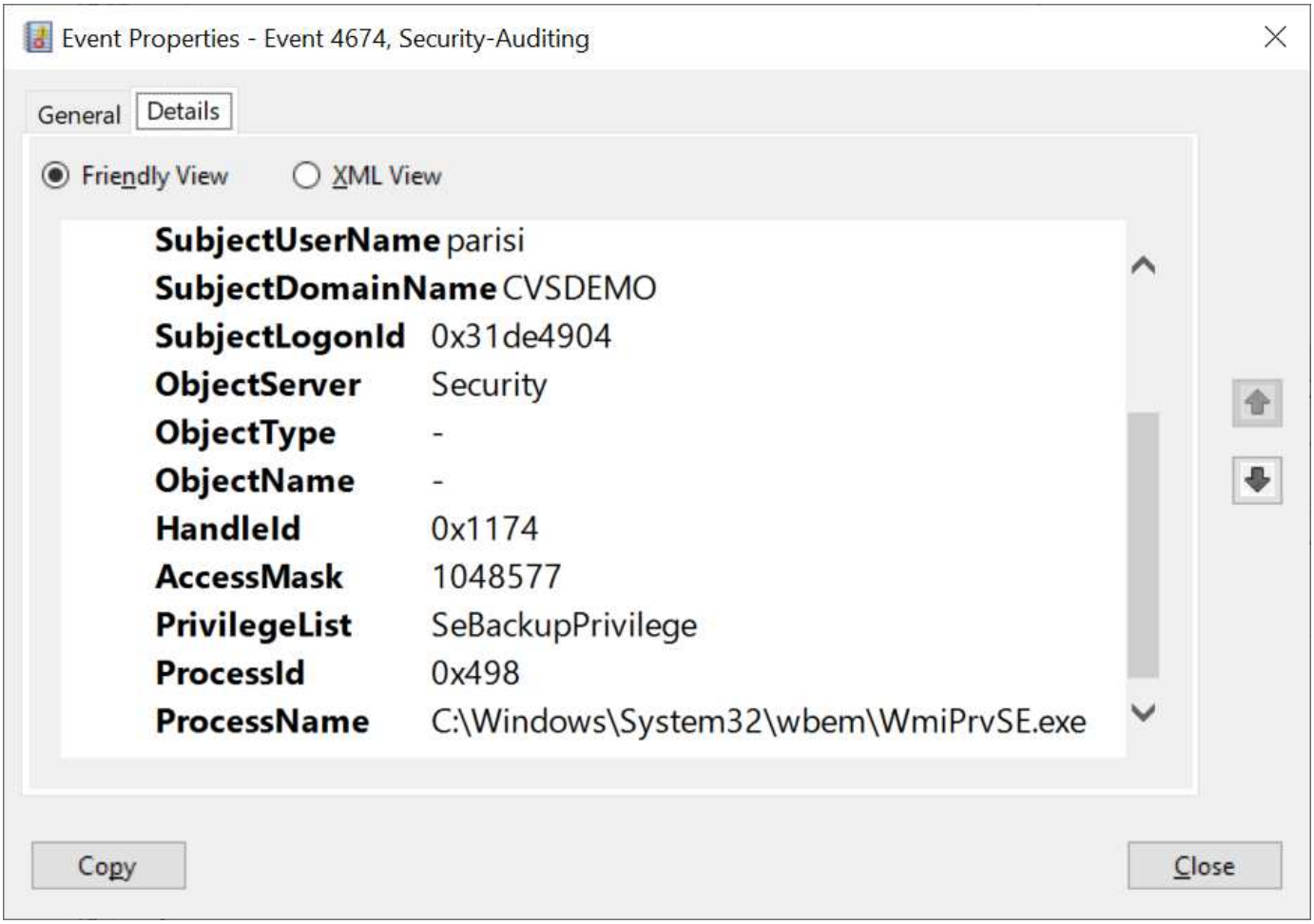
Región

Una región le permite especificar la ubicación donde reside la conexión de Active Directory. Esta región debe ser la misma región que el volumen Google Cloud NetApp Volumes .

- **Usuarios NFS locales con LDAP.** En esta sección, también hay una opción para Permitir usuarios NFS locales con LDAP. Esta opción debe dejarse sin seleccionar si desea ampliar el soporte de membresía de grupos de usuarios de UNIX más allá de la limitación de 16 grupos de NFS (grupos extendidos). Sin embargo, el uso de grupos extendidos requiere un servidor LDAP configurado para identidades UNIX. Si no tiene un servidor LDAP, deje esta opción sin seleccionar. Si tiene un servidor LDAP y también desea utilizar usuarios UNIX locales (como root), seleccione esta opción.

Usuarios de respaldo

Esta opción le permite especificar los usuarios de Windows que tienen permisos de respaldo en el volumen de Google Cloud NetApp Volumes . Los privilegios de respaldo (SeBackupPrivilege) son necesarios para que algunas aplicaciones realicen copias de seguridad y restauren correctamente los datos en volúmenes NAS. Este usuario tiene un alto nivel de acceso a los datos en el volumen, por lo que debe considerar "Habilitar la auditoría del acceso de ese usuario" . Una vez habilitado, los eventos de auditoría se muestran en Visor de eventos > Registros de Windows > Seguridad.



Usuarios con privilegios de seguridad

Esta opción le permite especificar usuarios de Windows que tienen permisos de modificación de seguridad en el volumen de Google Cloud NetApp Volumes . Los privilegios de seguridad (SeSecurityPrivilege) son necesarios para algunas aplicaciones("como SQL Server") para configurar correctamente los permisos durante la instalación. Este privilegio es necesario para administrar el registro de seguridad. Aunque este privilegio no es tan poderoso como SeBackupPrivilege, NetApp recomienda "auditar el acceso de los usuarios" con este nivel de privilegio si es necesario.

Para obtener más información, consulte "Privilegios especiales asignados al nuevo inicio de sesión" .

Cómo aparecen los Google Cloud NetApp Volumes en Active Directory

Los Google Cloud NetApp Volumes aparecen en Active Directory como un objeto de cuenta de máquina normal. Las convenciones de nomenclatura son las siguientes:

- CIFS/SMB y NFS Kerberos crean objetos de cuenta de máquina separados.
- NFS con LDAP habilitado crea una cuenta de máquina en Active Directory para enlaces LDAP de Kerberos.
- Los volúmenes de protocolo dual con LDAP comparten la cuenta de máquina CIFS/SMB para LDAP y SMB.
- Las cuentas de máquina CIFS/SMB utilizan una convención de nombres de NOMBRE-1234 (ID aleatoria de cuatro dígitos con guion agregado a cada nombre de <10 caracteres) para la cuenta de máquina. Puede definir NOMBRE mediante la configuración del nombre NetBIOS en la conexión de Active Directory

(consulte la sección "Detalles de la conexión de Active Directory ").

- NFS Kerberos utiliza NFS-NAME-1234 como convención de nomenclatura (hasta 15 caracteres). Si se utilizan más de 15 caracteres, el nombre es NFS-TRUNCATED-NAME-1234.
- Las instancias de NetApp Volumes-Performance solo para NFS con LDAP habilitado crean una cuenta de máquina SMB para vincularse al servidor LDAP con la misma convención de nombres que las instancias CIFS/SMB.
- Cuando se crea una cuenta de máquina SMB, se ocultan los recursos compartidos de administrador predeterminados (consulte la sección"Acciones ocultas predeterminadas") también se crean (c$, admin$, ipc$), pero esos recursos compartidos no tienen ACL asignadas y son inaccesibles.
- Los objetos de la cuenta de la máquina se colocan en CN=Computers de manera predeterminada, pero puede especificar una OU diferente cuando sea necesario. Ver la sección "Permisos necesarios para crear cuentas de máquinas SMB " para obtener información sobre qué derechos de acceso se necesitan para agregar o eliminar objetos de cuenta de máquina para Google Cloud NetApp Volumes.

Cuando Google Cloud NetApp Volumes agrega la cuenta de máquina SMB a Active Directory, se completan los siguientes campos:

- cn (con el nombre del servidor SMB especificado)
- dNSHostName (con SMBserver.domain.com)
- msDS-SupportedEncryptionTypes (permite DES_CBC_MD5, RC4_HMAC_MD5 si el cifrado AES no está habilitado; si el cifrado AES está habilitado, se permiten DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 para el intercambio de tickets Kerberos con la cuenta de la máquina para SMB)
- nombre (con el nombre del servidor SMB)
- sAMAccountName (con SMBserver$)
- servicePrincipalName (con los SPN host/smbserver.domain.com y host/smbserver para Kerberos)

Si desea deshabilitar tipos de cifrado Kerberos más débiles (enctype) en la cuenta de la máquina, puede cambiar el valor msDS-SupportedEncryptionTypes en la cuenta de la máquina a uno de los valores de la siguiente tabla para permitir solo AES.

Valor de msDS-SupportedEncryptionTypes	Enctype habilitado
2	DES_CBC_MD5
4	RC4_HMAC
8	Sólo AES128_CTS_HMAC_SHA1_96
16	Sólo AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 y AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 y AES256_CTS_HMAC_SHA1_96

Para habilitar el cifrado AES para las cuentas de máquinas SMB, haga clic en Habilitar cifrado AES para la autenticación de AD al crear la conexión de Active Directory.

Para activar el cifrado AES para NFS Kerberos, "Consulte la documentación de Google Cloud NetApp Volumes".

Otras dependencias del servicio de infraestructura NAS (KDC, LDAP y DNS)

Al utilizar Google Cloud NetApp Volumes para recursos compartidos NAS, es posible que se requieran dependencias externas para un funcionamiento adecuado. Estas dependencias entran en juego en circunstancias específicas. La siguiente tabla muestra varias opciones de configuración y qué dependencias, si las hay, son necesarias.

Configuración	Dependencias requeridas
Sólo NFSv3	Ninguno
Solo Kerberos NFSv3	Directorio activo de Windows: * KDC * DNS * LDAP
Sólo NFSv4.1	Configuración de mapeo de ID de cliente (/etc/idmap.conf)
NFSv4.1 solo Kerberos	• Configuración de mapeo de ID de cliente (/etc/idmap.conf) • Directorio activo de Windows: KDC DNS LDAP
Solo para PYMES	Directorio activo: * KDC * DNS
NAS multiprotocolo (NFS y SMB)	• Configuración de mapeo de ID de cliente (solo NFSv4.1; /etc/idmap.conf) • Directorio activo de Windows: KDC DNS LDAP

Rotación de claves Kerberos y restablecimiento de contraseñas para objetos de cuenta de máquina

Con las cuentas de máquinas SMB, Google Cloud NetApp Volumes programa restablecimientos periódicos de contraseñas para la cuenta de la máquina SMB. Estos restablecimientos de contraseña se realizan mediante el cifrado Kerberos y funcionan según un cronograma cada cuarto domingo a una hora aleatoria entre las 11 p. m. y la 1 a. m. Estos restablecimientos de contraseña cambian las versiones de clave Kerberos, rotan las tablas de claves almacenadas en el sistema Google Cloud NetApp Volumes y ayudan a mantener un mayor nivel de seguridad para los servidores SMB que se ejecutan en Google Cloud NetApp Volumes. Las contraseñas de las cuentas de la máquina son aleatorias y los administradores no las conocen.

En el caso de las cuentas de máquinas NFS Kerberos, los restablecimientos de contraseñas se realizan únicamente cuando se crea o intercambia una nueva tabla de claves con el KDC. Actualmente, esto no es posible hacerlo en Google Cloud NetApp Volumes.

Puertos de red para usar con LDAP y Kerberos

Al utilizar LDAP y Kerberos, debes determinar los puertos de red que usan estos servicios. Puedes encontrar una lista completa de los puertos que utiliza Google Cloud NetApp Volumes en "Documentación de Google Cloud NetApp Volumes sobre consideraciones de seguridad".

LDAP

Google Cloud NetApp Volumes actúa como un cliente LDAP y utiliza consultas de búsqueda LDAP estándar para búsquedas de usuarios y grupos de identidades UNIX. LDAP es necesario si pretende utilizar usuarios y grupos fuera de los usuarios predeterminados estándar proporcionados por Google Cloud NetApp Volumes. LDAP también es necesario si planea utilizar NFS Kerberos con principales de usuario (como usuario1@dominio.com). Actualmente, solo se admite LDAP mediante Microsoft Active Directory.

Para utilizar Active Directory como un servidor LDAP de UNIX, debe completar los atributos UNIX necesarios

en los usuarios y grupos que desea utilizar para las identidades UNIX. Google Cloud NetApp Volumes utiliza una plantilla de esquema LDAP predeterminada que consulta atributos en función de "RFC-2307-bis" . Como resultado, la siguiente tabla muestra los atributos mínimos necesarios de Active Directory que se deben completar para usuarios y grupos y para qué se utiliza cada atributo.

Para obtener más información sobre cómo configurar los atributos LDAP en Active Directory, consulta "Gestión de acceso de protocolo dual."

Atributo	Qué hace
fluido*	Especifica el nombre de usuario de UNIX
uidNumber*	Especifica el ID numérico del usuario de UNIX
gidNumber*	Especifica el ID numérico del grupo principal del usuario de UNIX
claseObjeto*	Especifica qué tipo de objeto se está utilizando; Google Cloud NetApp Volumes requiere que "usuario" esté incluido en la lista de clases de objetos (se incluye en la mayoría de las implementaciones de Active Directory de manera predeterminada).
nombre	Información general sobre la cuenta (nombre real, número de teléfono, etc., también conocidos como gecos)
Contraseña de usuario de Unix	No es necesario configurar esto; no se utiliza en búsquedas de identidad de UNIX para la autenticación NAS. Al configurar esto, el valor unixUserPassword configurado se coloca en texto sin formato.
DirectorioInicio de Unix	Define la ruta a los directorios de inicio de UNIX cuando un usuario se autentica contra LDAP desde un cliente Linux. Configure esto si desea utilizar LDAP para la funcionalidad del directorio de inicio de UNIX.
loginShell	Define la ruta al shell bash/profile para clientes Linux cuando un usuario se autentica contra LDAP.

*Indica que el atributo es necesario para el correcto funcionamiento de Google Cloud NetApp Volumes. Los atributos restantes son solo para uso del lado del cliente.

Atributo	Qué hace
cn*	Especifica el nombre del grupo UNIX. Al utilizar Active Directory para LDAP, esto se configura cuando se crea el objeto por primera vez, pero se puede cambiar más tarde. Este nombre no puede ser el mismo que el de otros objetos. Por ejemplo, si su usuario UNIX llamado user1 pertenece a un grupo llamado user1 en su cliente Linux, Windows no permite dos objetos con el mismo atributo cn. Para solucionar esto, cambie el nombre del usuario de Windows a un nombre único (como user1-UNIX); LDAP en Google Cloud NetApp Volumes usa el atributo uid para los nombres de usuario de UNIX.
gidNumber*	Especifica el ID numérico del grupo UNIX.
claseObjeto*	Especifica qué tipo de objeto se está utilizando; Google Cloud NetApp Volumes requiere que el grupo se incluya en la lista de clases de objetos (este atributo se incluye en la mayoría de las implementaciones de Active Directory de manera predeterminada).
Uid del miembro	Especifica qué usuarios de UNIX son miembros del grupo UNIX. Con Active Directory LDAP en Google Cloud NetApp Volumes, este campo no es necesario. El esquema LDAP de Google Cloud NetApp Volumes utiliza el campo Miembro para las membresías de grupos.
Miembro*	Requerido para membresías de grupos/grupos secundarios de UNIX. Este campo se completa agregando usuarios de Windows a grupos de Windows. Sin embargo, si los grupos de Windows no tienen atributos UNIX poblados, no se incluyen en las listas de membresía de grupos de usuarios de UNIX. Cualquier grupo que necesite estar disponible en NFS debe completar los atributos de grupo UNIX requeridos que se enumeran en esta tabla.

*Indica que el atributo es necesario para el correcto funcionamiento de Google Cloud NetApp Volumes. Los atributos restantes son solo para uso del lado del cliente.

Información de enlace LDAP

Para consultar usuarios en LDAP, Google Cloud NetApp Volumes debe vincularse (iniciar sesión) al servicio LDAP. Este inicio de sesión tiene permisos de solo lectura y se utiliza para consultar atributos LDAP UNIX para búsquedas de directorio. Actualmente, los enlaces LDAP solo son posibles mediante el uso de una cuenta de máquina SMB.

Sólo puede habilitar LDAP para `NetApp Volumes-Performance` instancias y utilícelo para volúmenes NFSv3, NFSv4.1 o de protocolo dual. Se debe establecer una conexión de Active Directory en la misma región que el volumen de Google Cloud NetApp Volumes para una implementación exitosa del volumen habilitado para LDAP.

Cuando LDAP está habilitado, ocurre lo siguiente en escenarios específicos.

- Si solo se usa NFSv3 o NFSv4.1 para el proyecto de Google Cloud NetApp Volumes , se crea una nueva cuenta de máquina en el controlador de dominio de Active Directory y el cliente LDAP en Google Cloud NetApp Volumes se vincula a Active Directory mediante las credenciales de la cuenta de máquina. No se crean recursos compartidos SMB para el volumen NFS y los recursos compartidos administrativos ocultos predeterminados (consulte la sección"Acciones ocultas predeterminadas") se han eliminado las ACL compartidas.
- Si se utilizan volúmenes de protocolo dual para el proyecto Google Cloud NetApp Volumes , solo se utiliza la cuenta de máquina única creada para el acceso SMB para vincular el cliente LDAP en Google Cloud NetApp Volumes a Active Directory. No se crean cuentas de máquina adicionales.
- Si los volúmenes SMB dedicados se crean por separado (antes o después de habilitar los volúmenes NFS con LDAP), la cuenta de la máquina para los enlaces LDAP se comparte con la cuenta de la máquina SMB.
- Si NFS Kerberos también está habilitado, se crean dos cuentas de máquina: una para recursos compartidos SMB y/o enlaces LDAP y otra para la autenticación NFS Kerberos.

Consultas LDAP

Aunque los enlaces LDAP están cifrados, las consultas LDAP se transmiten a través de la red en texto sin formato mediante el puerto LDAP común 389. Actualmente, este puerto conocido no se puede cambiar en Google Cloud NetApp Volumes. Como resultado, alguien con acceso al rastreo de paquetes en la red puede ver nombres de usuarios y grupos, identificaciones numéricas y membresías de grupos.

Sin embargo, las máquinas virtuales de Google Cloud no pueden detectar el tráfico de unidifusión de otras máquinas virtuales. Solo las máquinas virtuales que participan activamente en el tráfico LDAP (es decir, que pueden vincularse) pueden ver el tráfico del servidor LDAP. Para obtener más información sobre la detección de paquetes en Google Cloud NetApp Volumes, consulte la sección"Consideraciones sobre rastreo y detección de paquetes."

Valores predeterminados de configuración del cliente LDAP

Cuando LDAP está habilitado en una instancia de Google Cloud NetApp Volumes , se crea una configuración de cliente LDAP con detalles de configuración específicos de forma predeterminada. En algunos casos, las opciones no se aplican a Google Cloud NetApp Volumes (no son compatibles) o no son configurables.

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Lista de servidores LDAP	Establece nombres de servidor LDAP o direcciones IP que se utilizarán para consultas. Esto no se utiliza para Google Cloud NetApp Volumes. En su lugar, se utiliza el dominio de Active Directory para definir servidores LDAP.	No establecido	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Dominio de Active Directory	Establece el dominio de Active Directory que se utilizará para las consultas LDAP. Google Cloud NetApp Volumes aprovecha los registros SRV para LDAP en DNS para encontrar servidores LDAP en el dominio.	Establezca el dominio de Active Directory especificado en la conexión de Active Directory.	No
Servidores de Active Directory preferidos	Establece los servidores de Active Directory preferidos para utilizar con LDAP. No compatible con Google Cloud NetApp Volumes. En su lugar, utilice sitios de Active Directory para controlar la selección del servidor LDAP.	No establecido.	No
Vincular mediante credenciales de servidor SMB	Se vincula a LDAP mediante la cuenta de la máquina SMB. Actualmente, el único método de enlace LDAP compatible con Google Cloud NetApp Volumes.	Verdadero	No
Plantilla de esquema	La plantilla de esquema utilizada para consultas LDAP.	MS-AD-BIS	No
Puerto del servidor LDAP	El número de puerto utilizado para consultas LDAP. Actualmente, Google Cloud NetApp Volumes solo utiliza el puerto LDAP estándar 389. LDAPS/puerto 636 no es compatible actualmente.	389	No
¿Está habilitado LDAPS?	Controla si se utiliza LDAP sobre Secure Sockets Layer (SSL) para consultas y enlaces. Actualmente no es compatible con Google Cloud NetApp Volumes.	FALSO	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Tiempo de espera de consulta (seg.)	Tiempo de espera para consultas. Si las consultas tardan más que el valor especificado, las consultas fallan.	3	No
Nivel mínimo de autenticación de enlace	El nivel de enlace mínimo admitido. Debido a que Google Cloud NetApp Volumes usa cuentas de máquinas para enlaces LDAP y Active Directory no admite enlaces anónimos de manera predeterminada, esta opción no entra en juego por cuestiones de seguridad.	Anónimo	No
Vincular DN	El nombre de usuario/distinguido (DN) utilizado para los enlaces cuando se utiliza el enlace simple. Google Cloud NetApp Volumes usa cuentas de máquina para enlaces LDAP y actualmente no admite la autenticación de enlace simple.	No establecido	No
DN base	El DN base utilizado para búsquedas LDAP.	El dominio de Windows utilizado para la conexión de Active Directory, en formato DN (es decir, DC=dominio, DC=local).	No
Alcance de búsqueda base	El ámbito de búsqueda para búsquedas de DN base. Los valores pueden incluir base, un nivel o subárbol. Google Cloud NetApp Volumes solo admite búsquedas de subárboles.	Subárbol	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
DN de usuario	Define el DN donde comienzan las búsquedas del usuario para las consultas LDAP. Actualmente no es compatible con Google Cloud NetApp Volumes, por lo que todas las búsquedas de usuarios comienzan en el DN base.	No establecido	No
Ámbito de búsqueda del usuario	El ámbito de búsqueda para búsquedas de DN de usuario. Los valores pueden incluir base, un nivel o subárbol. Google Cloud NetApp Volumes no admite la configuración del alcance de búsqueda del usuario.	Subárbol	No
DN de grupo	Define el DN donde comienzan las búsquedas de grupo para las consultas LDAP. Actualmente no es compatible con Google Cloud NetApp Volumes, por lo que todas las búsquedas de grupos comienzan en el DN base.	No establecido	No
Ámbito de búsqueda de grupo	El ámbito de búsqueda para búsquedas de DN de grupo. Los valores pueden incluir base, un nivel o subárbol. Google Cloud NetApp Volumes no admite la configuración del alcance de búsqueda de grupo.	Subárbol	No
DN del grupo de red	Define el DN donde comienzan las búsquedas del grupo de red para las consultas LDAP. Actualmente no es compatible con Google Cloud NetApp Volumes, por lo que todas las búsquedas de grupos de redes comienzan en el DN base.	No establecido	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Ámbito de búsqueda del grupo de red	El ámbito de búsqueda para búsquedas de DN de grupos de red. Los valores pueden incluir base, un nivel o subárbol. Google Cloud NetApp Volumes no admite la configuración del alcance de búsqueda del grupo de redes.	Subárbol	No
Utilice start_tls sobre LDAP	Aprovecha Start TLS para conexiones LDAP basadas en certificados a través del puerto 389. Actualmente no es compatible con Google Cloud NetApp Volumes.	FALSO	No
Habilitar la búsqueda de grupo de red por host	Permite realizar búsquedas de grupos de redes por nombre de host en lugar de expandir los grupos de redes para enumerar a todos los miembros. Actualmente no es compatible con Google Cloud NetApp Volumes.	FALSO	No
DN de grupo de red por host	Define el DN donde se inician las búsquedas de grupo de red por host para las consultas LDAP. Actualmente, Netgroup-by-host no es compatible con Google Cloud NetApp Volumes.	No establecido	No
Ámbito de búsqueda de grupo de red por host	El ámbito de búsqueda para búsquedas de DN de grupo de red por host. Los valores pueden incluir base, un nivel o subárbol. Actualmente, Netgroup-by-host no es compatible con Google Cloud NetApp Volumes.	Subárbol	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Seguridad de la sesión del cliente	Define qué nivel de seguridad de sesión utiliza LDAP (firma, sello o ninguno). NetApp Volumes-Performance admite la firma LDAP, si Active Directory lo solicita. NetApp Volumes-SW no admite la firma LDAP. Actualmente no se admite el sellado para ninguno de los dos tipos de servicio.	Ninguno	No
Búsqueda de referencias LDAP	Al utilizar varios servidores LDAP, la búsqueda de referencias permite que el cliente haga referencia a otros servidores LDAP de la lista cuando no se encuentra una entrada en el primer servidor. Esto actualmente no es compatible con Google Cloud NetApp Volumes.	FALSO	No
Filtro de membresía de grupo	Proporciona un filtro de búsqueda LDAP personalizado que se puede utilizar al buscar membresías de grupos desde un servidor LDAP. Actualmente no es compatible con Google Cloud NetApp Volumes.	No establecido	No

Uso de LDAP para la asignación asimétrica de nombres

Google Cloud NetApp Volumes, de forma predeterminada, asigna usuarios de Windows y usuarios de UNIX con nombres de usuario idénticos de forma bidireccional sin necesidad de una configuración especial. Siempre que Google Cloud NetApp Volumes pueda encontrar un usuario UNIX válido (con LDAP), se produce una asignación de nombre 1:1. Por ejemplo, si el usuario de Windows `johnsmith` Se utiliza entonces si Google Cloud NetApp Volumes puede encontrar un usuario de UNIX llamado `johnsmith` En LDAP, la asignación de nombres se realiza correctamente para ese usuario y todos los archivos y carpetas creados por él. `johnsmith` Muestra la propiedad correcta del usuario y todas las ACL que lo afectan. `johnsmith` se respetan independientemente del protocolo NAS en uso. Esto se conoce como mapeo de nombres simétrico.

La asignación de nombres asimétrica ocurre cuando la identidad del usuario de Windows y la del usuario de UNIX no coinciden. Por ejemplo, si el usuario de Windows `johnsmith` tiene una identidad UNIX de `jsmith` Google Cloud NetApp Volumes necesita una forma de informar sobre la variación. Debido a que Google Cloud NetApp Volumes actualmente no admite la creación de reglas de asignación de nombres estáticos, se debe usar LDAP para buscar la identidad de los usuarios de Windows y UNIX para garantizar la propiedad adecuada de los archivos y las carpetas y los permisos esperados.

De forma predeterminada, Google Cloud NetApp Volumes incluye `LDAP` en el ns-switch de la instancia de la base de datos del mapa de nombres, de modo que para proporcionar la funcionalidad de mapeo de nombres mediante LDAP para nombres asimétricos, solo necesita modificar algunos de los atributos de usuario/grupo para reflejar lo que busca Google Cloud NetApp Volumes .

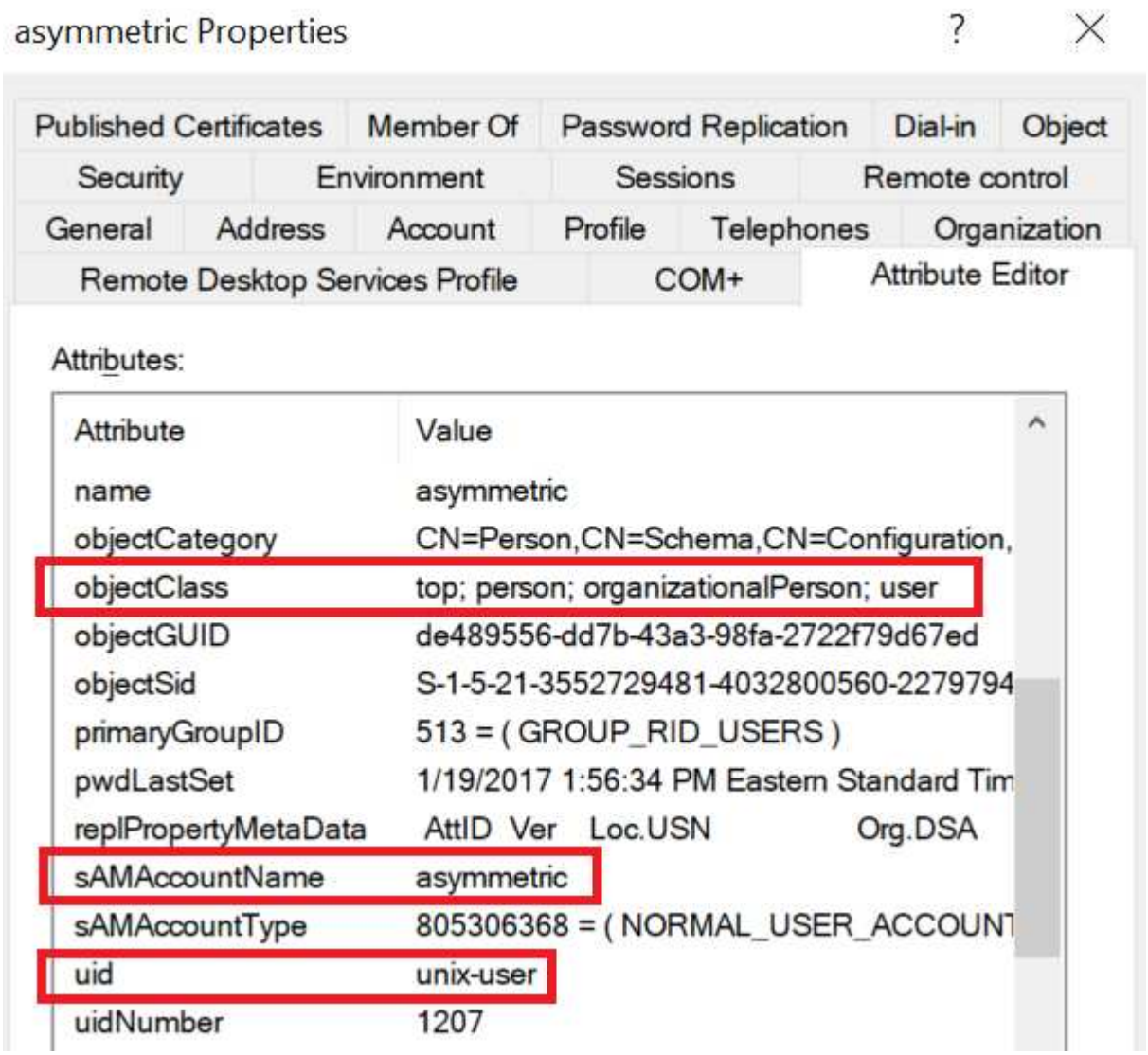
La siguiente tabla muestra qué atributos deben completarse en LDAP para la funcionalidad de mapeo de nombres asimétrico. En la mayoría de los casos, Active Directory ya está configurado para hacer esto.

Atributo de Google Cloud NetApp Volumes	**Qué hace**	**Valor utilizado por Google Cloud NetApp Volumes para la asignación de nombres**
Clase de objeto de Windows a UNIX	Especifica el tipo de objeto que se está utilizando. (Es decir, usuario, grupo, cuenta posix, etc.)	Debe incluir al usuario (puede contener varios otros valores, si lo desea).
Atributo de Windows a UNIX	que define el nombre de usuario de Windows en el momento de la creación. Google Cloud NetApp Volumes utiliza esto para búsquedas de Windows a UNIX.	No es necesario realizar ningún cambio aquí; sAMAccountName es el mismo que el nombre de inicio de sesión de Windows.
UID	Define el nombre de usuario de UNIX.	Nombre de usuario UNIX deseado.

Actualmente, Google Cloud NetApp Volumes no usa prefijos de dominio en las búsquedas LDAP, por lo que los entornos LDAP de múltiples dominios no funcionan correctamente con las búsquedas de mapas de nombres LDAP.

El siguiente ejemplo muestra un usuario con el nombre de Windows `asymmetric` , el nombre de UNIX `unix-user` , y el comportamiento que sigue al escribir archivos tanto desde SMB como desde NFS.

La siguiente figura muestra cómo se ven los atributos LDAP desde el servidor Windows.



Desde un cliente NFS, puedes consultar el nombre de UNIX pero no el nombre de Windows:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Cuando se escribe un archivo desde NFS como `unix-user` , el siguiente es el resultado del cliente NFS:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Desde un cliente de Windows, puede ver que el propietario del archivo está configurado como el usuario de Windows adecuado:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Por el contrario, los archivos creados por el usuario de Windows `asymmetric` desde un cliente SMB muestra el propietario de UNIX adecuado, como se muestra en el siguiente texto.

PYME:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

Número de serie:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

Enlace de canal LDAP

Debido a una vulnerabilidad en los controladores de dominio de Windows Active Directory, "Aviso de seguridad de Microsoft ADV190023" cambia la forma en que los controladores permiten enlaces LDAP.

El impacto para Google Cloud NetApp Volumes es el mismo que para cualquier cliente LDAP. Google Cloud NetApp Volumes actualmente no admite la vinculación de canales. Dado que Google Cloud NetApp Volumes admite la firma LDAP de forma predeterminada a través de la negociación, la vinculación del canal LDAP no debería ser un problema. Si tiene problemas para vincularse a LDAP con el enlace de canal habilitado, siga los pasos de solución en ADV190023 para permitir que los enlaces LDAP desde Google Cloud NetApp Volumes sean exitosos.

DNS

Tanto Active Directory como Kerberos dependen del DNS para la resolución de nombre de host a IP y de IP a nombre de host. El DNS requiere que el puerto 53 esté abierto. Google Cloud NetApp Volumes no realiza ninguna modificación en los registros DNS y actualmente no admite el uso de "DNS dinámico" en interfaces de red.

Puede configurar Active Directory DNS para restringir qué servidores pueden actualizar registros DNS. Para obtener más información, consulte "DNS seguro de Windows" .

Tenga en cuenta que los recursos dentro de un proyecto de Google utilizan de manera predeterminada Google Cloud DNS, que no está conectado con Active Directory DNS. Los clientes que utilizan Cloud DNS no pueden resolver las rutas UNC devueltas por Google Cloud NetApp Volumes. Los clientes de Windows unidos

al dominio de Active Directory están configurados para usar DNS de Active Directory y pueden resolver dichas rutas UNC.

Para unir un cliente a Active Directory, debes configurar su configuración de DNS para que use el DNS de Active Directory. Si lo deseas, puedes configurar Cloud DNS para que reenvíe las solicitudes al DNS de Active Directory. Consulta "¿Por qué mi cliente no puede resolver el nombre NetBIOS SMB?"para obtener más información.

Google Cloud NetApp Volumes actualmente no admite DNSSEC y las consultas DNS se realizan en texto sin formato.

Auditoría de acceso a archivos

Actualmente no es compatible con Google Cloud NetApp Volumes.

Protección antivirus

Debe realizar un análisis antivirus en Google Cloud NetApp Volumes en el cliente de un recurso compartido NAS. Actualmente no existe una integración de antivirus nativa con Google Cloud NetApp Volumes.

Operación del servicio

El equipo de Google Cloud NetApp Volumes administra los servicios de backend en Google Cloud y utiliza múltiples estrategias para proteger la plataforma y evitar accesos no deseados.

Cada cliente obtiene su propia subred única, cuyo acceso está restringido a otros clientes de manera predeterminada, y cada inquilino en Google Cloud NetApp Volumes obtiene su propio espacio de nombres y VLAN para un aislamiento total de los datos. Una vez autenticado un usuario, el motor de entrega de servicios (SDE) solo puede leer datos de configuración específicos de ese inquilino.

Seguridad física

Con la aprobación previa adecuada, solo los ingenieros en el sitio y los ingenieros de soporte de campo (FSE) con credencial de NetApp tienen acceso a la jaula y a los racks para realizar trabajos físicos. No se permite la gestión de almacenamiento ni de red. Sólo estos recursos en el sitio pueden realizar tareas de mantenimiento de hardware.

Para los ingenieros en el sitio, se genera un ticket para la declaración de trabajo (SOW) que incluye la identificación del rack y la ubicación del dispositivo (RU) y todos los demás detalles se incluyen en el ticket. Para los FSE de NetApp , se debe generar un ticket de visita al sitio ante el COLO y el ticket incluye los detalles del visitante, la fecha y la hora para fines de auditoría. El SOW para el FSE se comunica internamente a NetApp.

Equipo de operaciones

El equipo de operaciones de Google Cloud NetApp Volumes está formado por ingeniería de producción y un ingeniero de confiabilidad del sitio (SRE) para Google Cloud NetApp Volumes , además de ingenieros de soporte de campo de NetApp y socios para hardware. Todos los miembros del equipo de operaciones están acreditados para trabajar en Google Cloud y se mantienen registros detallados del trabajo para cada ticket generado. Además, existe un estricto proceso de control y aprobación de cambios para garantizar que cada decisión sea analizada adecuadamente.

El equipo de SRE administra el plano de control y cómo se enrutan los datos desde las solicitudes de UI al

hardware y software de back-end en Google Cloud NetApp Volumes. El equipo de SRE también administra los recursos del sistema, como los máximos de volumen e inodos. A los SRE no se les permite interactuar con los datos de los clientes ni tener acceso a ellos. Los SRE también brindan coordinación con las Autorizaciones de Devolución de Material (RMA), como solicitudes de reemplazo de memoria o disco nuevo para el hardware del backend.

Responsabilidades del cliente

Los clientes de Google Cloud NetApp Volumes administran el Active Directory de su organización y la administración de roles de usuario, así como las operaciones de volumen y datos. Los clientes pueden tener roles administrativos y pueden delegar permisos a otros usuarios finales dentro del mismo proyecto de Google Cloud utilizando los dos roles predefinidos que proporcionan NetApp y Google Cloud (Administrador y Visualizador).

El administrador puede vincular cualquier VPC dentro del proyecto del cliente a Google Cloud NetApp Volumes que el cliente considere apropiado. Es responsabilidad del cliente administrar el acceso a su suscripción a Google Cloud Marketplace y administrar las VPC que tienen acceso al plano de datos.

Protección contra SRE maliciosa

Una inquietud que podría surgir es ¿cómo protege Google Cloud NetApp Volumes contra escenarios en los que hay un SRE malicioso o cuando las credenciales de SRE se han visto comprometidas?

El acceso al entorno de producción está restringido a un número limitado de personas de SRE. Los privilegios administrativos están aún más restringidos a un puñado de administradores experimentados. Todas las acciones realizadas por cualquier persona en el entorno de producción de Google Cloud NetApp Volumes se registran y nuestra plataforma de inteligencia de amenazas de gestión de eventos e información de seguridad (SIEM) detecta cualquier anomalía en la línea de base o actividad sospechosa. Como resultado, se pueden rastrear y mitigar acciones maliciosas antes de que se produzcan demasiados daños al backend de Google Cloud NetApp Volumes .

Ciclo de vida del volumen

Google Cloud NetApp Volumes administra solo los objetos dentro del servicio, no los datos dentro de los volúmenes. Solo los clientes que acceden a los volúmenes pueden administrar los datos, las ACL, los propietarios de archivos, etc. Los datos de estos volúmenes están cifrados en reposo y el acceso está limitado a los inquilinos de la instancia de Google Cloud NetApp Volumes .

El ciclo de vida del volumen de Google Cloud NetApp Volumes es crear-actualizar-eliminar. Los volúmenes conservan copias instantáneas de los volúmenes hasta que se eliminan, y solo los administradores de Google Cloud NetApp Volumes validados pueden eliminar volúmenes en Google Cloud NetApp Volumes. Cuando un administrador solicita la eliminación de un volumen, se requiere un paso adicional: ingresar el nombre del volumen para verificar la eliminación. Después de eliminar un volumen, éste desaparece y no se puede recuperar.

En los casos en que se rescinde un contrato de Google Cloud NetApp Volumes , NetApp marca los volúmenes para su eliminación después de un período de tiempo específico. Antes de que expire ese período de tiempo, puede recuperar volúmenes a solicitud del cliente.

Certificaciones

Google Cloud NetApp Volumes para Google Cloud actualmente está certificado según los estándares ISO/IEC 27001:2013 e ISO/IEC 27018:2019. El servicio también recibió recientemente su informe de certificación SOC2 Tipo I. Para obtener información sobre el compromiso de NetApp con la seguridad y privacidad de los datos, consulte "Cumplimiento: seguridad y privacidad de datos" .

RGPD

Nuestros compromisos con la privacidad y el cumplimiento del GDPR están disponibles en varios de nuestros documentos de "contratos de clientes", como nuestro "Anexo Data Processing del cliente", que incluye el "Cláusulas contractuales estándar" proporcionado por la Comisión Europea. También incluimos estos compromisos en nuestra Privacy Policy, respaldada por los valores fundamentales establecidos en nuestro Code of Conduct corporativo.

Información adicional e información de contacto

Para obtener más información sobre la información que se describe en este documento, revise los siguientes documentos y/o sitios web:

- Documentación de Google Cloud para Google Cloud NetApp Volumes

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Acceso al servicio privado de Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentación de productos de NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Programa de módulo de validación criptográfica: NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- La solución de NetApp para ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: Kerberos NFS en ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Contáctanos

Permítanos saber cómo podemos mejorar este informe técnico.

Contáctenos en doccomments@netapp.com. Incluya en el asunto INFORME TÉCNICO 4918.

NetApp Disaster Recovery

Protección de datos 3-2-1 para VMware con SnapCenter Plug-in y NetApp Backup and Recovery para proteger las cargas de trabajo de VMware

La estrategia de respaldo 3-2-1 es un método de protección de datos aceptado por la industria, que proporciona un enfoque integral para salvaguardar datos valiosos. Esta estrategia es confiable y garantiza que incluso si ocurre algún desastre inesperado, todavía habrá una copia de los datos disponible.

Descripción general

La estrategia se compone de tres reglas fundamentales:

1. Conserve al menos tres copias de sus datos. Esto garantiza que incluso si se pierde o se corrompe una copia, todavía tendrá al menos dos copias restantes a las que recurrir.
2. Almacene dos copias de seguridad en diferentes medios o dispositivos de almacenamiento. La diversificación de los medios de almacenamiento ayuda a proteger contra fallas específicas del dispositivo o del medio. Si un dispositivo se daña o falla un tipo de medio, la otra copia de respaldo permanece intacta.
3. Por último, asegúrese de que al menos una copia de seguridad esté fuera del sitio. El almacenamiento externo funciona como medida de seguridad contra desastres localizados, como incendios o inundaciones, que podrían inutilizar las copias locales.

Este documento de la solución abarca una solución de backups 3-2-1 que usa SnapCenter Plug-in for VMware vSphere (SCV) para crear backups primarios y secundarios de nuestras máquinas virtuales on-premises y NetApp Backup and Recovery para máquinas virtuales para hacer backup de una copia de nuestros datos en almacenamiento en la cloud o en StorageGRID.

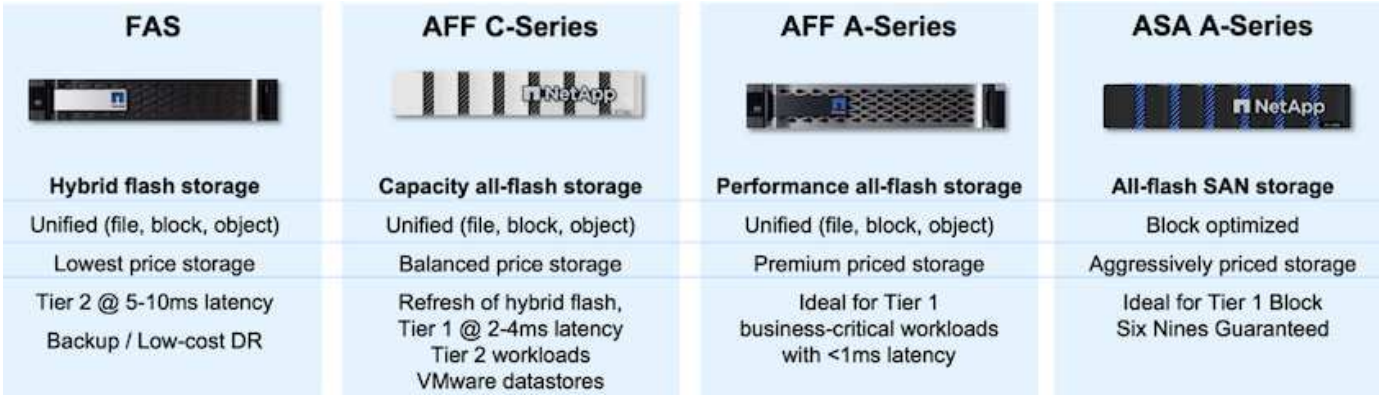
Casos de uso

Esta solución aborda los siguientes casos de uso:

- Copia de seguridad y restauración de máquinas virtuales y almacenes de datos locales mediante el SnapCenter Plug-in for VMware vSphere.
- Copia de seguridad y restauración de máquinas virtuales y datastores locales, alojados en clústeres de ONTAP y con backup en almacenamiento de objetos mediante NetApp Backup and Recovery para máquinas virtuales.

Almacenamiento de datos NetApp ONTAP

ONTAP es la solución de almacenamiento líder en la industria de NetApp que ofrece almacenamiento unificado ya sea que acceda a través de protocolos SAN o NAS. La estrategia de respaldo 3-2-1 garantiza que los datos locales estén protegidos en más de un tipo de medio y NetApp ofrece plataformas que van desde flash de alta velocidad hasta medios de menor costo.



Para obtener más información sobre todas las plataformas de hardware de NetApp, consulte "Almacenamiento de datos de NetApp" .

Plugin de SnapCenter para VMware vSphere

El complemento SnapCenter para VMware vSphere es una oferta de protección de datos que está estrechamente integrada con VMware vSphere y permite una fácil gestión de copias de seguridad y restauraciones de máquinas virtuales. Como parte de esa solución, SnapMirror proporciona un método rápido y confiable para crear una segunda copia de seguridad inmutable de los datos de la máquina virtual en un clúster de almacenamiento ONTAP secundario. Con esta arquitectura instalada, las operaciones de restauración de máquinas virtuales se pueden iniciar fácilmente desde las ubicaciones de respaldo principales o secundarias.

SCV se implementa como un dispositivo virtual Linux mediante un archivo OVA. El complemento ahora utiliza una arquitectura de complemento remoto. El complemento remoto se ejecuta fuera del servidor vCenter y está alojado en el dispositivo virtual SCV.

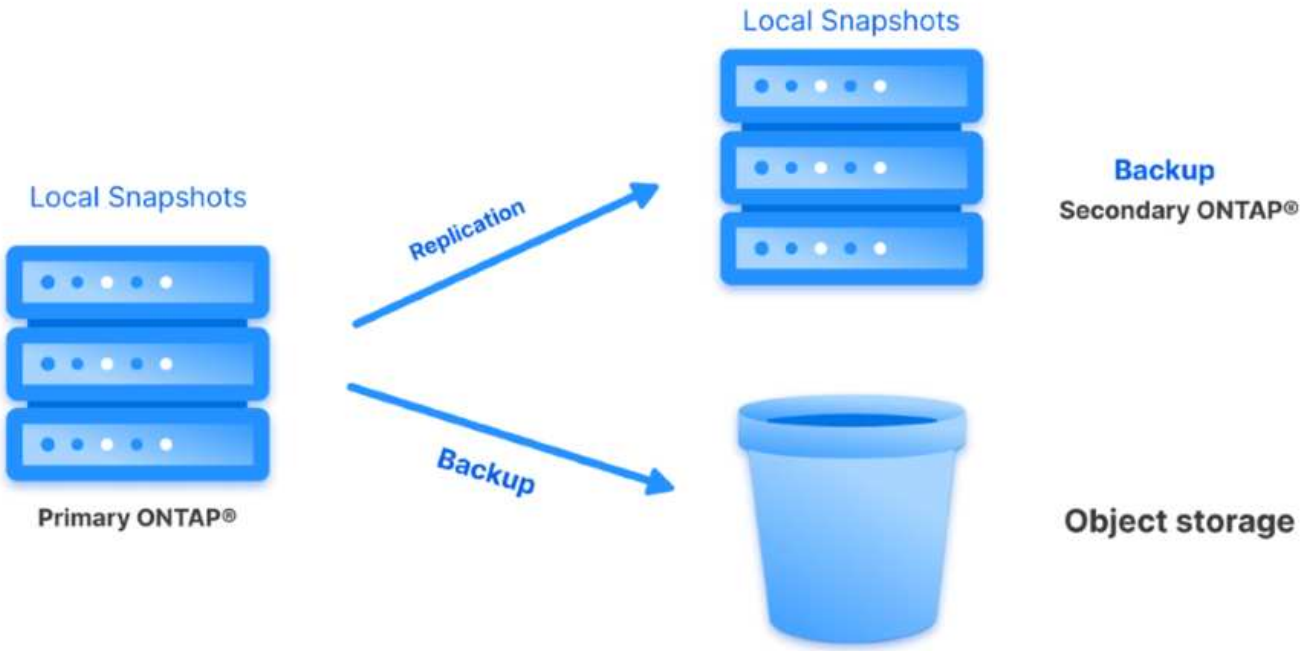
Para obtener información detallada sobre SCV, consulte "Documentación del SnapCenter Plug-in for VMware vSphere" .

NetApp Backup and Recovery para proteger las cargas de trabajo de VMware

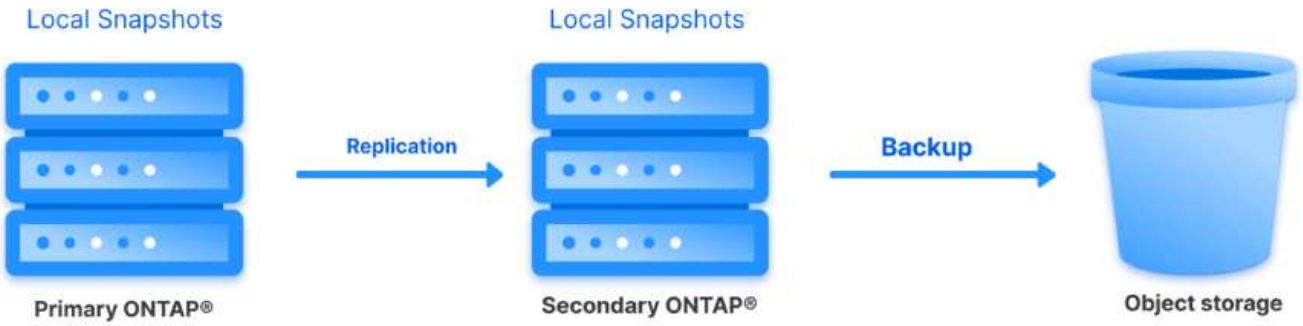
NetApp Backup and Recovery es una herramienta de gestión de datos basada en la nube que proporciona un único plano de control para una amplia gama de operaciones de backup y recuperación tanto en entornos on-premises como en la nube. Parte de la suite NetApp Backup and Recovery for VM es una función que se integra con SnapCenter Plug-in for VMware vSphere (on-premises) para ampliar una copia de los datos al almacenamiento de objetos en la nube. Esto establece una tercera copia de los datos fuera del sitio a partir de los backups del almacenamiento primario o secundario. NetApp Backup and Recovery for VMs te facilita configurar políticas de almacenamiento que transfieren copias de tus datos desde cualquiera de estas dos ubicaciones on-premises.

Elegir entre las copias de seguridad primaria y secundaria como origen en NetApp Backup and Recovery dará como resultado la implementación de una de estas dos topologías:

Topología en abanico – cuando el SnapCenter Plug-in for VMware vSphere inicia un backup, se toma inmediatamente una instantánea local. A continuación, SCV inicia una operación SnapMirror que replica la instantánea más reciente en el clúster ONTAP secundario. En NetApp Backup and Recovery, una política especifica el clúster ONTAP primario como origen de una copia de instantánea de los datos que se transferirán al almacenamiento de objetos en el proveedor de nube que elijas.



Topología en cascada – crear las copias de datos primarias y secundarias mediante SCV es idéntico a la topología en abanico mencionada anteriormente. Sin embargo, esta vez se crea una política en NetApp Backup and Recovery que especifica que el backup en el almacenamiento de objetos se originará desde el clúster ONTAP secundario.



NetApp Backup and Recovery puede crear copias de backup de snapshots de ONTAP locales en AWS Glacier, Azure Blob y el almacenamiento GCP Archive.







AWS Glacier and Deep Glacier | **Azure Blob Archive** | **GCP Archive Storage**

Además, puede utilizar NetApp StorageGRID como destino de respaldo de almacenamiento de objetos. Para obtener más información sobre StorageGRID , consulte "Página de inicio de StorageGRID" .

▼ **Descripción general de la implementación de la solución**

Esta lista recoge los pasos a grandes rasgos necesarios para configurar esta solución y realizar operaciones de backup y restauración desde SCV y NetApp Console:

1. Configure la relación SnapMirror entre los clústeres ONTAP que se utilizarán para copias de datos primarias y secundarias.
2. Configurar el complemento SnapCenter para VMware vSphere.
   a. Agregar sistemas de almacenamiento
   b. Crear políticas de respaldo
   c. Crear grupos de recursos
   d. Ejecutar los primeros trabajos de copia de seguridad
3. Configura NetApp Backup and Recovery para máquinas virtuales
   a. Añadir entorno de trabajo
   b. Descubra los dispositivos SCV y vCenter
   c. Crear políticas de respaldo
   d. Activar copias de seguridad
4. Restaurar máquinas virtuales desde el almacenamiento primario y secundario mediante SCV.
5. Restaurar máquinas virtuales desde el almacenamiento de objetos mediante NetApp Console.

▼ **Prerrequisitos**

El propósito de esta solución es demostrar la protección de datos de las máquinas virtuales que se ejecutan en VMware vSphere y se encuentran en almacenes de datos NFS alojados por NetApp ONTAP. Esta solución asume que los siguientes componentes están configurados y listos para usar:

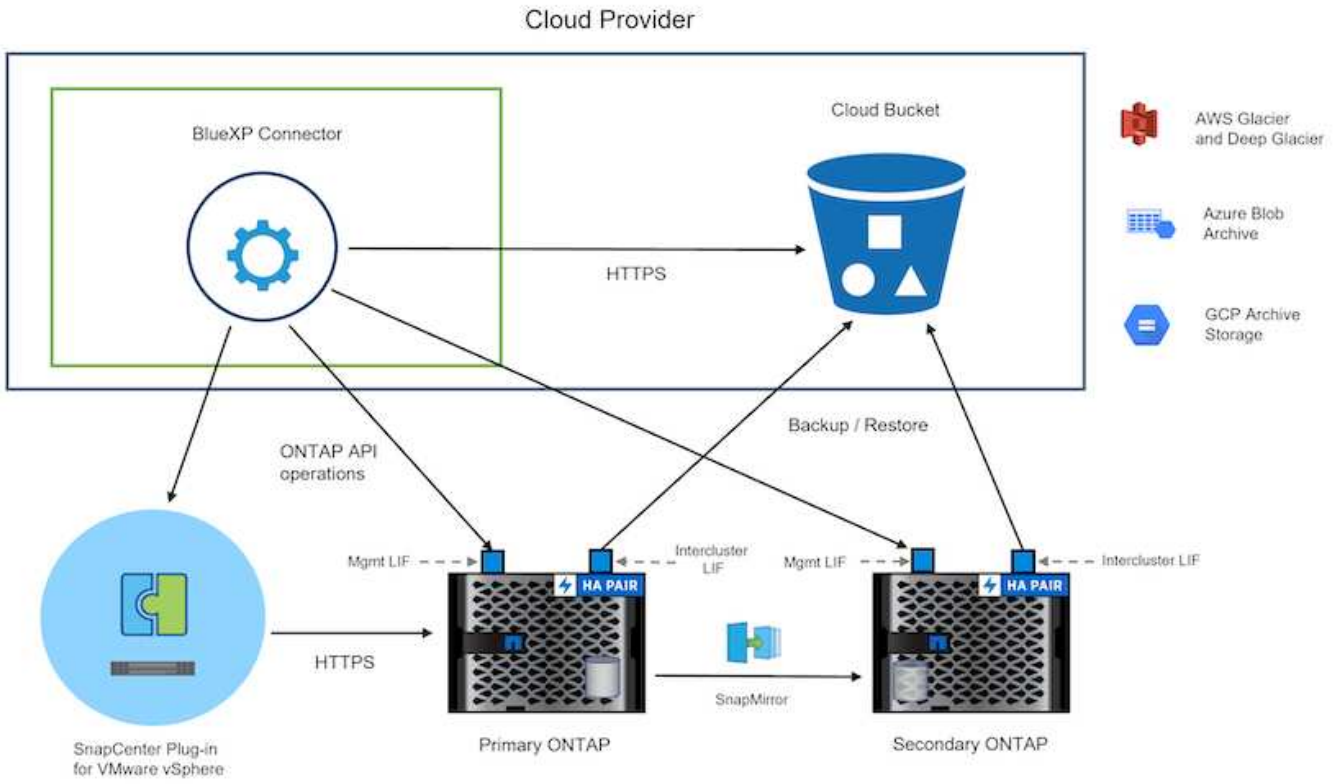
1. Clúster de almacenamiento ONTAP con almacenes de datos NFS o VMFS conectados a VMware vSphere. Se admiten almacenes de datos NFS y VMFS. Para esta solución se utilizaron almacenes de datos NFS.
2. Clúster de almacenamiento ONTAP secundario con relaciones SnapMirror establecidas para volúmenes utilizados para almacenes de datos NFS.
3. Se ha instalado el agente de NetApp Console para el proveedor de nube usado para los backups del

almacenamiento de objetos.

4. Las máquinas virtuales que se respaldarán se encuentran en almacenes de datos NFS que residen en el clúster de almacenamiento ONTAP principal.
5. Conectividad de red entre el agente de NetApp Console y las interfaces de gestión del clúster de almacenamiento ONTAP local.
6. Conectividad de red entre el agente de NetApp Console y la máquina virtual del dispositivo SCV local, así como entre el agente de NetApp Console y vCenter.
7. Conectividad de red entre los LIF entre clústeres de ONTAP locales y el servicio de almacenamiento de objetos.
8. DNS configurado para la administración de SVM en clústeres de almacenamiento ONTAP primarios y secundarios. Para obtener más información, consulte "Configurar DNS para la resolución del nombre de host" .

Arquitectura de alto nivel

La prueba/validación de esta solución se realizó en un laboratorio que puede o no coincidir con el entorno de implementación final.



Implementación de la solución

En esta solución, ofrecemos instrucciones detalladas para implementar y validar una solución que utiliza SnapCenter Plug-in for VMware vSphere, junto con Backup and Recovery, para realizar el backup y la recuperación de máquinas virtuales Windows y Linux dentro de un clúster de VMware vSphere ubicado en un centro de datos on-premises. Las máquinas virtuales de esta configuración se almacenan en datastores NFS alojados en un clúster de almacenamiento ONTAP A300. Además, un clúster de almacenamiento ONTAP A300 independiente sirve como destino secundario para volúmenes replicados mediante SnapMirror. Además, el almacenamiento de objetos alojado en Amazon Web Services y Azure Blob se utilizó como destino para una

tercera copia de los datos.

Repasaremos cómo crear relaciones de SnapMirror para las copias secundarias de nuestros backups gestionados por SCV y la configuración de las tareas de backup tanto en SCV como en NetApp Console.

Para obtener información detallada sobre el SnapCenter Plug-in for VMware vSphere, consulte "Documentación del SnapCenter Plug-in for VMware vSphere" .

Para obtener información detallada sobre Backup and Recovery, consulta "Documentación de copia de seguridad y recuperación".

Establecer relaciones SnapMirror entre clústeres ONTAP

El SnapCenter Plug-in for VMware vSphere utiliza la tecnología ONTAP SnapMirror para administrar el transporte de copias secundarias de SnapMirror y/o SnapVault a un clúster ONTAP secundario.

Las políticas de respaldo de SCV tienen la opción de utilizar relaciones SnapMirror o SnapVault . La principal diferencia es que al utilizar la opción SnapMirror , el programa de retención configurado para las copias de seguridad en la política será el mismo en las ubicaciones principal y secundaria. SnapVault está diseñado para archivar y al utilizar esta opción se puede establecer un programa de retención separado con la relación SnapMirror para las copias de instantáneas en el clúster de almacenamiento ONTAP secundario.

La configuración de las relaciones de SnapMirror se puede hacer en NetApp Console, donde muchos de los pasos están automatizados, o se puede hacer con System Manager y la CLI de ONTAP. Todos estos métodos se analizan a continuación.

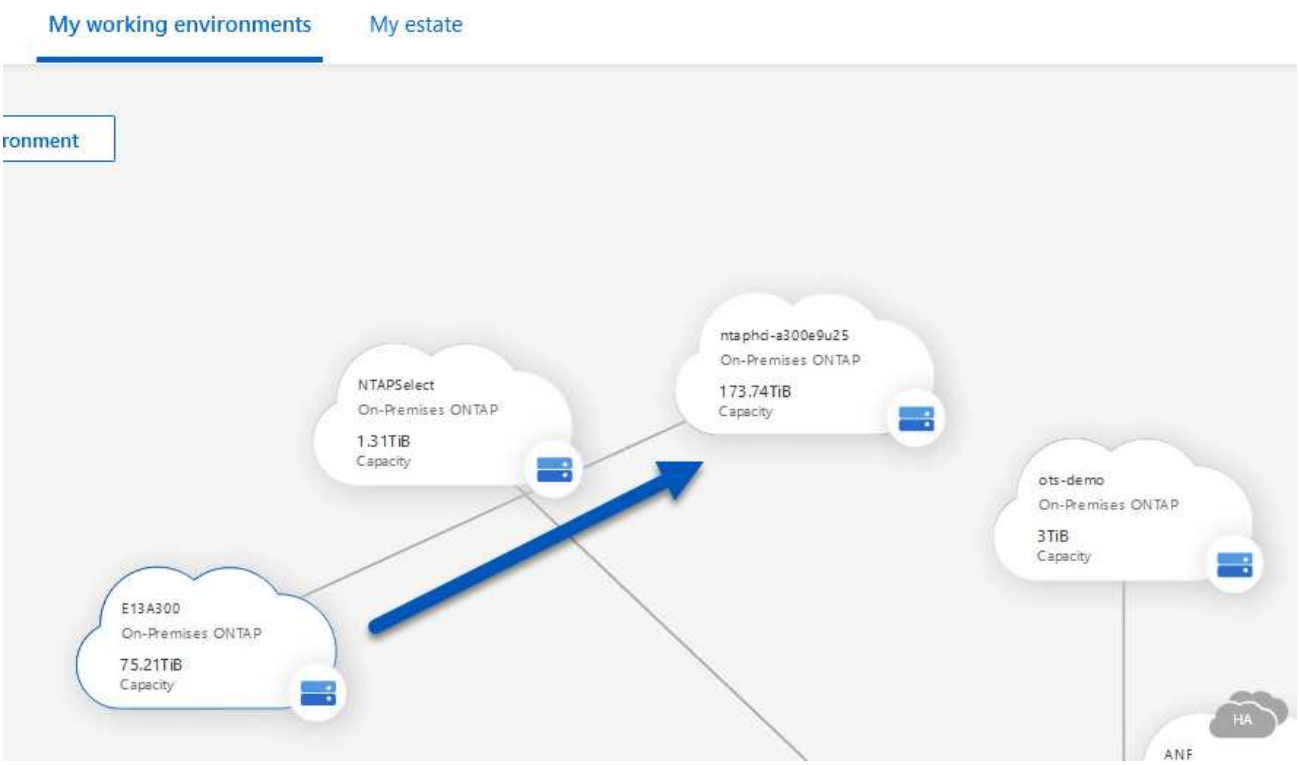
Establecer relaciones de SnapMirror con NetApp Console

Debes completar los siguientes pasos desde NetApp Console:

▼ **Configuración de replicación para sistemas de almacenamiento ONTAP primarios y secundarios**

Empieza iniciando sesión en la NetApp Console y ve a Systems.

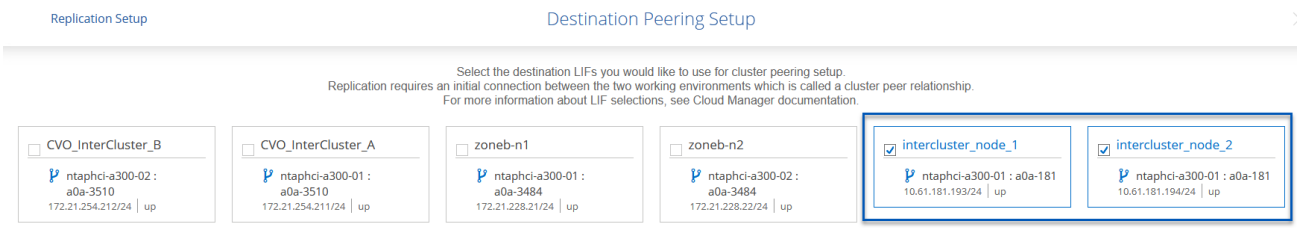
1. Arrastre y suelte el sistema de almacenamiento ONTAP de origen (principal) en el sistema de almacenamiento ONTAP de destino (secundario).



2. Desde el menú que aparece seleccione **Replicación**.

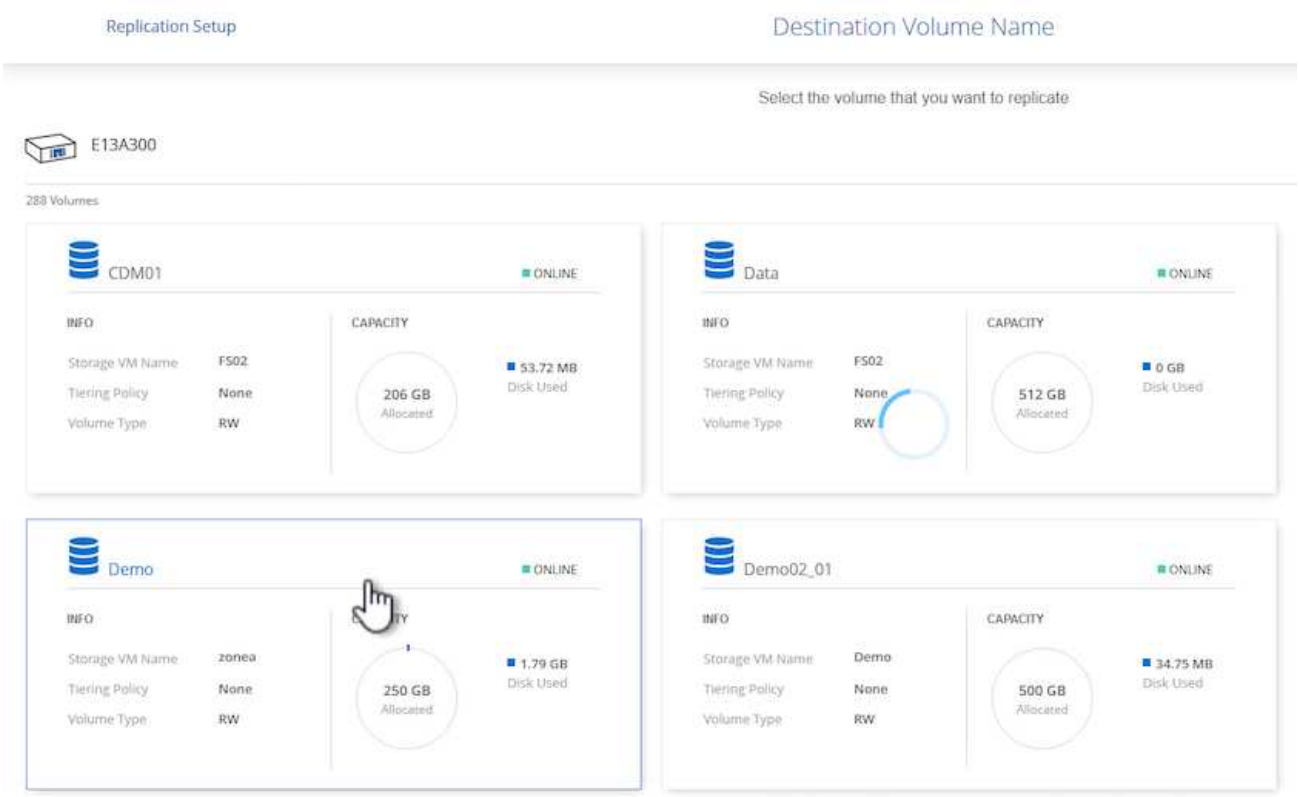


3. En la página **Configuración de emparejamiento de destino**, seleccione los LIF entre clústeres de destino que se utilizarán para la conexión entre sistemas de almacenamiento.



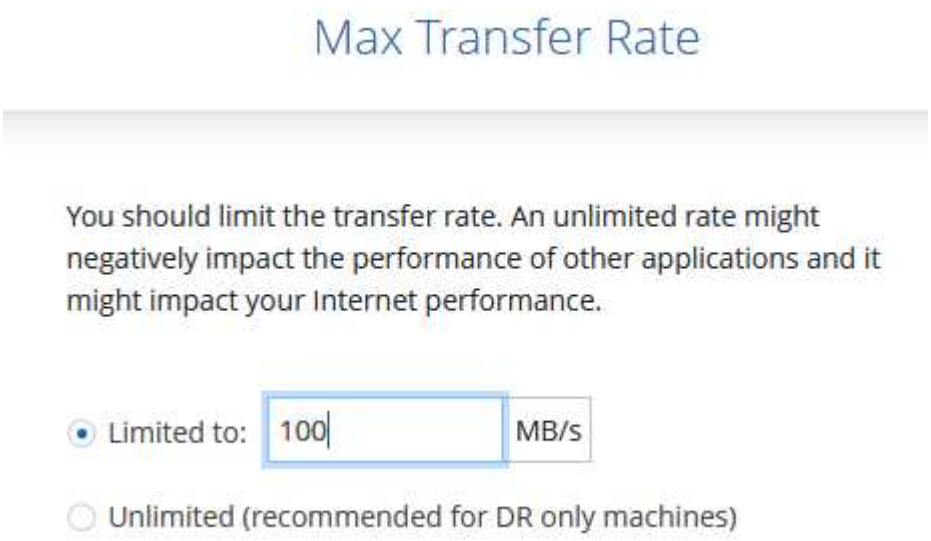
4. En la página **Nombre del volumen de destino**, primero seleccione el volumen de origen y luego complete el nombre del volumen de destino y seleccione el SVM de destino y el agregado. Haga clic en

Siguiente para continuar.

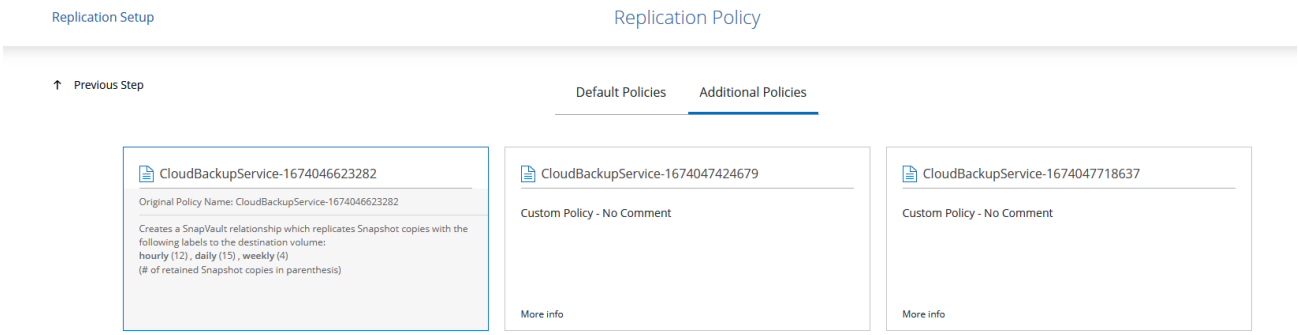




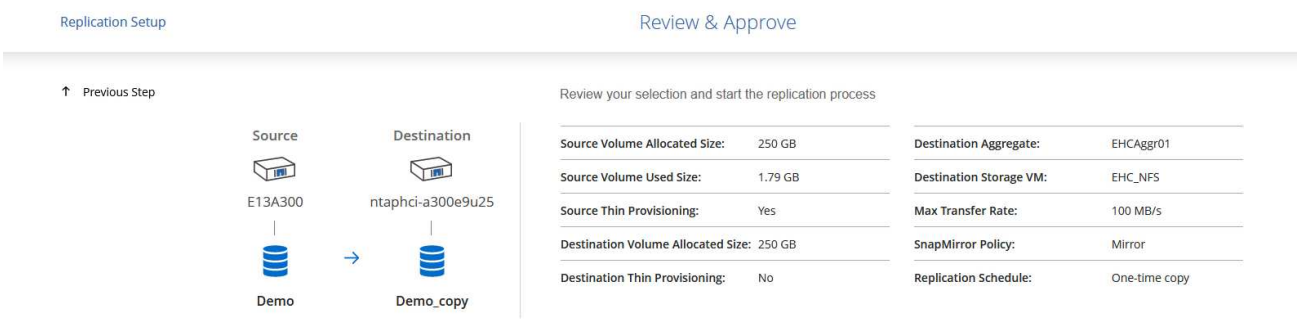
5. Seleccione la velocidad de transferencia máxima para que se produzca la replicación.



6. Elija la política que determinará el programa de retención para las copias de seguridad secundarias. Esta política se puede crear de antemano (consulte el proceso manual a continuación en el paso **Crear una política de retención de instantáneas**) o se puede cambiar después del hecho si así se desea.



7. Por último, revise toda la información y haga clic en el botón **Ir** para iniciar el proceso de configuración de la replicación.



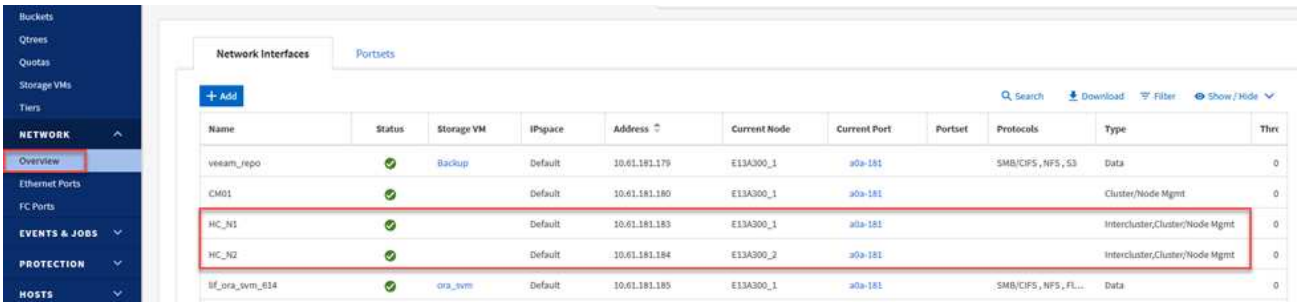
Establecer relaciones de SnapMirror con System Manager y ONTAP CLI

Todos los pasos necesarios para establecer relaciones de SnapMirror se pueden realizar con el Administrador del sistema o la CLI de ONTAP . La siguiente sección proporciona información detallada para ambos métodos:

▼ Registrar las interfaces lógicas entre clústeres de origen y destino

Para los clústeres ONTAP de origen y destino, 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 mediante la CLI, ejecute el siguiente comando:

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

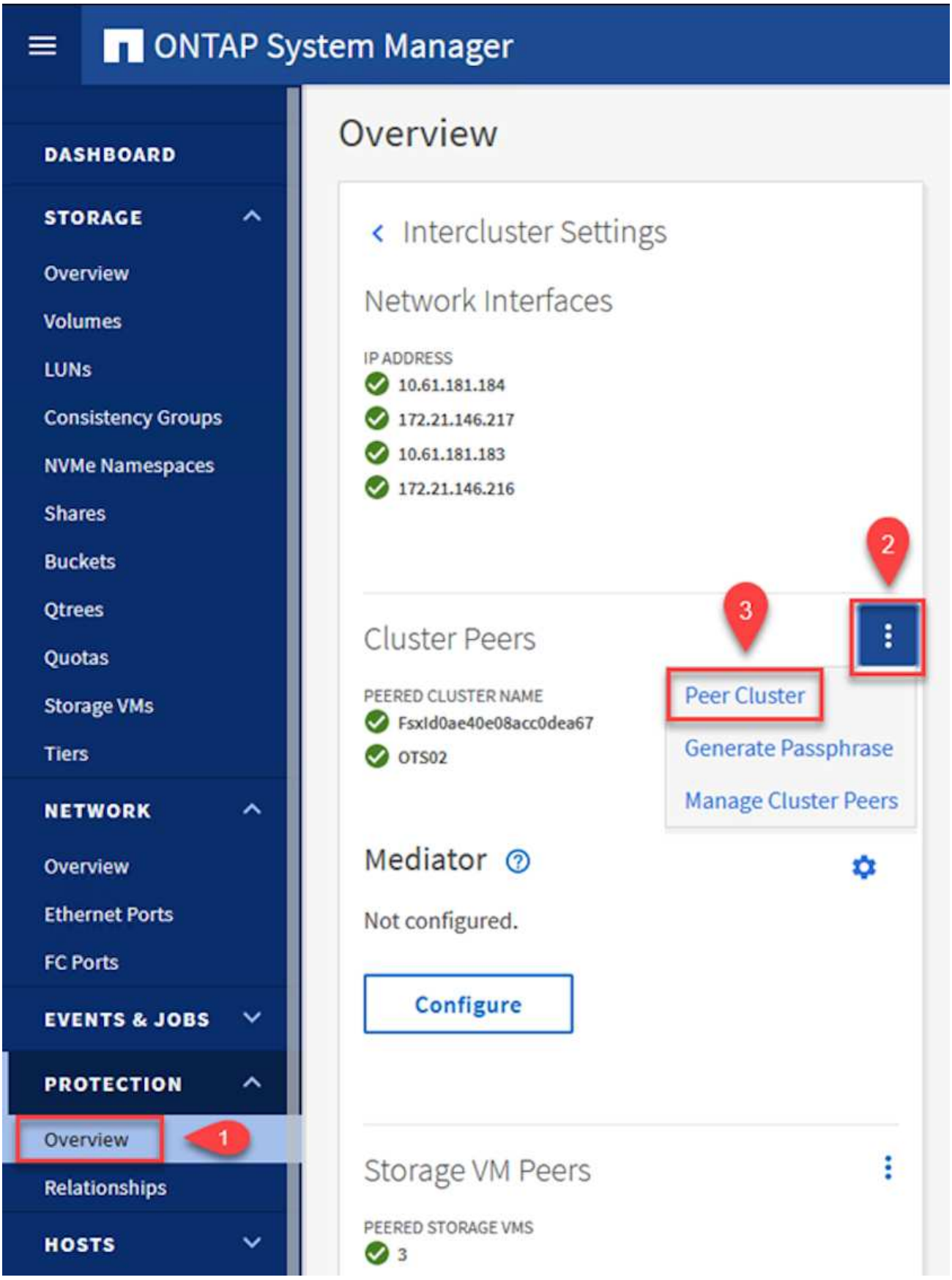
▼ **Establecer peering de clústeres entre clústeres ONTAP**

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 ONTAP 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.

```
ONTAP-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.



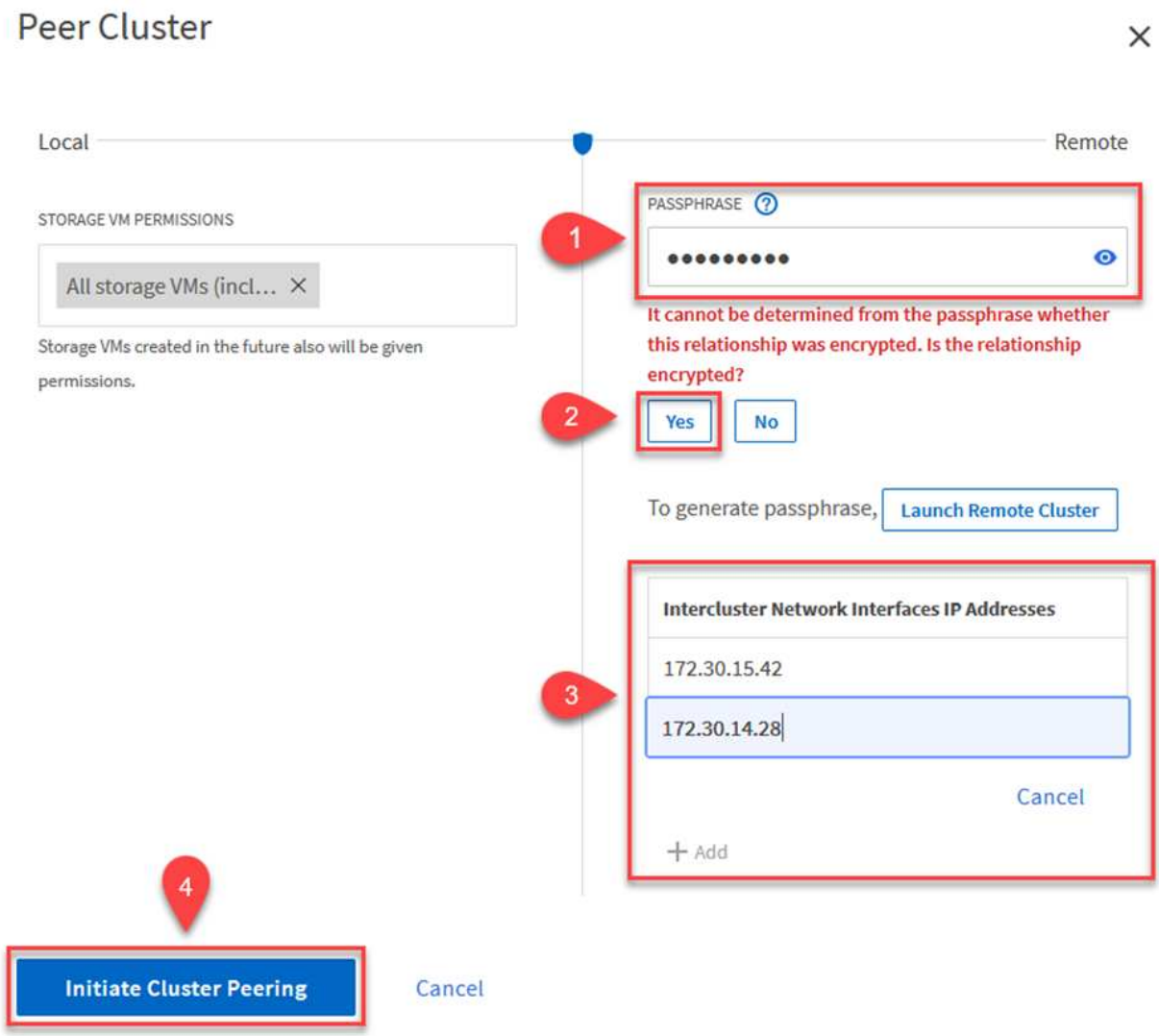
3. En el cuadro de diálogo Clúster de pares, complete la información requerida:
   a. Ingrese la frase de contraseña que se utilizó para establecer la relación de clúster de pares en el

clúster ONTAP de destino.

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

c. Introduzca las direcciones IP LIF entre clústeres del clúster ONTAP 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 ONTAP de destino con el siguiente comando:

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

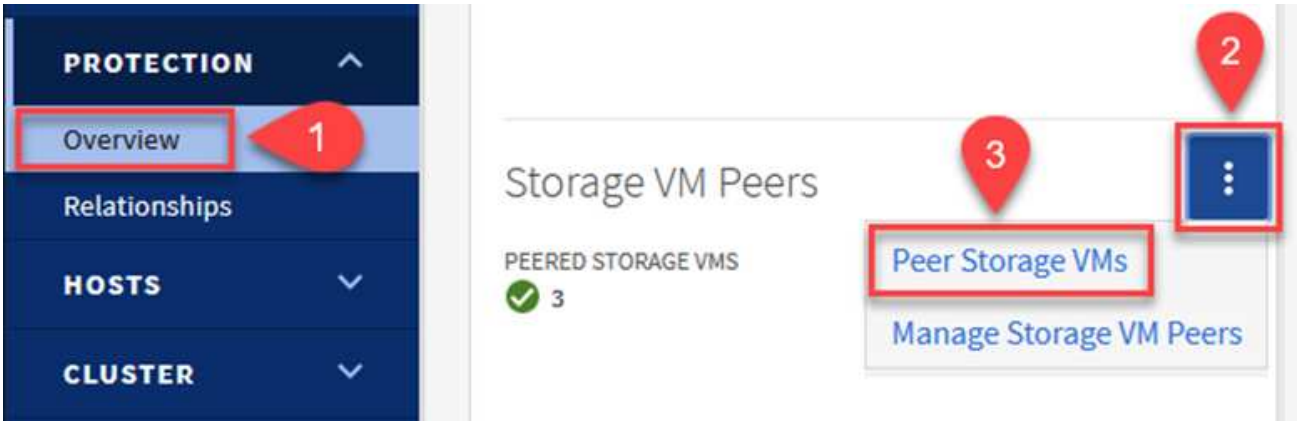
▼ **Establecer una relación de peering de SVM**

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 .

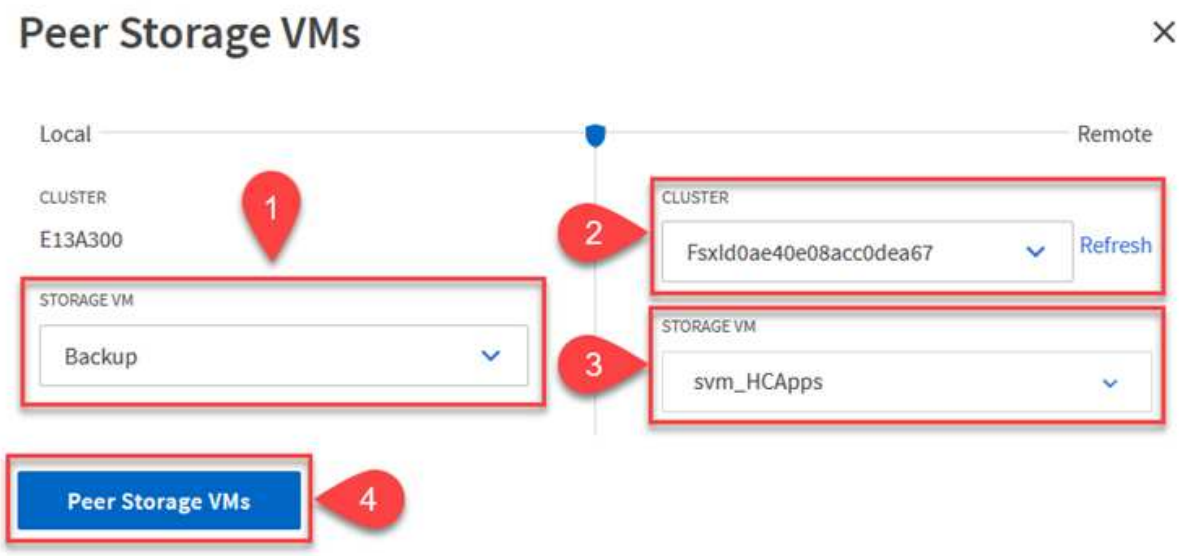
1. Desde el clúster ONTAP de destino, utilice el siguiente comando desde la CLI para crear la relación de pares de SVM:

```
ONTAP-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**

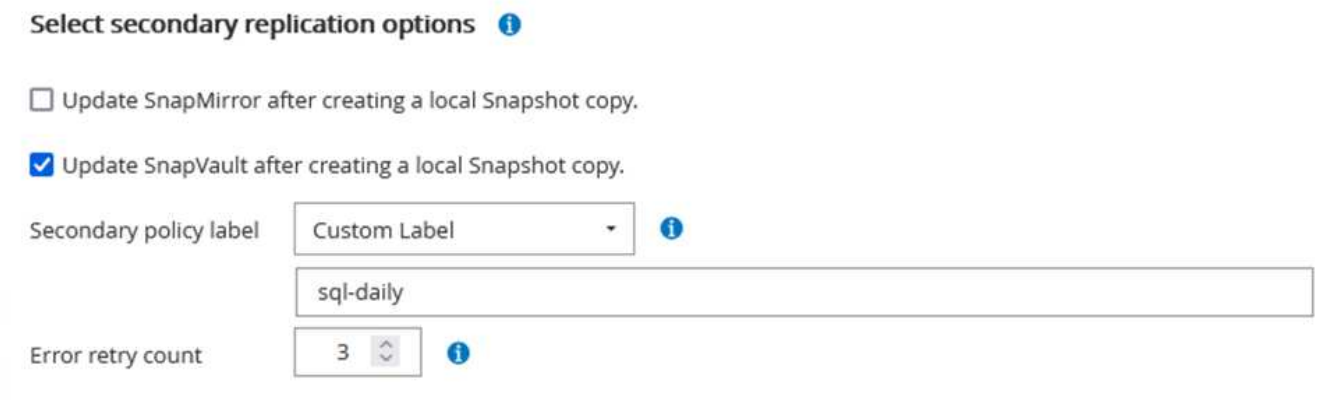
SnapCenter administra los programas de retención de las copias de seguridad que existen como copias instantáneas en el sistema de almacenamiento principal. Esto se establece al crear una política en

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.

```
ONTAP-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 .

```
ONTAP-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:

```
ONTAP-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 ONTAP que será el destinatario de copias de instantáneas de nuestros volúmenes de origen, ejecute el siguiente comando en el clúster de ONTAP de destino:

```
ONTAP-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 el clúster ONTAP de destino:

```
ONTAP-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.

Para crear un volumen, ejecute el siguiente comando en el clúster ONTAP de destino:

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

Configurar el SnapCenter Plug-in for VMware vSphere

Una vez instalado, se puede acceder al SnapCenter Plug-in for VMware vSphere desde la interfaz de administración de vCenter Server Appliance. SCV administrará las copias de seguridad de los almacenes de datos NFS montados en los hosts ESXi y que contienen las máquinas virtuales Windows y Linux.

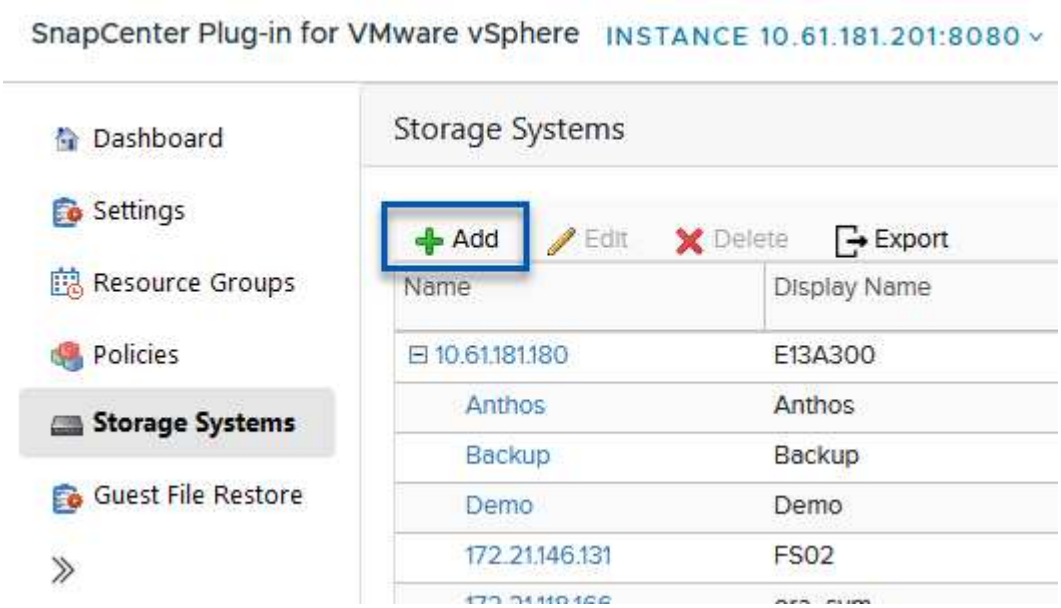
Revisar el "Flujo de trabajo de protección de datos" sección de la documentación de SCV para obtener más información sobre los pasos necesarios para configurar las copias de seguridad.

Para configurar copias de seguridad de sus máquinas virtuales y almacenes de datos, deberá completar los siguientes pasos desde la interfaz del complemento.

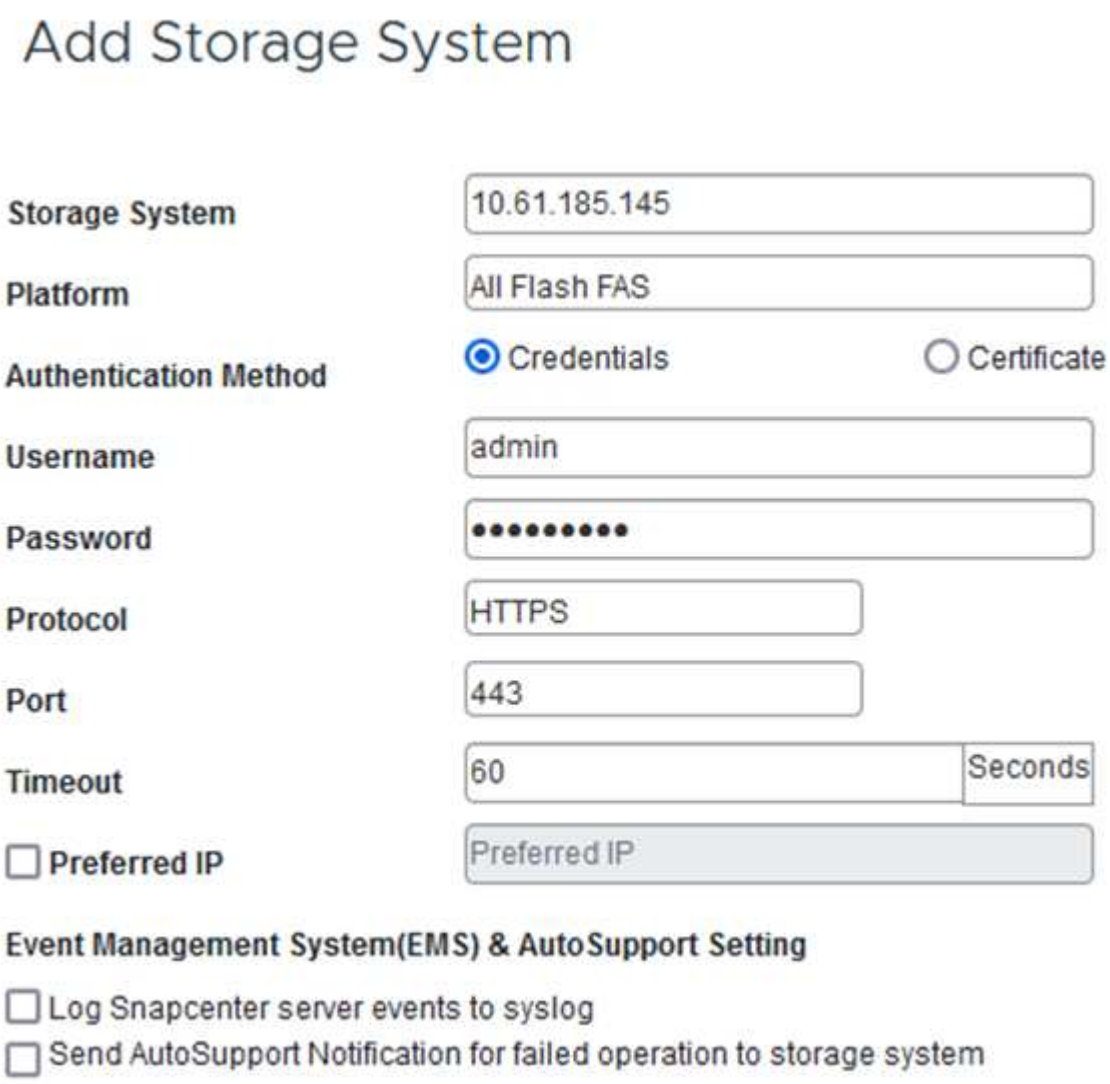
▼ **Sistemas de almacenamiento Discovery ONTAP**

Descubra los clústeres de almacenamiento de ONTAP que se utilizarán para copias de seguridad primarias y secundarias.

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Sistemas de almacenamiento** en el menú de la izquierda y haga clic en el botón **Agregar**.



2. Complete las credenciales y el tipo de plataforma para el sistema de almacenamiento ONTAP principal y haga clic en **Agregar**.



3. Repita este procedimiento para el sistema de almacenamiento ONTAP secundario.

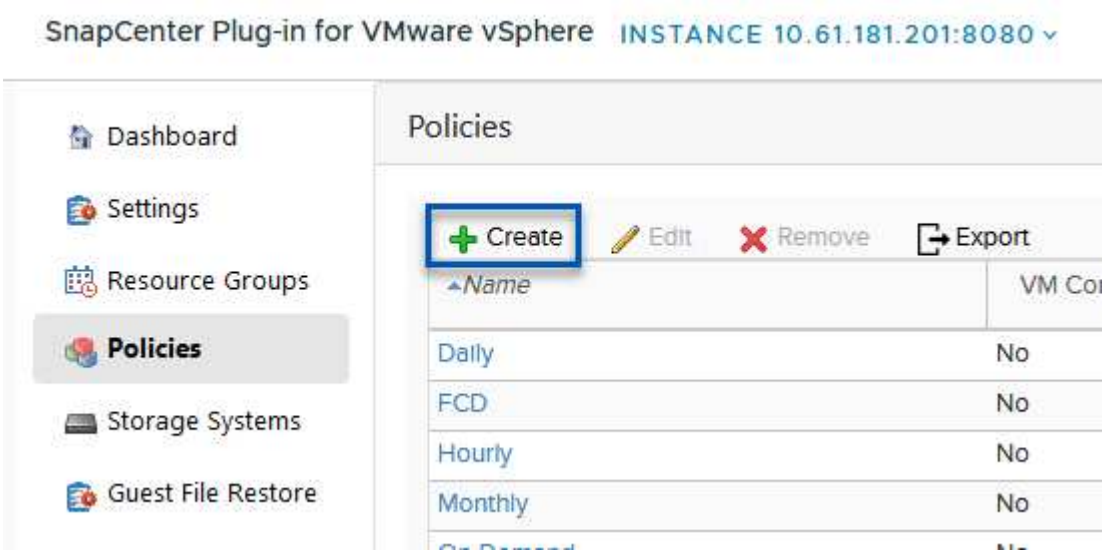
▼ **Crear políticas de respaldo de SCV**

Las políticas especifican el período de retención, la frecuencia y las opciones de replicación para las copias de seguridad administradas por SCV.

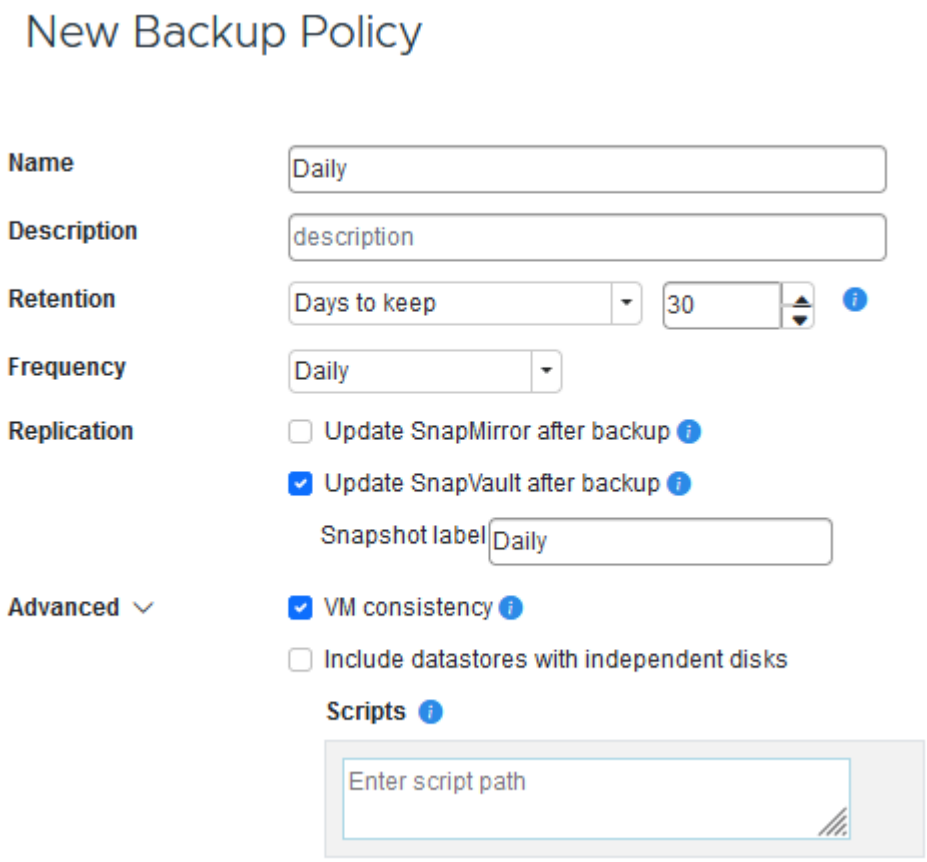
Revisar el "Crear políticas de respaldo para máquinas virtuales y almacenes de datos" sección de la documentación para obtener más información.

Para crear políticas de respaldo complete los siguientes pasos:

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Políticas** en el menú de la izquierda y haga clic en el botón **Crear**.



2. Especifique un nombre para la política, el período de retención, la frecuencia y las opciones de replicación, y la etiqueta de la instantánea.



Al crear una política en el complemento SnapCenter , verá opciones para SnapMirror y SnapVault. Si elige SnapMirror, el programa de retención especificado en la política será el mismo para las instantáneas principales y secundarias. Si elige SnapVault, el programa de retención de la instantánea secundaria se basará en un programa separado implementado con la relación SnapMirror . Esto es útil cuando desea períodos de retención más largos para las copias de seguridad secundarias.

Las etiquetas de Snapshot son útiles, ya que se pueden usar para aplicar políticas con un período de retención específico para las copias de SnapVault replicadas en el clúster secundario de ONTAP. Cuando se usa SCV con NetApp Data Services, el campo de etiqueta de Snapshot debe estar en blanco o coincidir con la etiqueta especificada en la política de backup.

3. Repita el procedimiento para cada política requerida. Por ejemplo, políticas separadas para copias de seguridad diarias, semanales y mensuales.

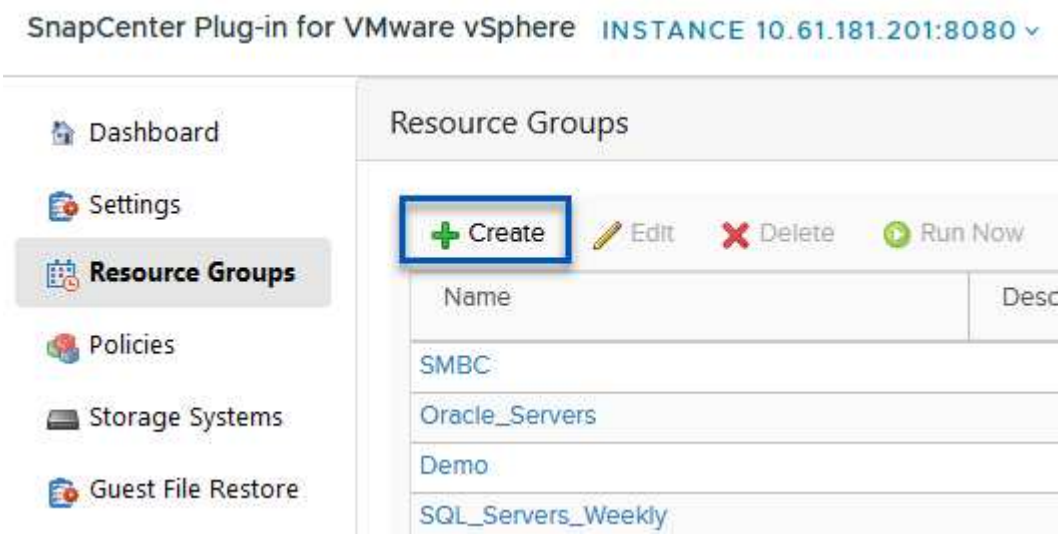
▼ **Crear grupos de recursos**

Los grupos de recursos contienen los almacenes de datos y las máquinas virtuales que se incluirán en un trabajo de respaldo, junto con la política y el programa de respaldo asociados.

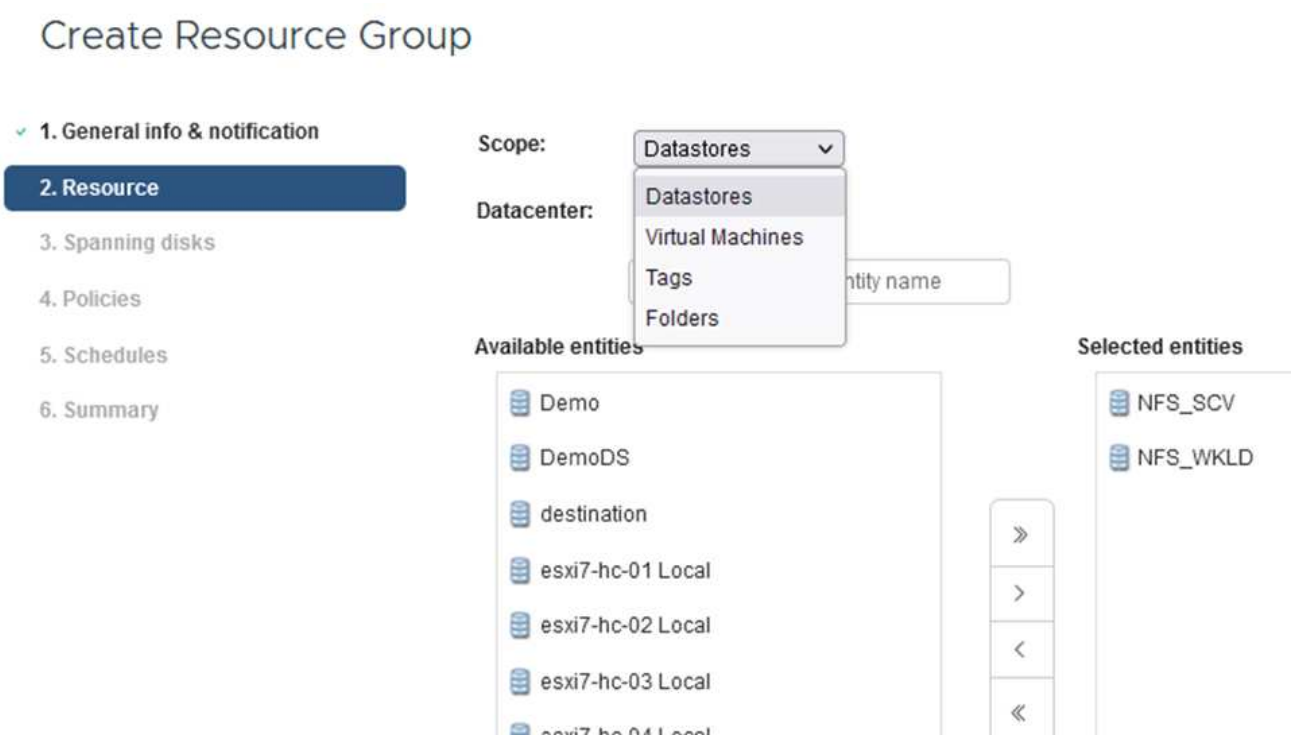
Revisar el "Crear grupos de recursos" sección de la documentación para obtener más información.

Para crear grupos de recursos, complete los siguientes pasos.

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Grupos de recursos** en el menú de la izquierda y haga clic en el botón **Crear**.

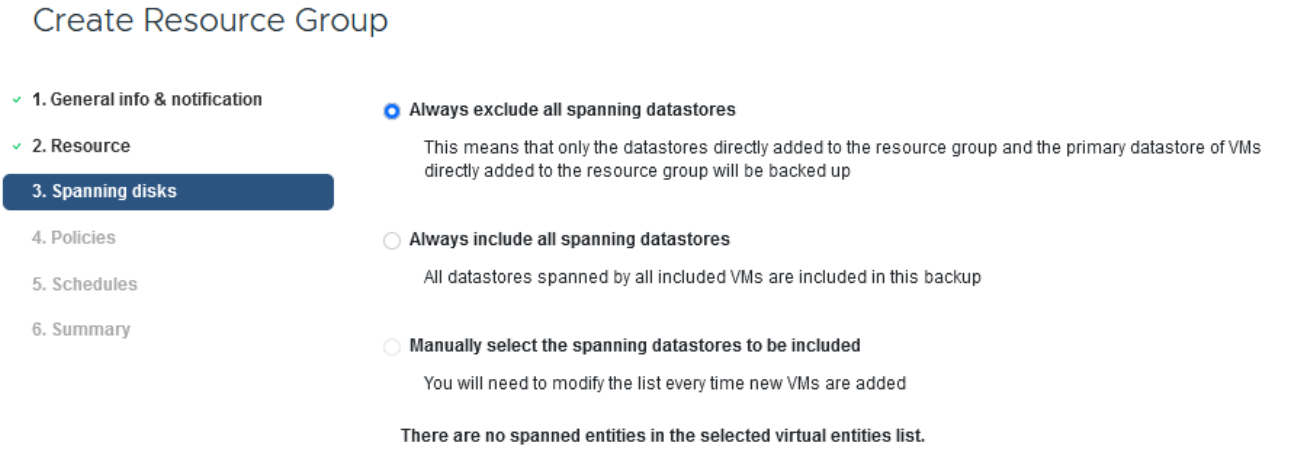


2. En el asistente Crear grupo de recursos, ingrese un nombre y una descripción para el grupo, así como la información necesaria para recibir notificaciones. Haga clic en **Siguiente**
3. En la página siguiente, seleccione los almacenes de datos y las máquinas virtuales que desee incluir en el trabajo de respaldo y luego haga clic en **Siguiente**.



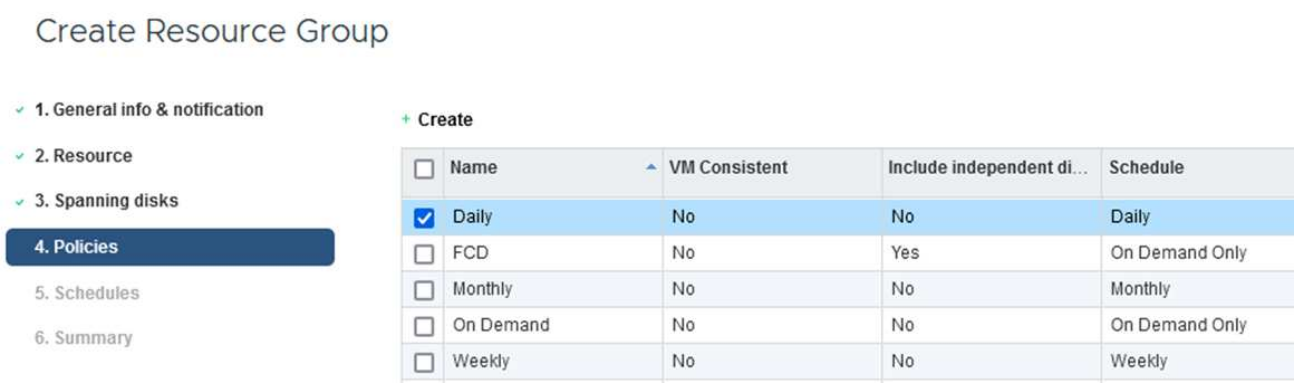
Tiene la opción de seleccionar máquinas virtuales específicas o almacenes de datos completos. Independientemente de lo que elija, se realiza un respaldo de todo el volumen (y del almacén de datos), ya que la copia de seguridad es el resultado de tomar una instantánea del volumen subyacente. En la mayoría de los casos, es más fácil elegir el almacén de datos completo. Sin embargo, si desea limitar la lista de máquinas virtuales disponibles al restaurar, puede elegir solo un subconjunto de máquinas virtuales para realizar una copia de seguridad.

4. Elija opciones para abarcar almacenes de datos para máquinas virtuales con VMDK que residen en múltiples almacenes de datos y luego haga clic en **Siguiente**.



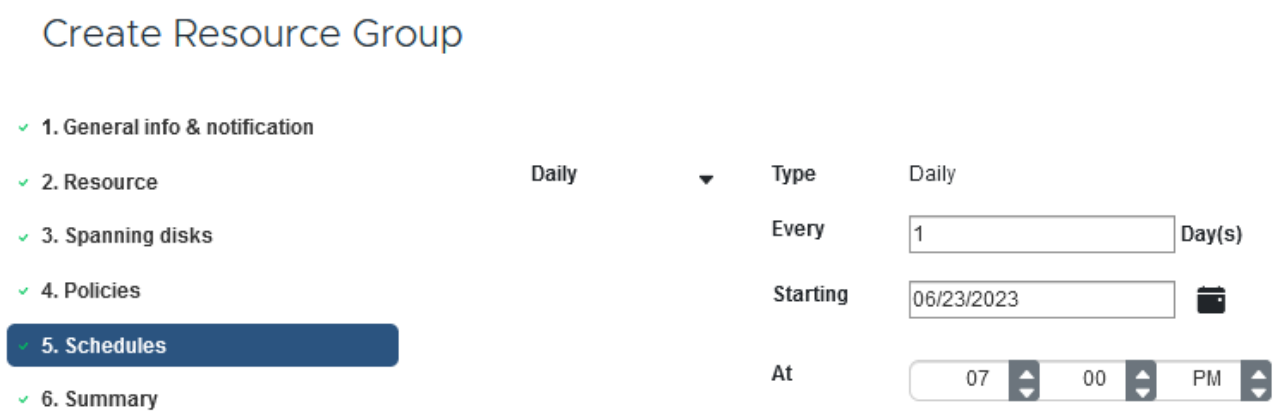
La función de copia de seguridad y recuperación para proteger las cargas de trabajo de VMware no admite actualmente la realización de copias de seguridad de máquinas virtuales con archivos VMDK que abarquen varios datastores.

5. En la página siguiente, seleccione las políticas que se asociarán con el grupo de recursos y haga clic en **Siguiente**.



Al realizar una copia de seguridad de snapshots gestionadas por SCV en almacenamiento de objetos mediante Backup and Recovery, cada grupo de recursos solo puede asociarse a una única política.

6. Seleccione una programación que determinará en qué momentos se ejecutarán las copias de seguridad. Haga clic en **Siguiente**.

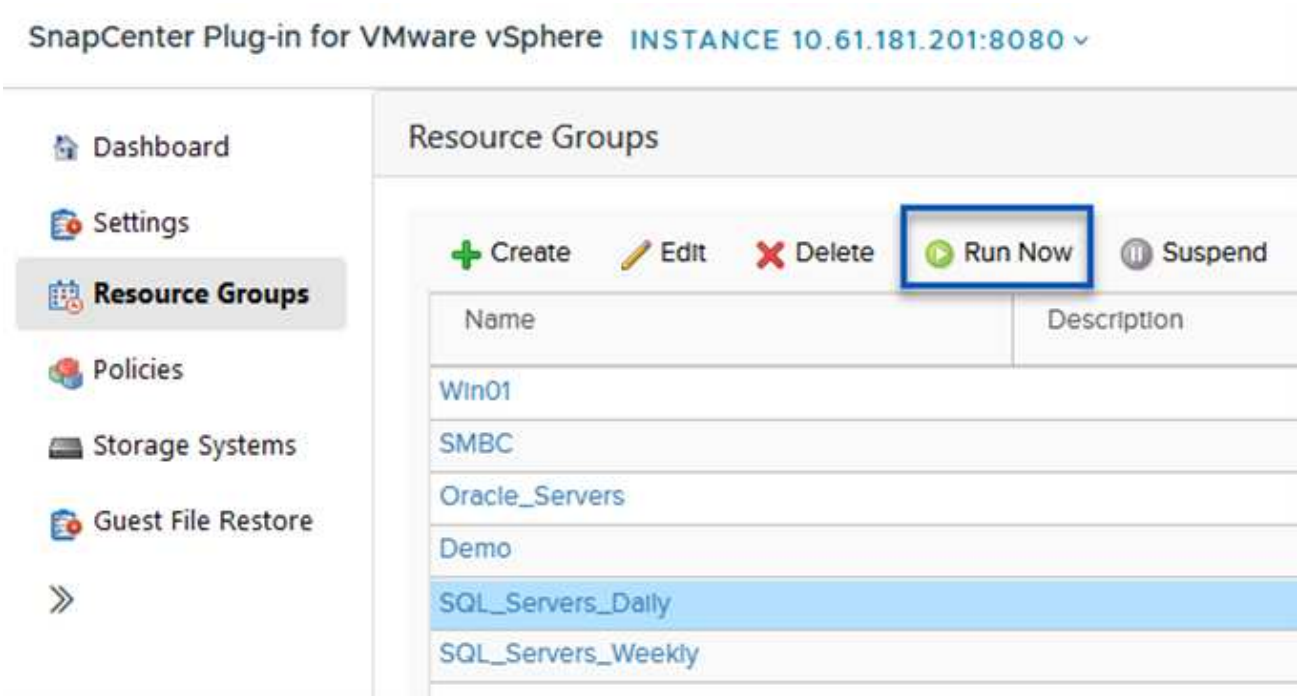


7. Por último, revise la página de resumen y luego haga clic en **Finalizar** para completar la creación del grupo de recursos.

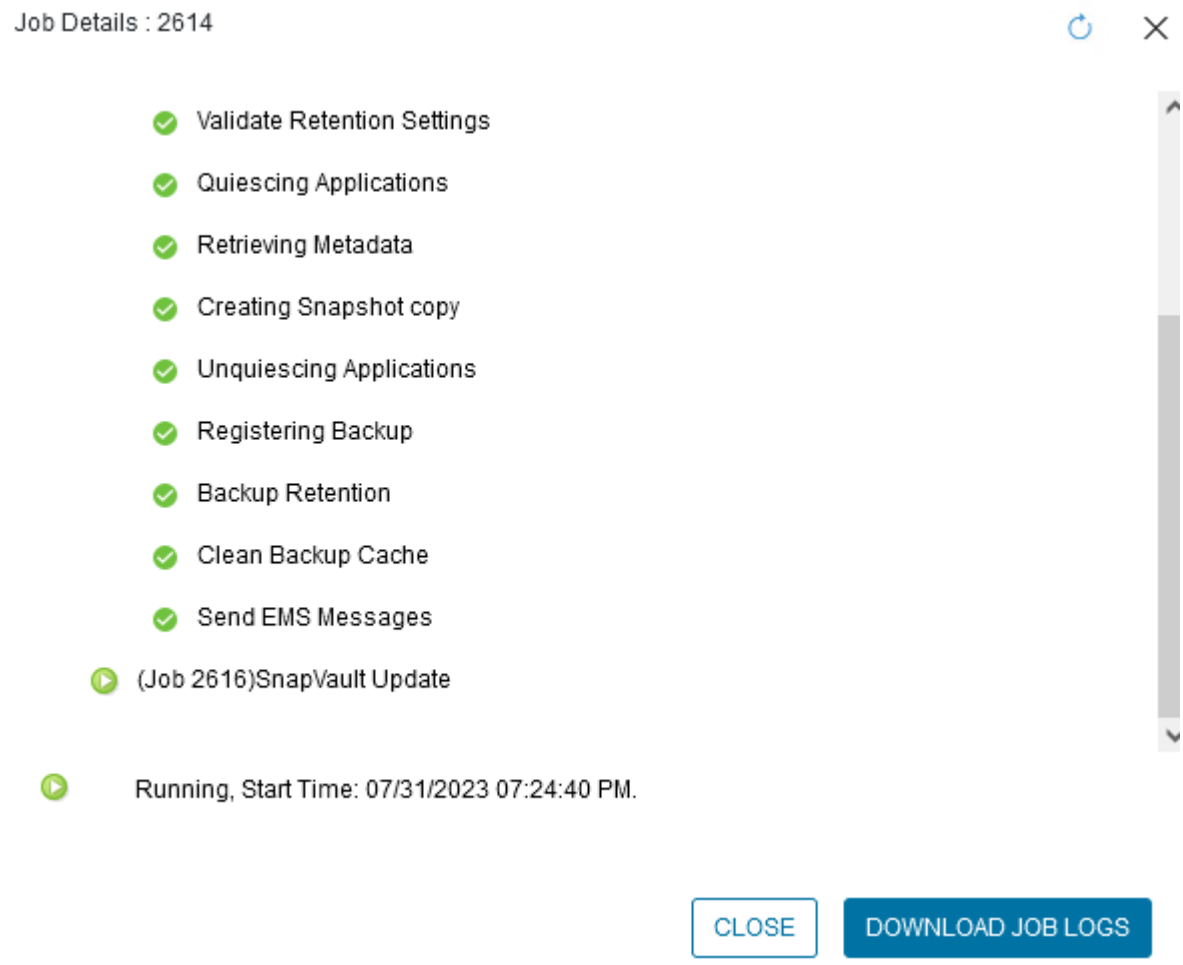
▼ Ejecutar una tarea de respaldo

En este último paso, ejecuta una tarea de copia de seguridad y supervisa su progreso. Debes completar correctamente al menos una tarea de copia de seguridad en SCV antes de poder detectar recursos desde NetApp Console.

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Grupos de recursos** en el menú de la izquierda.
2. Para iniciar un trabajo de respaldo, seleccione el grupo de recursos deseado y haga clic en el botón **Ejecutar ahora**.



3. Para supervisar el trabajo de respaldo, navegue hasta **Panel de control** en el menú de la izquierda. En **Actividades laborales recientes**, haga clic en el número de identificación del trabajo para monitorear el progreso del trabajo.



Configura backups en almacenamiento de objetos en NetApp Console

Para que NetApp Console gestione la infraestructura de datos de forma eficaz, necesitas instalar antes un agente de Console. El agente de Console ejecuta las acciones necesarias para detectar recursos y gestionar las operaciones de datos.

Para obtener más información sobre el agente de NetApp Console, consulta "Conoce los agentes de Console" en la documentación de NetApp Console.

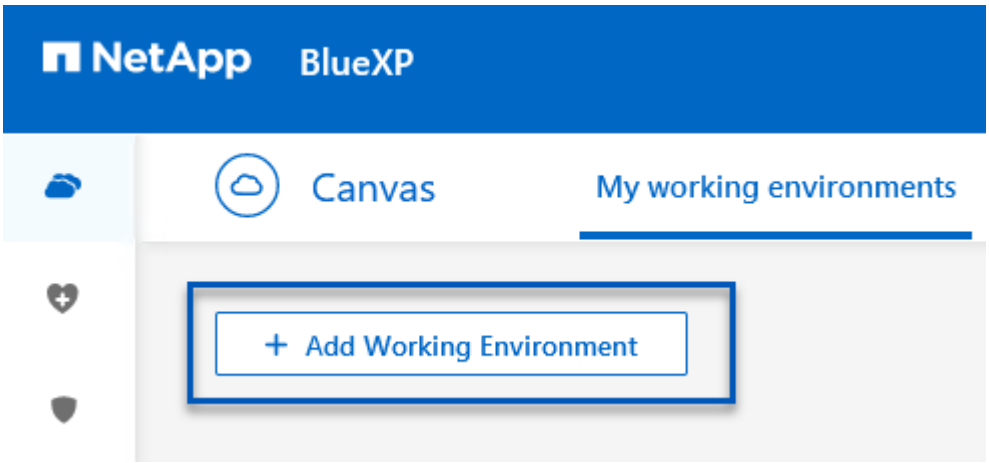
Una vez que instales el agente para el proveedor de nube que estés utilizando, podrás ver una representación gráfica del almacenamiento de objetos desde Systems.

Para configurar Backup and Recovery para hacer copias de seguridad de los datos gestionados por SCV on-premises, sigue estos pasos:

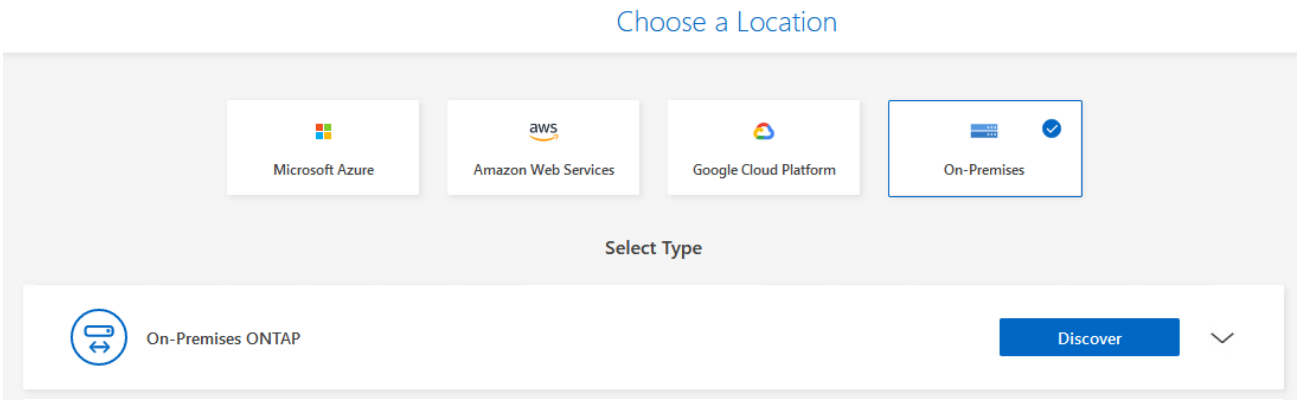
▼ **Añade el sistema de almacenamiento ONTAP a Systems**

El primer paso es añadir los sistemas de almacenamiento ONTAP locales a NetApp Console.

1. En Systems, haz clic en **+ Add** para empezar.



2. Seleccione **En las instalaciones** de la selección de ubicaciones y luego haga clic en el botón **Descubrir**.



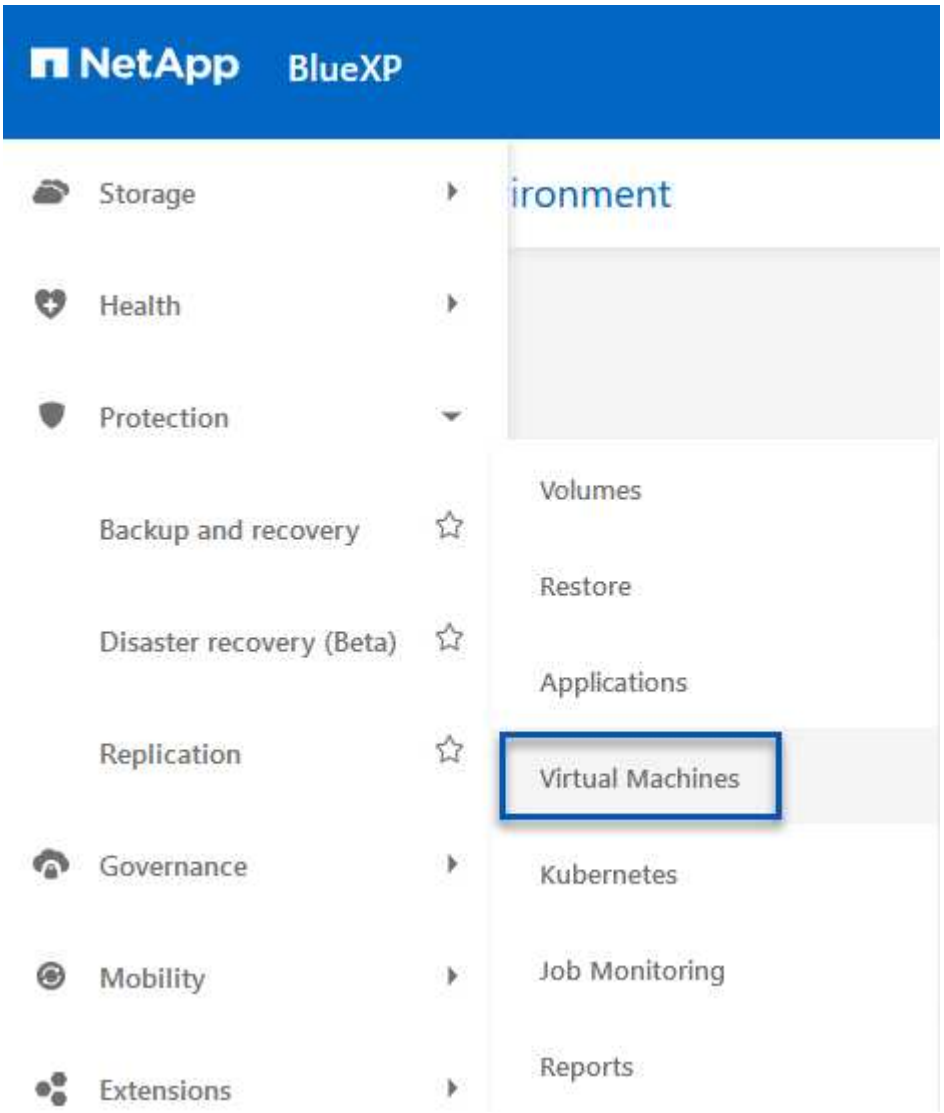
3. Complete las credenciales para el sistema de almacenamiento ONTAP y haga clic en el botón **Descubrir** para agregar el entorno de trabajo.



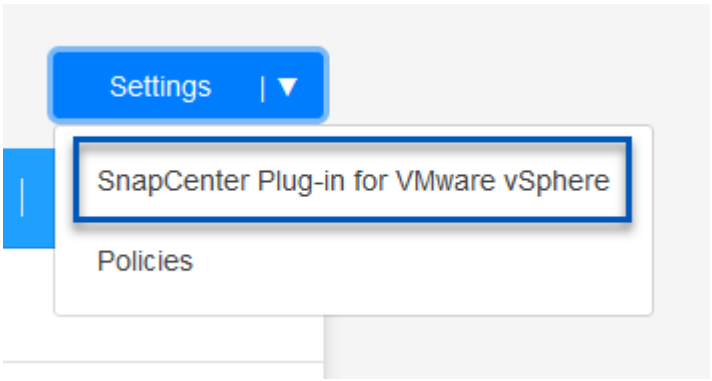
▼ **Descubra el dispositivo SCV local y vCenter**

Para descubrir el almacén de datos local y los recursos de la máquina virtual, agregue información para el agente de datos SCV y credenciales para el dispositivo de administración de vCenter.

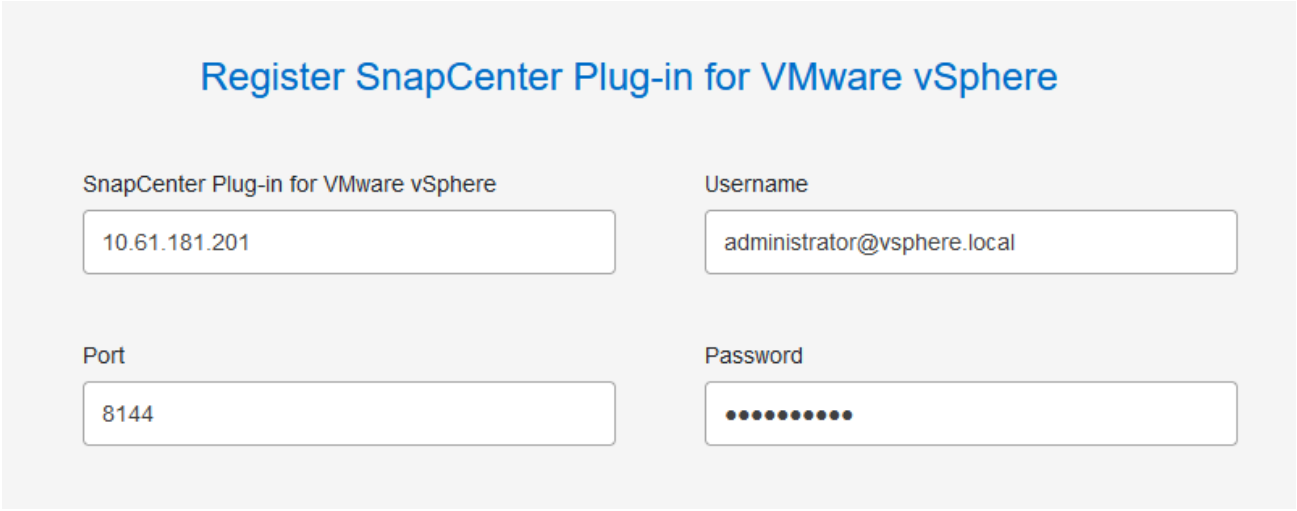
1. En la selección del menú de la izquierda de NetApp Console **Protection > Backup and recovery > Workloads >VMware**



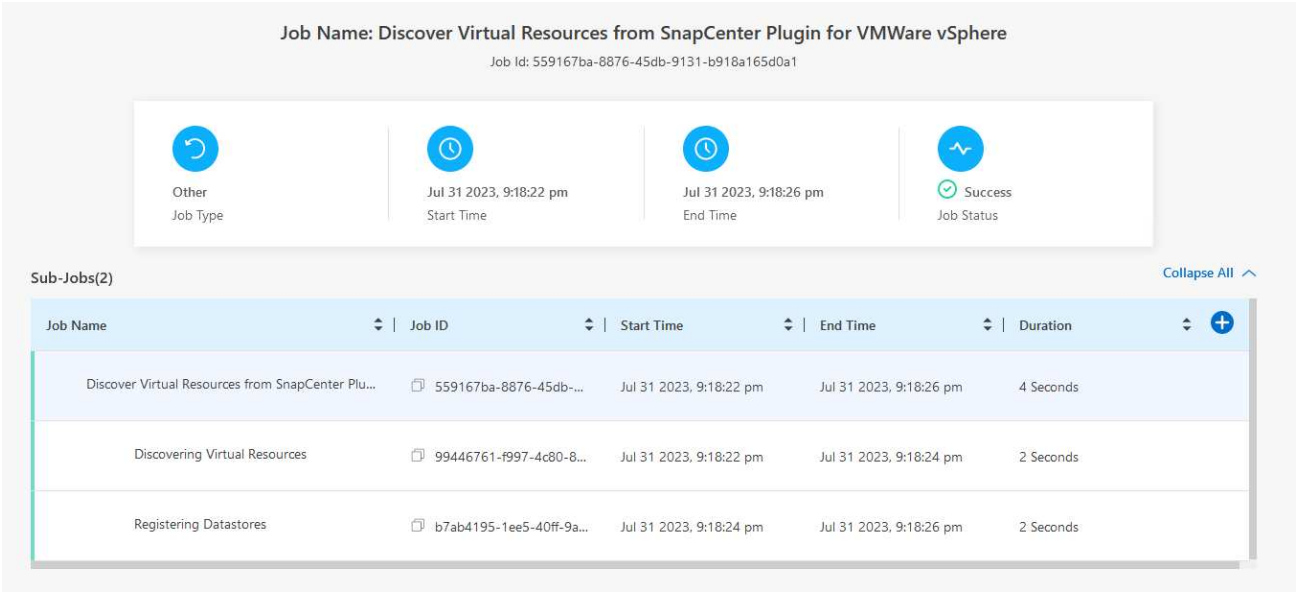
2. Desde la pantalla principal de Máquinas Virtuales acceda al menú desplegable **Configuración** y seleccione * SnapCenter Plug-in for VMware vSphere*.



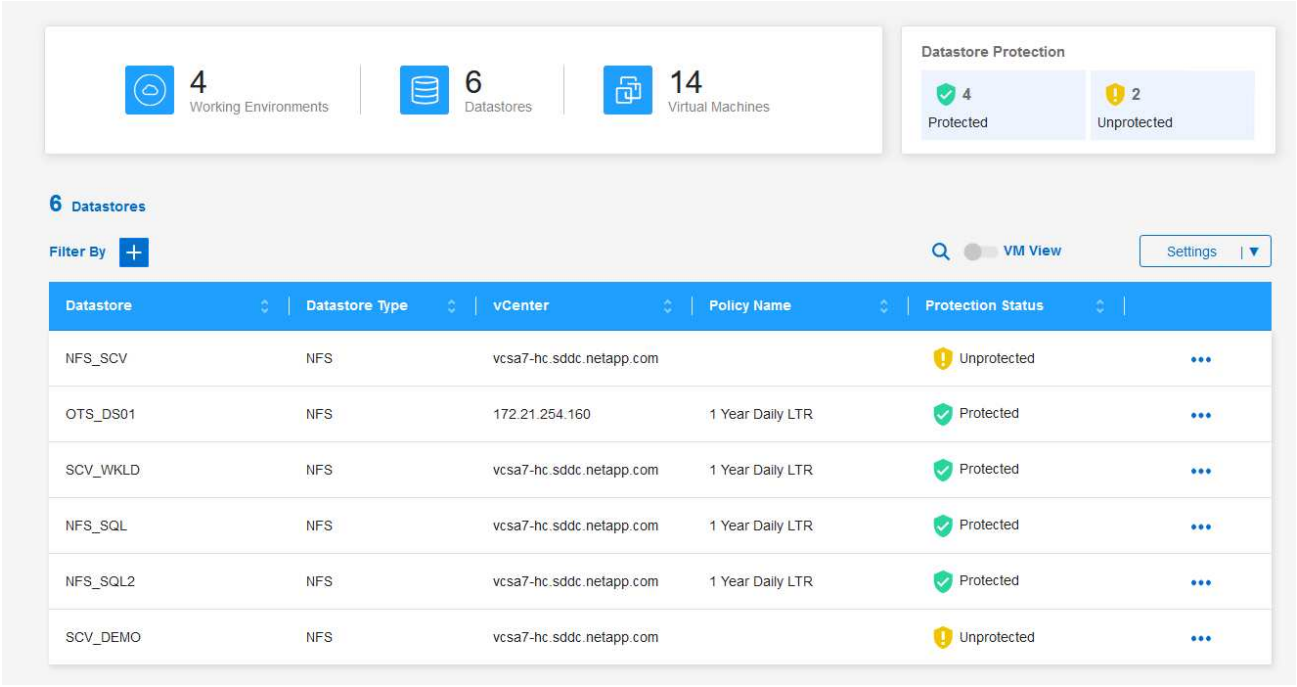
3. Haga clic en el botón **Registrar** y luego ingrese la dirección IP y el número de puerto para el dispositivo de complemento SnapCenter y el nombre de usuario y la contraseña para el dispositivo de administración de vCenter. Haga clic en el botón **Registrarse** para comenzar el proceso de descubrimiento.



4. El progreso de los trabajos se puede monitorear desde la pestaña Monitoreo de trabajos.



5. Una vez que se complete el descubrimiento, podrá ver los almacenes de datos y las máquinas virtuales en todos los dispositivos SCV descubiertos.

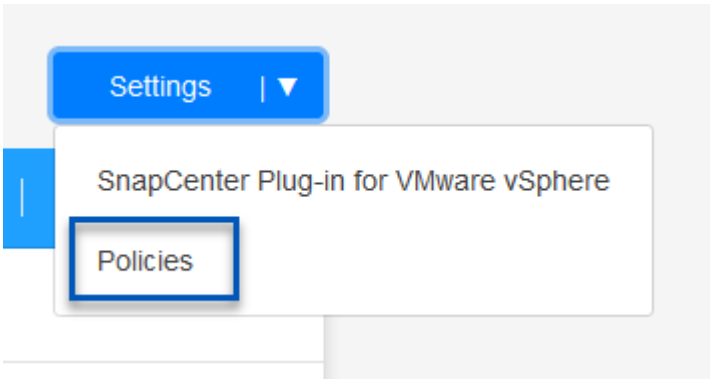


▼ Crear políticas de respaldo

En NetApp Backup and Recovery for Virtual Machines, crea políticas para especificar el período de retención, el origen del backup y la política de archivado.

Para obtener más información sobre cómo crear grupos de protección, consulta "Crear un grupo de protección".

1. Desde la página principal de NetApp Backup and Recovery for Virtual Machines, accede al menú desplegable **Settings** y selecciona **Policies**.



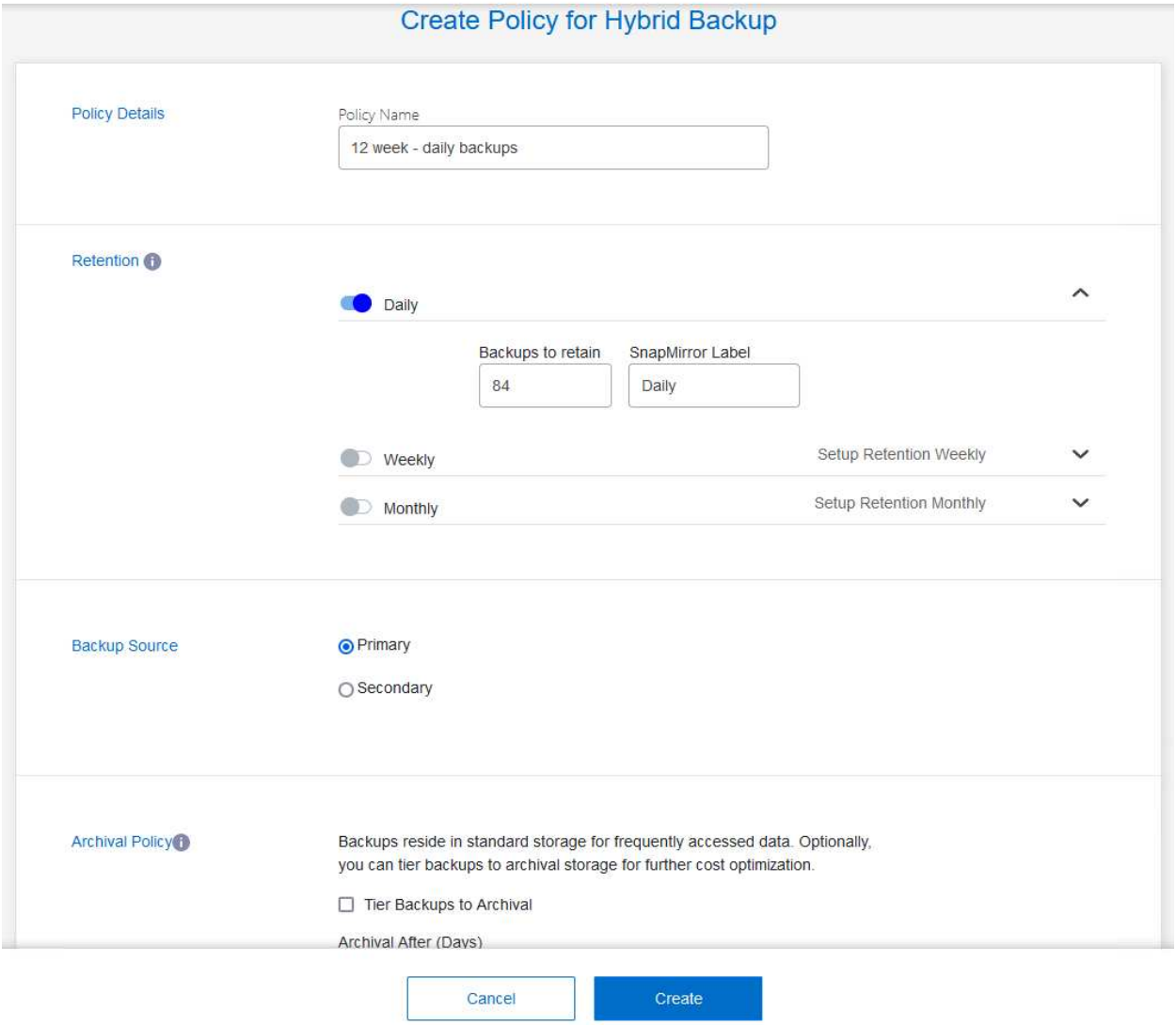
2. Haga clic en **Crear política** para acceder a la ventana **Crear política para copia de seguridad híbrida**.

   a. Agregar un nombre para la política

   b. Seleccione el período de retención deseado

   c. Seleccione si las copias de seguridad se obtendrán del sistema de almacenamiento ONTAP local primario o secundario

   d. De manera opcional, especifique después de qué período de tiempo las copias de seguridad se almacenarán en niveles en el almacenamiento de archivo para obtener ahorros de costos adicionales.



La etiqueta SnapMirror ingresada aquí se utiliza para identificar a qué copias de seguridad se aplicará la política. El nombre de la etiqueta debe coincidir con el nombre de la etiqueta en la política SCV local correspondiente.

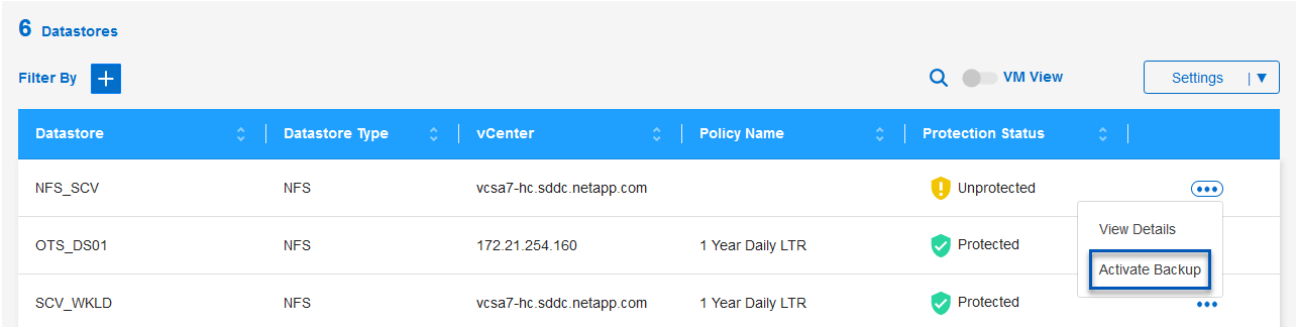
3. Haga clic en **Crear** para completar la creación de la política.

▼ **Copia de seguridad de almacenes de datos en Amazon Web Services**

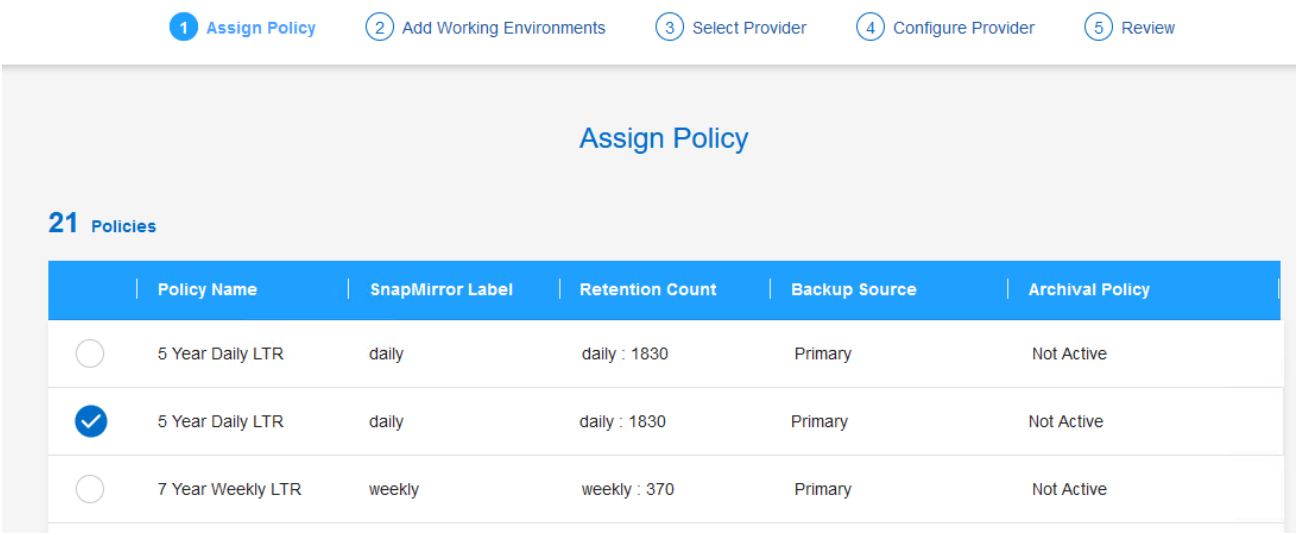
El paso final es activar la protección de datos para los almacenes de datos individuales y las máquinas virtuales. Los siguientes pasos describen cómo activar las copias de seguridad en AWS.

Para obtener más información consulta "Haz copias de seguridad de las cargas de trabajo de VMware".

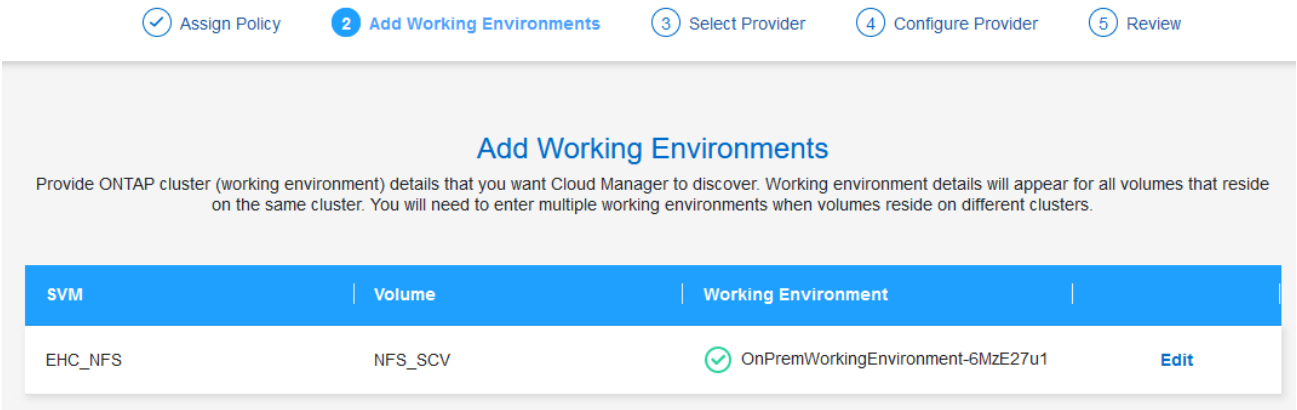
1. Desde la página principal de NetApp Backup and Recovery for Virtual Machines, accede al menú desplegable de configuración del datastore del que quieres hacer una copia de seguridad y selecciona **Activar copia de seguridad**.



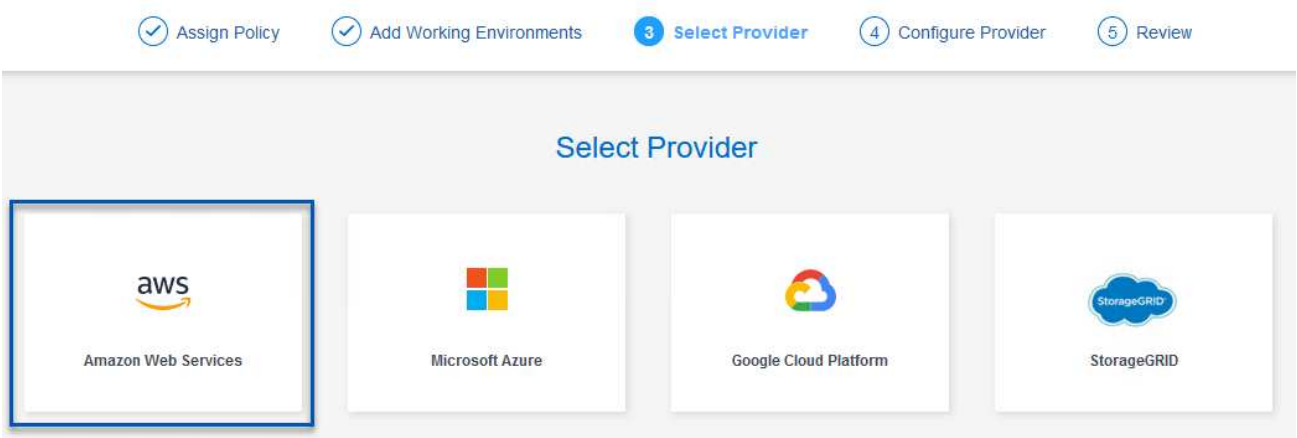
2. Asigne la política que se utilizará para la operación de protección de datos y haga clic en **Siguiente**.



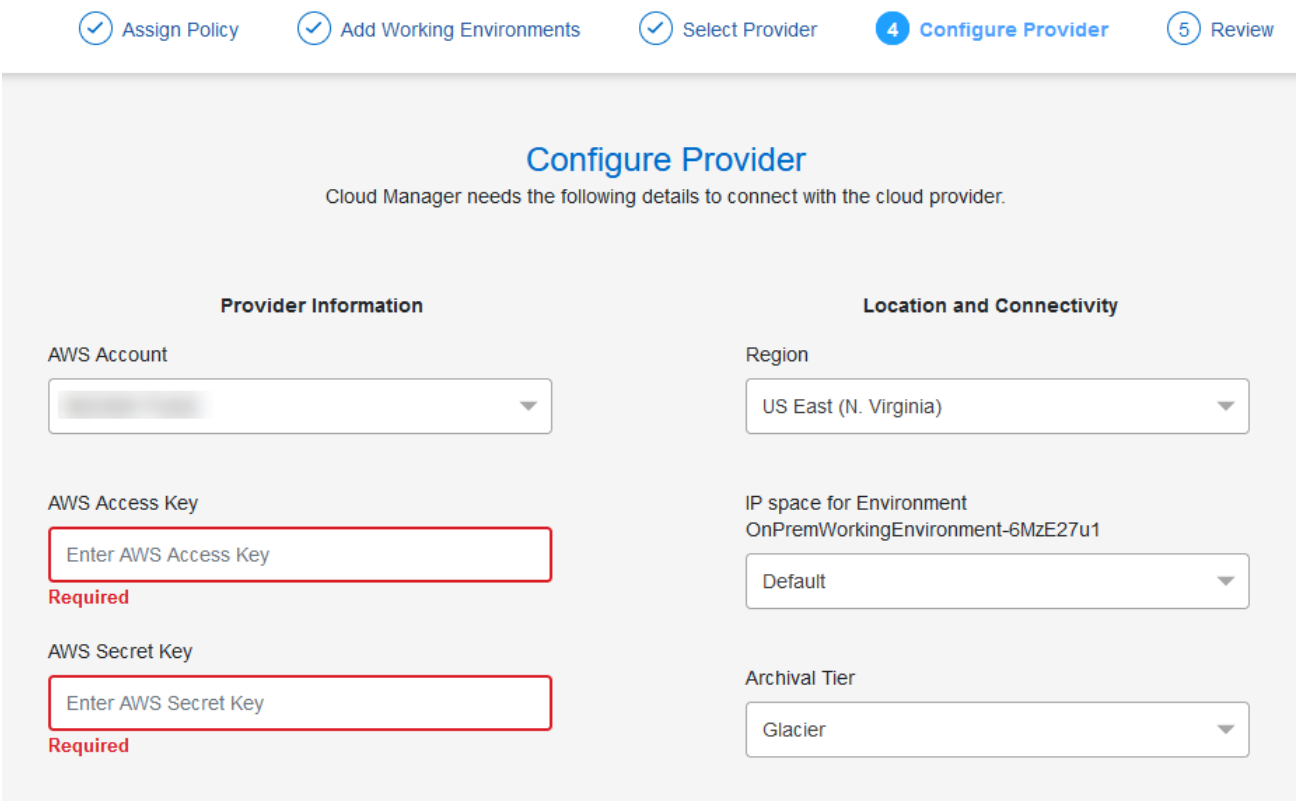
3. En la página **Agregar entornos de trabajo**, el almacén de datos y el entorno de trabajo deben aparecer con una marca de verificación si el entorno de trabajo se ha descubierto previamente. Si el entorno de trabajo no ha sido descubierto previamente puedes agregarlo aquí. Haga clic en **Siguiente** para continuar.



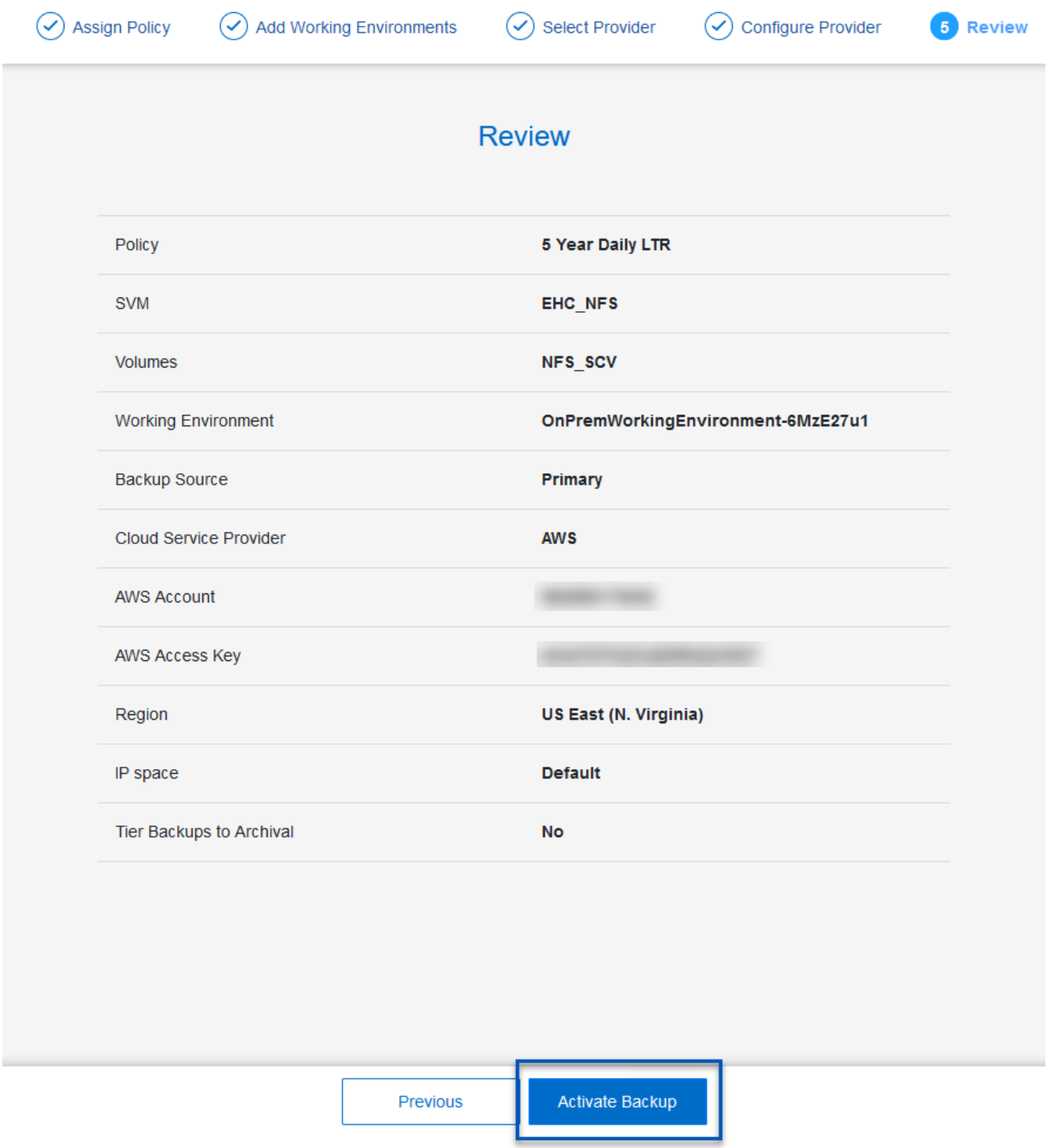
4. En la página **Seleccionar proveedor**, haga clic en AWS y luego haga clic en el botón **Siguiente** para continuar.



5. Complete la información de credenciales específicas del proveedor para AWS, incluida la clave de acceso y la clave secreta de AWS, la región y el nivel de archivo que se utilizará. Además, seleccione el espacio de IP de ONTAP para el sistema de almacenamiento de ONTAP local. Haga clic en **Siguiente**.



6. Por último, revise los detalles del trabajo de respaldo y haga clic en el botón **Activar respaldo** para iniciar la protección de datos del almacén de datos.



En este momento, es posible que la transferencia de datos no comience de inmediato. NetApp Backup and Recovery busca cada hora las instantáneas pendientes y, a continuación, las transfiere al almacenamiento de objetos.

Restaurar máquinas virtuales en caso de pérdida de datos

Garantizar la protección de sus datos es solo un aspecto de la protección integral de datos. Igualmente crucial es la capacidad de restaurar rápidamente los datos desde cualquier ubicación en caso de pérdida de datos o de un ataque de ransomware. Esta capacidad es vital para mantener operaciones comerciales sin problemas y alcanzar los objetivos del punto de recuperación.

NetApp ofrece una estrategia 3-2-1 altamente adaptable, que proporciona un control personalizado sobre los cronogramas de retención en las ubicaciones de almacenamiento primario, secundario y de objetos. Esta estrategia proporciona la flexibilidad de adaptar los enfoques de protección de datos a necesidades específicas.

Esta sección proporciona una visión general del proceso de restauración de datos tanto desde el SnapCenter Plug-in for VMware vSphere como desde NetApp Backup and Recovery para máquinas virtuales.

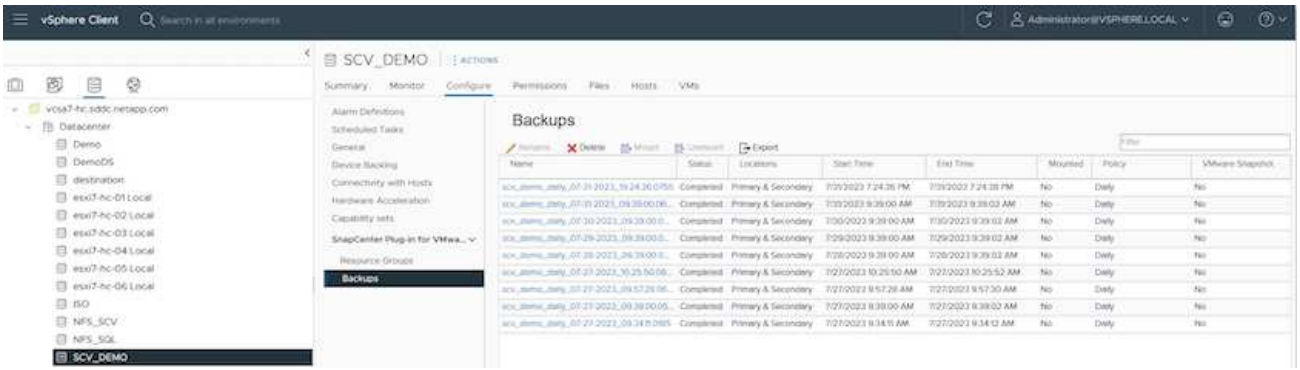
Restauración de máquinas virtuales desde el SnapCenter Plug-in for VMware vSphere

Para esta solución, las máquinas virtuales se restauraron en ubicaciones originales y alternativas. No todos los aspectos de las capacidades de restauración de datos de SCV estarán cubiertos en esta solución. Para obtener información detallada sobre todo lo que SCV tiene para ofrecer, consulte el "Restaurar máquinas virtuales a partir de copias de seguridad" en la documentación del producto.

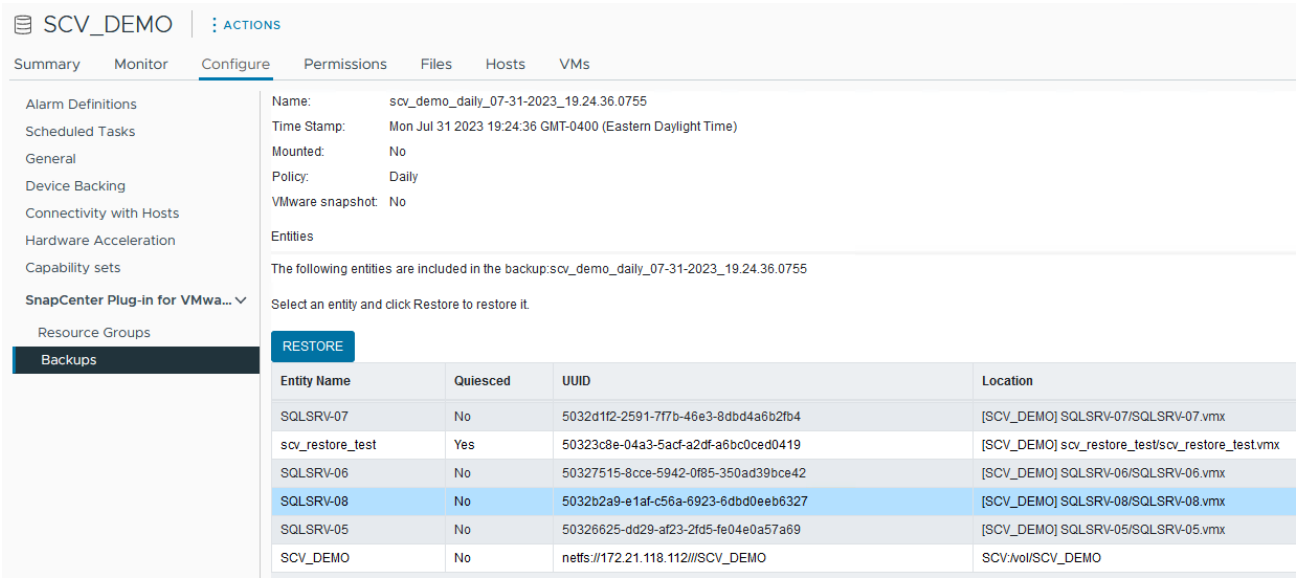
▼ **Restaurar máquinas virtuales desde SCV**

Complete los siguientes pasos para restaurar una máquina virtual desde el almacenamiento primario o secundario.

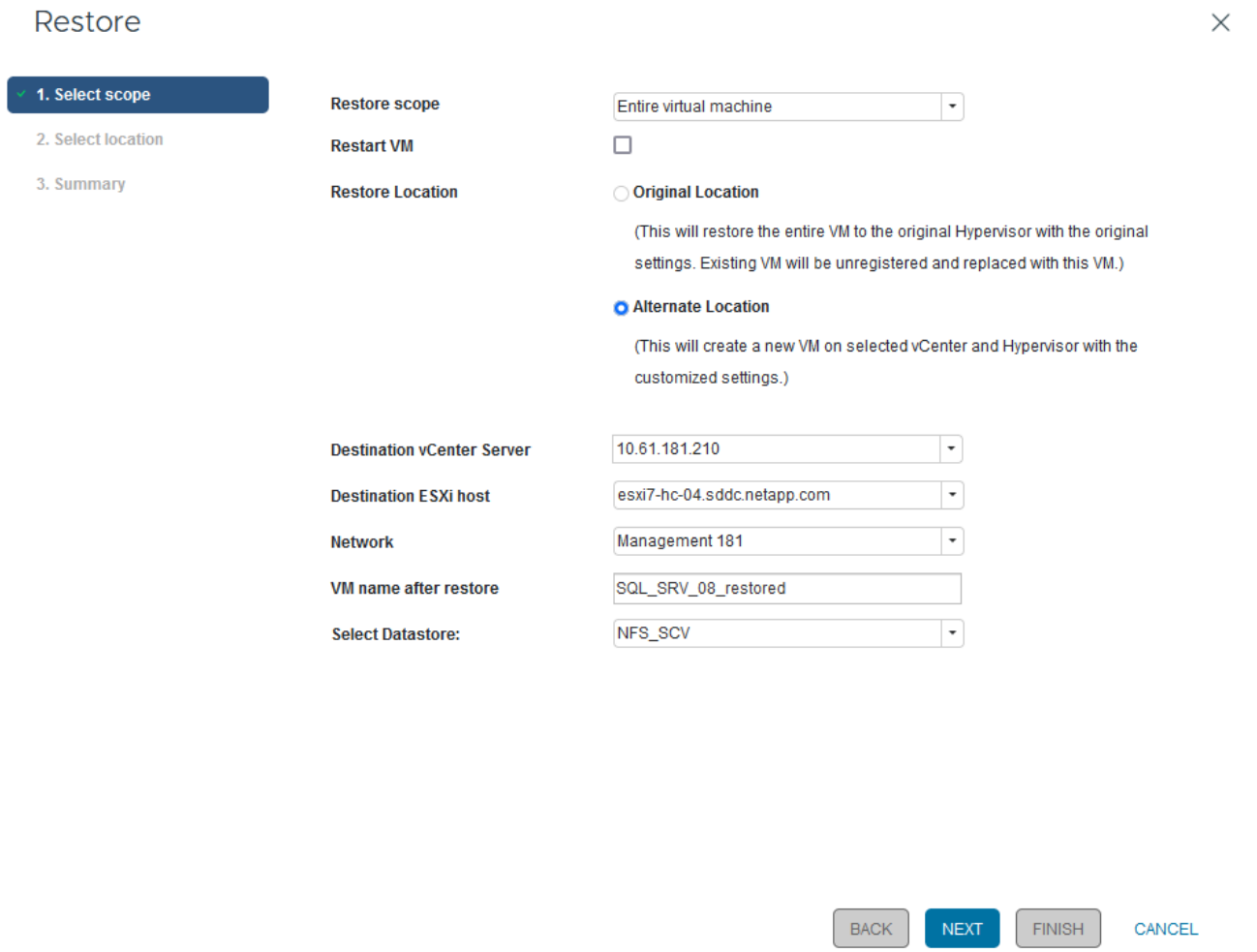
1. Desde el cliente vCenter, navegue a **Inventario > Almacenamiento** y haga clic en el almacén de datos que contiene las máquinas virtuales que desea restaurar.
2. Desde la pestaña **Configurar** haga clic en **Copias de seguridad** para acceder a la lista de copias de seguridad disponibles.



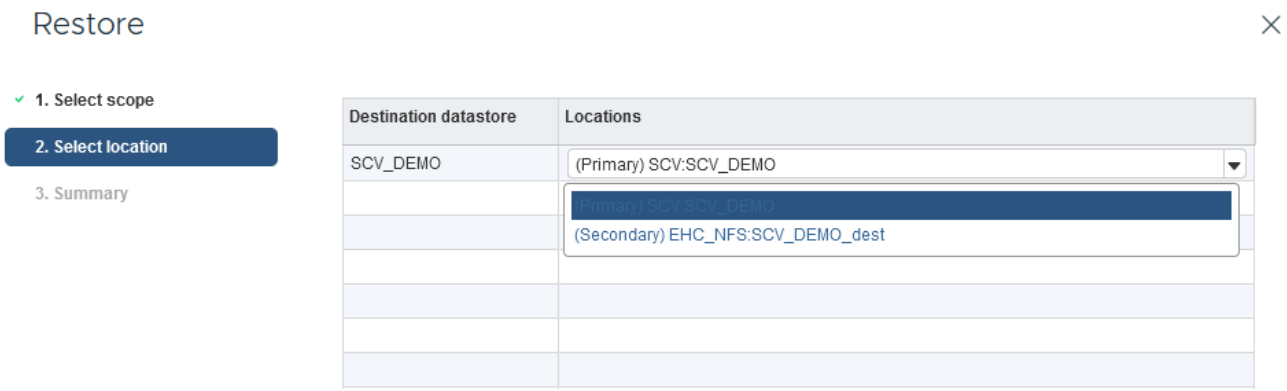
3. Haga clic en una copia de seguridad para acceder a la lista de máquinas virtuales y luego seleccione una máquina virtual para restaurar. Haga clic en **Restaurar**.



4. Desde el asistente de restauración, seleccione restaurar toda la máquina virtual o un VMDK específico. Seleccione instalar en la ubicación original o en una ubicación alternativa, proporcione el nombre de la máquina virtual después de la restauración y el almacén de datos de destino. Haga clic en **Siguiente**.



5. Elija realizar la copia de seguridad desde la ubicación de almacenamiento principal o secundaria.



6. Por último, revise un resumen del trabajo de respaldo y haga clic en Finalizar para comenzar el proceso de restauración.

Restaurar máquinas virtuales desde NetApp Backup and Recovery for Virtual Machines

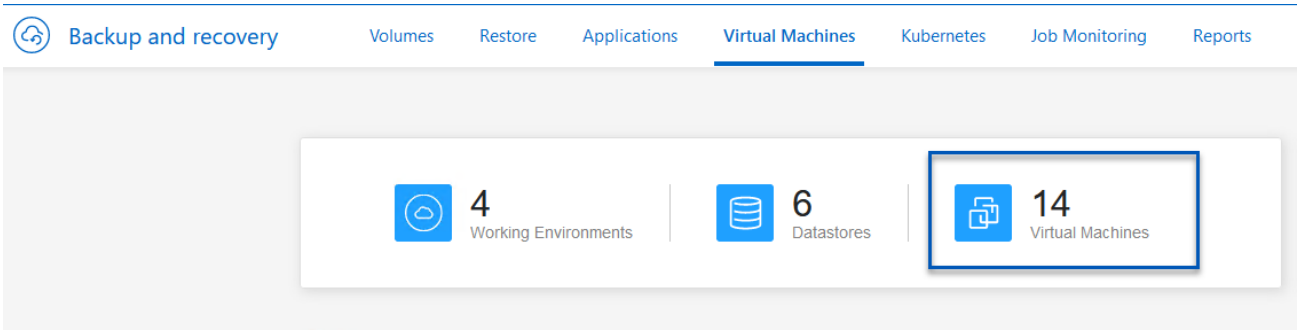
NetApp Backup and Recovery for Virtual Machines permite restaurar las máquinas virtuales a su ubicación original. Se accede a las funciones de restauración a través de la consola web de NetApp Backup and Recovery.

Para obtener más información consulta "Restaurar datos de máquinas virtuales desde la nube".

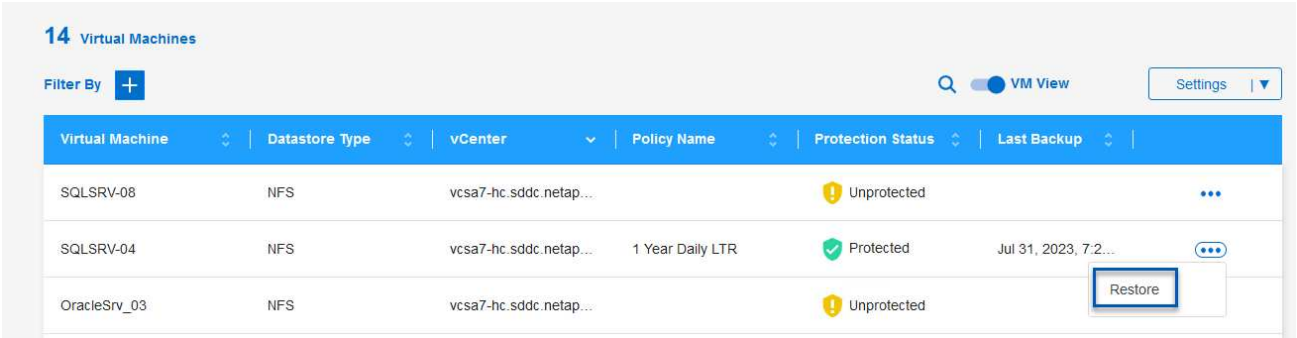
▼ **Restaura máquinas virtuales desde NetApp Backup and Recovery**

Para restaurar una máquina virtual desde NetApp Backup and Recovery, sigue estos pasos.

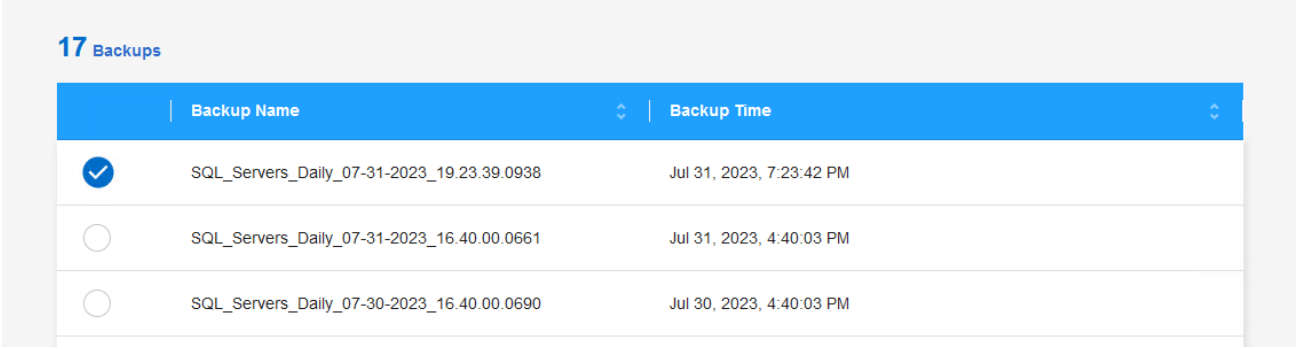
1. Vaya a **Protección > Copia de seguridad y recuperación > Máquinas virtuales** y haga clic en Máquinas virtuales para ver la lista de máquinas virtuales disponibles para restaurar.



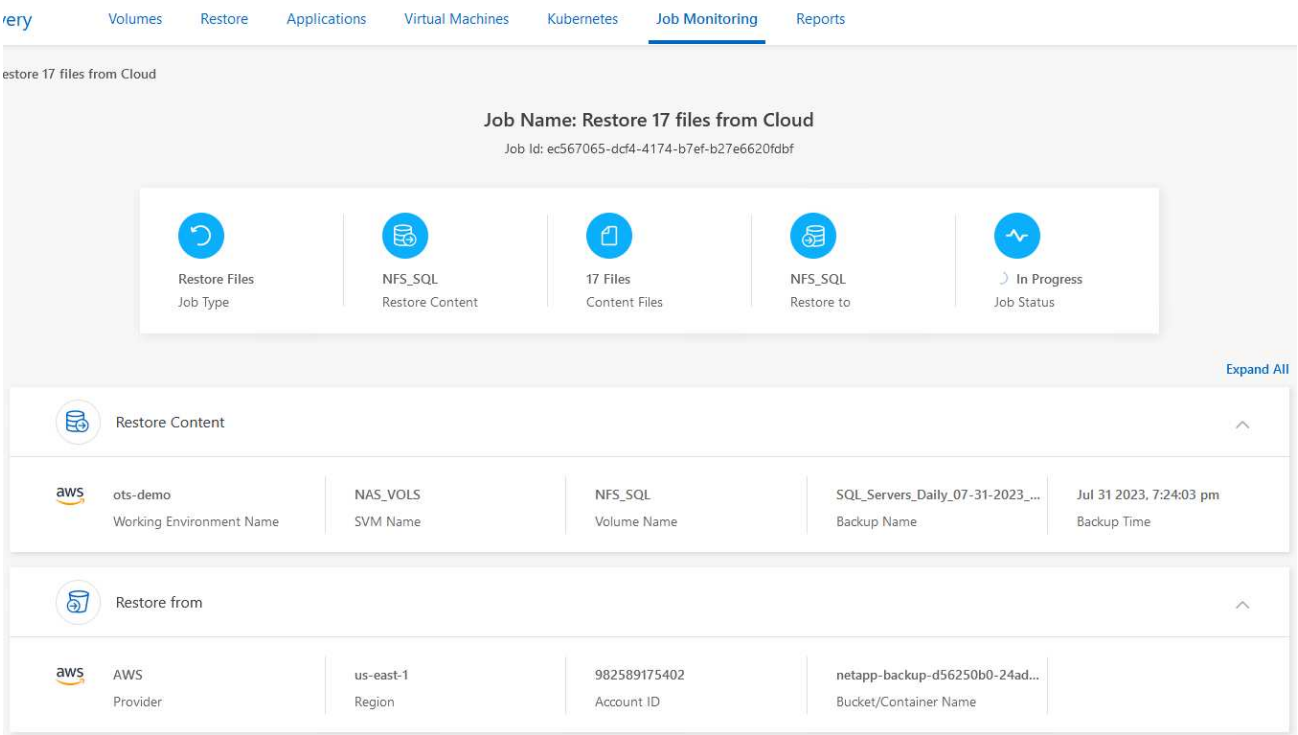
2. Acceda al menú desplegable de configuración de la máquina virtual que se restaurará y seleccione



3. Seleccione la copia de seguridad que desea restaurar y haga clic en **Siguiente**.



4. Revise un resumen del trabajo de respaldo y haga clic en **Restaurar** para iniciar el proceso de restauración.
5. Supervise el progreso del trabajo de restauración desde la pestaña **Supervisión del trabajo**.



Conclusión

La estrategia de backup 3-2-1, cuando se implementa con SnapCenter Plug-in for VMware vSphere y NetApp Backup and Recovery para máquinas virtuales, ofrece una solución sólida, fiable y rentable para la protección de datos. Esta estrategia no solo garantiza la redundancia y la accesibilidad de los datos, sino que también ofrece la flexibilidad de restaurar datos desde cualquier ubicación y tanto desde sistemas de almacenamiento ONTAP locales como desde almacenamiento de objetos basado en la nube.

El caso de uso que se presenta en esta documentación se centra en tecnologías de protección de datos probadas que destacan la integración entre NetApp, VMware y los principales proveedores de cloud. El SnapCenter Plug-in for VMware vSphere proporciona una integración perfecta con VMware vSphere, lo que permite una gestión eficiente y centralizada de las operaciones de protección de datos. Esta integración agiliza los procesos de backup y recuperación de las máquinas virtuales, lo que permite programar, supervisar y realizar operaciones de restauración flexibles fácilmente dentro del ecosistema de VMware. NetApp Backup

and Recovery para máquinas virtuales proporciona el uno (1) de 3-2-1 al ofrecer backups seguros en entrehierro de los datos de las máquinas virtuales en almacenamiento de objetos basado en cloud. La interfaz intuitiva y el flujo de trabajo lógico proporcionan una plataforma segura para el archivado a largo plazo de datos críticos.

Información adicional

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

- "Documentación del SnapCenter Plug-in for VMware vSphere"
- "NetApp documentación de la consola"

NetApp Disaster Recovery

Descripción general

La recuperación ante desastres es una de las principales preocupaciones de todos los administradores de VMware. Como VMware encapsula servidores completos en una serie de archivos que conforman la máquina virtual, los administradores aprovechan técnicas basadas en almacenamiento en bloques, como clones, instantáneas y réplicas, para proteger estas máquinas virtuales. Las cabinas ONTAP ofrecen replicación integrada para transferir datos de volumen y, por lo tanto, las máquinas virtuales que residen en los LUN de datastore designados, de un sitio a otro. NetApp Disaster Recovery se integra con vSphere y automatiza todo el flujo de trabajo para una conmutación por error y una conmutación de retorno fluidas en caso de desastre. Al combinar la replicación de almacenamiento con la automatización inteligente, los administradores ahora tienen una forma manejable no solo de configurar, automatizar y probar los planes de recuperación ante desastres, sino también los medios para ejecutarlos fácilmente en caso de desastre.

La parte que consume más tiempo de una conmutación por error de DR en un entorno VMware vSphere es la ejecución de los pasos necesarios para inventariar, registrar, reconfigurar y encender las máquinas virtuales en el sitio de DR. Una solución ideal tiene un RPO bajo (medido en minutos) y un RTO bajo (medido en minutos a horas). Un factor que a menudo se pasa por alto en una solución de DR es la capacidad de probar la solución de DR de manera eficiente en un intervalo periódico.

Para diseñar una solución de recuperación ante desastres, tenga en cuenta los siguientes factores:

- El objetivo de tiempo de recuperación (RTO). El RTO es la rapidez con la que una empresa puede recuperarse de un desastre o, más específicamente, el tiempo que lleva ejecutar el proceso de recuperación para que los servicios empresariales estén disponibles nuevamente.
- El objetivo del punto de recuperación (RPO). El RPO es la antigüedad de los datos recuperados después de que se pusieron a disposición, en relación con el momento en que ocurrió el desastre.
- Escalabilidad y adaptabilidad. Este factor incluye la capacidad de aumentar los recursos de almacenamiento de forma incremental a medida que aumenta la demanda.

Para obtener más información técnica sobre las soluciones disponibles, consulte:

- "NetApp Disaster Recovery para almacenes de datos NFS"

- "NetApp Disaster Recovery para almacenes de datos VMFS"

NetApp Disaster Recovery para almacenes de datos NFS

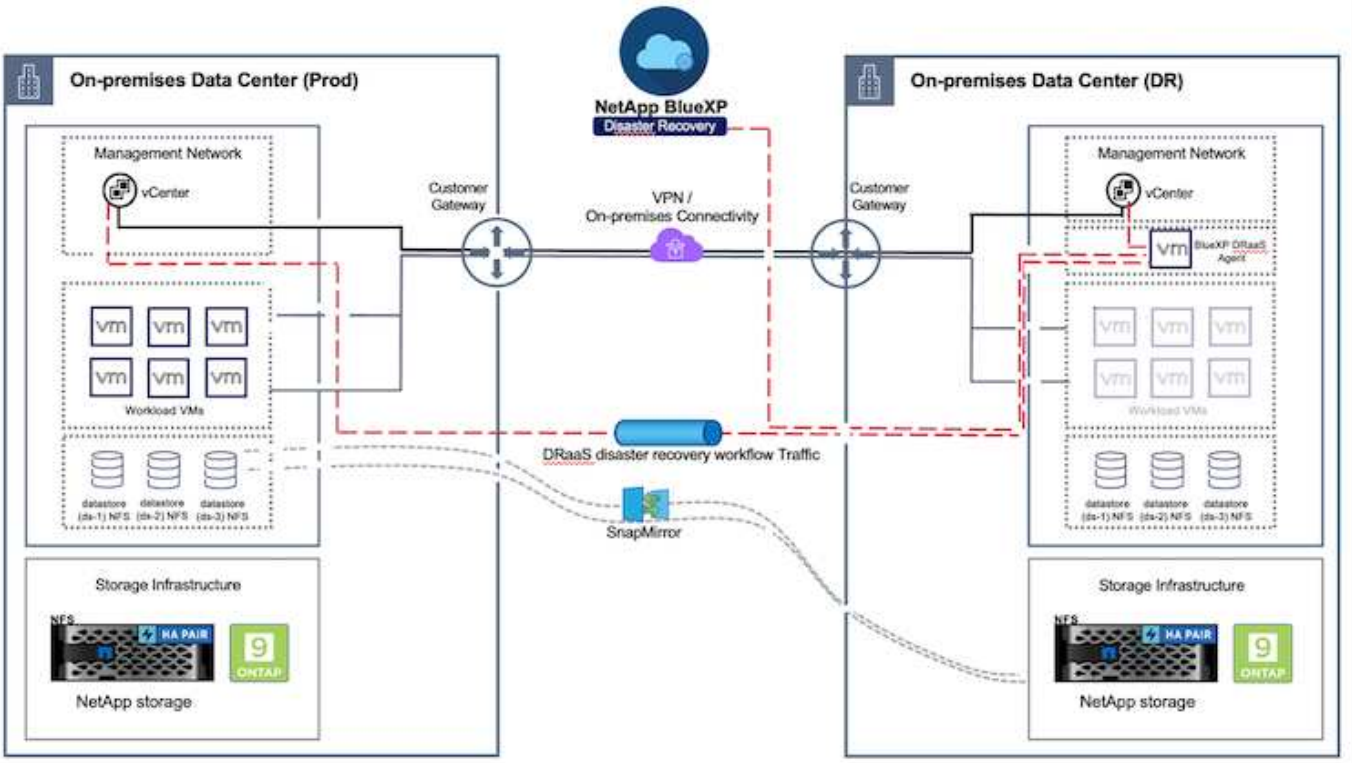
NetApp Disaster Recovery para almacenes de datos NFS

La implementación de la recuperación ante desastres a través de la replicación a nivel de bloque desde el sitio de producción al sitio de recuperación ante desastres es un método resiliente y rentable para proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos, como ataques de ransomware. Al utilizar la replicación SnapMirror de NetApp , las cargas de trabajo de VMware que se ejecutan en sistemas ONTAP locales con almacén de datos NFS se pueden replicar a otro sistema de almacenamiento ONTAP ubicado en un centro de datos de recuperación designado donde también se implementa VMware.

En esta sección del documento se describe la configuración de NetApp Disaster Recovery para configurar la recuperación ante desastres de las máquinas virtuales de VMware locales en otro sitio designado. Como parte de esta configuración, se incluye el agente de Console, la incorporación de las cabinas ONTAP, la definición de sitios y la asociación de VMware vCenter. Además, este documento detalla cómo configurar la replicación entre sitios y cómo configurar y probar un plan de recuperación. La última sección incluye instrucciones para realizar una conmutación por error completa del sitio y cómo volver atrás cuando el sitio principal se haya recuperado y vuelva a estar en línea.

Con Disaster Recovery, que forma parte de NetApp Data Services, las empresas pueden detectar fácilmente sus vCenters de VMware locales y el almacenamiento ONTAP. Luego, las organizaciones pueden crear grupos de recursos, crear un plan de recuperación, asociarlo con grupos de recursos y probar o ejecutar el failover y el failback. SnapMirror proporciona replicación de bloques a nivel de almacenamiento para mantener los dos sitios actualizados con cambios incrementales, lo que da como resultado un objetivo de punto de recuperación (RPO) de hasta 5 minutos. Además, es posible simular procedimientos de recuperación ante desastres sin afectar la producción ni generar costos de almacenamiento adicionales.

Disaster Recovery aprovecha la tecnología FlexClone de ONTAP para crear una copia con gestión eficiente del espacio del datastore NFS a partir de la última Snapshot replicada en el sitio de recuperación ante desastres. Después de completar la prueba de recuperación ante desastres, los clientes pueden eliminar fácilmente el entorno de prueba sin afectar a los recursos de producción replicados reales. En caso de un failover real, Disaster Recovery coordina todos los pasos necesarios para poner en marcha automáticamente las máquinas virtuales protegidas en el sitio de recuperación ante desastres designado con solo unos clics. El servicio también revertirá la relación de SnapMirror al sitio principal y replicará cualquier cambio del sitio secundario al principal para una operación de failback, cuando sea necesario. Todas estas capacidades tienen un coste mucho menor que otras alternativas conocidas.

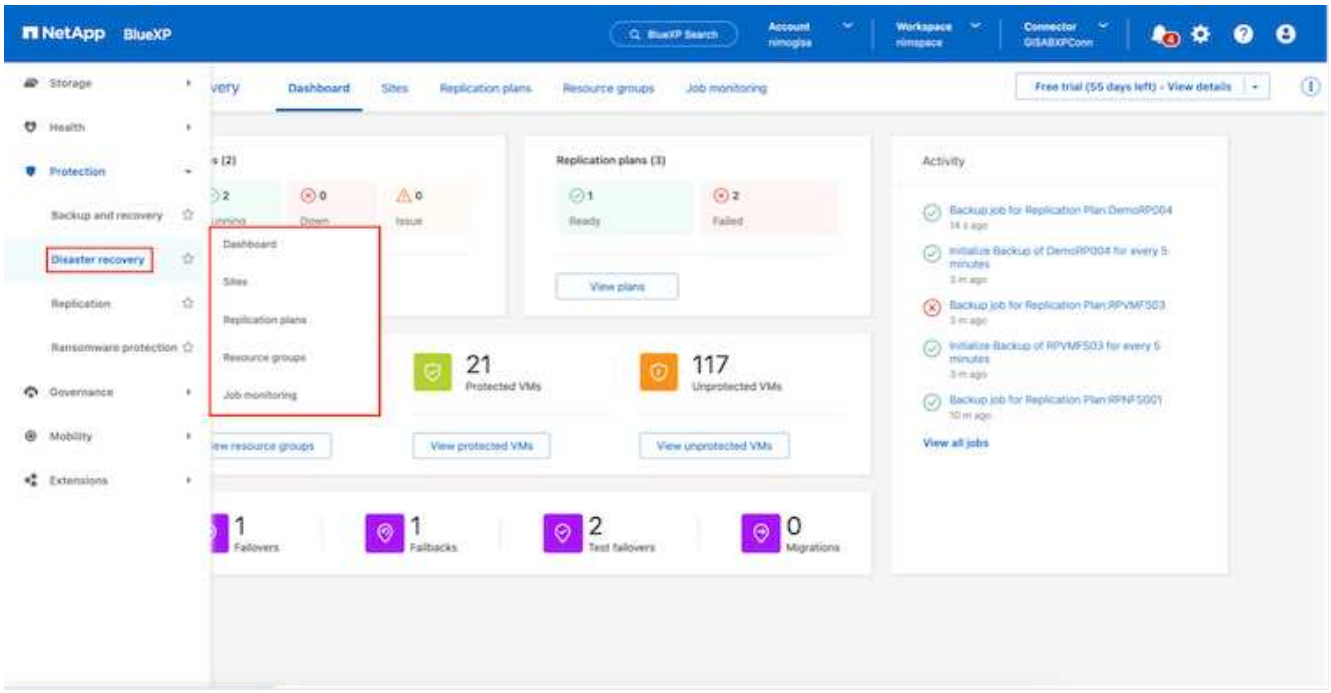


Para obtener información actualizada y conocer las versiones compatibles de vCenter Server, ESXi y ONTAP para la recuperación ante desastres, consulta "Configuraciones compatibles con la recuperación ante desastres".

Empezando

Para empezar a utilizar NetApp Disaster Recovery, utiliza NetApp console y luego accede al servicio.

1. Inicia sesión en NetApp Console.
2. En la navegación izquierda de NetApp Console, selecciona Protección > Recuperación ante desastres.
3. Aparece el Disaster Recovery Dashboard.

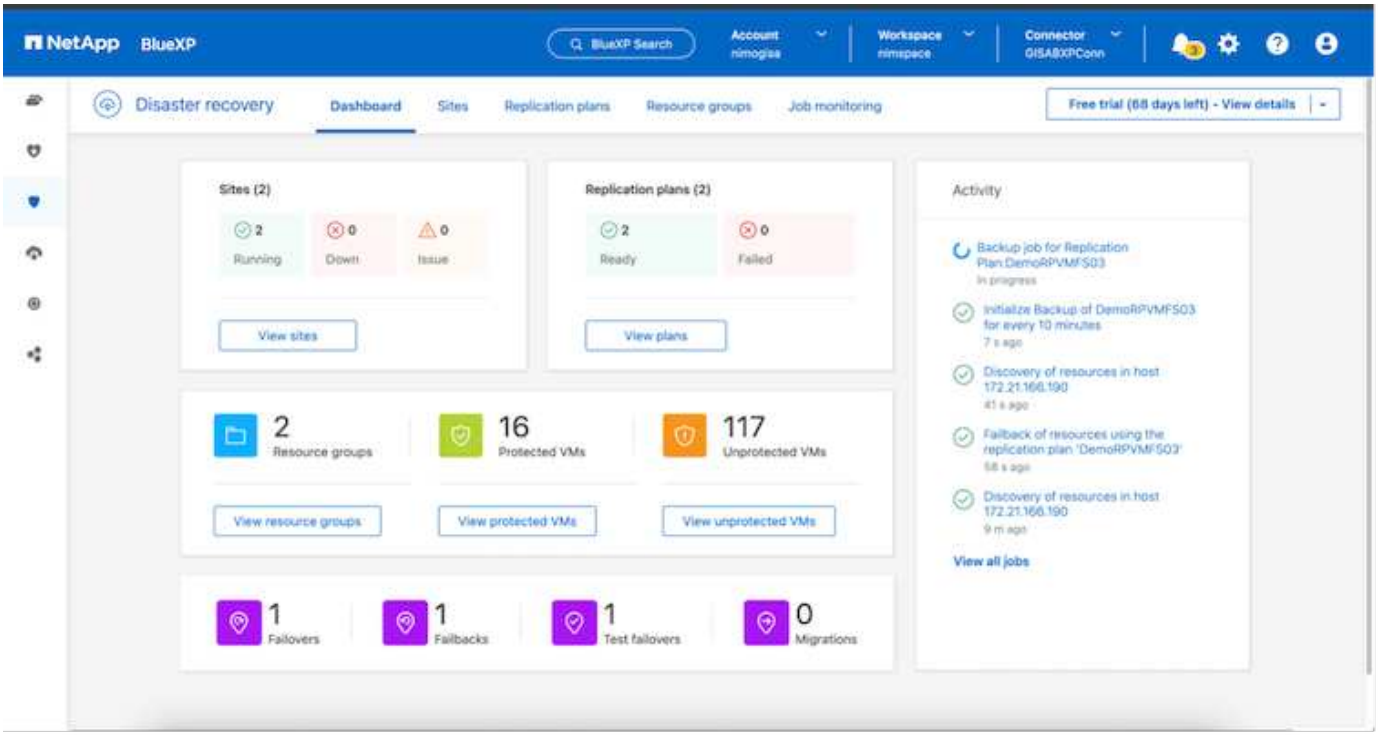


Antes de configurar el plan de recuperación ante desastres, asegúrate de que se cumplan los siguientes requisitos previos:

- El agente de NetApp Console está implementado.
- El agente tiene conectividad con los sistemas vCenter de origen y destino y con los sistemas de almacenamiento.
- Hay disponible un clúster de ONTAP con una SVM con el servicio de NFS habilitado.
- Los sistemas de almacenamiento locales de NetApp que alojan almacenes de datos NFS para VMware se añaden a NetApp Console.
- La resolución de DNS debe estar vigente cuando se utilizan nombres DNS. De lo contrario, utilice direcciones IP para vCenter.
- La replicación de SnapMirror está configurada para los volúmenes de almacén de datos basados en NFS designados.
- Asegúrese de que el entorno tenga versiones compatibles de vCenter Server y servidores ESXi.

Una vez establecida la conectividad entre los sitios de origen y destino, proceda con los pasos de configuración, que deberían tomar un par de clics y entre 3 y 5 minutos.

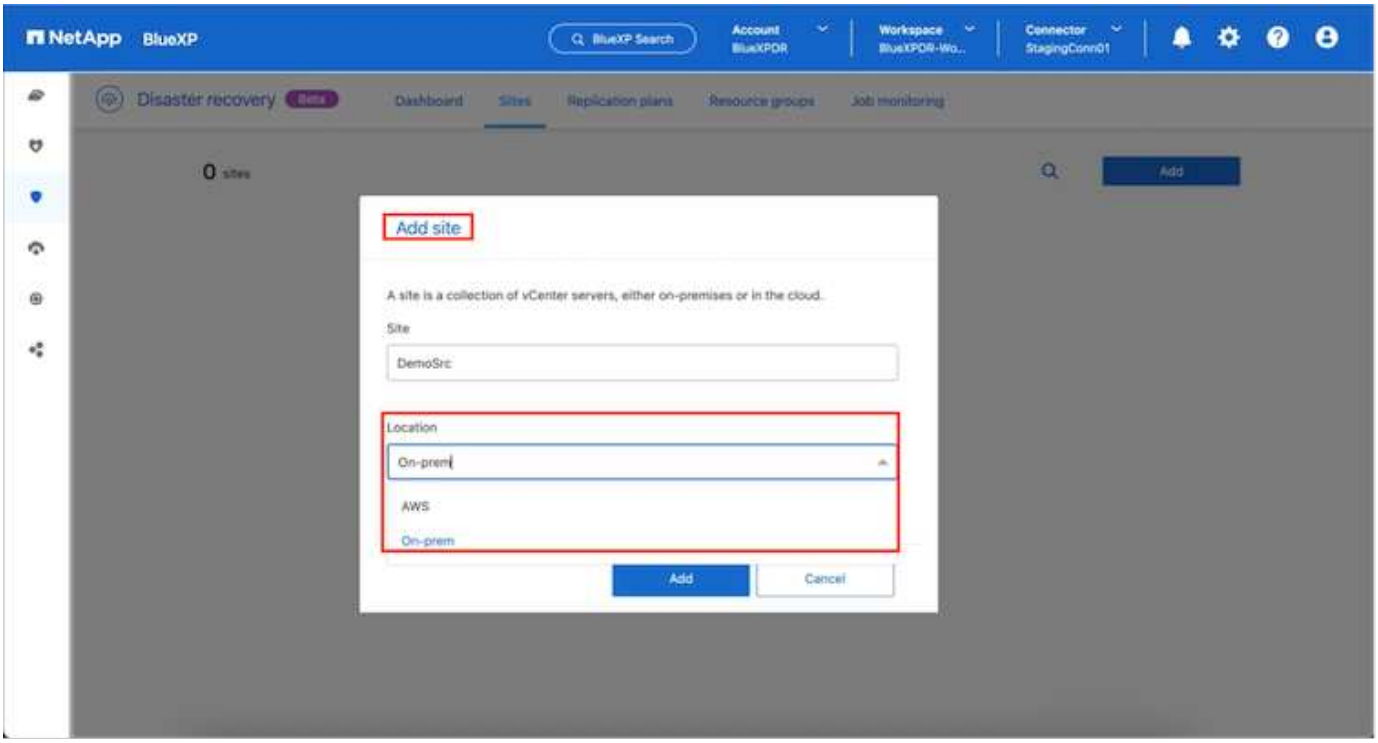
NetApp recomienda instalar el agente de NetApp Console en el sitio de destino o en un tercer sitio, de modo que el agente de NetApp Console pueda comunicarse a través de la red con los recursos de origen y de destino.



Configuración de NetApp Disaster Recovery

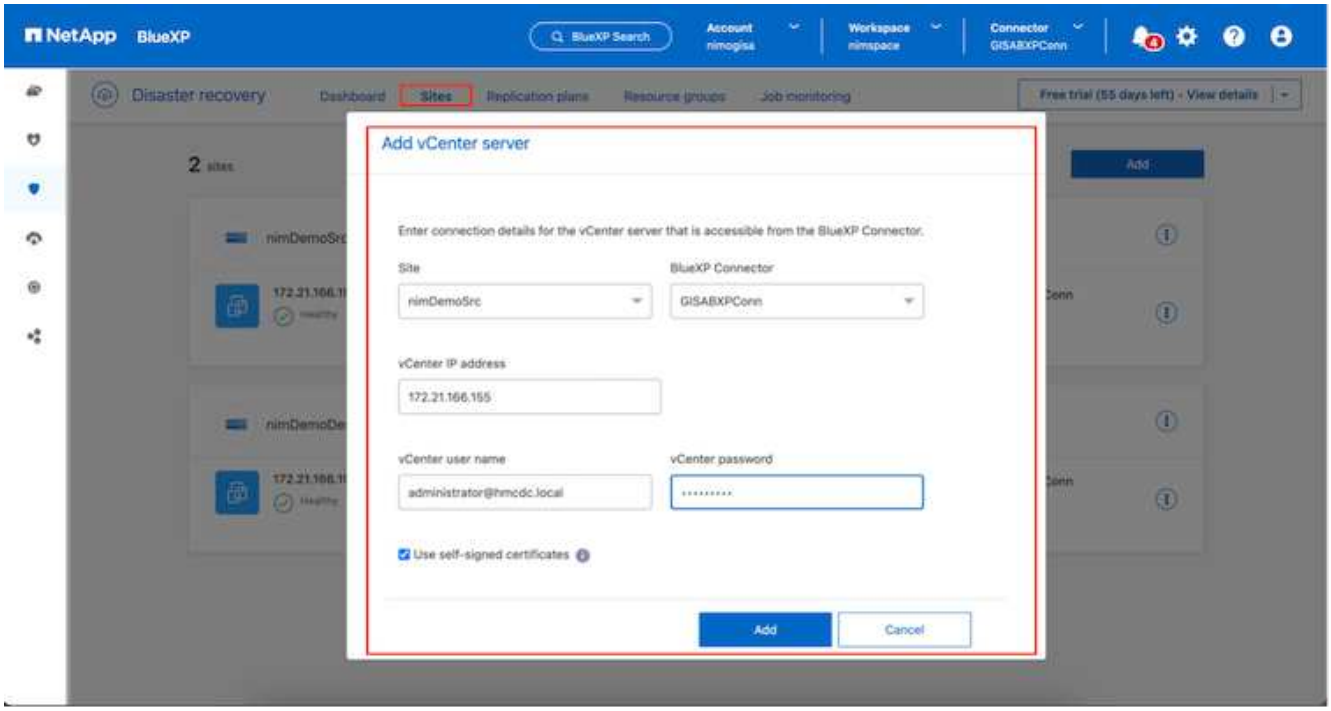
El primer paso para prepararte para la recuperación ante desastres es detectar y añadir el vCenter local y los recursos de almacenamiento a NetApp Disaster Recovery.

Abre NetApp Console y selecciona **Protección > Recuperación ante desastres** en la navegación izquierda. Haz clic en **Sitios**, escribe un nombre y elige el tipo de ubicación. Luego, haz clic en el botón **Add vCenter**.

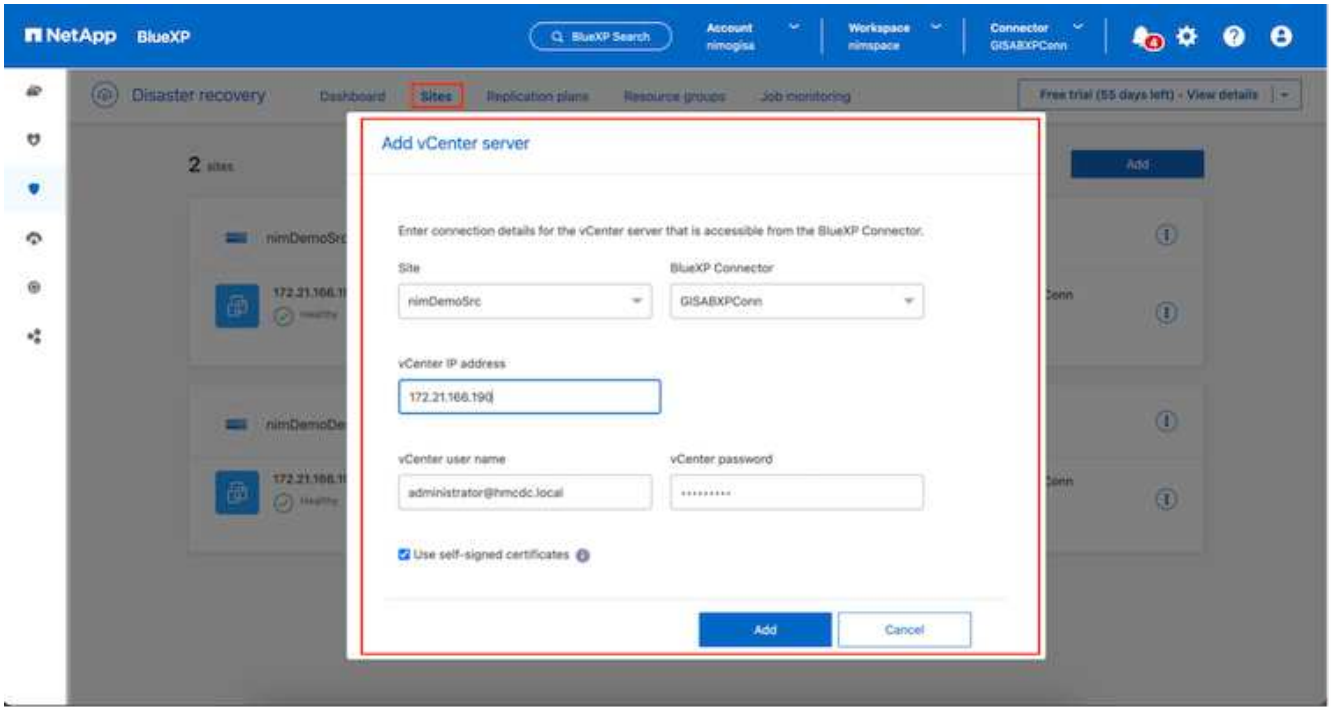


Agregue las siguientes plataformas:

- **Fuente**. vCenter local.



- **Destino**. Centro de datos SDDC de VMC.



Una vez que se agregan los vCenters, se activa el descubrimiento automático.

Configuración de la replicación de almacenamiento entre la matriz del sitio de origen y la matriz del sitio de destino

SnapMirror ofrece replicación de datos en un entorno de NetApp. Basada en la tecnología Snapshot de NetApp, la replicación de SnapMirror es extremadamente eficiente porque solo replica los bloques que se han

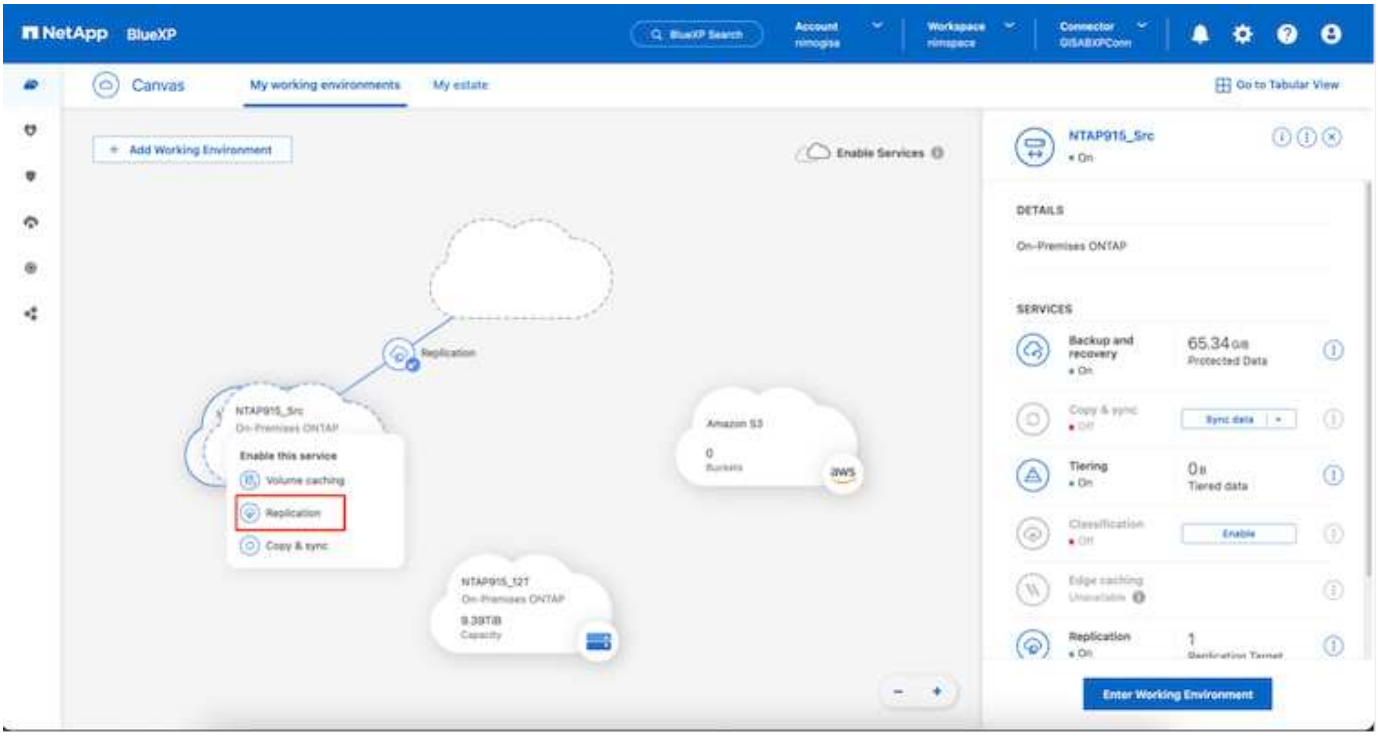
cambiado o añadido desde la actualización anterior. SnapMirror se configura fácilmente mediante NetApp OnCommand System Manager o la CLI de ONTAP. NetApp Data Services también crea la relación de SnapMirror siempre que el emparejamiento del clúster y la SVM se haya configurado previamente.

En los casos en los que el almacenamiento primario no se haya perdido por completo, SnapMirror ofrece un método eficaz para resincronizar los sitios primario y de recuperación ante desastres. SnapMirror puede resincronizar los dos sitios, transfiriendo únicamente los datos modificados o nuevos desde el sitio de recuperación ante desastres al sitio primario, simplemente invirtiendo las relaciones de SnapMirror. Esto significa que los planes de replicación en Disaster Recovery pueden resincronizarse en cualquier dirección tras una conmutación por error sin volver a copiar todo el volumen. Si una relación se resincroniza en sentido inverso, solo se envían de vuelta al destino los datos nuevos que se hayan escrito desde la última sincronización correcta de la copia Snapshot.

Si ya has configurado una relación de SnapMirror para el volumen a través de la CLI o System Manager, NetApp Data Services detecta la relación y continúa con el resto de las operaciones del flujo de trabajo.

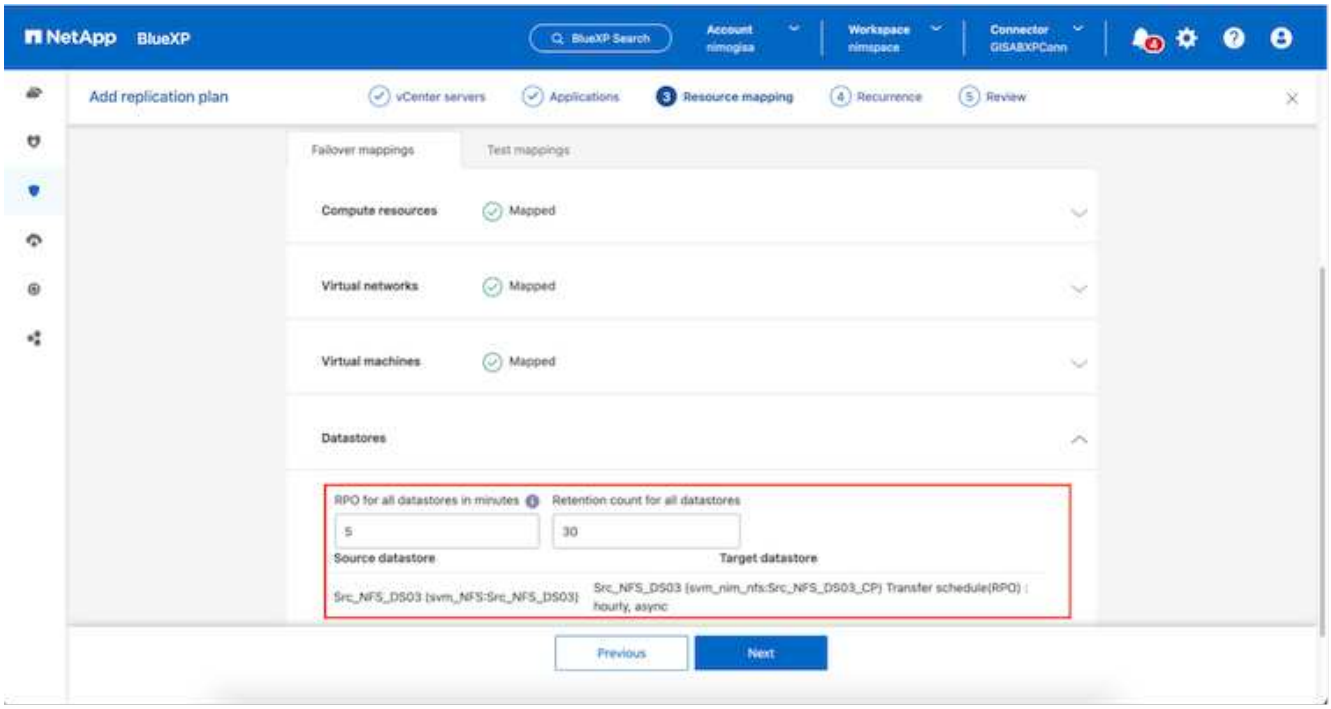
Cómo configurarlo para VMware Disaster Recovery

El proceso para crear la replicación de SnapMirror sigue siendo el mismo para cualquier aplicación. El proceso puede ser manual o automatizado. La forma más sencilla es aprovechar NetApp Console para configurar la replicación de SnapMirror usando una simple acción de arrastrar y soltar el sistema ONTAP de origen del entorno sobre el de destino para activar el asistente que te guía durante el resto del proceso.



La recuperación ante desastres también puede automatizar este proceso, siempre que se cumplan los dos criterios siguientes:

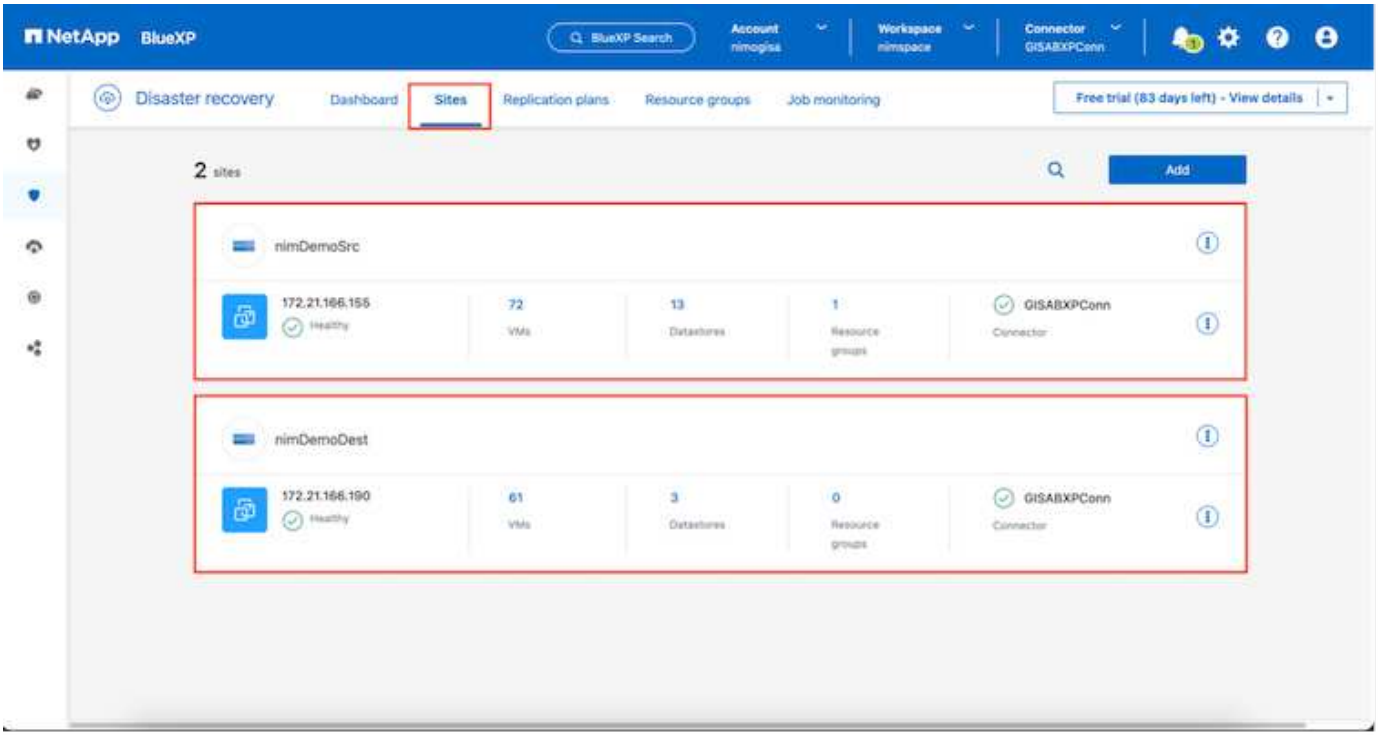
- Los clústeres de origen y destino tienen una relación de pares.
- El SVM de origen y el SVM de destino tienen una relación de pares.



Si ya se ha configurado una relación SnapMirror para el volumen a través de la CLI, Disaster Recovery detecta la relación y continúa con el resto de las operaciones del flujo de trabajo.

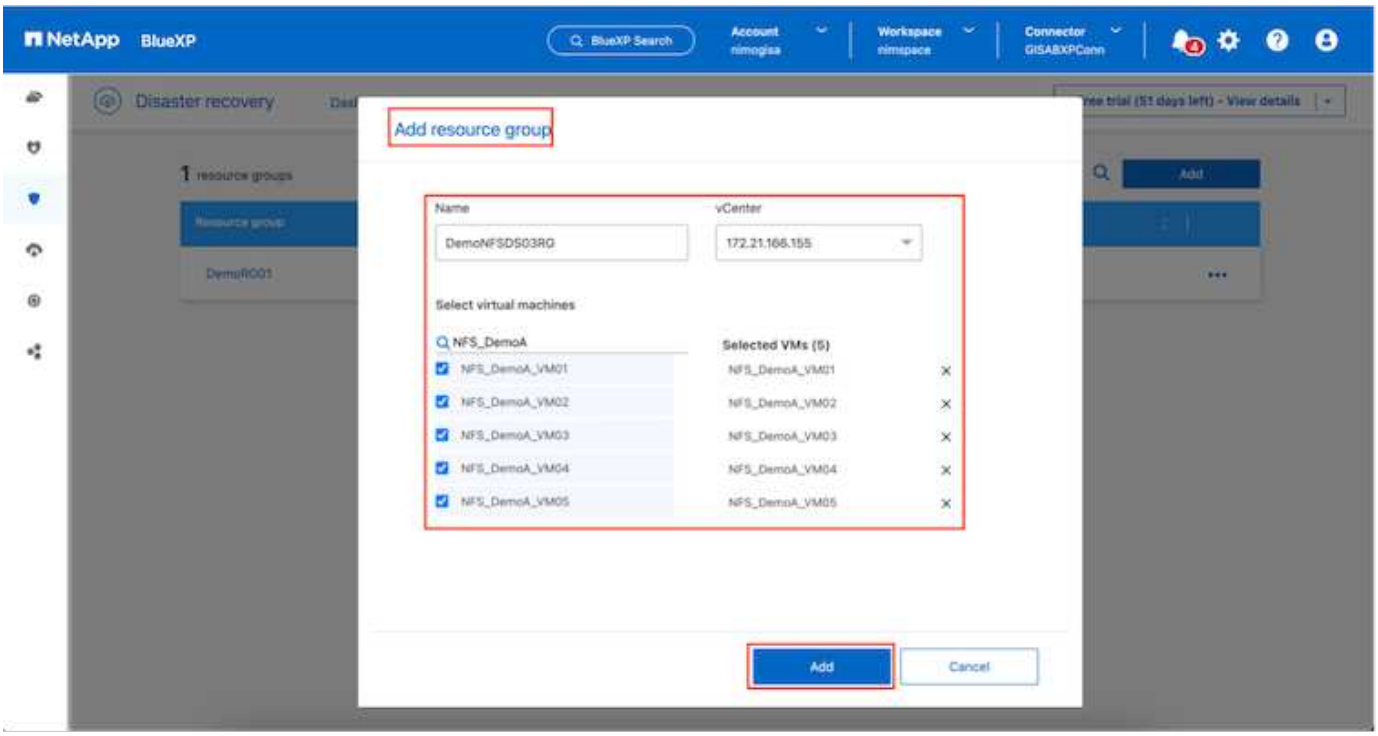
¿Qué puede hacer Disaster Recovery por ti?

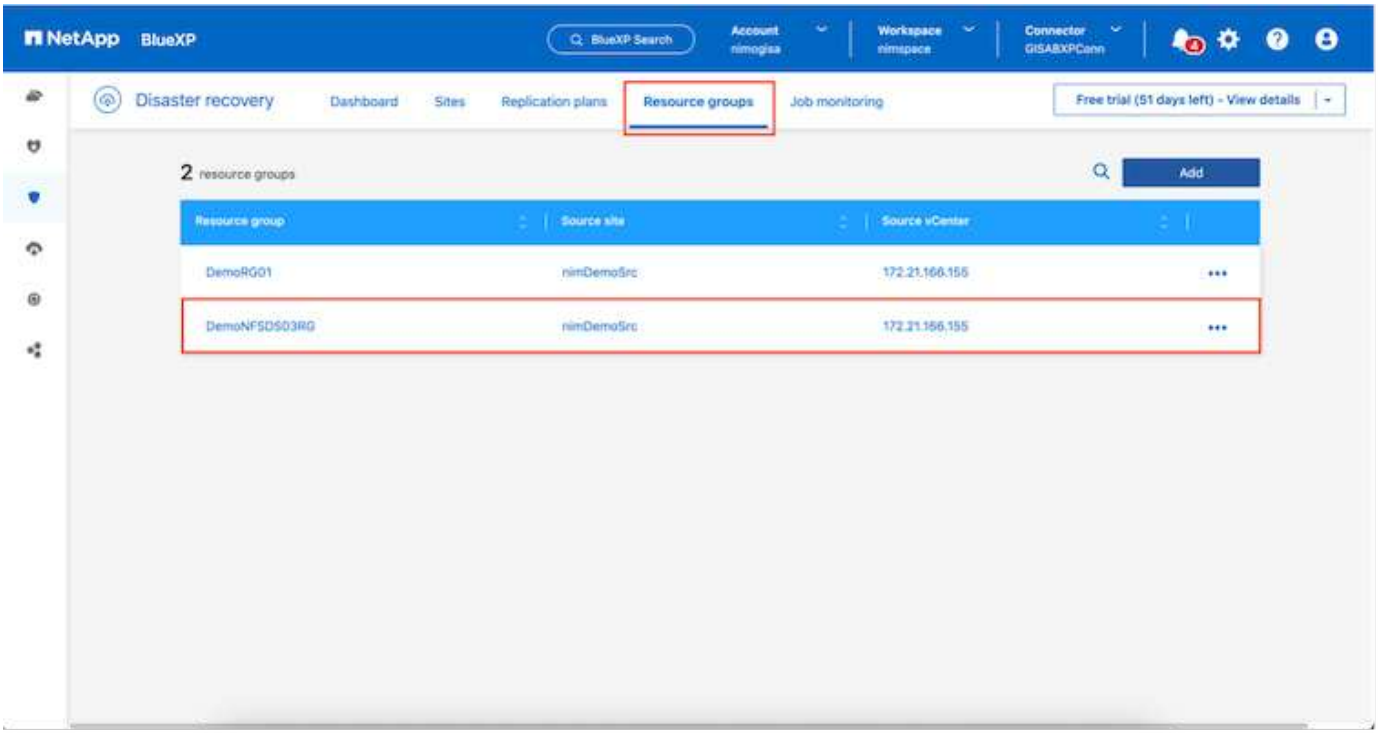
Una vez añadidos los sitios de origen y destino, Disaster Recovery realiza una detección exhaustiva automática y muestra las VMs junto con los metadatos asociados. Disaster Recovery también detecta automáticamente las redes y los grupos de puertos que usan las VMs y los completa.



Una vez añadidos los sitios, las máquinas virtuales se pueden agrupar en grupos de recursos. Los grupos de

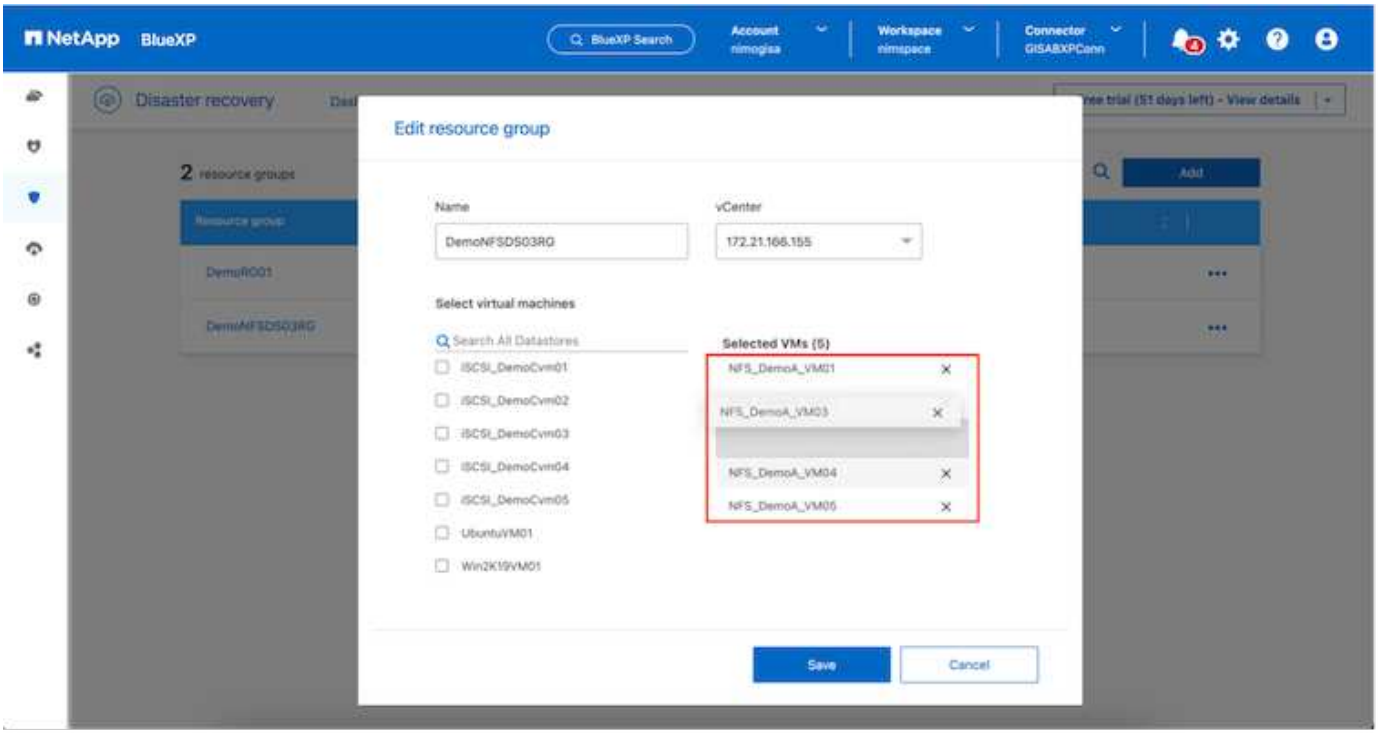
recursos de Disaster Recovery te permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque y retrasos de arranque, que se pueden ejecutar durante la recuperación. Para empezar a crear grupos de recursos, ve a **Resource Groups** y haz clic en **Create New Resource Group**.



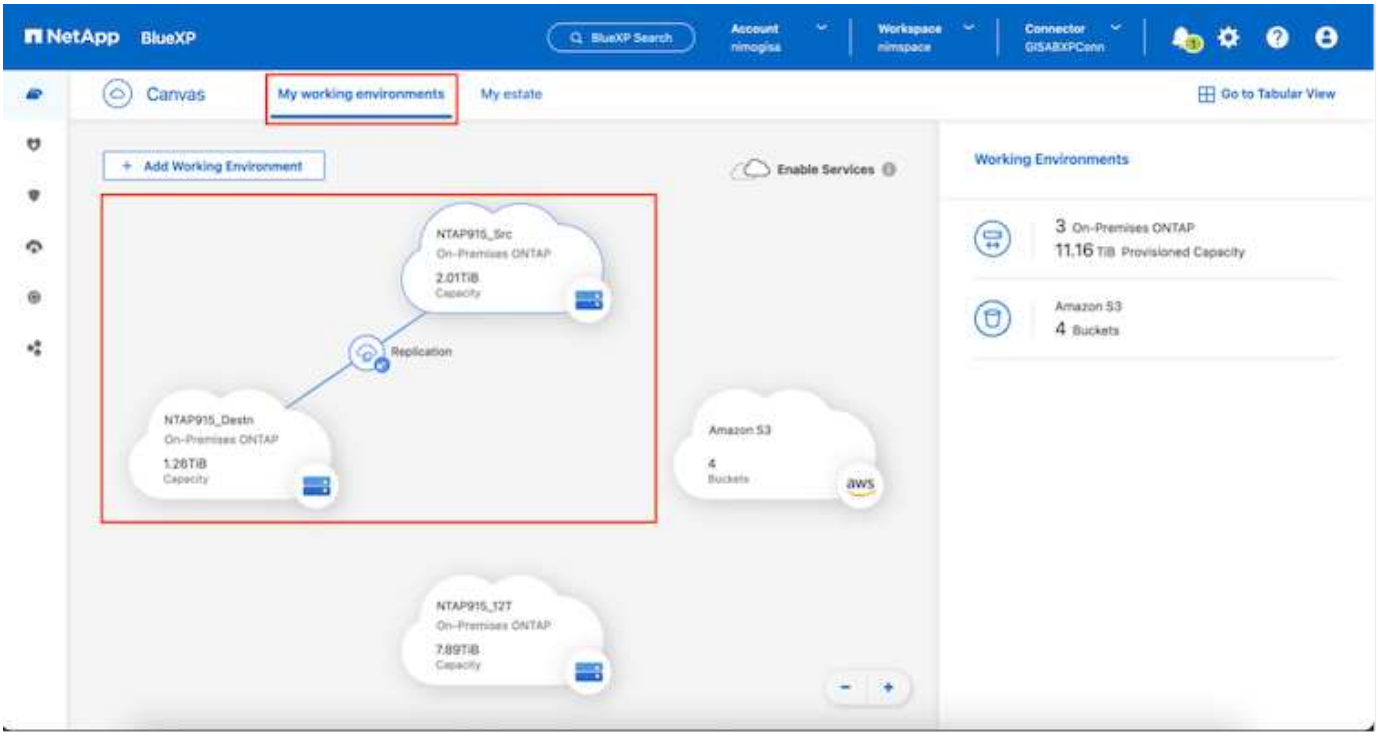


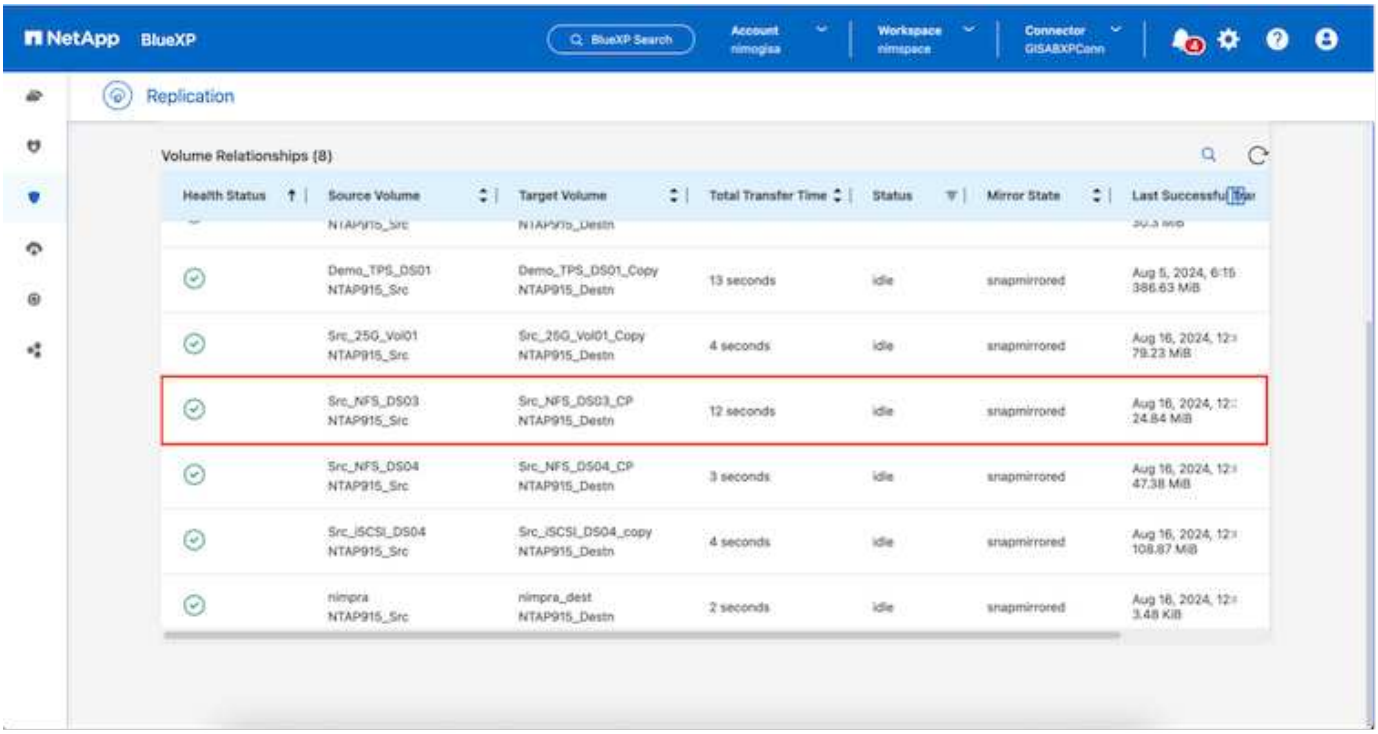
El grupo de recursos también se puede crear mientras se crea un plan de replicación.

El orden de arranque de las máquinas virtuales se puede definir o modificar durante la creación de grupos de recursos mediante un simple mecanismo de arrastrar y soltar.



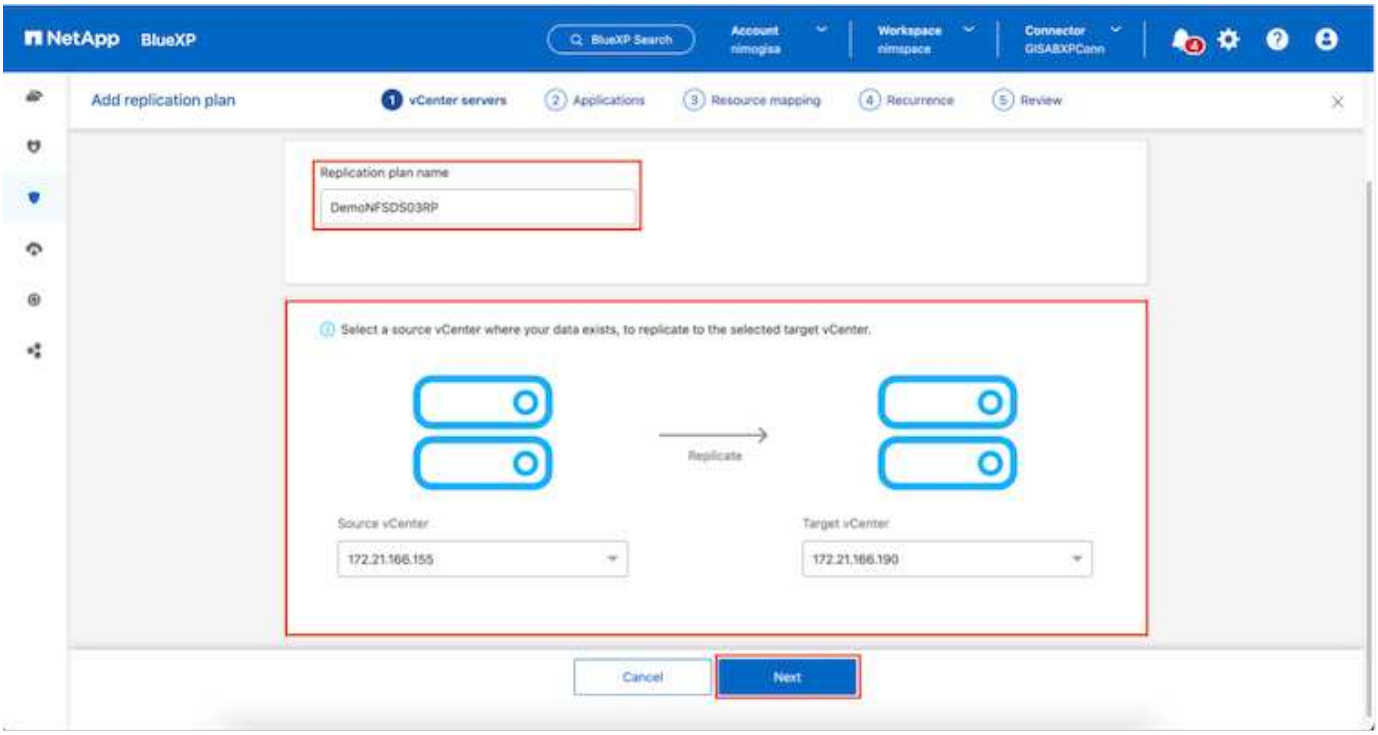
Una vez creados los grupos de recursos, el siguiente paso es crear el plan de ejecución o un plan para recuperar máquinas virtuales y aplicaciones en caso de desastre. Como se menciona en los requisitos previos, la replicación de SnapMirror se puede configurar de antemano o DRaaS puede configurarla utilizando el RPO y el recuento de retención especificados durante la creación del plan de replicación.





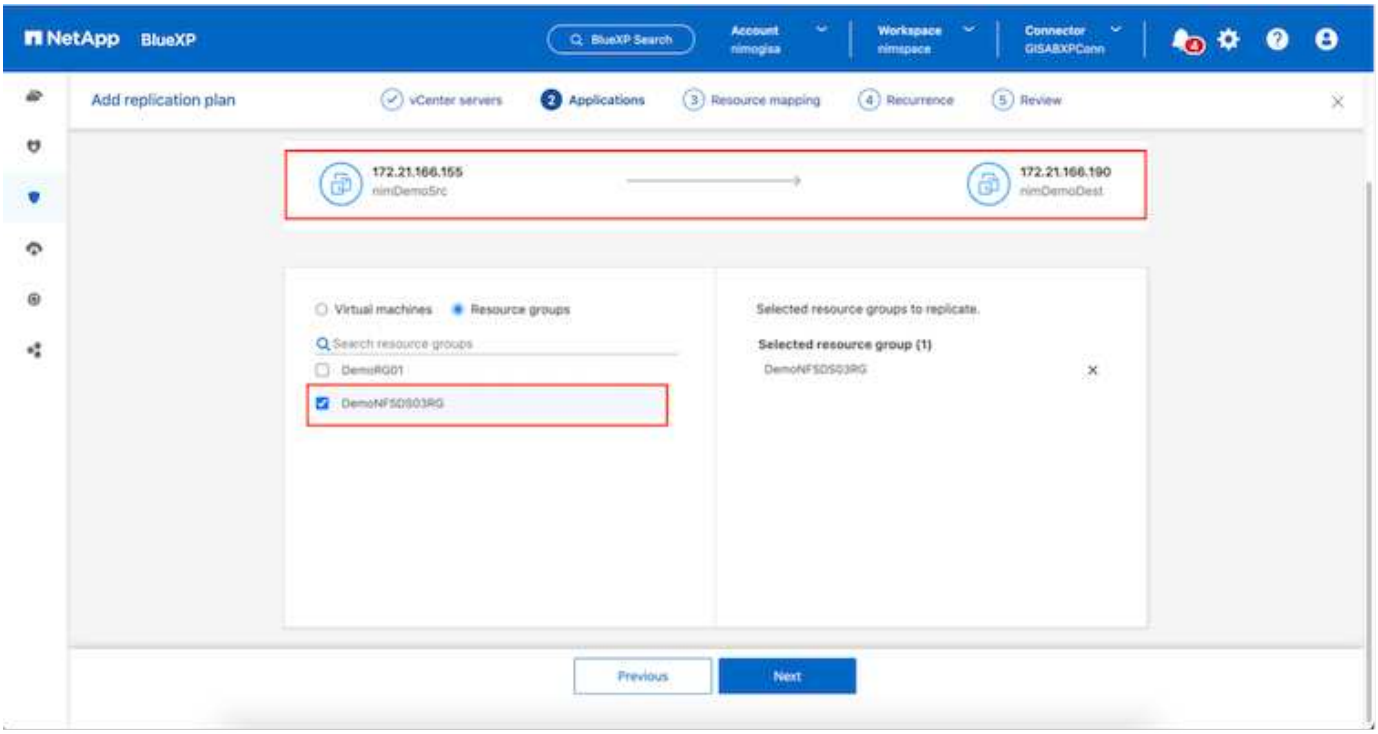
Configure el plan de replicación seleccionando las plataformas vCenter de origen y destino en el menú desplegable y elija los grupos de recursos que se incluirán en el plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones y el mapeo de clústeres y redes. Para definir el plan de recuperación, navegue a la pestaña **Plan de replicación** y haga clic en **Agregar plan**.

Primero, seleccione el vCenter de origen y luego seleccione el vCenter de destino.



El siguiente paso es seleccionar los grupos de recursos existentes. Si no se crean grupos de recursos, el asistente ayuda a agrupar las máquinas virtuales necesarias (básicamente, crea grupos de recursos funcionales) en función de los objetivos de recuperación. Esto también ayuda a definir la secuencia de

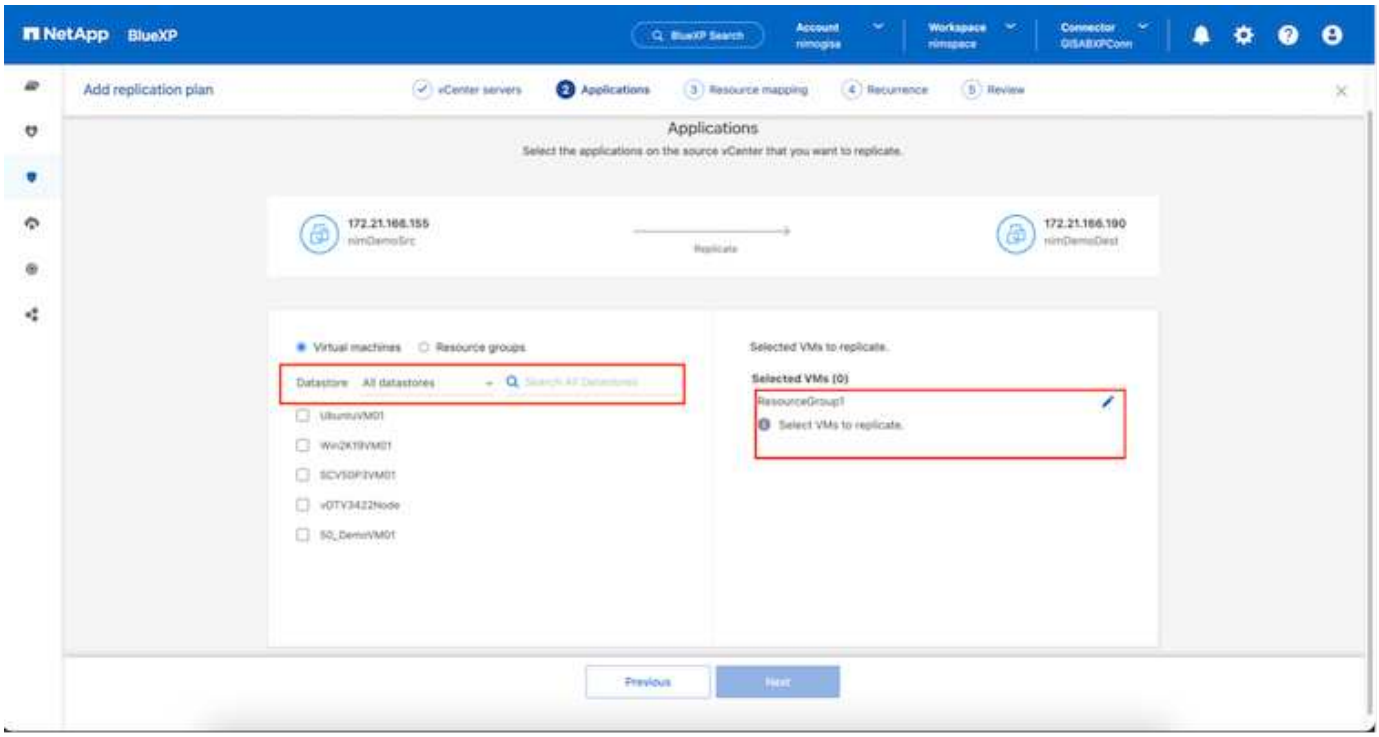
operaciones de cómo se deben restaurar las máquinas virtuales de la aplicación.



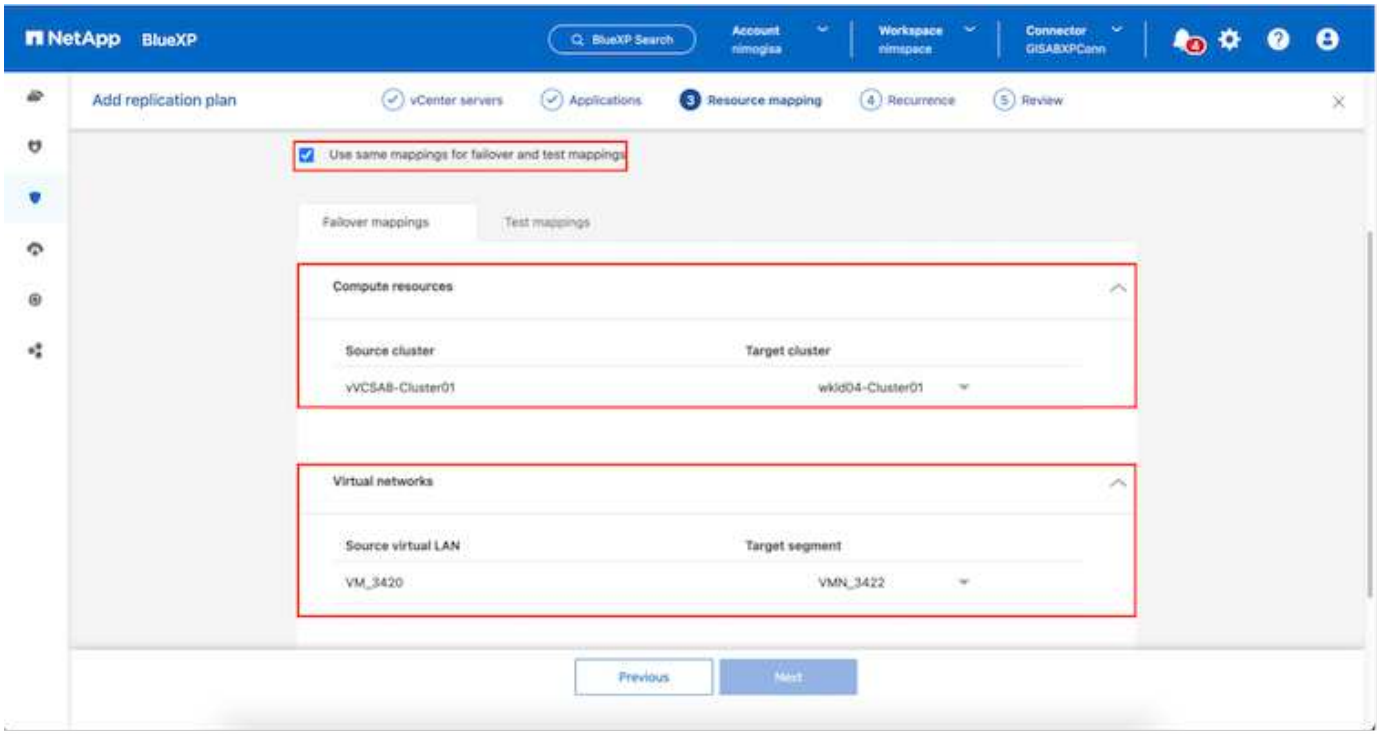
El grupo de recursos permite establecer el orden de arranque mediante la funcionalidad de arrastrar y soltar. Se puede utilizar para modificar fácilmente el orden en que se encenderán las máquinas virtuales durante el proceso de recuperación.

Cada máquina virtual dentro de un grupo de recursos se inicia en secuencia según el orden. Se inician dos grupos de recursos en paralelo.

La siguiente captura de pantalla muestra la opción para filtrar máquinas virtuales o almacenes de datos específicos según los requisitos organizativos si no se crean grupos de recursos de antemano.

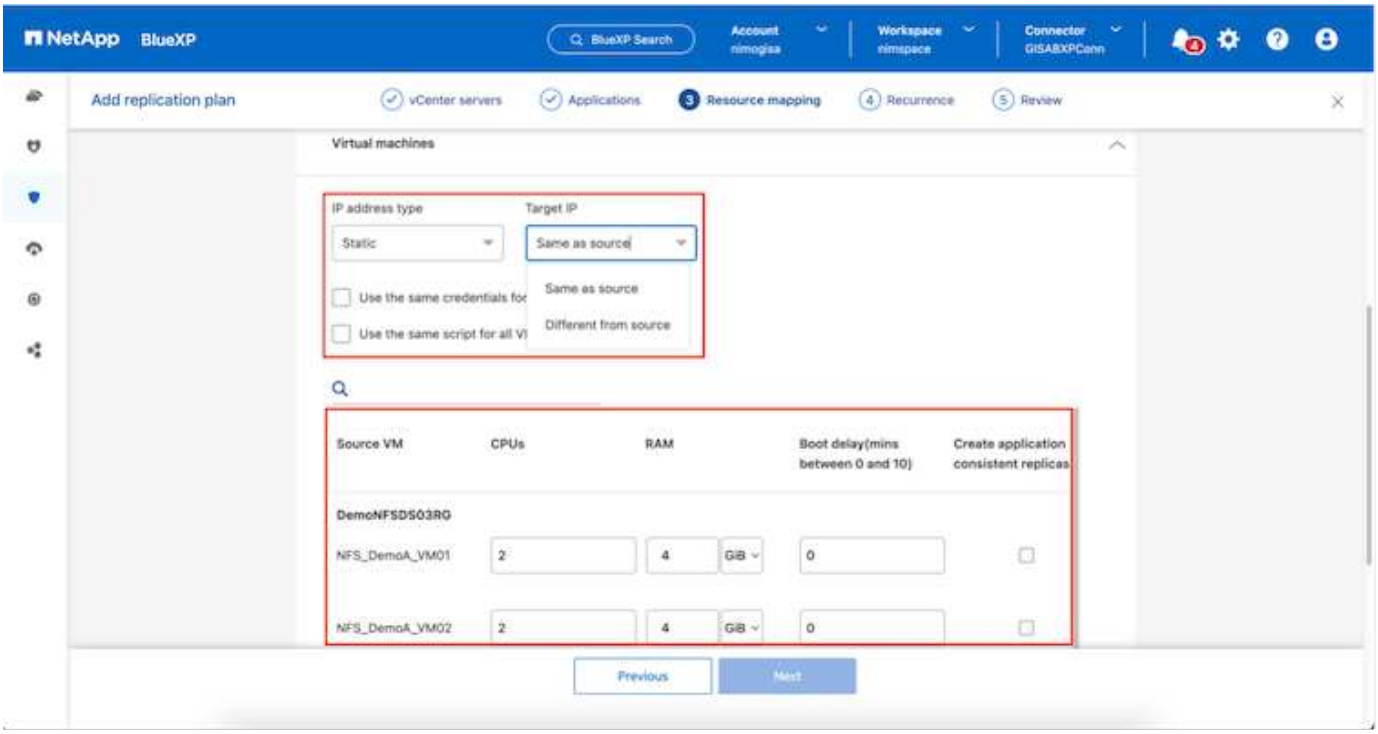


Una vez seleccionados los grupos de recursos, crea las asignaciones de conmutación por error. En este paso, especifica cómo se asignan los recursos del entorno de origen al de destino. Esto incluye recursos de computación y redes virtuales. Personalización de direcciones IP, scripts previos y posteriores, retrasos de arranque, consistencia de las aplicaciones, etc. Para obtener información detallada, consulta "Crear un plan de replicación".

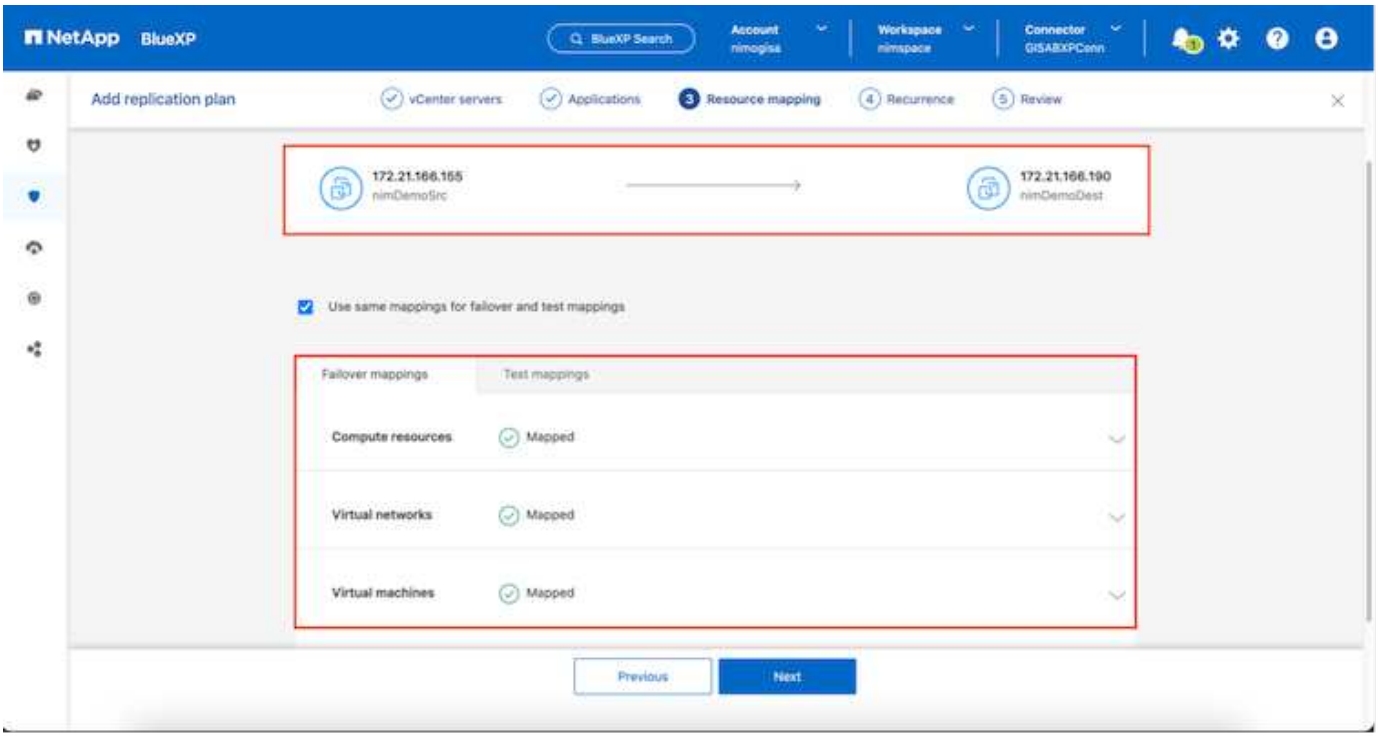


De forma predeterminada, se utilizan los mismos parámetros de mapeo para las operaciones de prueba y de conmutación por error. Para configurar diferentes asignaciones para el entorno de prueba, seleccione la opción Asignación de prueba después de desmarcar la casilla de

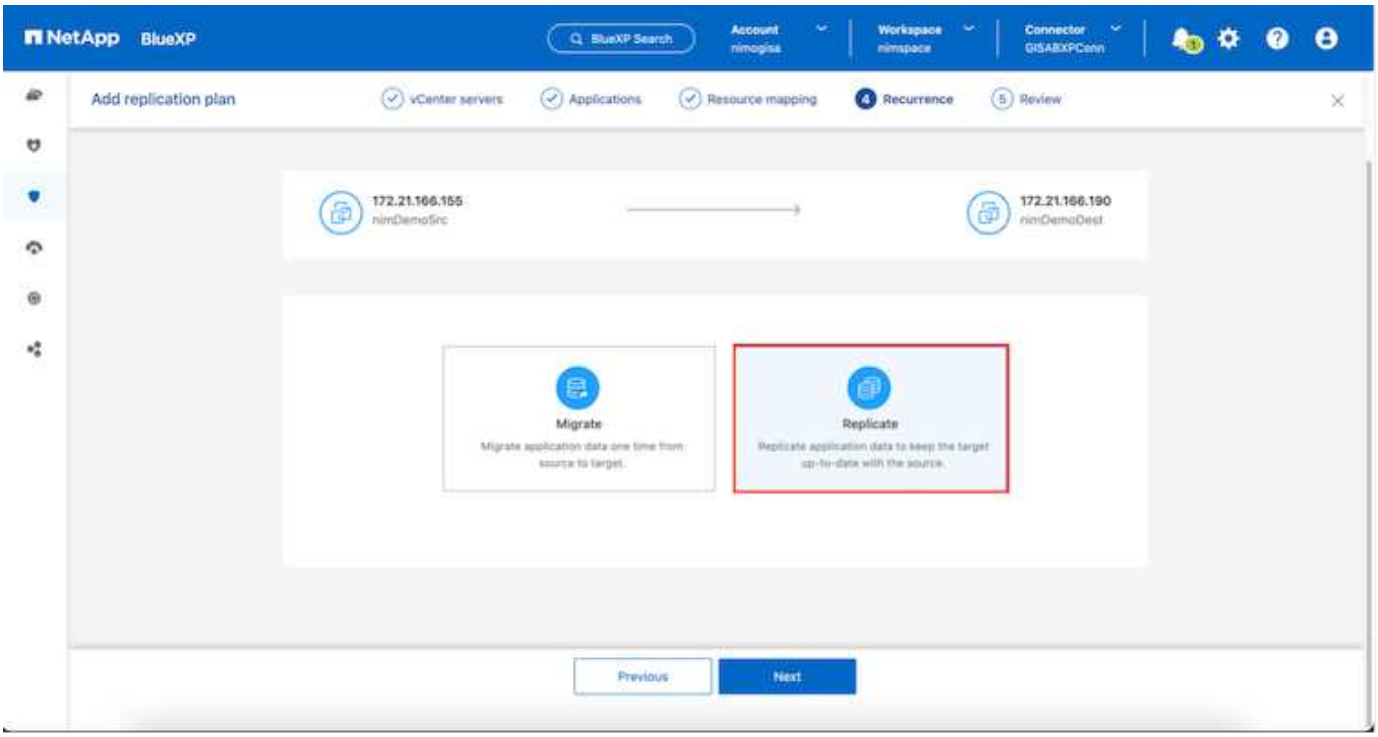
verificación como se muestra a continuación:



Una vez completado el mapeo de recursos, haga clic en Siguiente.

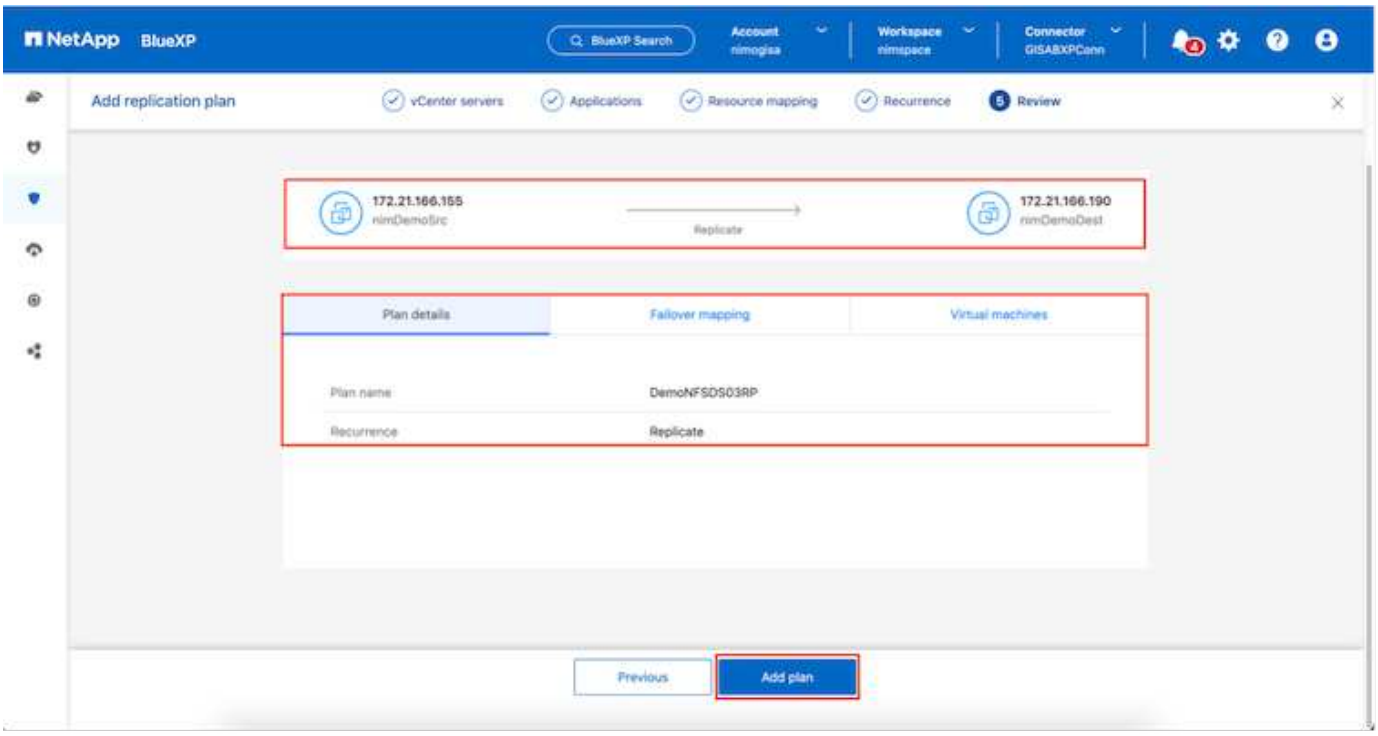


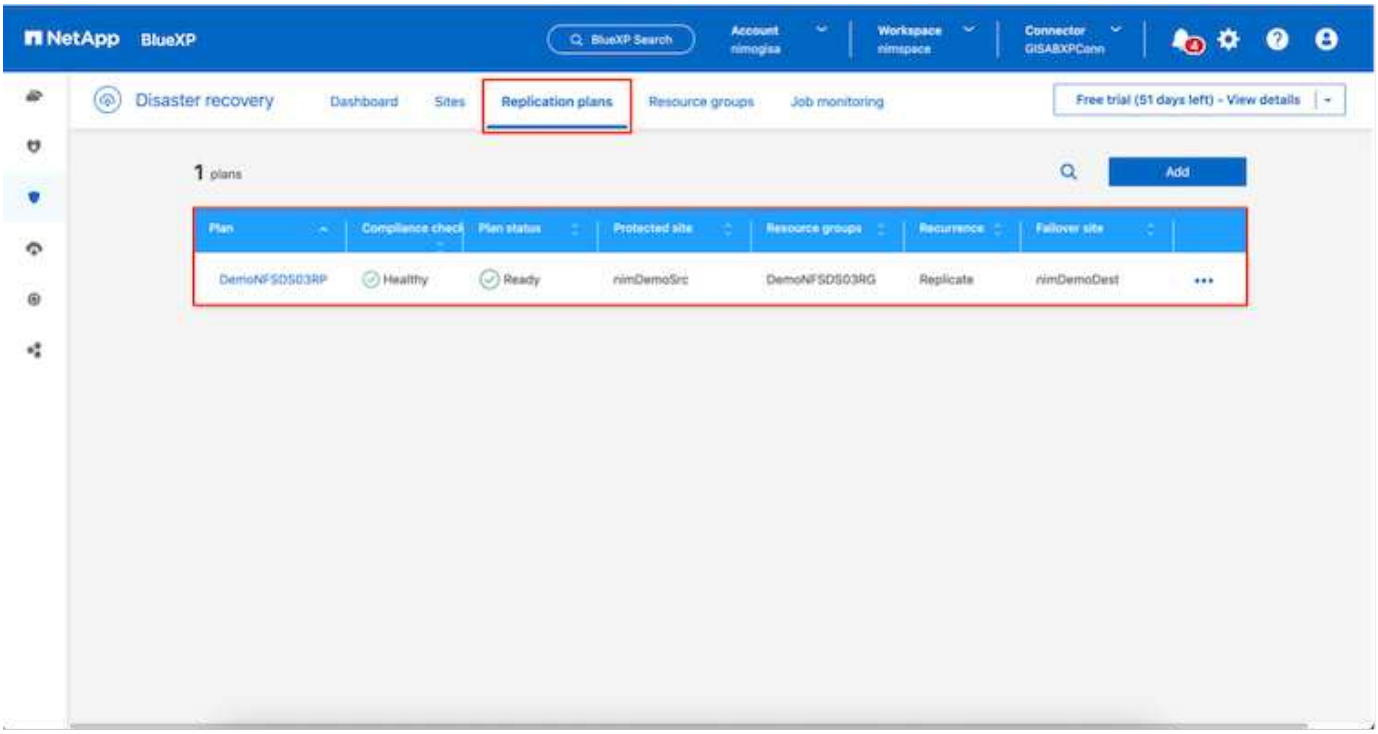
Seleccione el tipo de recurrencia. En palabras simples, seleccione la opción Migrar (migración única mediante conmutación por error) o replicación continua recurrente. En este tutorial, se selecciona la opción Replicar.



Una vez hecho esto, revise los mapeos creados y luego haga clic en **Agregar plan**.

> En un plan de replicación se pueden incluir VMs de diferentes volúmenes y SVM. Dependiendo de la ubicación de la VM (ya sea en el mismo volumen o en un volumen distinto dentro de la misma SVM, o en volúmenes distintos en diferentes SVM), Disaster Recovery crea una Snapshot de grupo de consistencia.



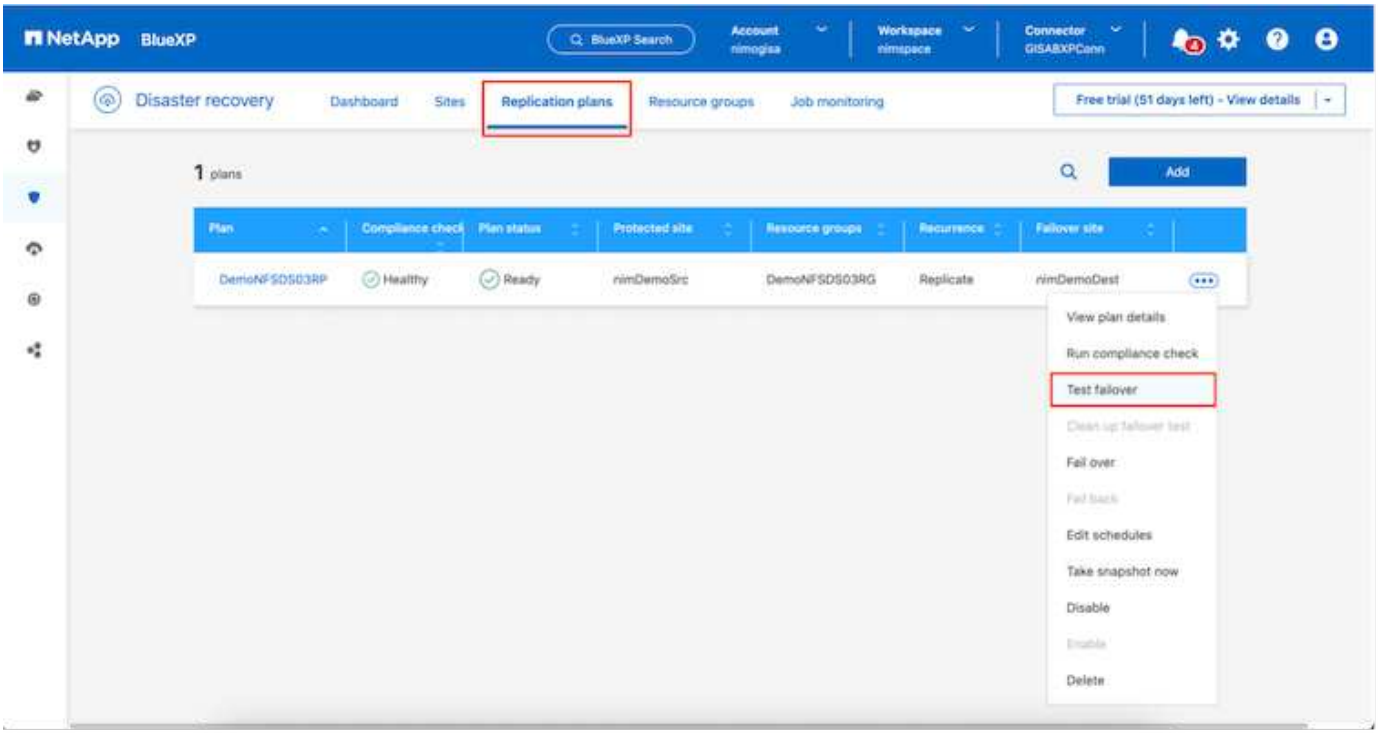


La recuperación ante desastres consta de los siguientes flujos de trabajo:

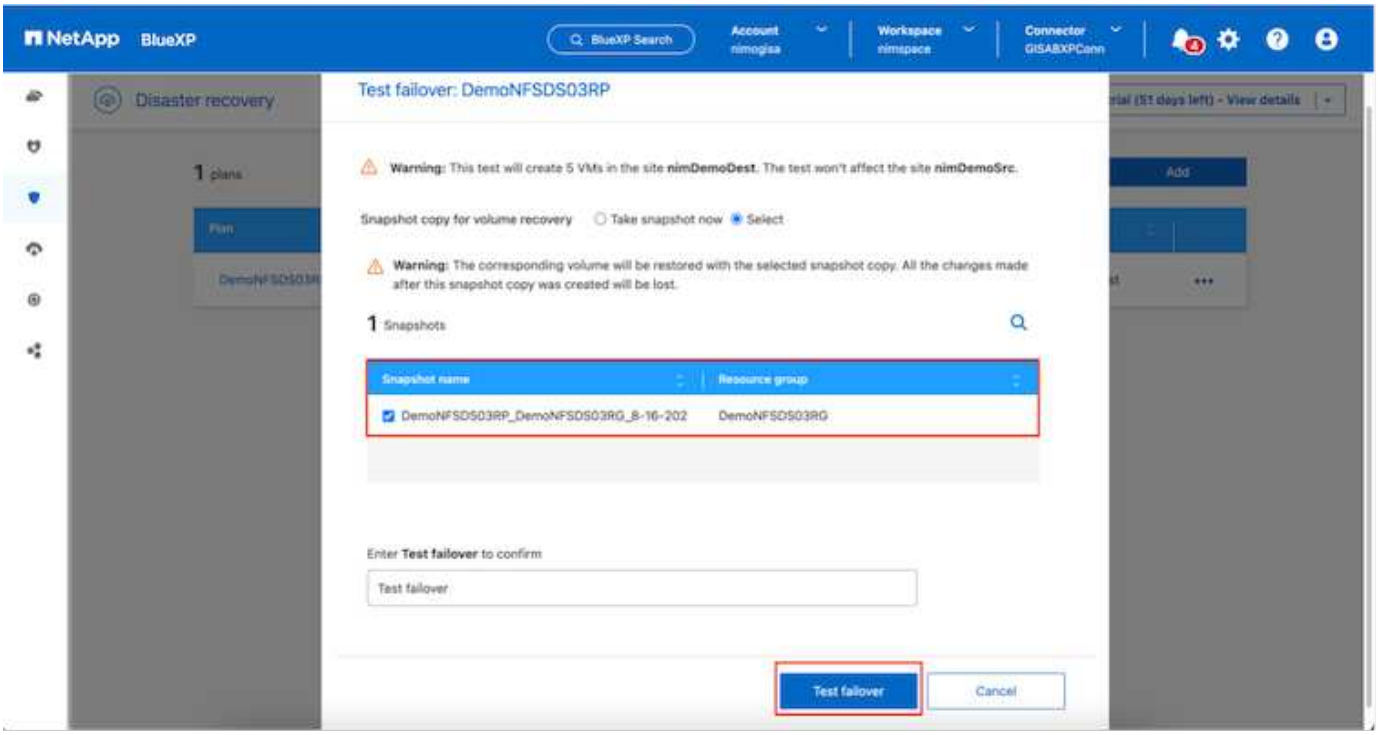
- Conmutación por error de prueba (incluidas simulaciones automatizadas periódicas)
- Prueba de conmutación por error de limpieza
- Conmutación por error
- Recuperación por recuperación

Prueba de conmutación por error

La conmutación por error de prueba en Disaster Recovery es un procedimiento operativo que permite a los administradores de VMware validar por completo sus planes de recuperación sin interrumpir sus entornos de producción. Durante una conmutación por error de prueba, Disaster Recovery crea copias NetApp FlexClone con gestión eficiente del espacio de los volúmenes replicados del almacén de datos NFS en el sistema de almacenamiento de DR. A continuación, estos volúmenes FlexClone se montan en los hosts ESXi del sitio de DR, y las VMs se encienden en una red de prueba aislada. Este proceso permite a los administradores verificar que sus planes de recuperación ante desastres funcionarán según lo previsto en caso de que se produzca un desastre real.



Disaster Recovery incorpora la posibilidad de seleccionar la instantánea como una función opcional en la operación de conmutación por error de prueba. Esta función permite al administrador de VMware verificar que cualquier cambio realizado recientemente en el entorno se replique en el sitio de destino y, por lo tanto, esté presente durante la prueba. Entre dichos cambios se incluyen los parches del sistema operativo invitado de la máquina virtual.

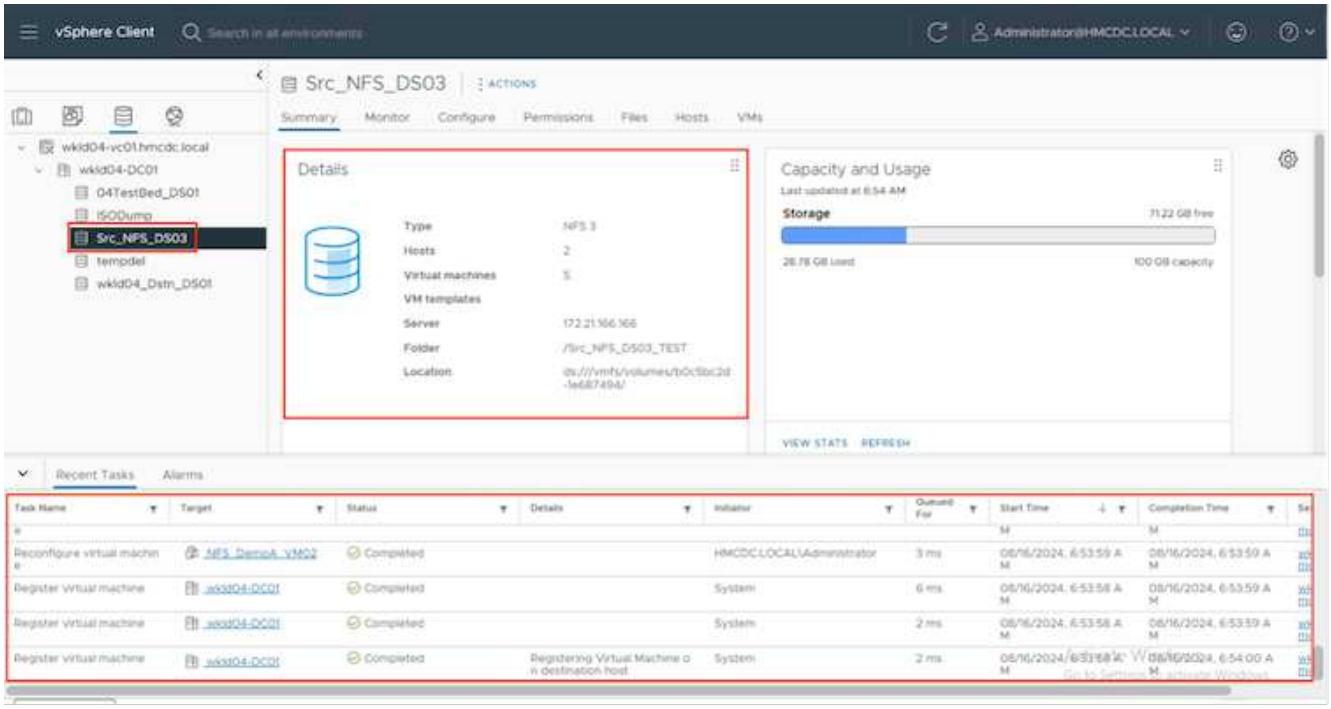


Cuando el administrador de VMware ejecuta una operación de conmutación por error de prueba, Disaster Recovery automatiza las siguientes tareas:

- Activar relaciones de SnapMirror para actualizar el almacenamiento en el sitio de destino con cualquier

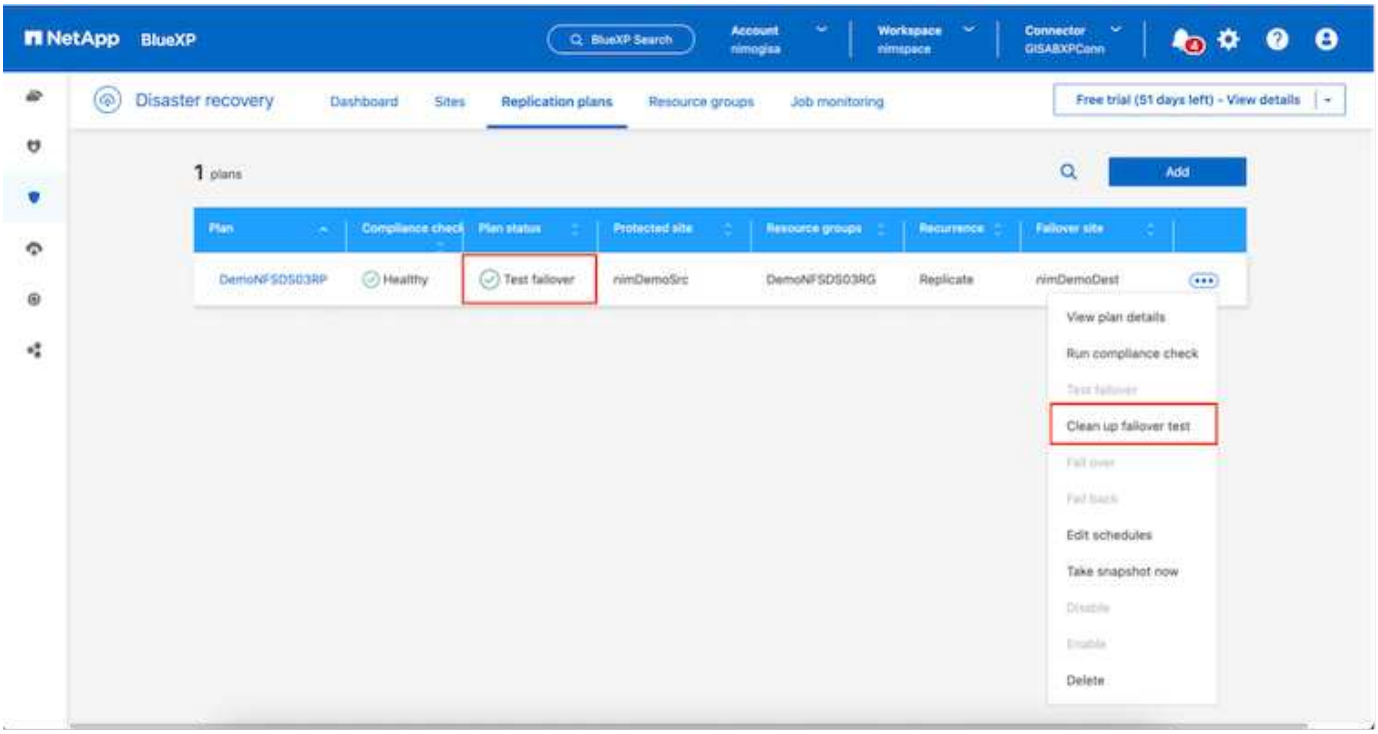
cambio reciente que se haya realizado en el sitio de producción.

- Creación de volúmenes NetApp FlexClone de los volúmenes FlexVol en la matriz de almacenamiento DR.
- Conexión de los almacenes de datos NFS en los volúmenes FlexClone a los hosts ESXi en el sitio de recuperación ante desastres.
- Conectar los adaptadores de red de la máquina virtual a la red de prueba especificada durante la asignación.
- Reconfigurar la configuración de red del sistema operativo invitado de la máquina virtual según lo definido para la red en el sitio de recuperación ante desastres.
- Ejecutar cualquier comando personalizado que se haya almacenado en el plan de replicación.
- Encender las máquinas virtuales en el orden definido en el plan de replicación.



Operación de prueba de conmutación por error de limpieza

La operación de prueba de conmutación por error de limpieza se produce después de que se haya completado la prueba del plan de replicación y el administrador de VMware responda al mensaje de limpieza.



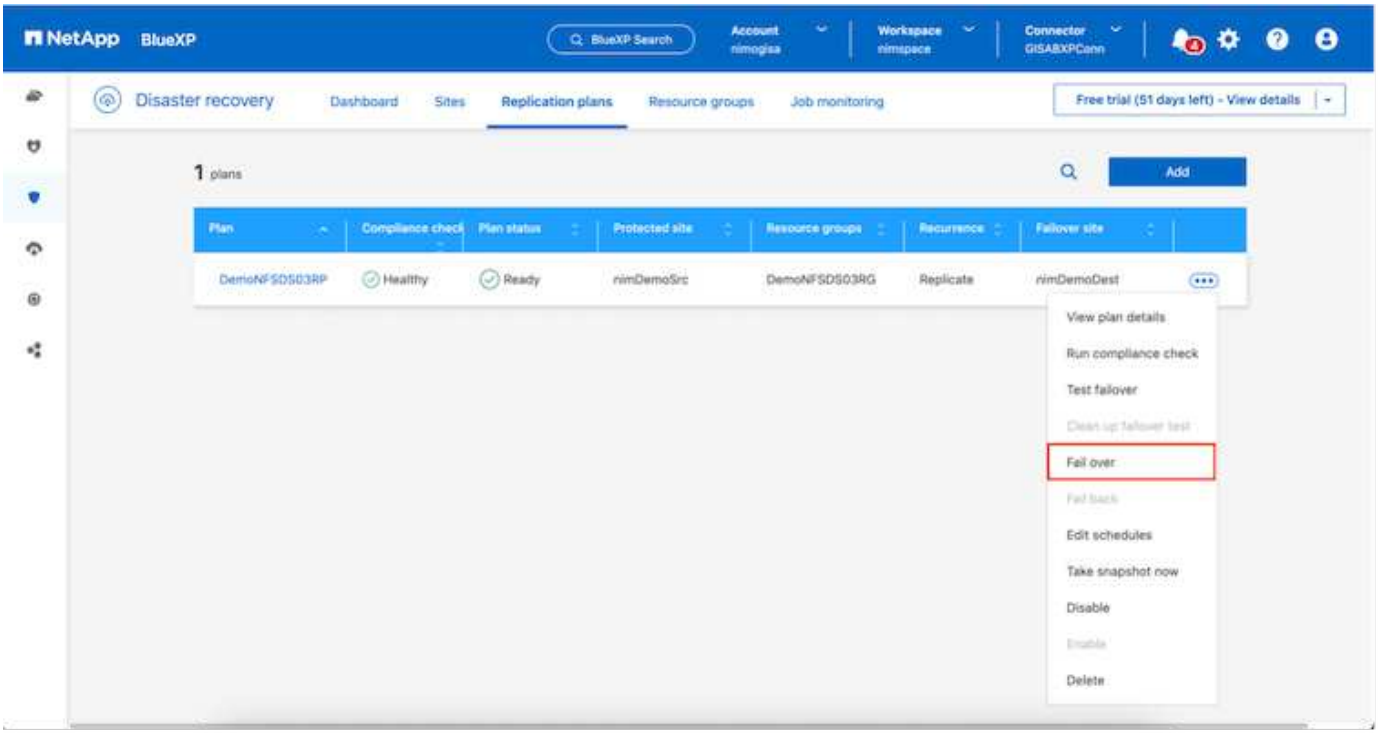
Esta acción restablecerá las máquinas virtuales (VM) y el estado del plan de replicación al estado listo.

Cuando el administrador de VMware lleva a cabo una operación de recuperación, Disaster Recovery realiza el siguiente proceso:

1. Apaga cada VM recuperada en la copia FlexClone que se utilizó para la prueba.
2. Elimina el volumen FlexClone que se utilizó para presentar las máquinas virtuales recuperadas durante la prueba.

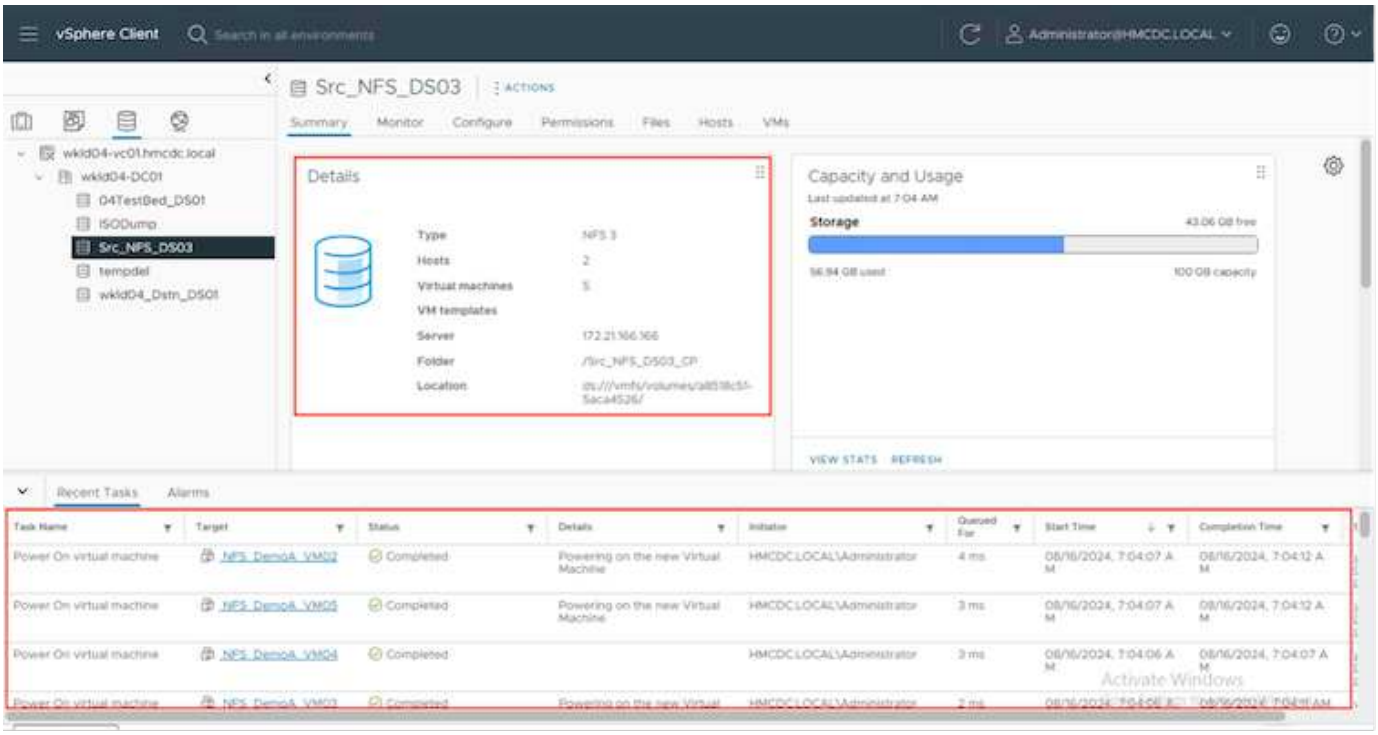
Migración planificada y conmutación por error

Disaster Recovery tiene dos métodos para realizar una conmutación por error real: la migración planificada y la conmutación por error. El primer método, la migración planificada, incorpora el apagado de las máquinas virtuales y la sincronización de la replicación del almacenamiento en el proceso para recuperar o mover de forma efectiva las máquinas virtuales al sitio de destino. La migración planificada requiere acceso al sitio de origen. El segundo método, la conmutación por error, es una conmutación por error planificada o no planificada en la que las máquinas virtuales se recuperan en el sitio de destino a partir del último intervalo de replicación del almacenamiento que se pudo completar. Según el RPO diseñado en la solución, se puede esperar cierta pérdida de datos en el escenario de DR.



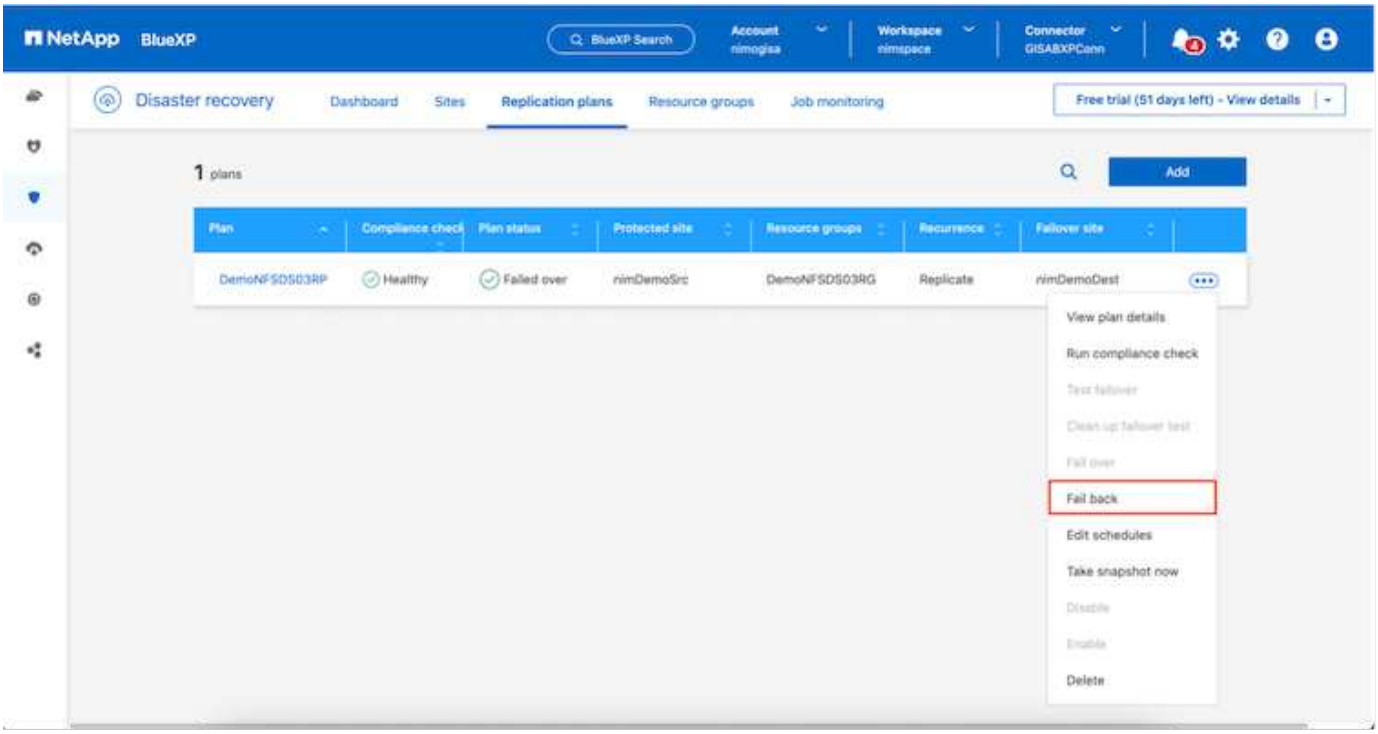
Cuando el administrador de VMware realiza una operación de conmutación por error, Disaster Recovery automatiza las siguientes tareas:

- Romper y conmutar por error las relaciones de NetApp SnapMirror .
- Conecte los almacenes de datos NFS replicados a los hosts ESXi en el sitio de recuperación ante desastres.
- Conecte los adaptadores de red de la máquina virtual a la red del sitio de destino apropiado.
- Reconfigure la configuración de red del sistema operativo invitado de la máquina virtual según lo definido para la red en el sitio de destino.
- Ejecute cualquier comando personalizado (si hay alguno) que se haya almacenado en el plan de replicación.
- Encienda las máquinas virtuales en el orden definido en el plan de replicación.



Recuperación por recuperación

Una conmutación por recuperación es un procedimiento opcional que restaura la configuración original de los sitios de origen y destino después de una recuperación.



Los administradores de VMware pueden configurar y ejecutar un procedimiento de conmutación por error cuando estén listos para restaurar los servicios en el sitio de origen original.

NOTA: Disaster Recovery replica (resincroniza) cualquier cambio de vuelta a la máquina virtual de origen original antes de invertir la dirección de la replicación. Este proceso parte de una relación que ha completado

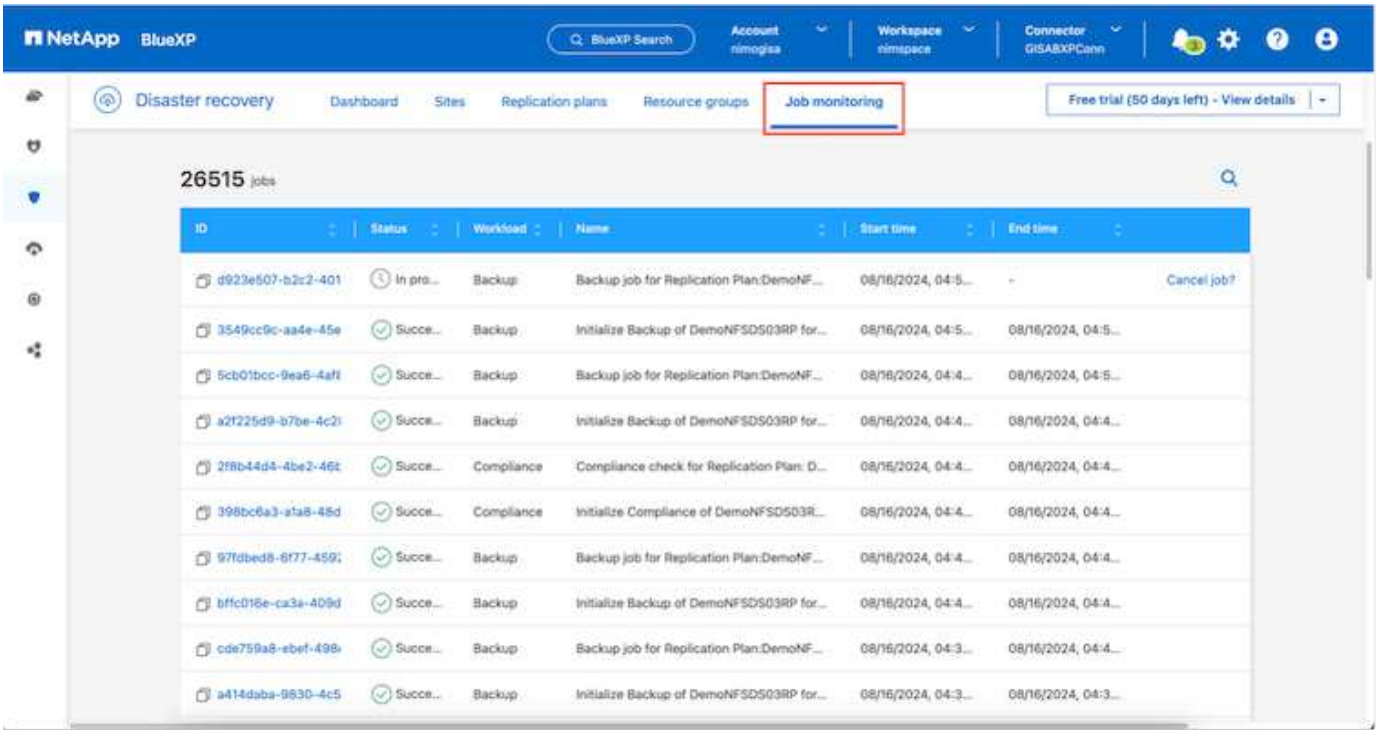
la conmutación por error a un destino e implica los siguientes pasos:

- Apague y anule el registro de las máquinas virtuales y los volúmenes en el sitio de destino se desmontan.
- Romper la relación SnapMirror en la fuente original se rompe para hacerla de lectura/escritura.
- Vuelva a sincronizar la relación SnapMirror para revertir la replicación.
- Monte el volumen en la fuente, encienda y registre las máquinas virtuales de origen.

Para obtener más información sobre cómo acceder a Disaster Recovery y configurarlo, consulta "Más información sobre NetApp Disaster Recovery para VMware".

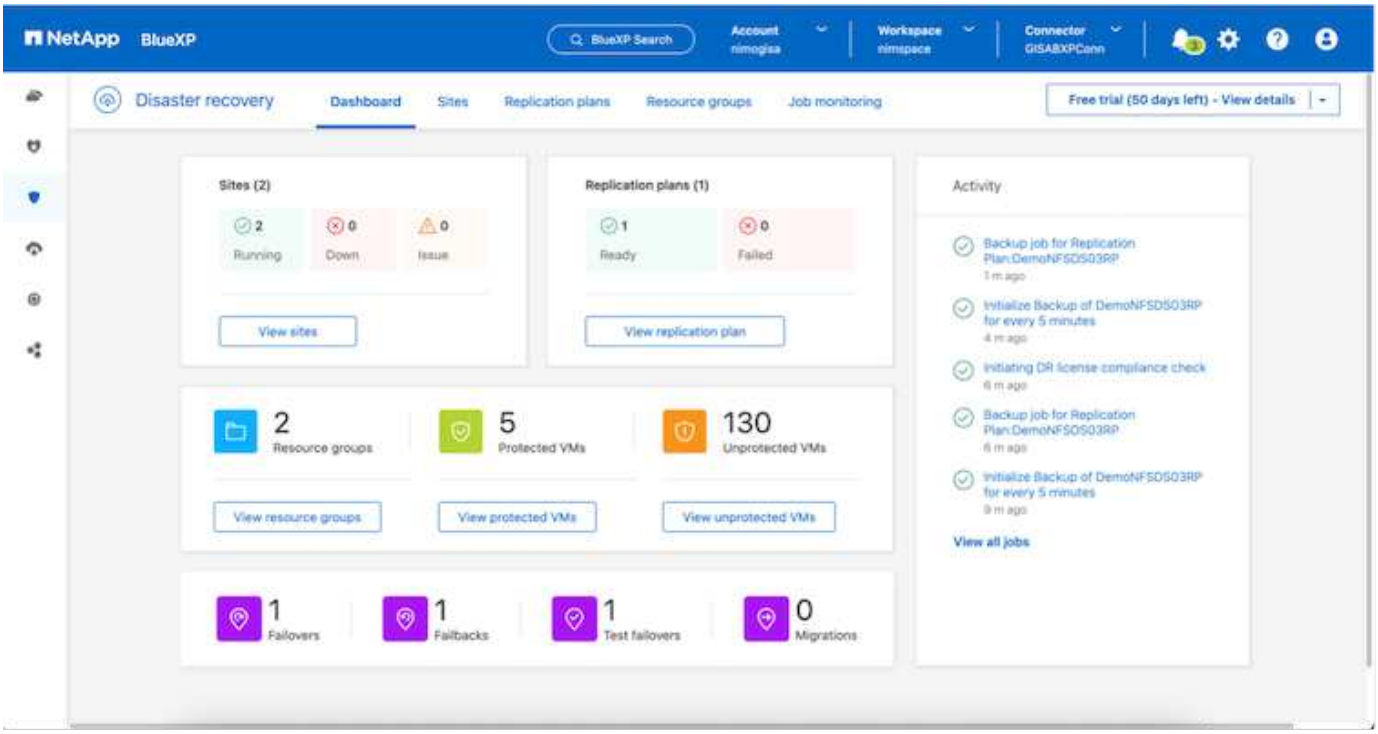
Monitoreo y tablero de control

Desde NetApp Console o la CLI de ONTAP, puedes supervisar el estado de salud de la replicación de los volúmenes del datastore correspondientes, y el estado de una conmutación por error o una conmutación por error de prueba se puede seguir a través de Job Monitoring.



Si un trabajo está actualmente en progreso o en cola y desea detenerlo, existe una opción para cancelarlo.

Con el panel de recuperación ante desastres, podrás evaluar con total confianza el estado de los sitios de recuperación ante desastres y los planes de replicación. Esto permite a los administradores identificar rápidamente los sitios y planes en buen estado, desconectados o degradados.



Esto proporciona una solución poderosa para gestionar un plan de recuperación ante desastres personalizado y adaptado. La conmutación por error se puede realizar de forma planificada o con solo hacer clic en un botón cuando ocurre un desastre y se toma la decisión de activar el sitio de recuperación ante desastres.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado o utilizar el"simulador de soluciones" .

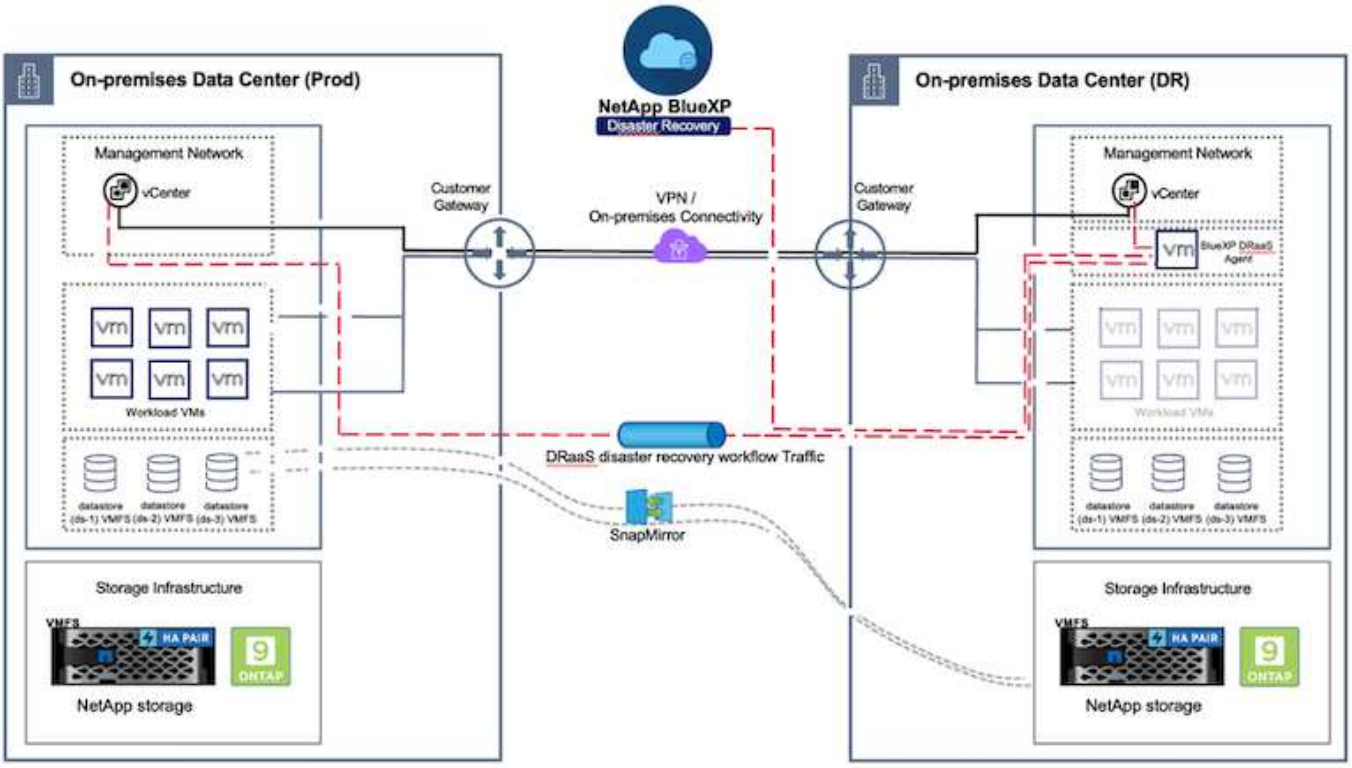
NetApp Disaster Recovery para almacenes de datos VMFS

La recuperación ante desastres mediante la replicación a nivel de bloque desde el sitio de producción al sitio de recuperación ante desastres es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos, como ataques de ransomware. Con la replicación SnapMirror de NetApp , las cargas de trabajo de VMware que se ejecutan en sistemas ONTAP locales que utilizan un almacén de datos VMFS se pueden replicar en otro sistema de almacenamiento ONTAP en un centro de datos de recuperación designado donde reside VMware.

Esta sección del documento describe la configuración de NetApp Diaster Recovery para configurar la recuperación ante desastres de máquinas virtuales de VMware locales en otro sitio designado. Como parte de esta configuración, se incluyen el agente de NetApp Console, la incorporación de los sistemas ONTAP, la definición de sitios y la asociación de VMware vCenter. Además, este documento detalla cómo configurar la replicación entre sitios y cómo configurar y probar un plan de recuperación. La última sección incluye instrucciones para realizar una conmutación por error completa del sitio y cómo revertir la conmutación por error cuando el sitio principal se recupere y vuelva a estar en línea.

Mediante Disaster Recovery, que forma parte de NetApp Data Services, los clientes pueden detectar sus VMware vCenters locales junto con el almacenamiento ONTAP, crear agrupaciones de recursos, crear un plan de recuperación ante desastres, asociarlo a grupos de recursos y probar o ejecutar la conmutación por error y la conmutación de retorno. SnapMirror ofrece replicación de bloques a nivel de almacenamiento para mantener los dos sitios actualizados con los cambios incrementales, lo que da como resultado un RPO de hasta 5 minutos. También es posible simular procedimientos de recuperación ante desastres como un

simulacro periódico sin afectar los datastores de producción y replicados ni generar costes de almacenamiento adicionales. NetApp Data Services aprovecha la tecnología FlexClone de ONTAP para crear una copia con gestión eficiente del espacio del datastore VMFS a partir de la última Snapshot replicada en el sitio de recuperación ante desastres. Una vez completada la prueba de recuperación ante desastres, los clientes pueden simplemente eliminar el entorno de prueba, de nuevo sin afectar en absoluto a los recursos de producción replicados reales. Cuando surge la necesidad (planificada o no planificada) de una conmutación por error real, con unos pocos clics, Disaster Recovery coordinará todos los pasos necesarios para poner en marcha automáticamente las máquinas virtuales protegidas en el sitio de recuperación ante desastres designado. El servicio también revertirá la relación de SnapMirror al sitio principal y replicará cualquier cambio del secundario al principal para una operación de conmutación de retorno, cuando sea necesario. Todo esto se puede lograr con una fracción del coste en comparación con otras alternativas conocidas.

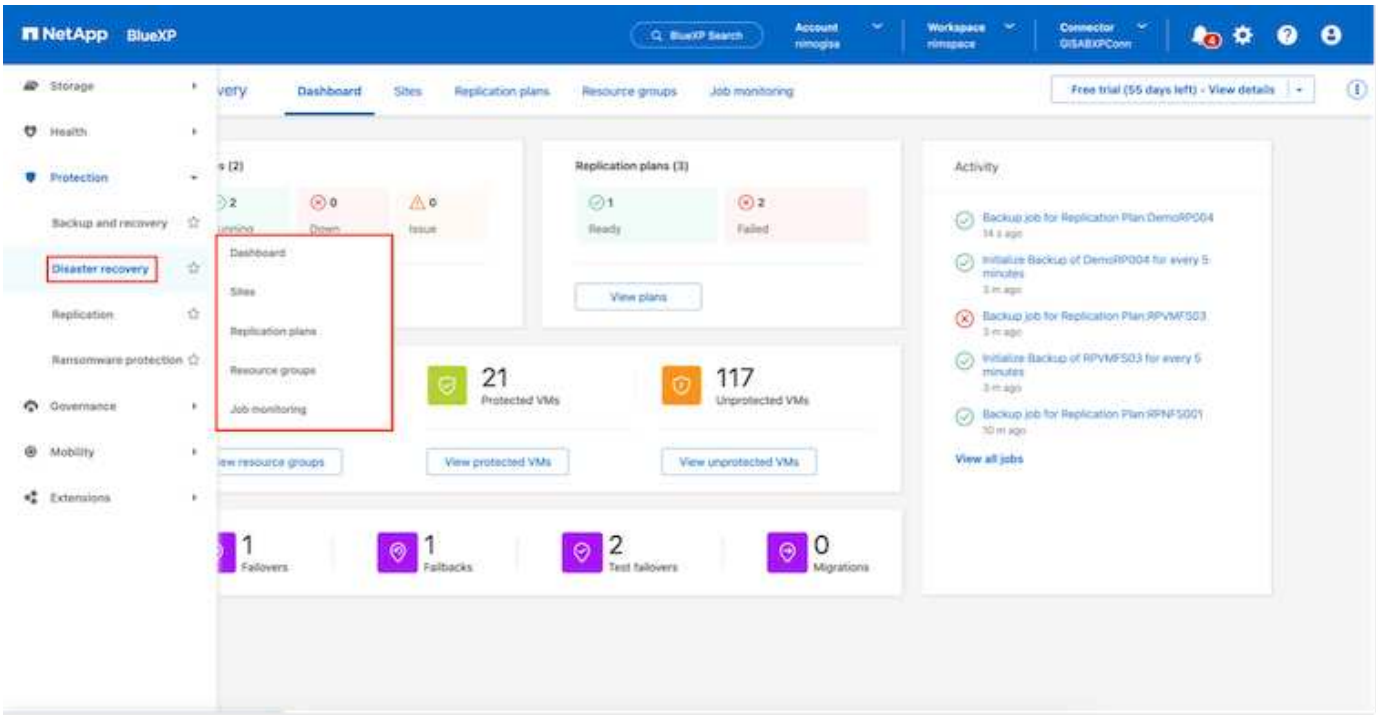


Para obtener información actualizada y conocer las versiones compatibles de vCenter Server, ESXi y ONTAP para la recuperación ante desastres, consulta "Configuraciones compatibles con la recuperación ante desastres".

Empezando

Para empezar a usar Disaster Recovery, utiliza NetApp Console y luego accede al servicio.

1. Inicia sesión en NetApp Console.
2. En el panel de navegación izquierdo de NetApp Console, selecciona «Protección» > «Recuperación ante desastres».
3. Aparece el Disaster Recovery Dashboard.

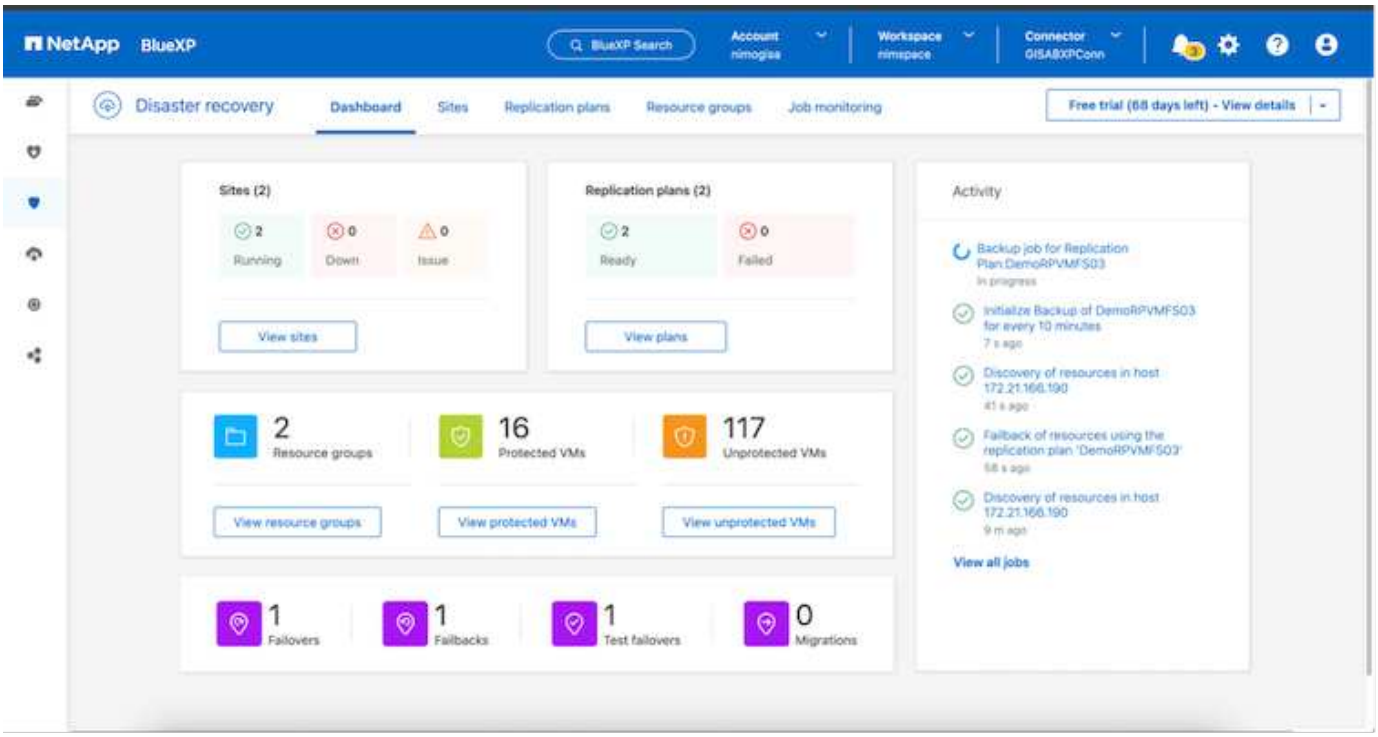


Antes de configurar el plan de recuperación ante desastres, asegúrese de que se cumplan los siguientes requisitos previos:

- El agente de NetApp Console se implementa en una VPC de AWS.
- Las instancias del agente de NetApp Console tienen conectividad con los sistemas de vCenter y de almacenamiento de origen y destino.
- Los sistemas de almacenamiento locales de NetApp que alojan almacenes de datos VMFS para VMware se añaden en NetApp Console.
- La resolución de DNS debe estar vigente cuando se utilizan nombres DNS. De lo contrario, utilice direcciones IP para vCenter.
- La replicación de SnapMirror está configurada para los volúmenes de almacén de datos basados en VMFS designados.

Una vez establecida la conectividad entre los sitios de origen y destino, continúe con los pasos de configuración, que deberían tomar entre 3 y 5 minutos.

NetApp recomienda implementar el agente de NetApp Console en el sitio de recuperación ante desastres o en un tercer sitio, de modo que el agente de NetApp Console pueda comunicarse a través de la red con los recursos de origen y de destino durante interrupciones reales o desastres naturales.

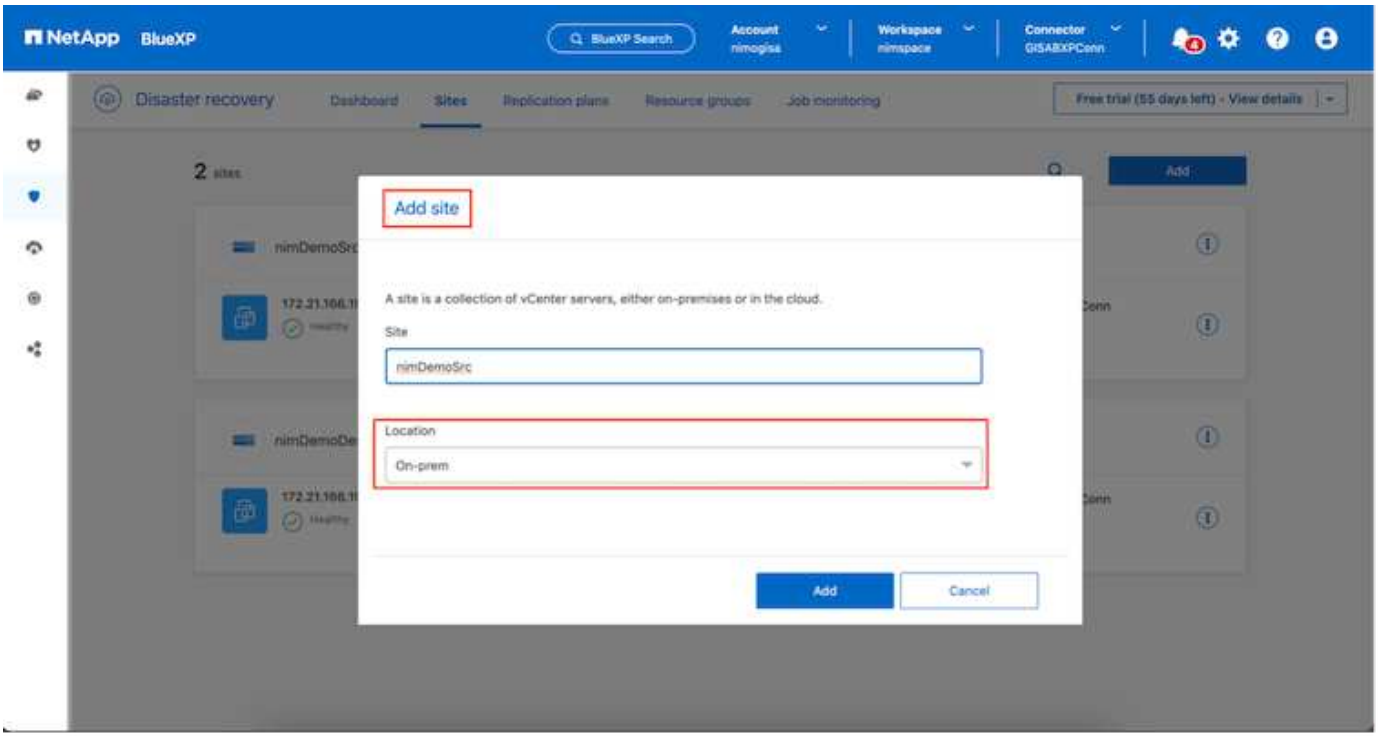


La compatibilidad con almacenes de datos VMFS locales a locales se encuentra en versión preliminar tecnológica al momento de escribir este documento. Esta capacidad es compatible con almacenes de datos VMFS basados en protocolos FC e ISCSI.

Configuración de recuperación ante desastres

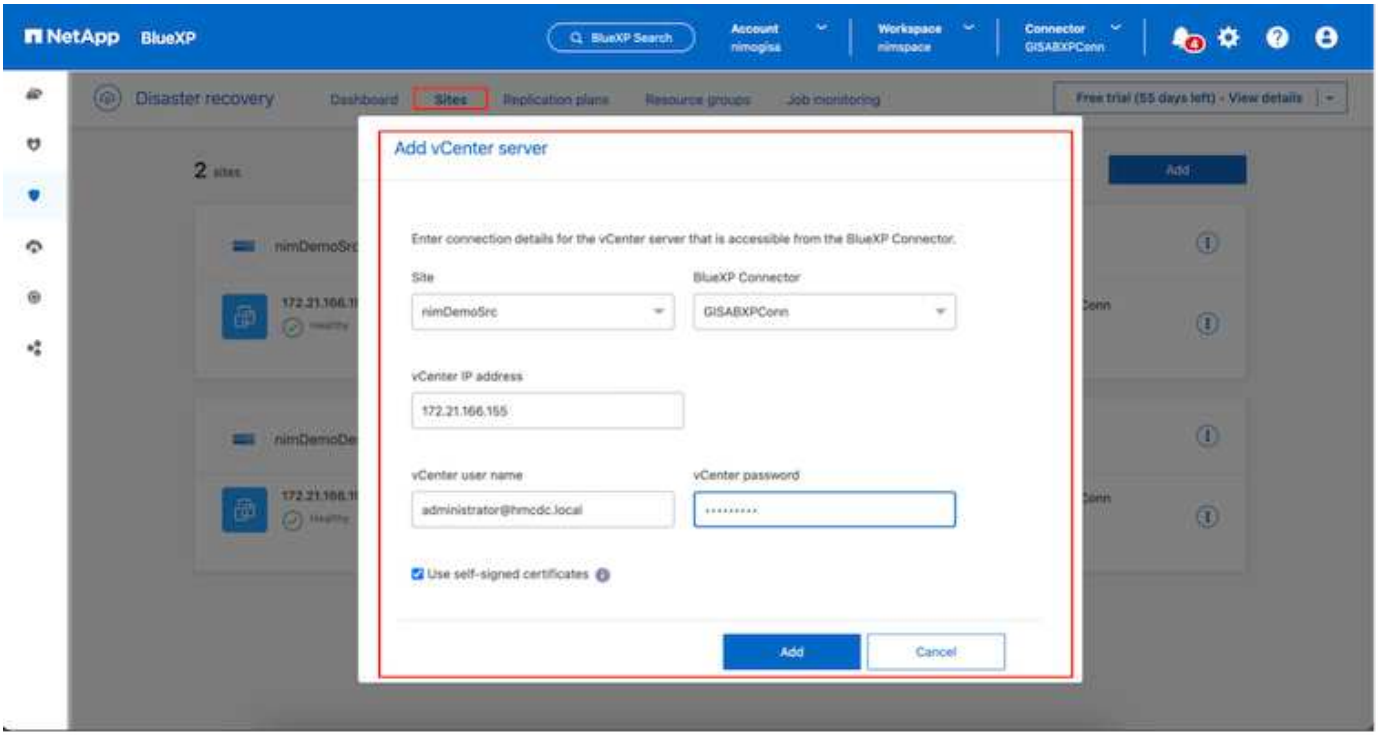
El primer paso para prepararte para la recuperación ante desastres es detectar y añadir los recursos de almacenamiento y vCenter en las instalaciones a Disaster Recovery.

Asegúrate de que los sistemas de almacenamiento ONTAP estén añadidos al entorno de trabajo dentro del lienzo. Abre NetApp Console y selecciona **Protección > Recuperación ante desastres** en la navegación de la izquierda. Selecciona **Detectar servidores de vCenter** o usa el menú superior, selecciona **Sitios > Añadir > Añadir vCenter**.

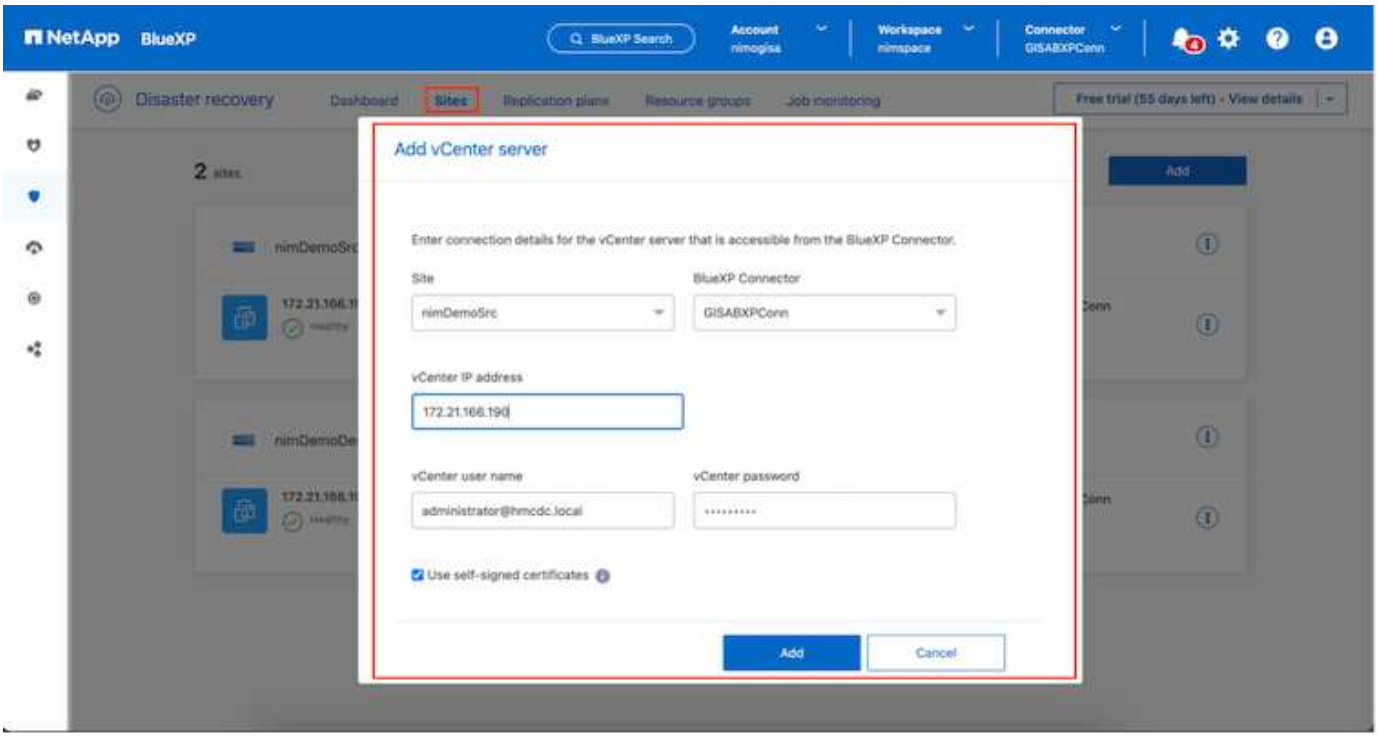


Agregue las siguientes plataformas:

- **Fuente**. vCenter local.



- **Destino**. Centro de datos SDDC de VMC.



Una vez que se agregan los vCenters, se activa el descubrimiento automático.

Configuración de la replicación de almacenamiento entre el sitio de origen y el de destino

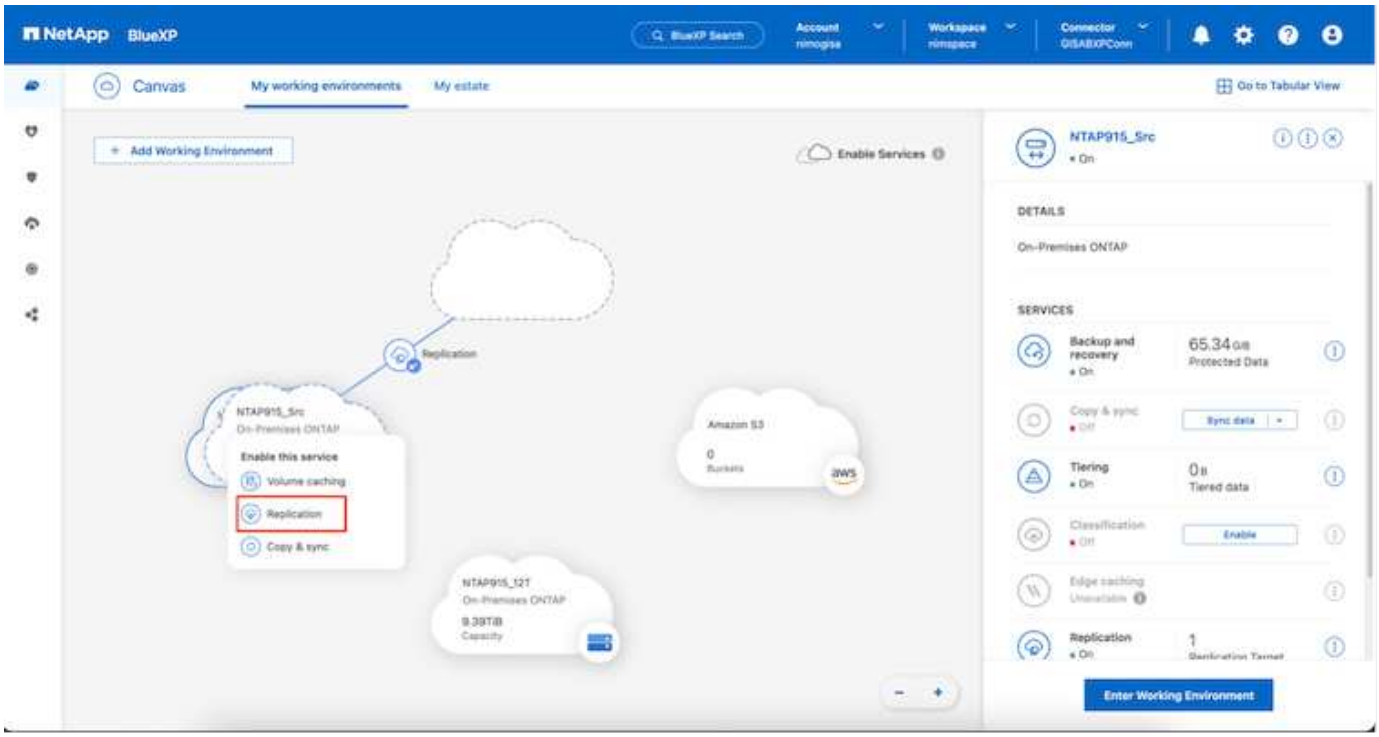
SnapMirror utiliza instantáneas de ONTAP para administrar la transferencia de datos de una ubicación a otra. Inicialmente, se copia una copia completa basada en una instantánea del volumen de origen al destino para realizar una sincronización de línea base. A medida que se producen cambios en los datos en la fuente, se crea una nueva instantánea y se compara con la instantánea de referencia. Luego, los bloques que se han modificado se replican en el destino, y la instantánea más nueva se convierte en la línea de base actual, o la instantánea común más nueva. Esto permite que el proceso se repita y que se envíen actualizaciones incrementales al destino.

Cuando se establece una relación SnapMirror , el volumen de destino está en un estado de solo lectura en línea y, por lo tanto, aún es accesible. SnapMirror trabaja con bloques físicos de almacenamiento, en lugar de a nivel de archivos u otro nivel lógico. Esto significa que el volumen de destino es una réplica idéntica del de origen, incluidas instantáneas, configuraciones de volumen, etc. Si el volumen de origen utiliza funciones de eficiencia de espacio de ONTAP , como compresión de datos y deduplicación de datos, el volumen replicado conservará estas optimizaciones.

Al romper la relación de SnapMirror , el volumen de destino se puede escribir y normalmente se utiliza para realizar una conmutación por error cuando se utiliza SnapMirror para sincronizar datos con un entorno de recuperación ante desastres. SnapMirror es lo suficientemente sofisticado para permitir que los datos modificados en el sitio de conmutación por error se resincronicen de manera eficiente con el sistema principal, en caso de que más tarde vuelva a estar en línea, y luego permitir que se restablezca la relación original de SnapMirror .

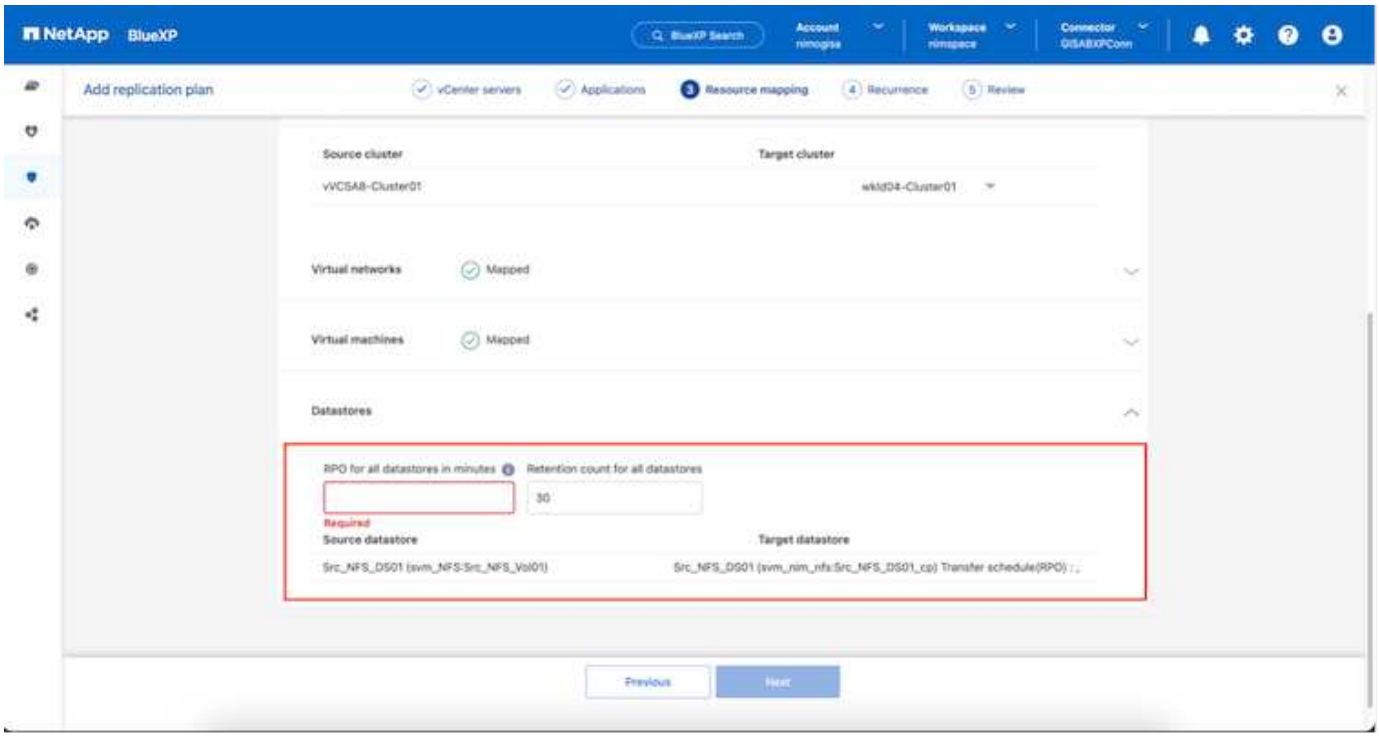
Cómo configurarlo para VMware Disaster Recovery

El proceso para crear la replicación de SnapMirror sigue siendo el mismo para cualquier aplicación. El proceso puede ser manual o automatizado. La forma más sencilla es usar NetApp Console para configurar la replicación de SnapMirror mediante una simple acción de arrastrar y soltar el sistema ONTAP de origen del entorno sobre el de destino para activar el asistente que te guía durante el resto del proceso.



NetApp Data Services también puede automatizar este proceso siempre que se cumplan los dos criterios siguientes:

- Los clústeres de origen y destino tienen una relación de pares.
- El SVM de origen y el SVM de destino tienen una relación de pares.

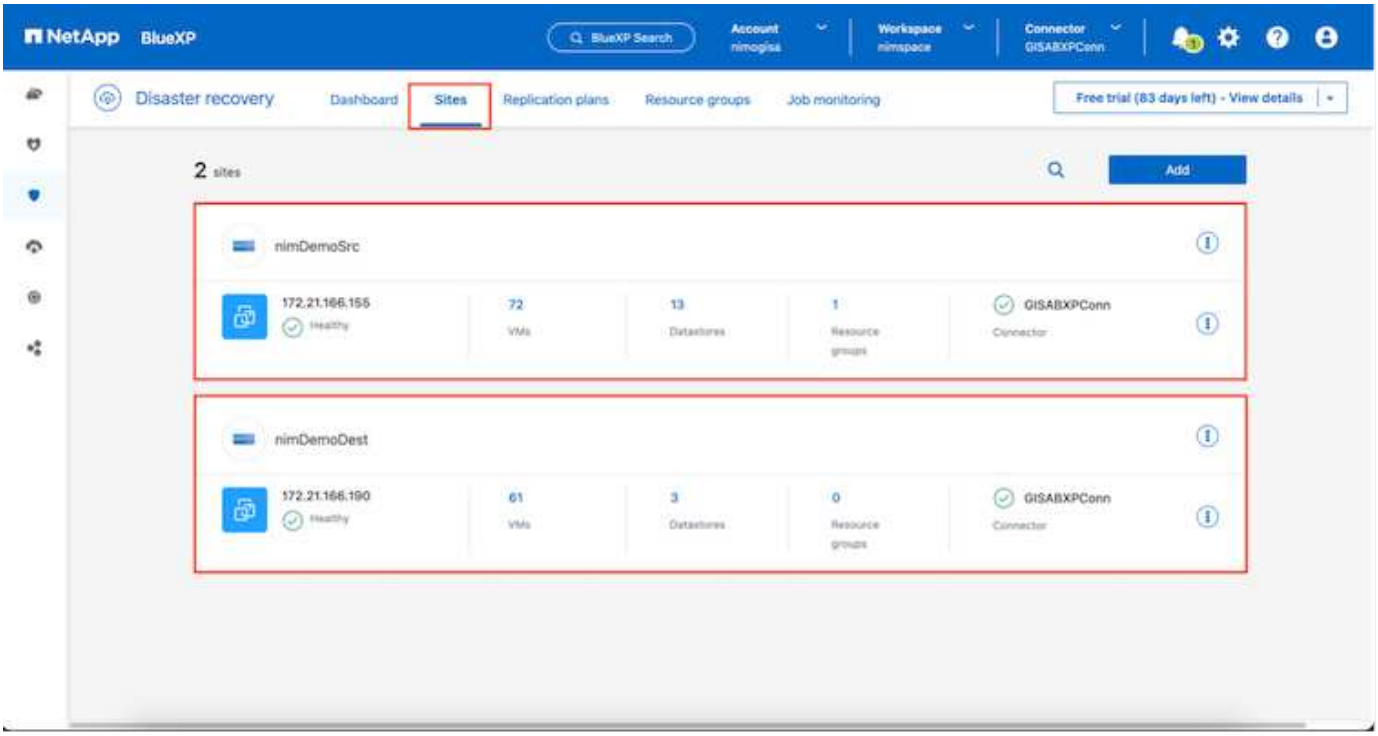


Si ya se ha configurado una relación de SnapMirror para el volumen a través de la CLI, NetApp Console detecta la relación y continúa con el resto de las operaciones del flujo de trabajo.

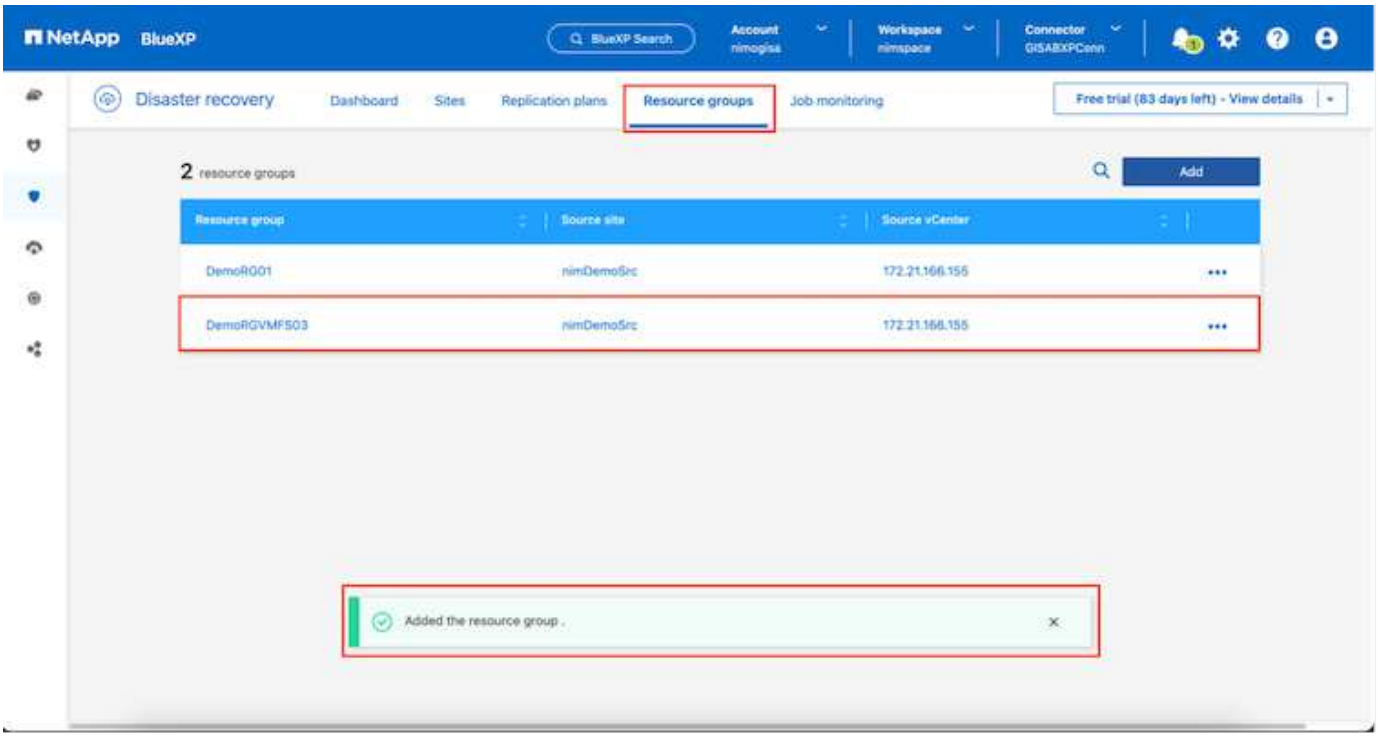
Además de los enfoques anteriores, también puedes crear la replicación de SnapMirror mediante la CLI de ONTAP o System Manager. Independientemente del método que uses para sincronizar los datos con SnapMirror, Disaster Recovery organiza el flujo de trabajo para que las operaciones de recuperación ante desastres sean fluidas y eficientes.

¿Qué puede hacer Disaster Recovery por ti?

Una vez añadidos los sitios de origen y destino, Disaster Recovery realiza una detección exhaustiva automática y muestra las VMs junto con los metadatos asociados. Disaster Recovery también detecta automáticamente las redes y los grupos de puertos que usan las VMs y los completa.

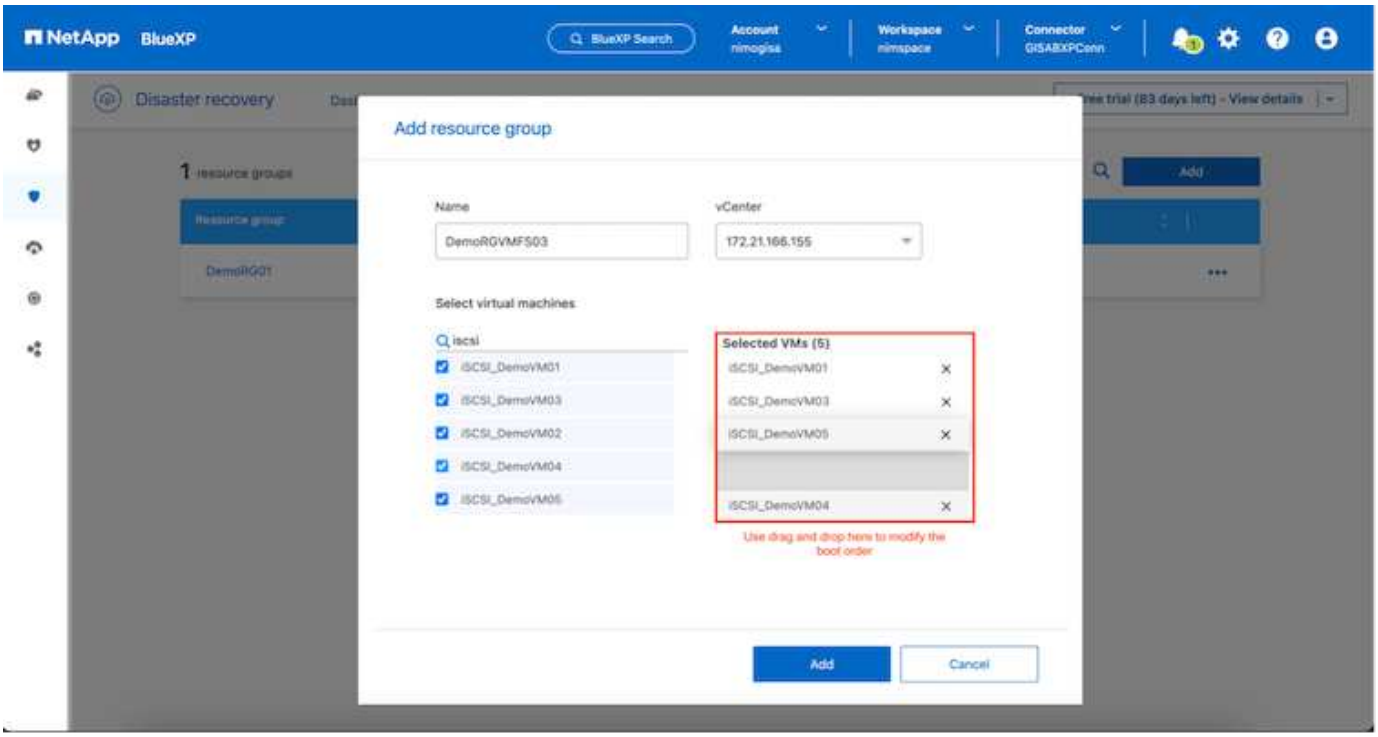


Una vez añadidos los sitios, las máquinas virtuales se pueden agrupar en grupos de recursos. Los grupos de recursos de Disaster Recovery te permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque y retrasos de arranque, que se pueden ejecutar durante la recuperación. Para empezar a crear grupos de recursos, ve a **Resource Groups** y haz clic en **Create New Resource Group**.

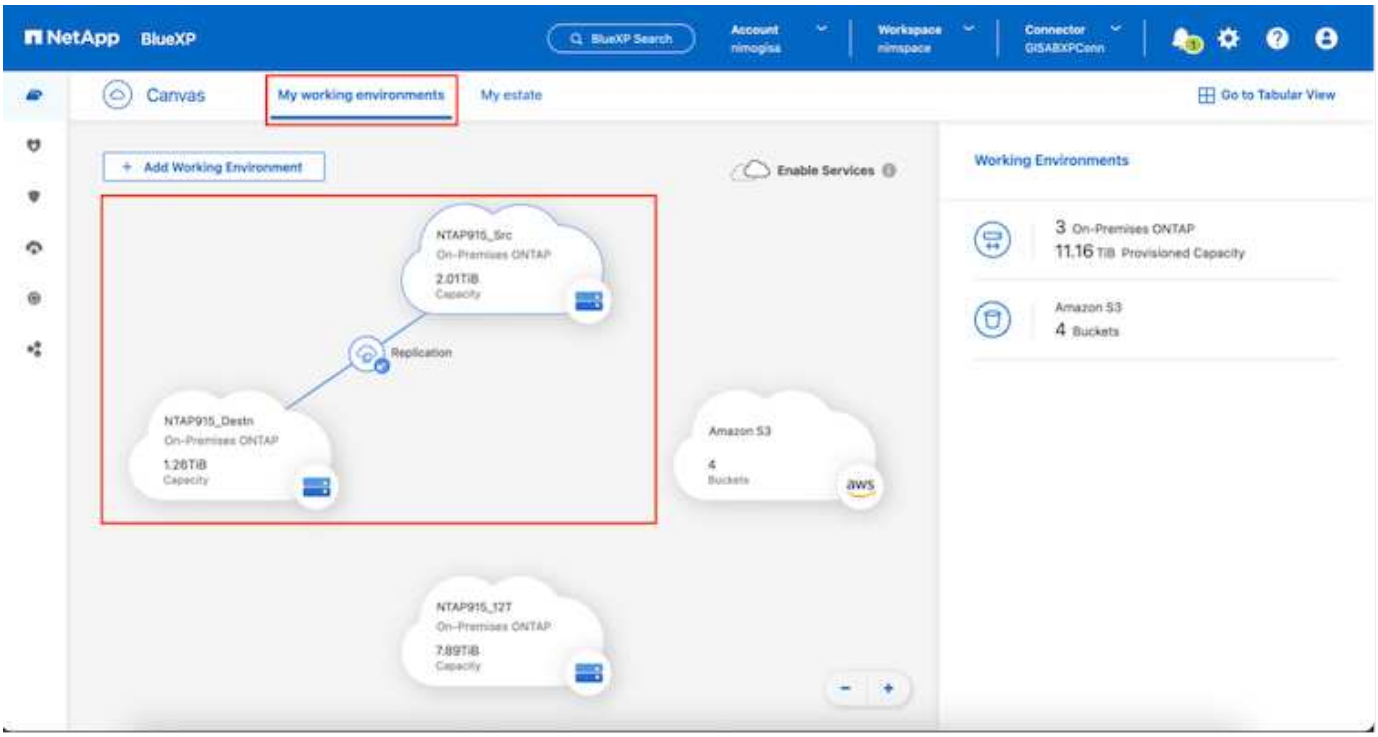


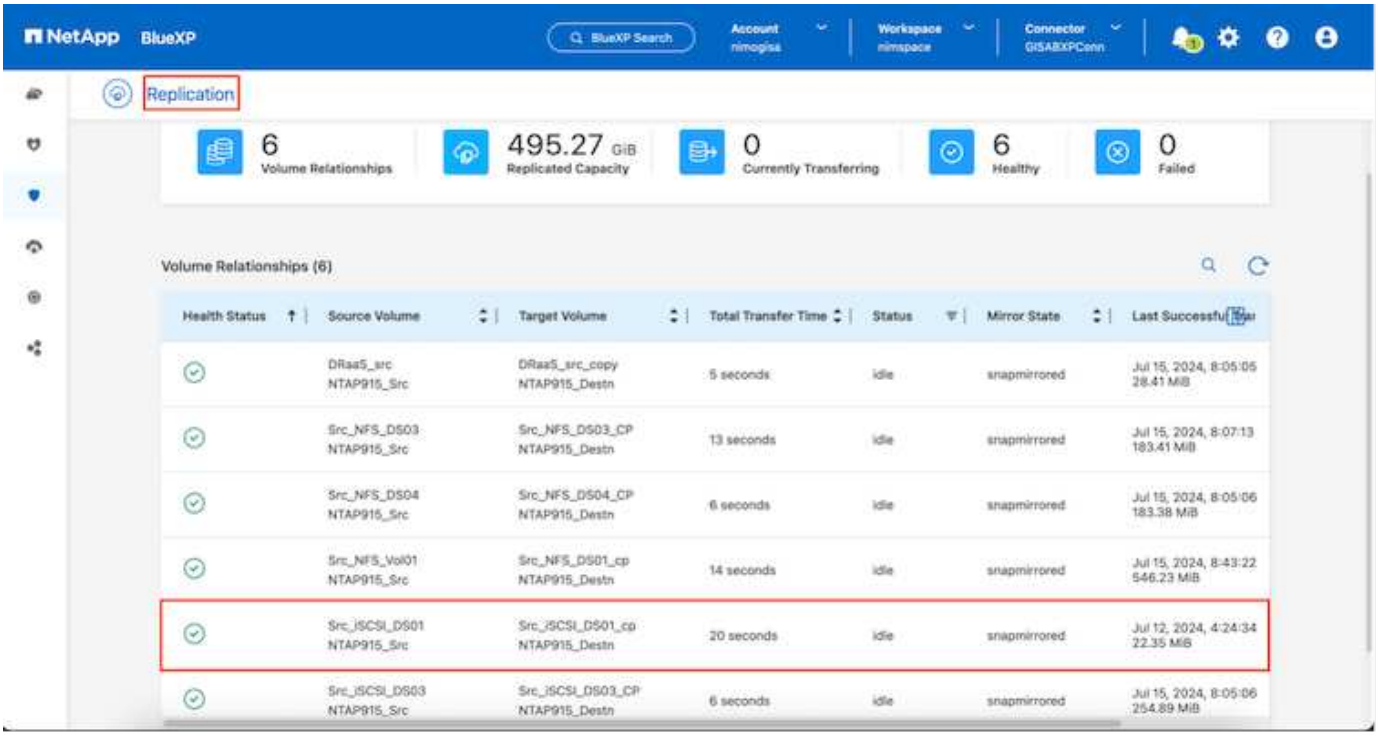
El grupo de recursos también se puede crear mientras se crea un plan de replicación.

El orden de arranque de las máquinas virtuales se puede definir o modificar durante la creación de grupos de recursos mediante un simple mecanismo de arrastrar y soltar.



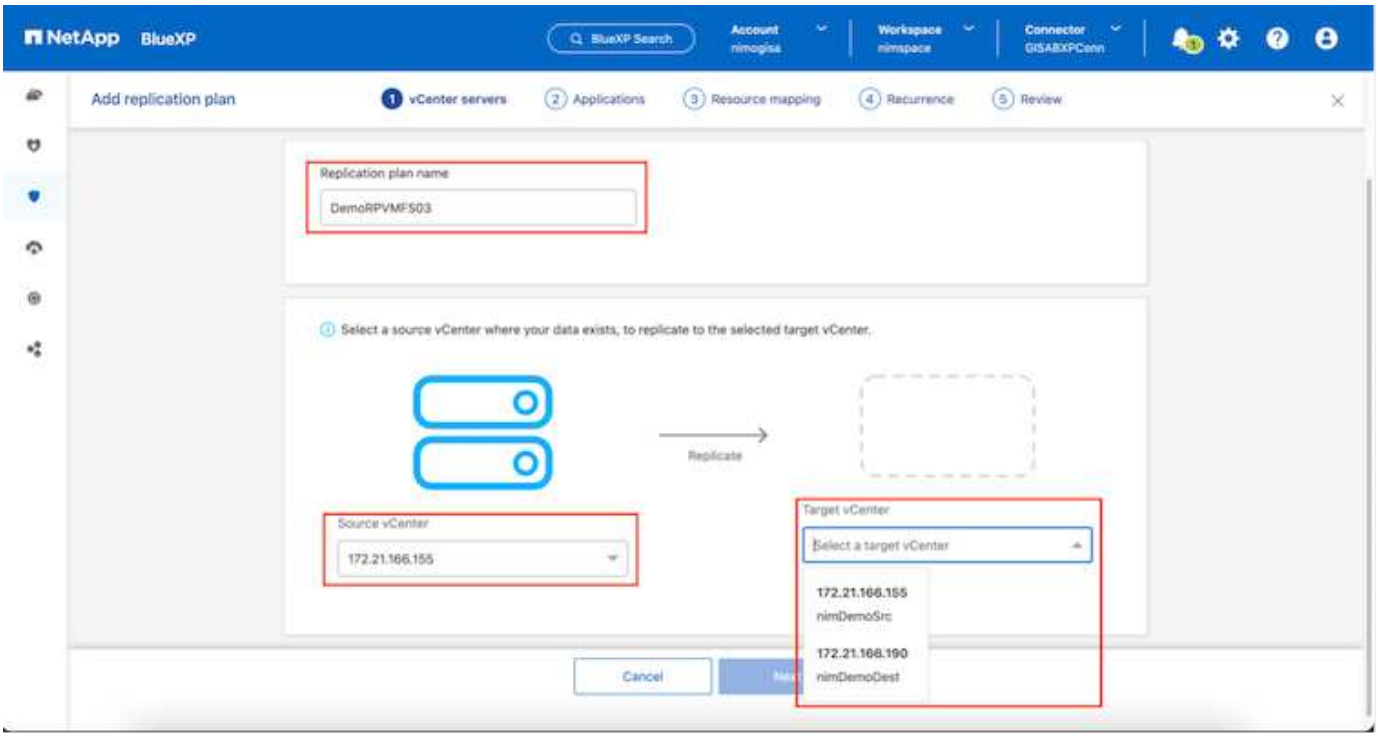
Una vez creados los grupos de recursos, el siguiente paso es crear el plan de ejecución o un plan para recuperar máquinas virtuales y aplicaciones en caso de desastre. Como se menciona en los requisitos previos, la replicación de SnapMirror se puede configurar de antemano o DRaaS puede configurarla utilizando el RPO y el recuento de retención especificados durante la creación del plan de replicación.



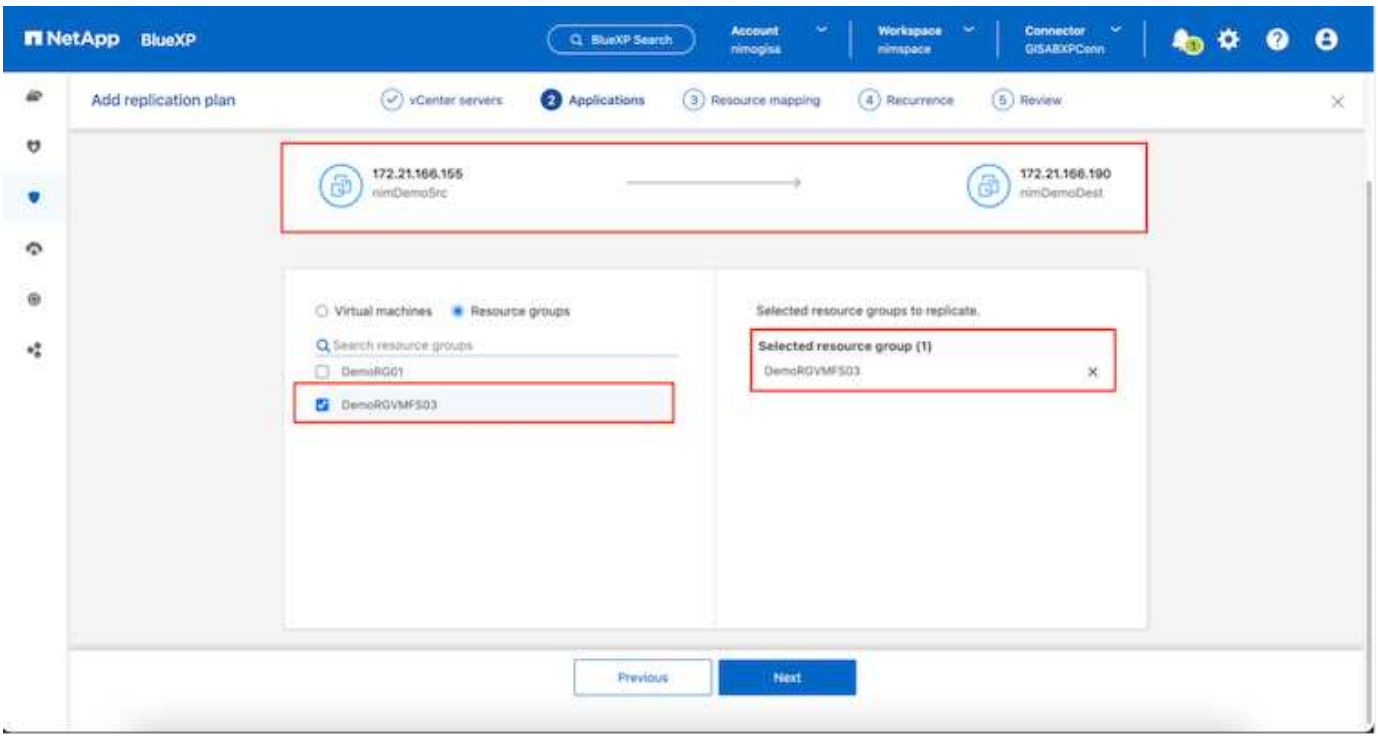


Configure el plan de replicación seleccionando las plataformas vCenter de origen y destino en el menú desplegable y elija los grupos de recursos que se incluirán en el plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones y el mapeo de clústeres y redes. Para definir el plan de recuperación, navegue a la pestaña **Plan de replicación** y haga clic en **Agregar plan**.

Primero, seleccione el vCenter de origen y luego seleccione el vCenter de destino.



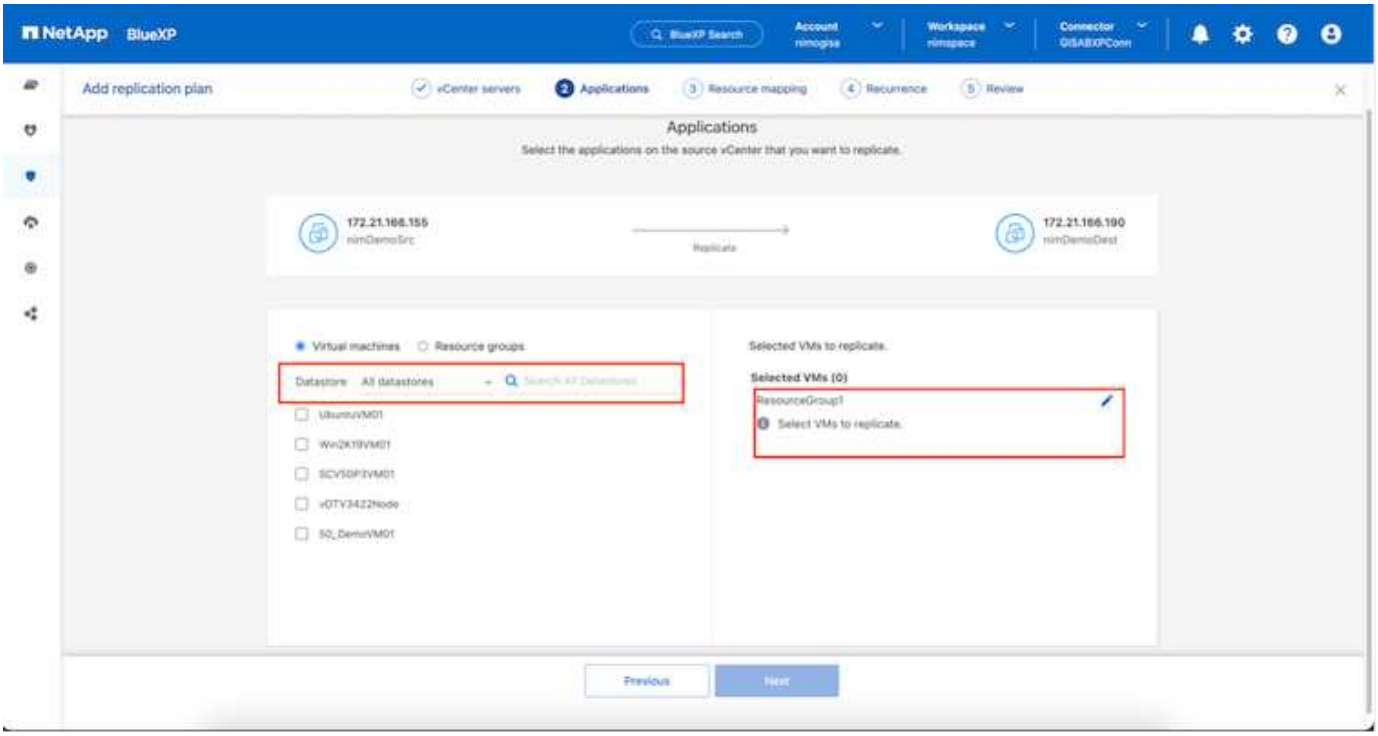
El siguiente paso es seleccionar los grupos de recursos existentes. Si no se crean grupos de recursos, el asistente ayuda a agrupar las máquinas virtuales necesarias (básicamente, crea grupos de recursos funcionales) en función de los objetivos de recuperación. Esto también ayuda a definir la secuencia de operaciones de cómo se deben restaurar las máquinas virtuales de la aplicación.



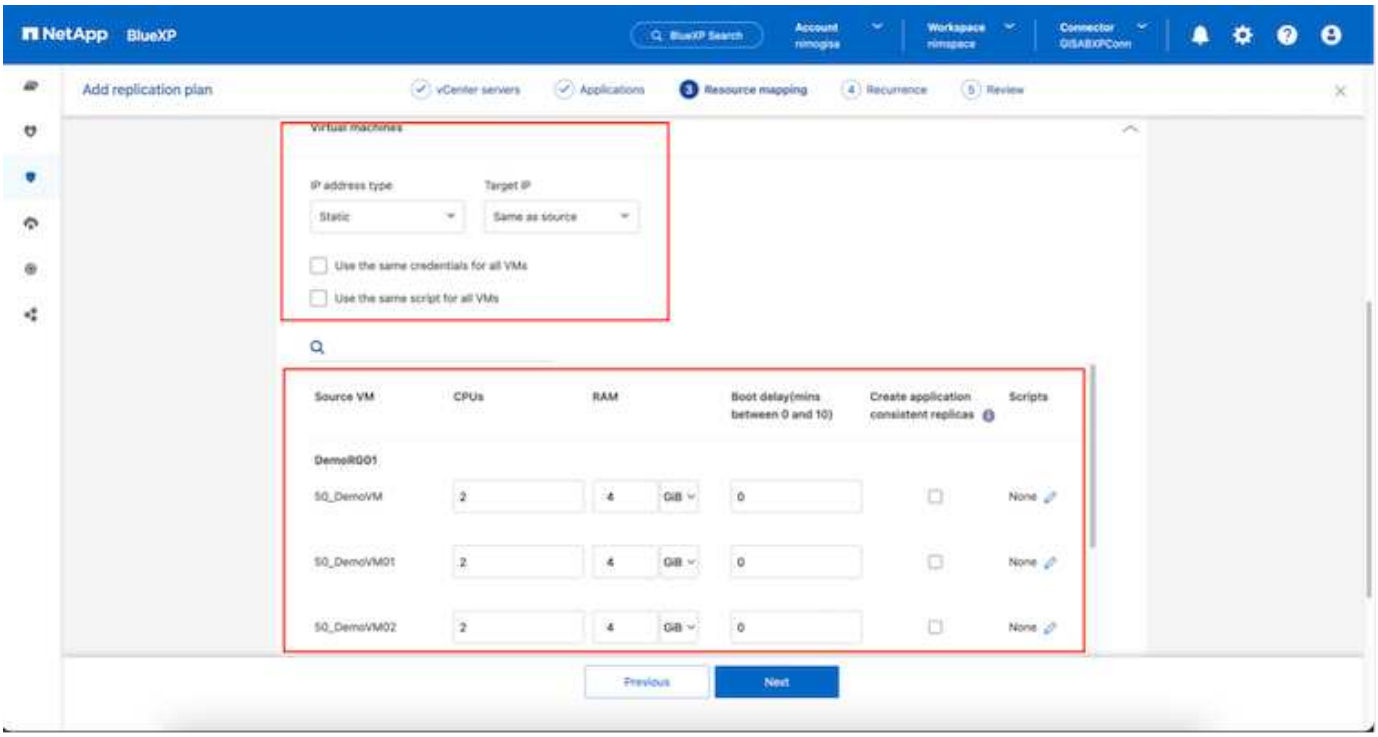
El grupo de recursos permite establecer el orden de arranque mediante la funcionalidad de arrastrar y soltar. Se puede utilizar para modificar fácilmente el orden en que se encenderán las máquinas virtuales durante el proceso de recuperación.

Cada máquina virtual dentro de un grupo de recursos se inicia en secuencia según el orden. Se inician dos grupos de recursos en paralelo.

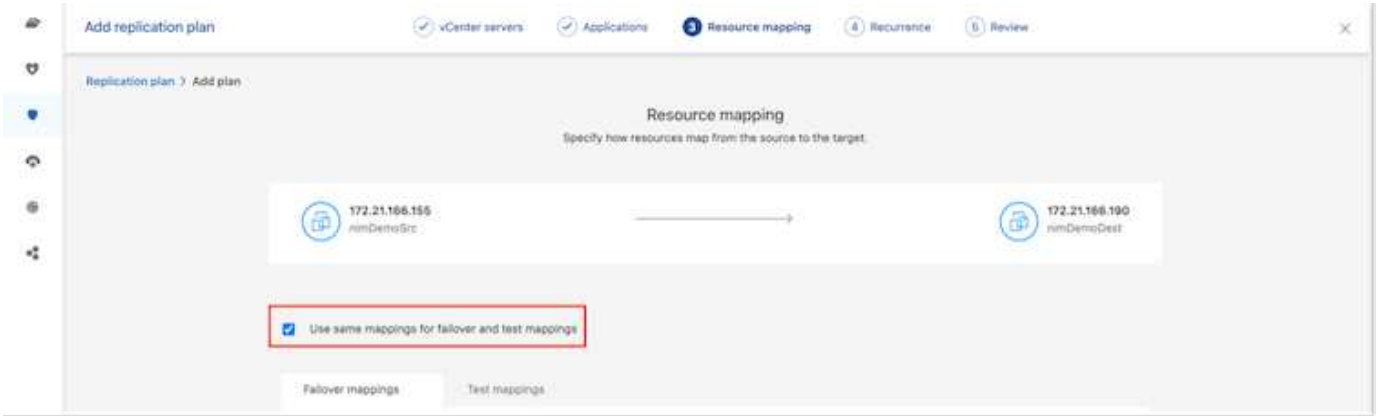
La siguiente captura de pantalla muestra la opción para filtrar máquinas virtuales o almacenes de datos específicos según los requisitos organizativos si no se crean grupos de recursos de antemano.



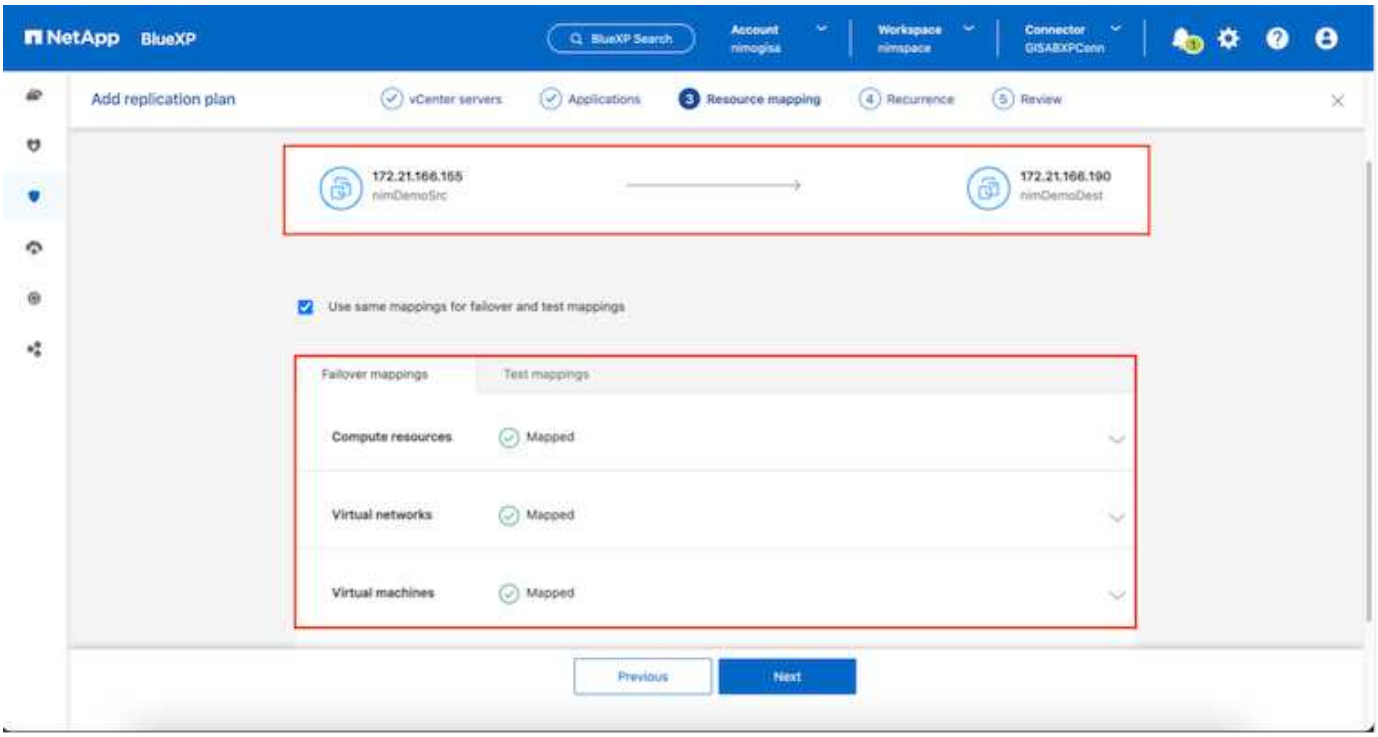
Una vez seleccionados los grupos de recursos, crea las asignaciones de conmutación por error. En este paso, especifica cómo se asignan los recursos del entorno de origen al de destino. Esto incluye recursos de computación y redes virtuales. Personalización de direcciones IP, scripts previos y posteriores, retrasos de arranque, consistencia de las aplicaciones, etc. Para obtener información detallada, consulta "Crear un plan de replicación".



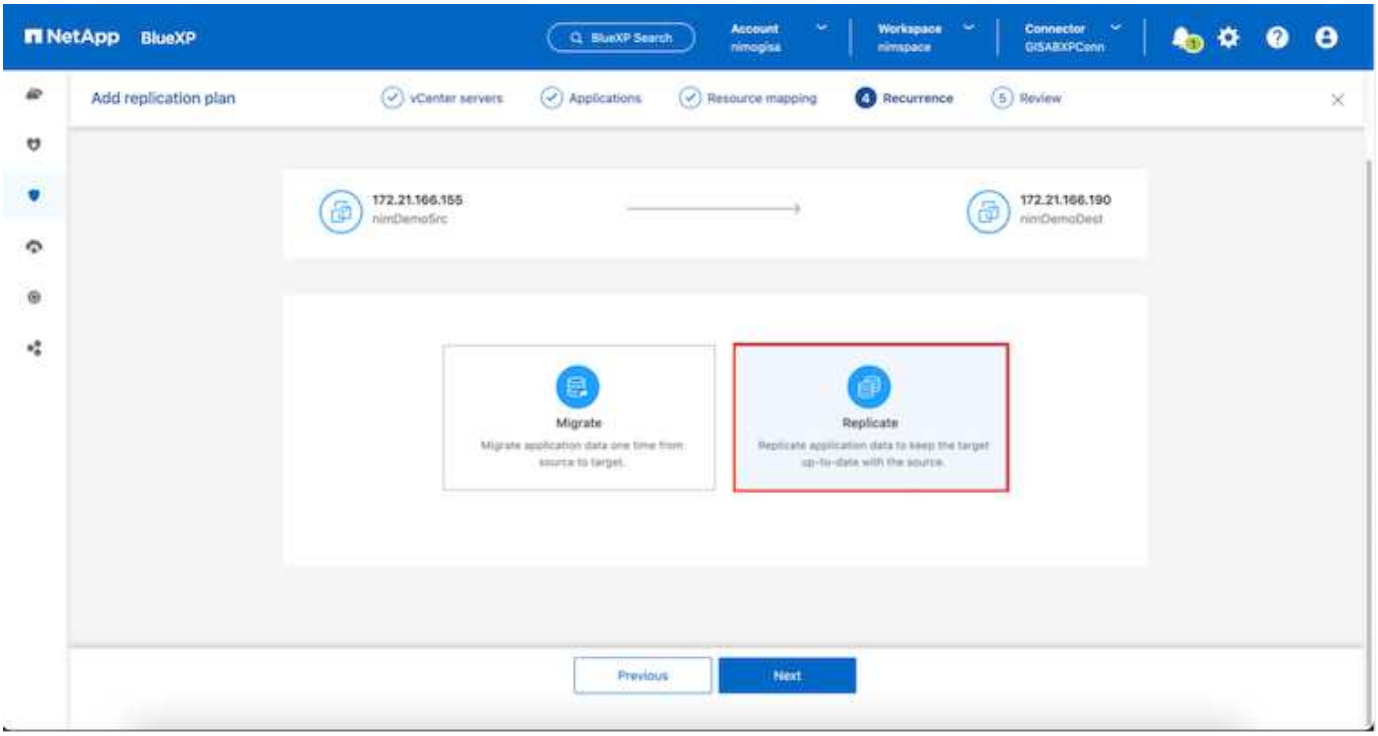
De forma predeterminada, se utilizan los mismos parámetros de mapeo para las operaciones de prueba y de conmutación por error. Para aplicar diferentes asignaciones para el entorno de prueba, seleccione la opción Asignación de prueba después de desmarcar la casilla de verificación como se muestra a continuación:



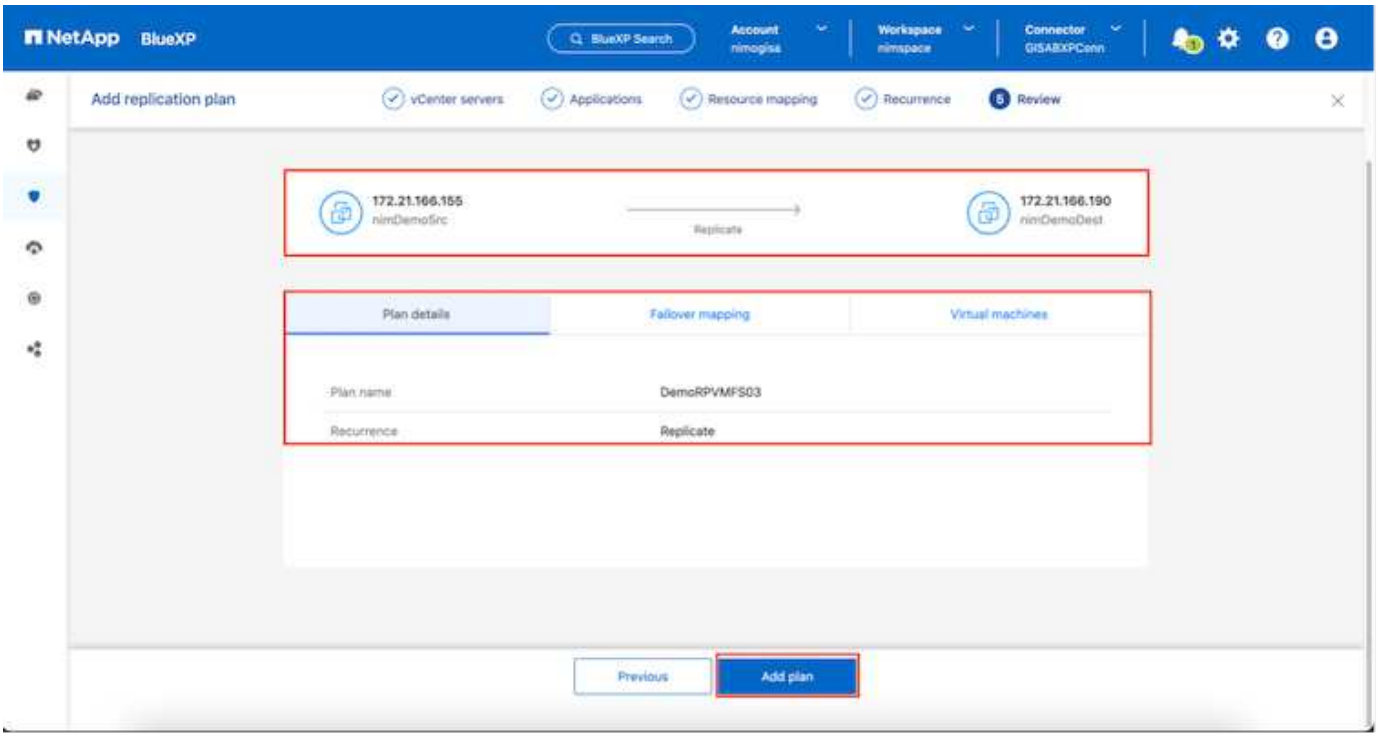
Una vez completado el mapeo de recursos, haga clic en Siguiente.

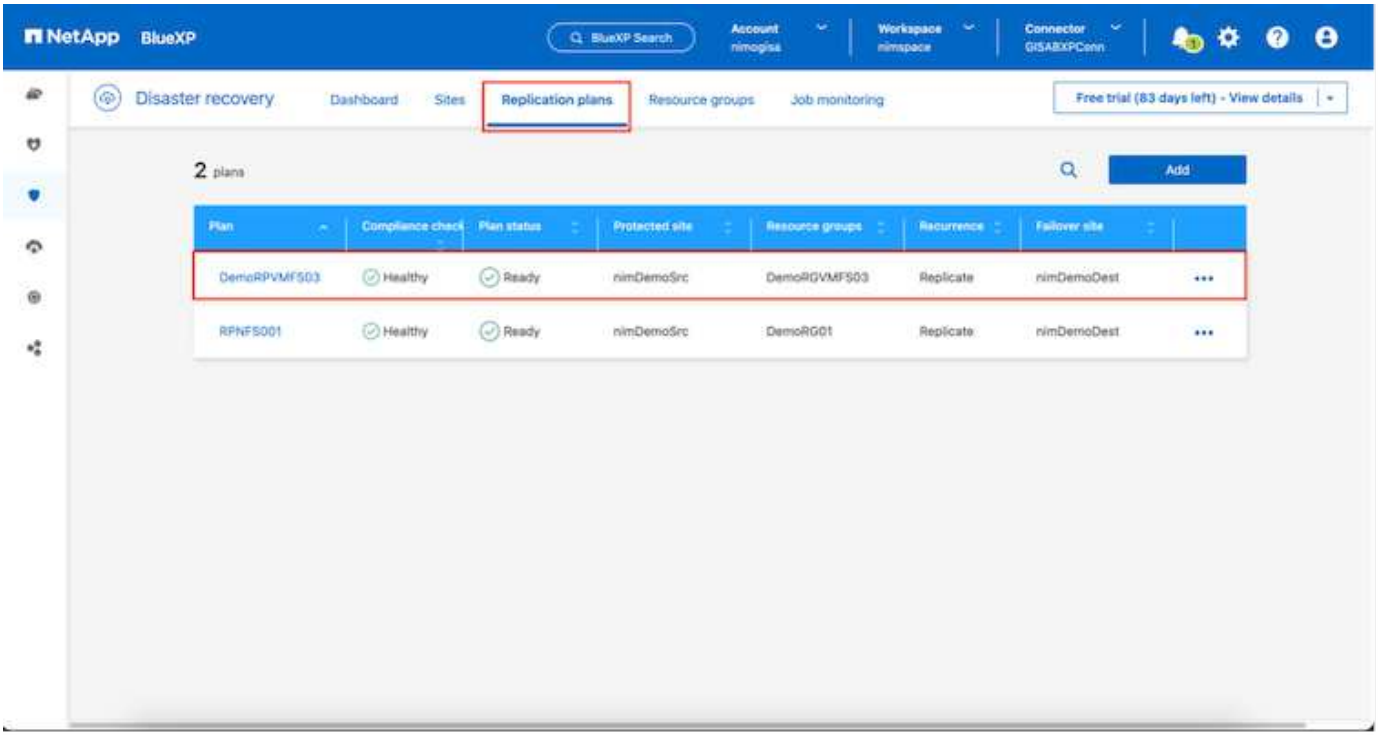


Seleccione el tipo de recurrencia. En palabras simples, seleccione la opción Migrar (migración única mediante conmutación por error) o replicación continua recurrente. En este tutorial, se selecciona la opción Replicar.

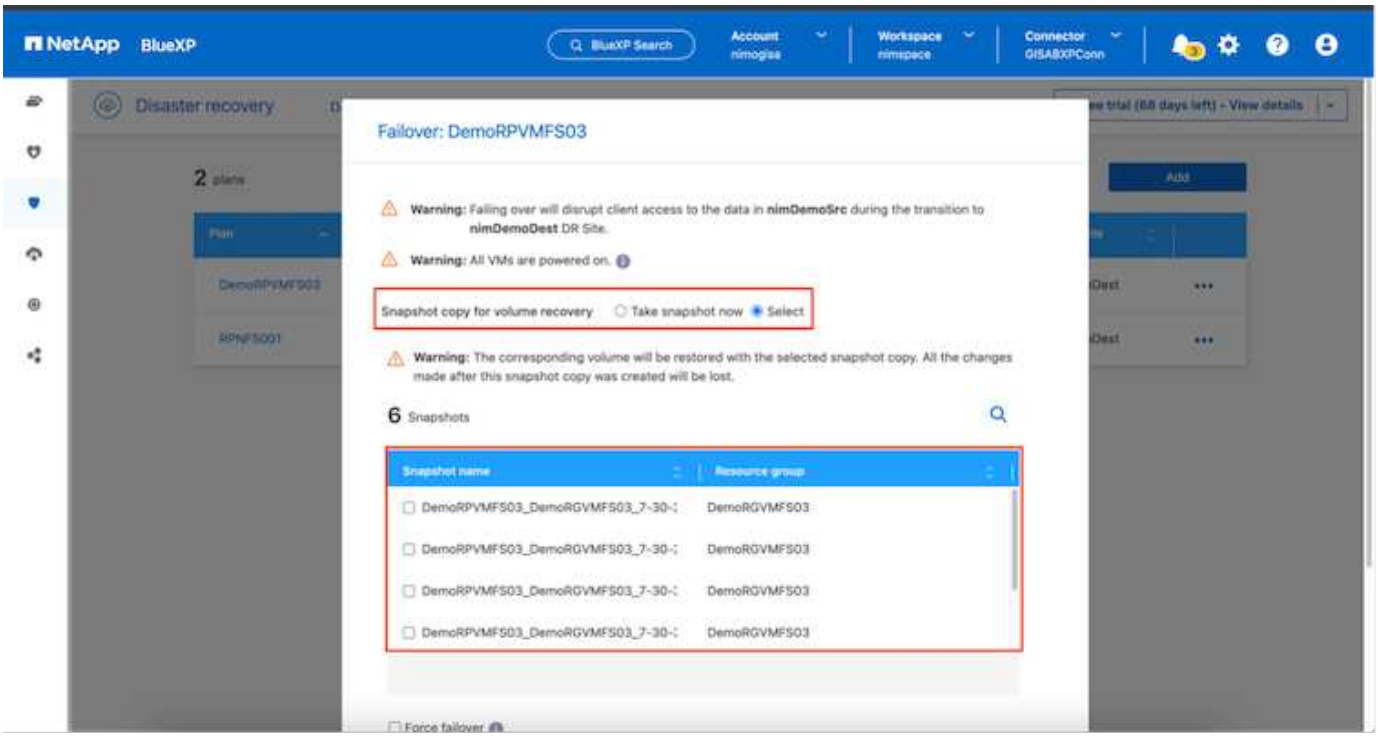


Una vez hecho esto, revise los mapeos creados y luego haga clic en Agregar plan.

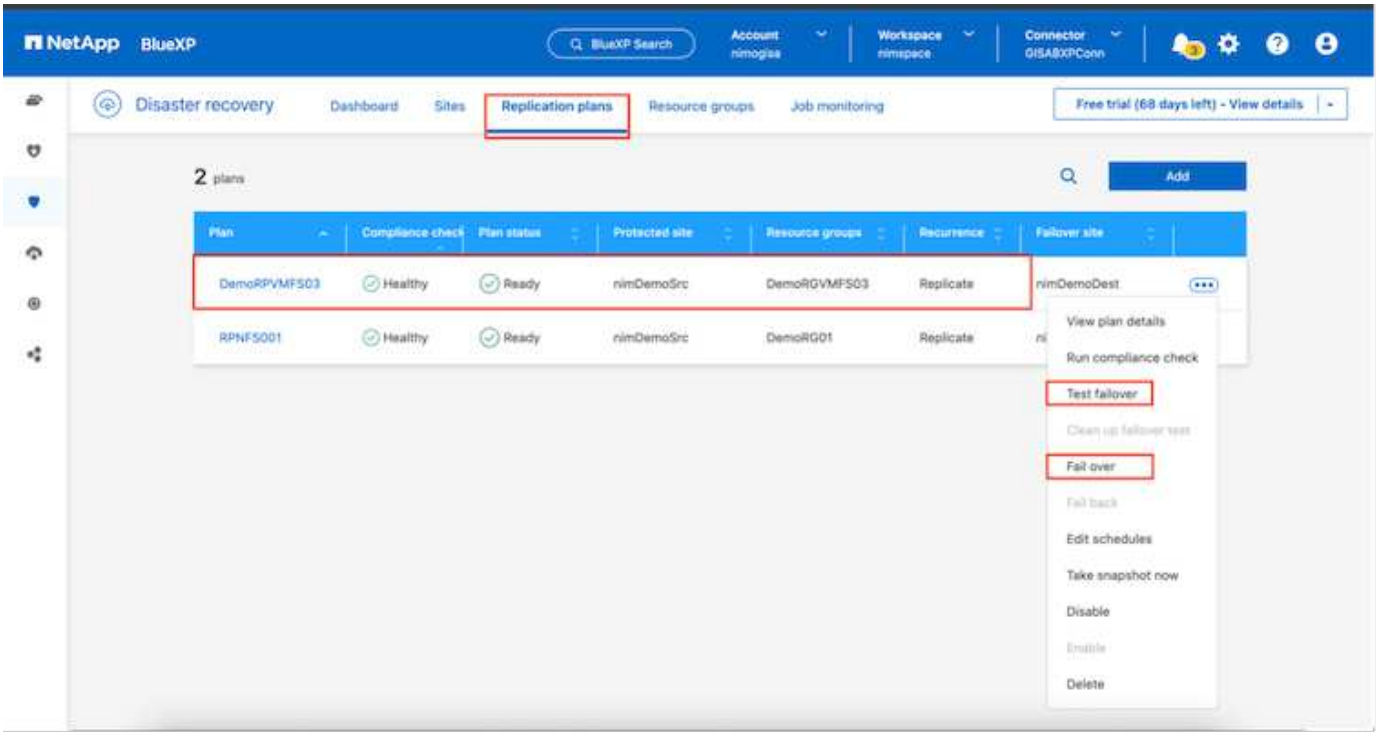




Una vez creado el plan de replicación, puedes realizar la conmutación por error según los requisitos seleccionando la opción de conmutación por error, la opción de conmutación por error de prueba o la opción de migrar. Disaster Recovery garantiza que el proceso de replicación se ejecute según el plan cada 30 minutos. Durante las opciones de conmutación por error y conmutación por error de prueba, puedes utilizar la copia Snapshot de SnapMirror más reciente, o puedes seleccionar una copia Snapshot específica de una copia Snapshot de un momento específico (según la política de retención de SnapMirror). La opción de momento específico puede ser muy útil si se produce un evento de corrupción como el ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. Disaster Recovery muestra todos los puntos de recuperación disponibles.



Para activar o probar la conmutación por error con la configuración especificada en el plan de replicación, haga clic en **Conmutación por error** o **Probar conmutación por error**.

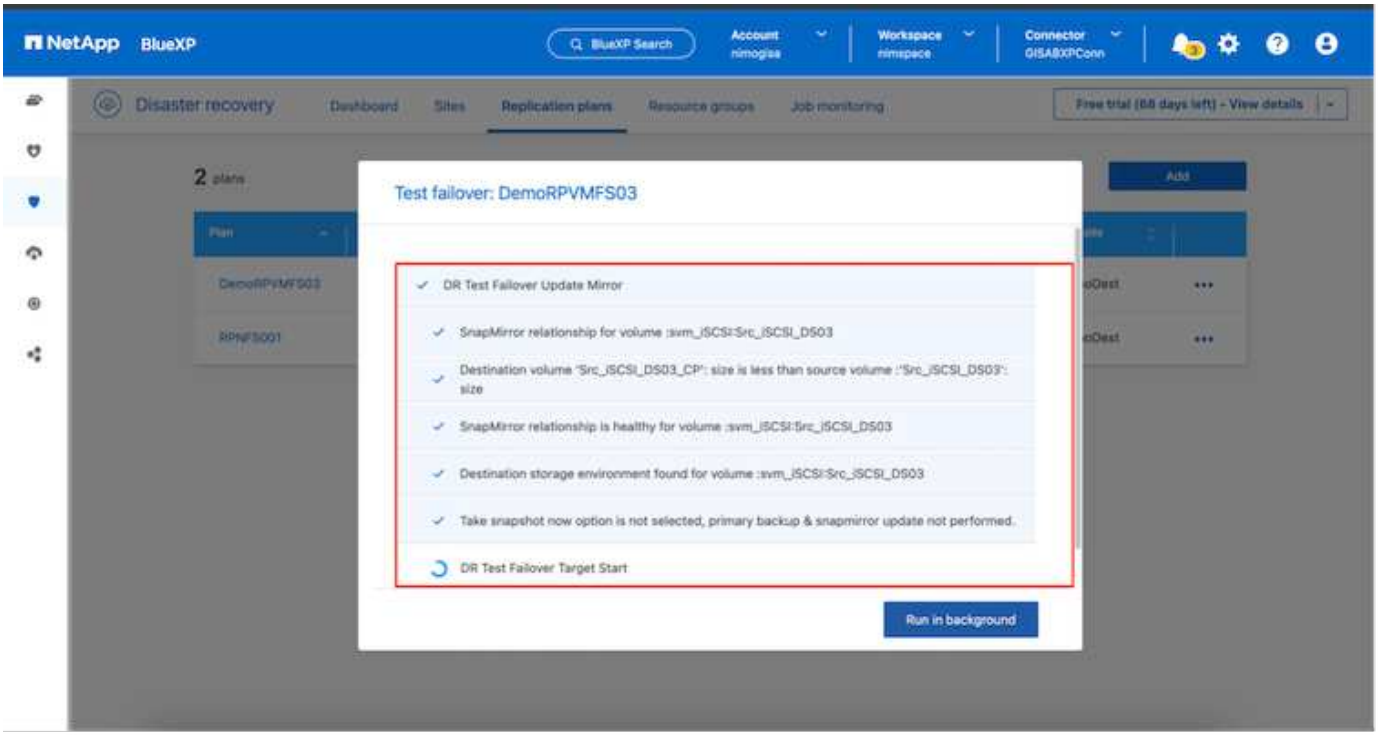


¿Qué sucede durante una operación de conmutación por error o de prueba?

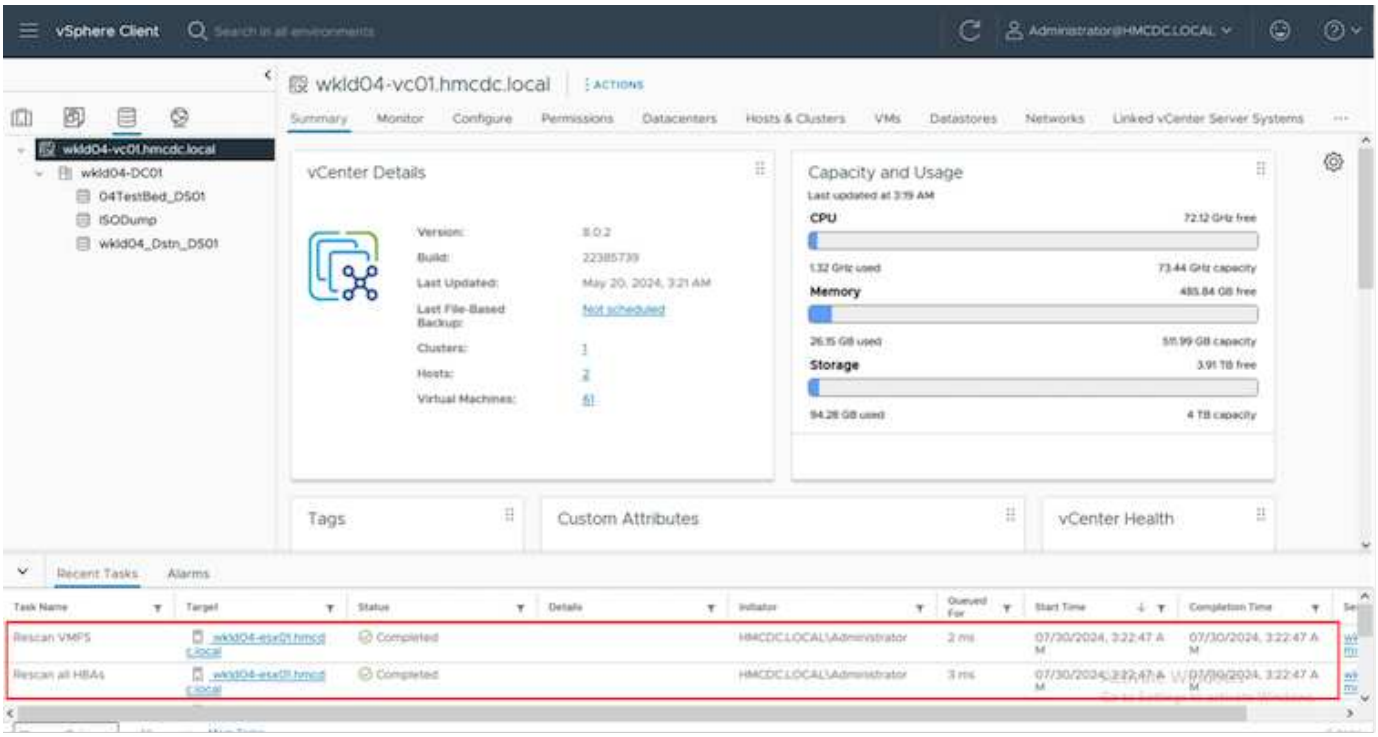
Durante una operación de conmutación por error de prueba, Disaster Recovery crea un volumen FlexClone en el sistema de almacenamiento ONTAP de destino mediante la copia Snapshot más reciente o una Snapshot seleccionada del volumen de destino.

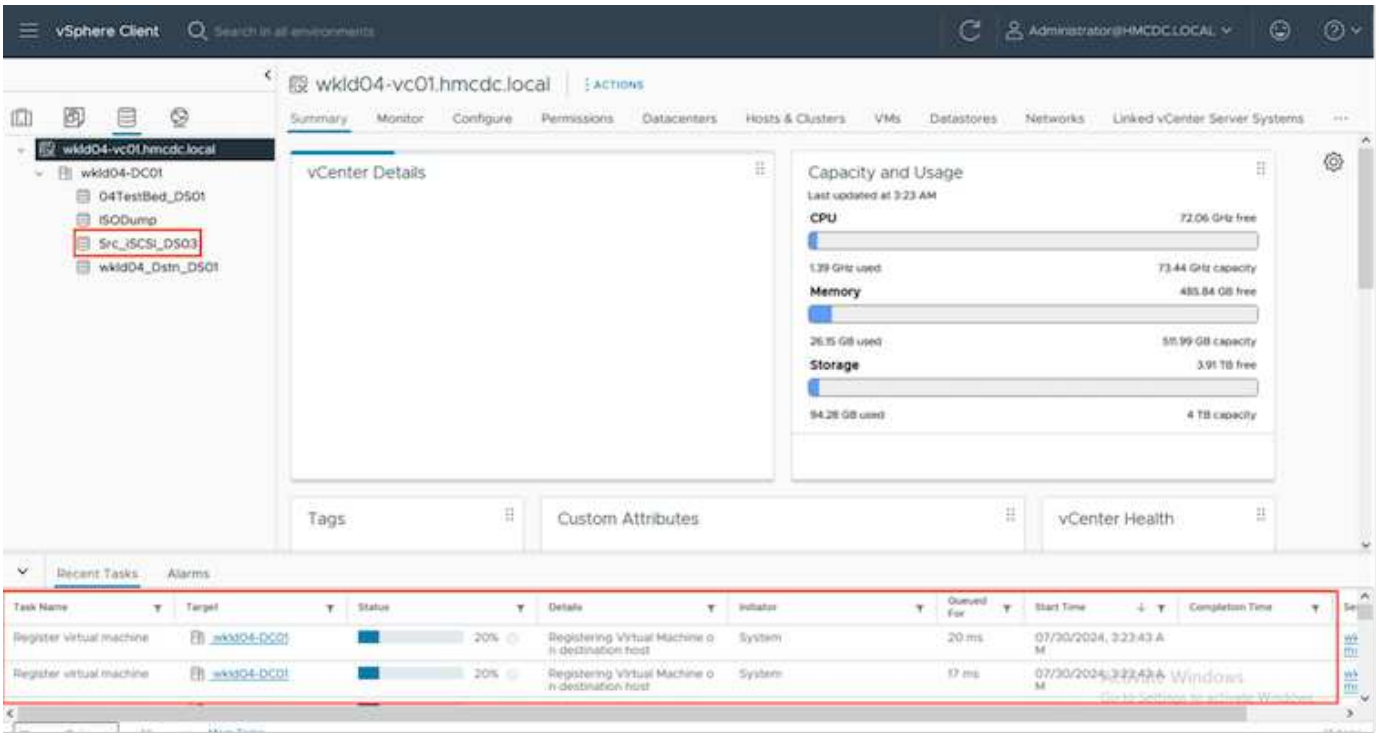
Una operación de conmutación por error de prueba crea un volumen clonado en el sistema de almacenamiento ONTAP de destino.

Ejecutar una operación de recuperación de prueba no afecta la replicación de SnapMirror .



Durante el proceso, Disaster Recovery no asigna el volumen de destino original. En su lugar, crea un nuevo volumen FlexClone a partir de la Snapshot seleccionada y asigna a los hosts ESXi un datastore temporal que respalda el volumen FlexClone.

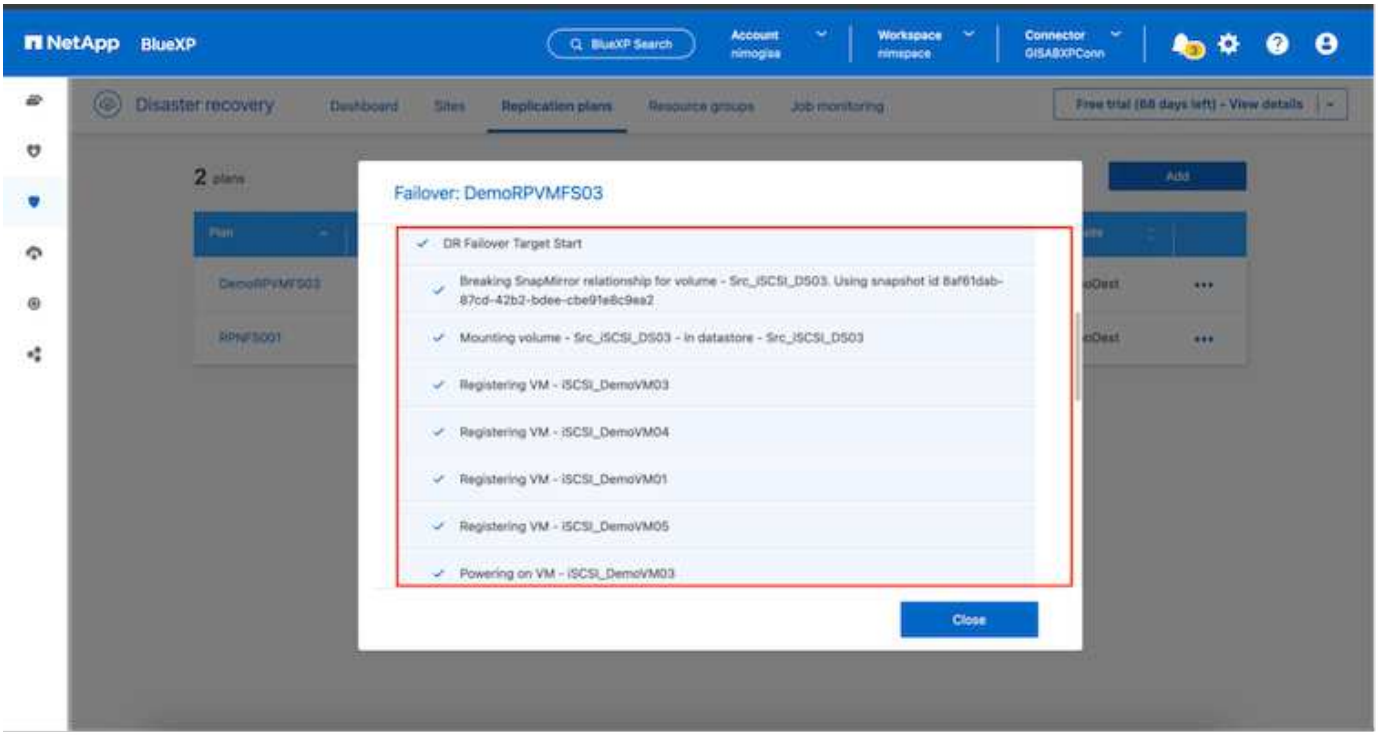




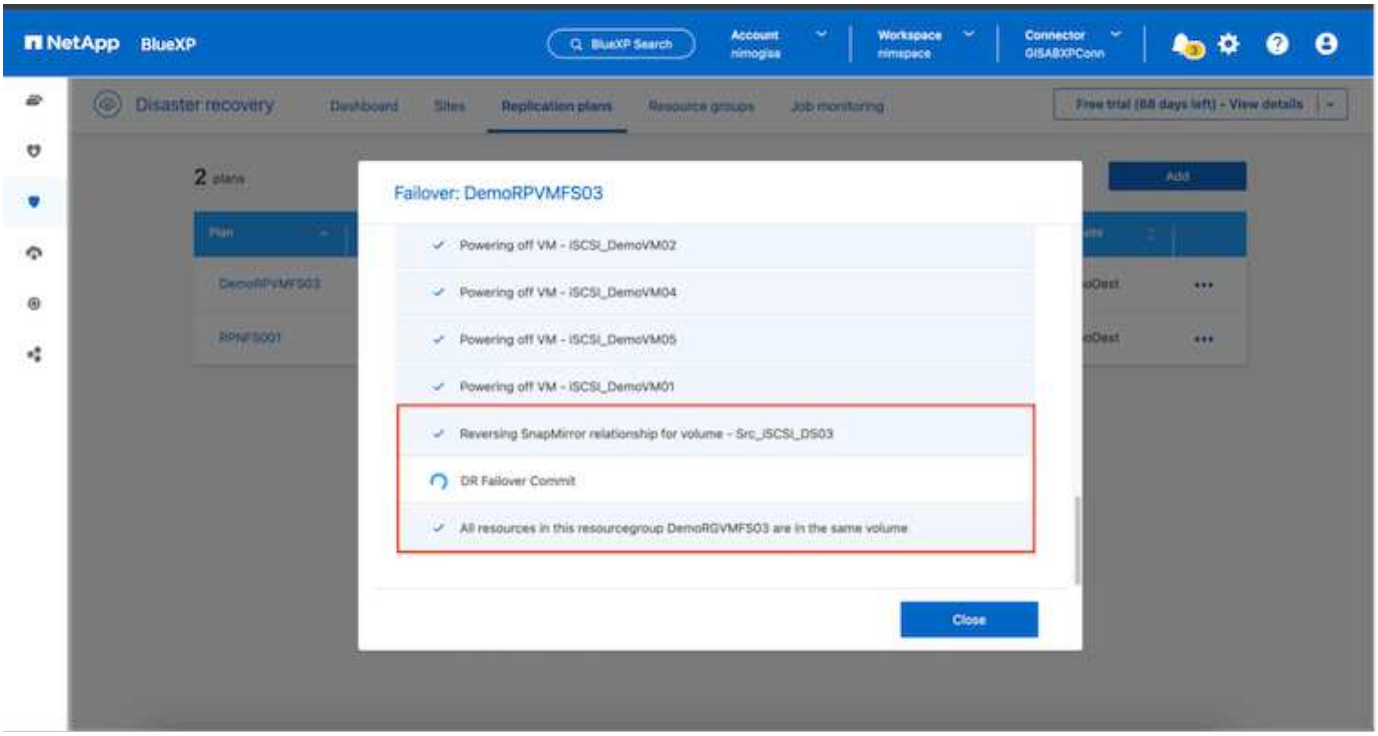
Cuando se complete la operación de conmutación por error de prueba, se puede activar la operación de limpieza mediante **"Clean Up failover test"**. Durante esta operación, Disaster Recovery destruye el volumen FlexClone que se utilizó en la operación.

En caso de que se produzca un desastre real, Disaster Recovery realiza los siguientes pasos:

1. Rompe la relación SnapMirror entre los sitios.
2. Monta el volumen del almacén de datos VMFS después de la renovación para su uso inmediato.
3. Registrar las máquinas virtuales
4. Encender las máquinas virtuales



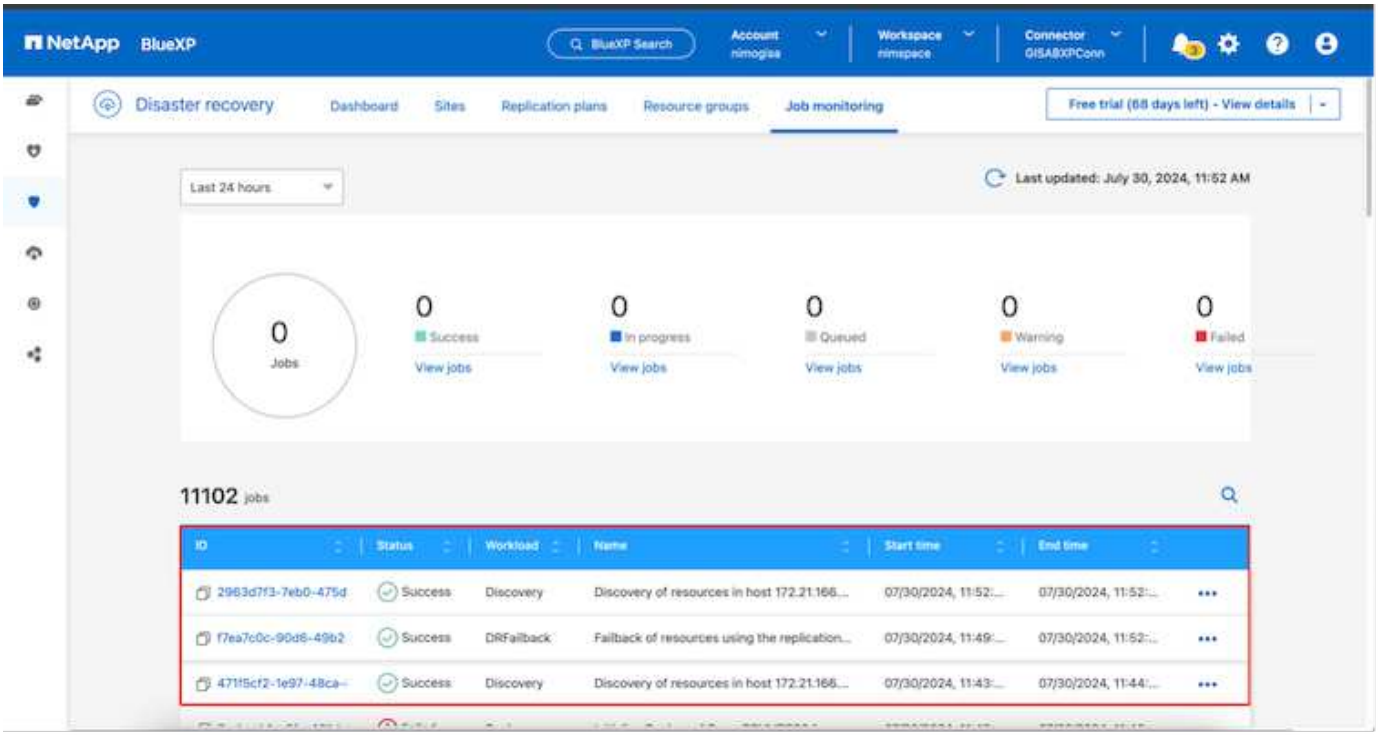
Una vez que el sitio principal esté en funcionamiento, Disaster Recovery permite la resincronización inversa para SnapMirror y habilita la conmutación de retorno, que de nuevo se puede realizar con solo hacer clic en un botón.



Y si se elige la opción de migrar, se considera como un evento de conmutación por error planificado. En este caso, se activa un paso adicional que consiste en apagar las máquinas virtuales en el sitio de origen. El resto de los pasos siguen siendo los mismos que en el evento de conmutación por error.

Desde NetApp Console o la CLI de ONTAP, puedes supervisar el estado de salud de la replicación de los volúmenes del datastore correspondientes, y el estado de una conmutación por error o una conmutación por

error de prueba se puede seguir a través de Job Monitoring.



Esto proporciona una solución poderosa para gestionar un plan de recuperación ante desastres personalizado y adaptado. La conmutación por error se puede realizar de forma planificada o con solo hacer clic en un botón cuando ocurre un desastre y se toma la decisión de activar el sitio de recuperación ante desastres.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado o utilizar el"simulador de soluciones" .

Multicloud híbrido de NetApp con cargas de trabajo de contenedores Red Hat OpenShift

Empezar

Soluciones multicloud híbridas de NetApp para cargas de trabajo de contenedores Red Hat OpenShift

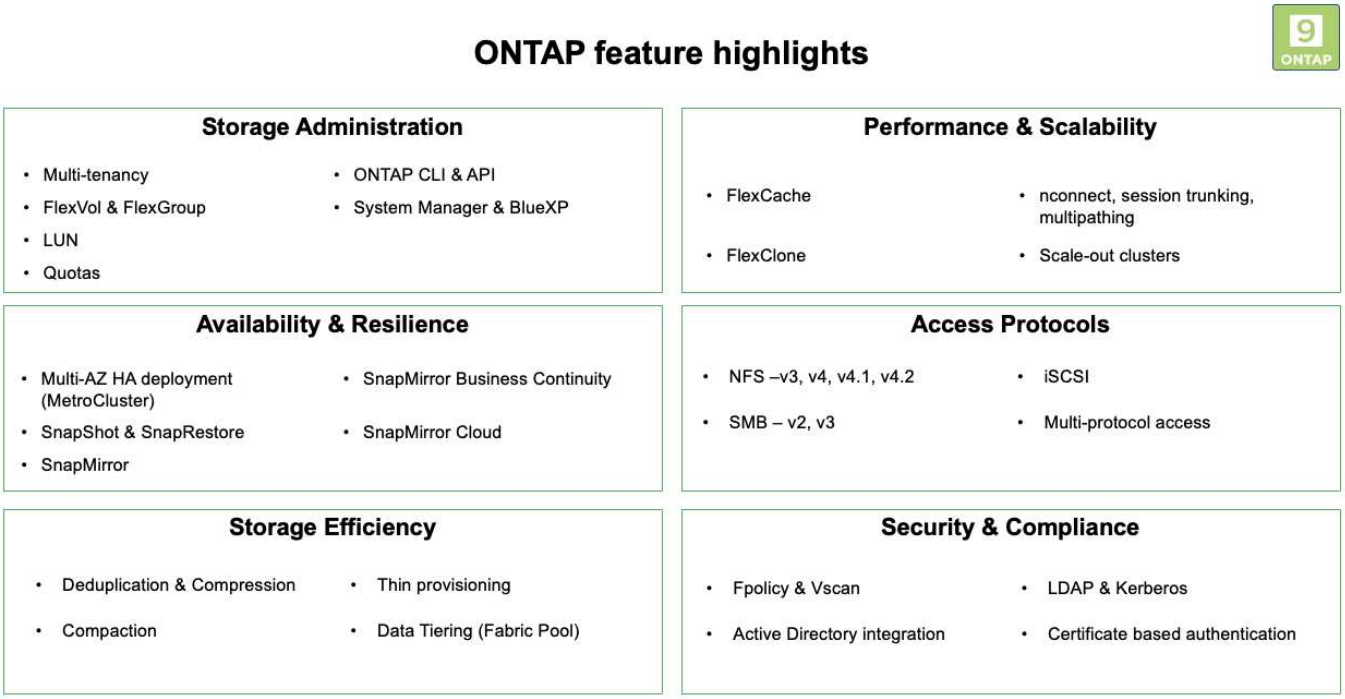
NetApp está observando un aumento significativo en el número de clientes que modernizan sus aplicaciones empresariales heredadas y crean nuevas aplicaciones utilizando contenedores y plataformas de orquestación creadas alrededor de Kubernetes. Red Hat OpenShift Container Platform es un ejemplo que vemos adoptado por muchos de nuestros clientes.

Descripción general

A medida que más y más clientes comienzan a adoptar contenedores dentro de sus empresas, NetApp está perfectamente posicionado para ayudar a satisfacer las necesidades de almacenamiento persistente de sus aplicaciones con estado y las necesidades clásicas de administración de datos, como protección de datos, seguridad de datos y migración de datos. Sin embargo, estas necesidades se satisfacen utilizando diferentes estrategias, herramientas y métodos.

Las opciones de almacenamiento basadas en **NetApp ONTAP** que se enumeran a continuación brindan seguridad, protección de datos, confiabilidad y flexibilidad para contenedores e implementaciones de Kubernetes.

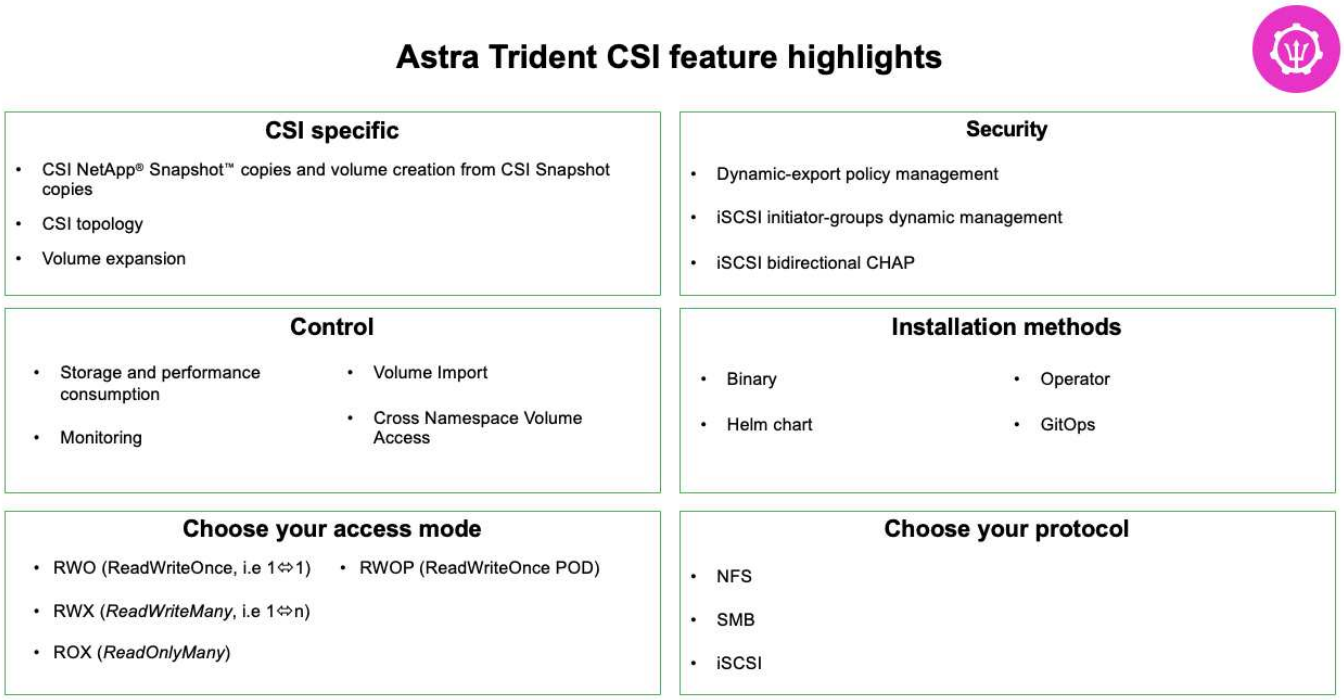
- Almacenamiento autogestionado en instalaciones locales:
  - Almacenamiento conectado a red (FAS) de NetApp , matrices All Flash FAS de NetApp (AFF), matrices All SAN de NetApp (ASA) y ONTAP Select
- Almacenamiento administrado por el proveedor en las instalaciones locales:
  - NetApp Keystone ofrece almacenamiento como servicio (STaaS)
- Almacenamiento autogestionado en la nube:
  - NetApp Cloud Volumes ONTAP(CVO) proporciona almacenamiento autogestionado en los hiperescaladores
- Almacenamiento administrado por el proveedor en la nube:
  - Amazon FSx for NetApp ONTAP, Azure NetApp Files y Google Cloud NetApp Volumes proporcionan almacenamiento basado en archivos en la nube.



NetApp Console te permite gestionar todos tus activos de almacenamiento y datos desde un único plano de control o interfaz.

Puedes usar NetApp Console para crear y administrar almacenamiento en la nube (por ejemplo, Cloud Volumes ONTAP y Azure NetApp Files), para mover, proteger y analizar datos, y para controlar muchos dispositivos de almacenamiento locales y perimetrales.

- NetApp Trident** es un orquestador de almacenamiento compatible con CSI que permite un consumo rápido y sencillo de almacenamiento persistente respaldado por una variedad de las opciones de almacenamiento de NetApp mencionadas anteriormente. Es un software de código abierto mantenido y soportado por NetApp.



Las cargas de trabajo de contenedores críticas para el negocio necesitan más que solo volúmenes persistentes. Sus requisitos de gestión de datos también requieren protección y migración de los objetos de la aplicación Kubernetes.

> Los datos de la aplicación incluyen objetos de Kubernetes además de los datos del usuario: algunos ejemplos son los siguientes: - objetos de Kubernetes como especificaciones de pods, PVC, implementaciones, servicios - objetos de configuración personalizados como mapas de configuración y secretos - datos persistentes como copias de instantáneas, copias de seguridad, clones - recursos personalizados como CR y CRD

NetApp Trident Protect, disponible como complemento gratuito de NetApp Trident, ofrece capacidades avanzadas de gestión de datos de aplicaciones que mejoran la funcionalidad y la disponibilidad de las aplicaciones Kubernetes con estado respaldadas por sistemas de almacenamiento NetApp ONTAP. Trident Protect simplifica la gestión, protección y movimiento de cargas de trabajo en contenedores tanto en nubes públicas como en entornos locales. También ofrece sólidas capacidades de automatización a través de su API y CLI.

Esta documentación de referencia proporciona validación de la protección de datos de aplicaciones basadas en contenedores, implementadas en la plataforma RedHat OpenShift utilizando Trident Protect. Además, la solución proporciona detalles de alto nivel para la implementación y el uso de Red Hat Advanced Cluster Management (ACM) para administrar las plataformas de contenedores. El documento también destaca los detalles para la integración del almacenamiento de NetApp con las plataformas de contenedores Red Hat OpenShift utilizando el aprovisionador Trident CSI.

Propuestas de valor de las soluciones multicloud híbridas de NetApp para cargas de trabajo de contenedores Red Hat OpenShift

La mayoría de los clientes no comienzan a construir entornos basados en Kubernetes sin ninguna infraestructura existente. Quizás sean una tienda de TI tradicional que ejecuta la mayoría de sus aplicaciones empresariales en máquinas virtuales (en grandes entornos

VMware, por ejemplo). Luego comienzan a construir pequeños entornos basados en contenedores para satisfacer las necesidades de sus equipos de desarrollo de aplicaciones modernas. Estas iniciativas suelen comenzar siendo pequeñas y comienzan a volverse más generalizadas a medida que los equipos aprenden estas nuevas tecnologías y habilidades, y empiezan a reconocer los numerosos beneficios de adoptarlas. La buena noticia para los clientes es que NetApp puede satisfacer las necesidades de ambos entornos. Este conjunto de soluciones para multicloud híbrido con Red Hat OpenShift permitirá a los clientes de NetApp adoptar tecnologías y servicios de nube modernos sin tener que revisar toda su infraestructura y organización. Ya sea que las aplicaciones y los datos del cliente estén alojados localmente, en la nube, se ejecuten en máquinas virtuales o en contenedores, NetApp puede brindar administración, protección, seguridad y portabilidad de datos consistentes. Con estas nuevas soluciones, el mismo valor que NetApp ha entregado en entornos de centros de datos locales durante décadas estará disponible en todo el horizonte de datos de la empresa, sin necesidad de realizar inversiones significativas para reequiparse, adquirir nuevas habilidades o formar nuevos equipos. NetApp está bien posicionado para ayudar a los clientes a resolver estos desafíos comerciales independientemente de la fase en la que se encuentren en su recorrido hacia la nube.

Nube híbrida multicloud de NetApp con Red Hat Openshift:

- Ofrece a los clientes diseños y prácticas validados que demuestran las mejores formas para que los clientes administren, protejan, aseguren y migren sus datos y aplicaciones cuando utilizan Red Hat OpenShift con soluciones de almacenamiento basadas en NetApp .
- Presentar las mejores prácticas para clientes que ejecutan Red Hat OpenShift con almacenamiento NetApp en entornos VMware, infraestructura de hardware o una combinación de ambos.
- Demostrar estrategias y opciones tanto para entornos locales como para entornos en la nube, así como para entornos híbridos donde se utilizan ambos.

Soluciones compatibles de NetApp Hybrid Multicloud para cargas de trabajo de contenedores Red Hat OpenShift

La solución prueba y valida la migración y la protección de datos centralizada con OpenShift Container Platform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp Console y NetApp Trident Protect.

Para esta solución, NetApp prueba y valida los siguientes escenarios. La solución se divide en múltiples escenarios en función de las siguientes características:

- en las instalaciones
- nube
  - clústeres OpenShift autogestionados y almacenamiento NetApp autogestionado
  - Clústeres OpenShift administrados por el proveedor y almacenamiento NetApp administrado por el proveedor

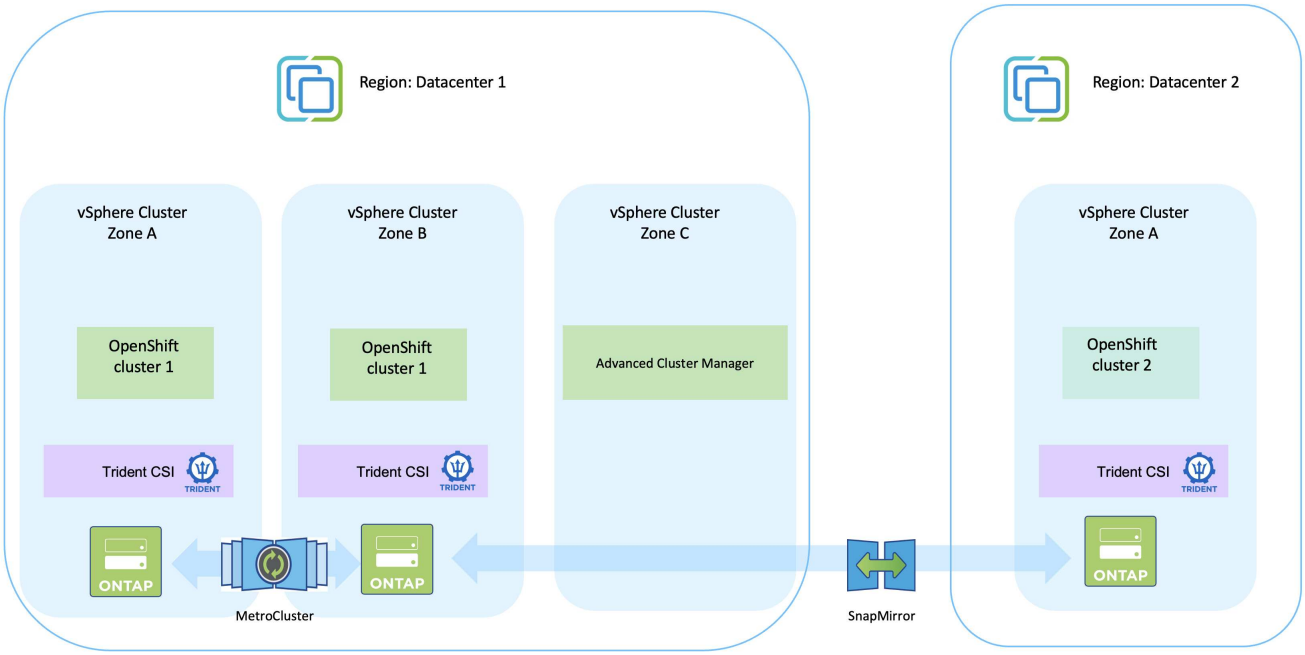
Desarrollaremos soluciones y casos de uso adicionales en el futuro.

Escenario 1: Protección y migración de datos dentro del entorno local mediante Trident Protect

En las instalaciones: clústeres OpenShift autogestionados y almacenamiento NetApp autogestionado

- Usa Trident Protect para proteger las aplicaciones y admitir la migración entre los clústeres locales.

Escenario 1

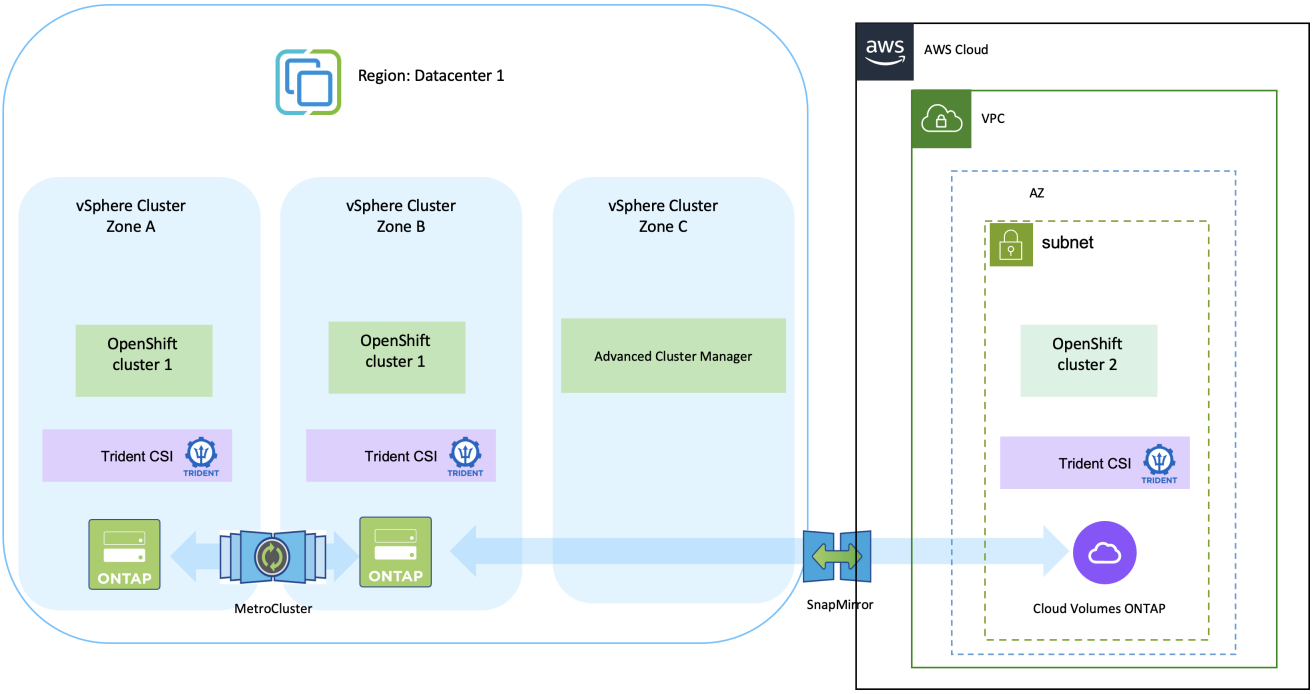


Escenario 2: Protección de datos y migración del entorno local al entorno de AWS mediante Trident Protect

En las instalaciones: clúster OpenShift autogestionado y almacenamiento autogestionado Nube de AWS: clúster OpenShift autogestionado y almacenamiento autogestionado

- Usa Trident Protect para proteger aplicaciones y ayudar con la migración entre los clústeres locales y los clústeres autogestionados de OpenShift en AWS.

Escenario 2

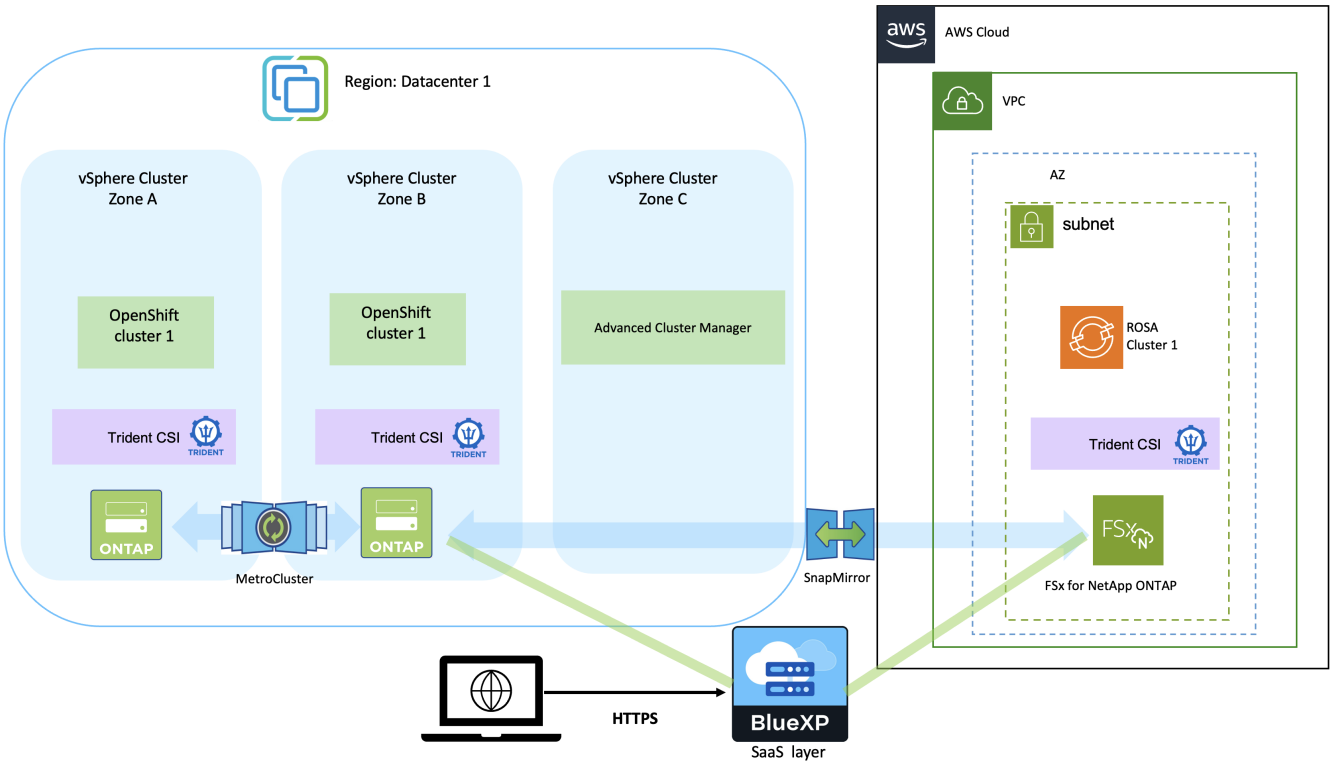


Escenario 3: Protección de datos y migración del entorno local al entorno de AWS

En las instalaciones: clúster OpenShift autoadministrado y almacenamiento autoadministrado AWS Cloud: clúster OpenShift administrado por el proveedor (ROSA) y almacenamiento administrado por el proveedor (FSx ONTAP)

- Con NetApp Console, realiza la replicación de volúmenes persistentes (FSx ONTAP).
- Usando OpenShift GitOps, recrea los metadatos de la aplicación.

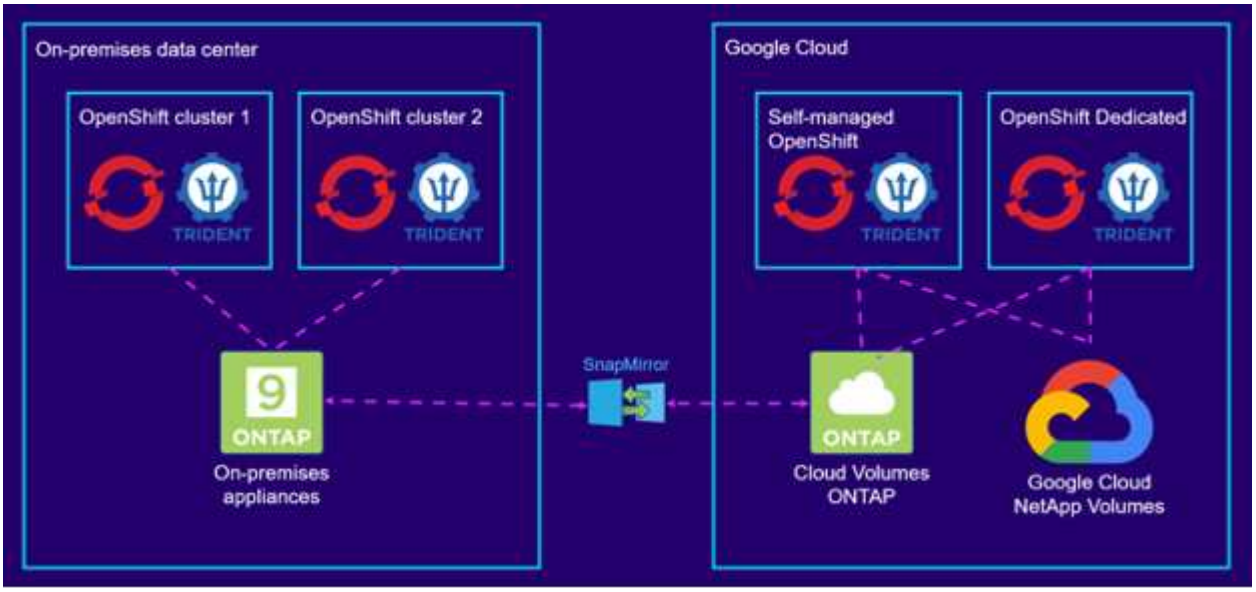
Escenario 3



Escenario 4: Protección de datos y migración del entorno local al entorno de GCP mediante Trident Protect

En las instalaciones: clúster OpenShift autogestionado y almacenamiento autogestionado Google Cloud: clúster OpenShift autogestionado y almacenamiento autogestionado

- Utiliza Trident Protect para proteger aplicaciones y admitir la migración entre los clústeres locales y Google Cloud OpenShift.

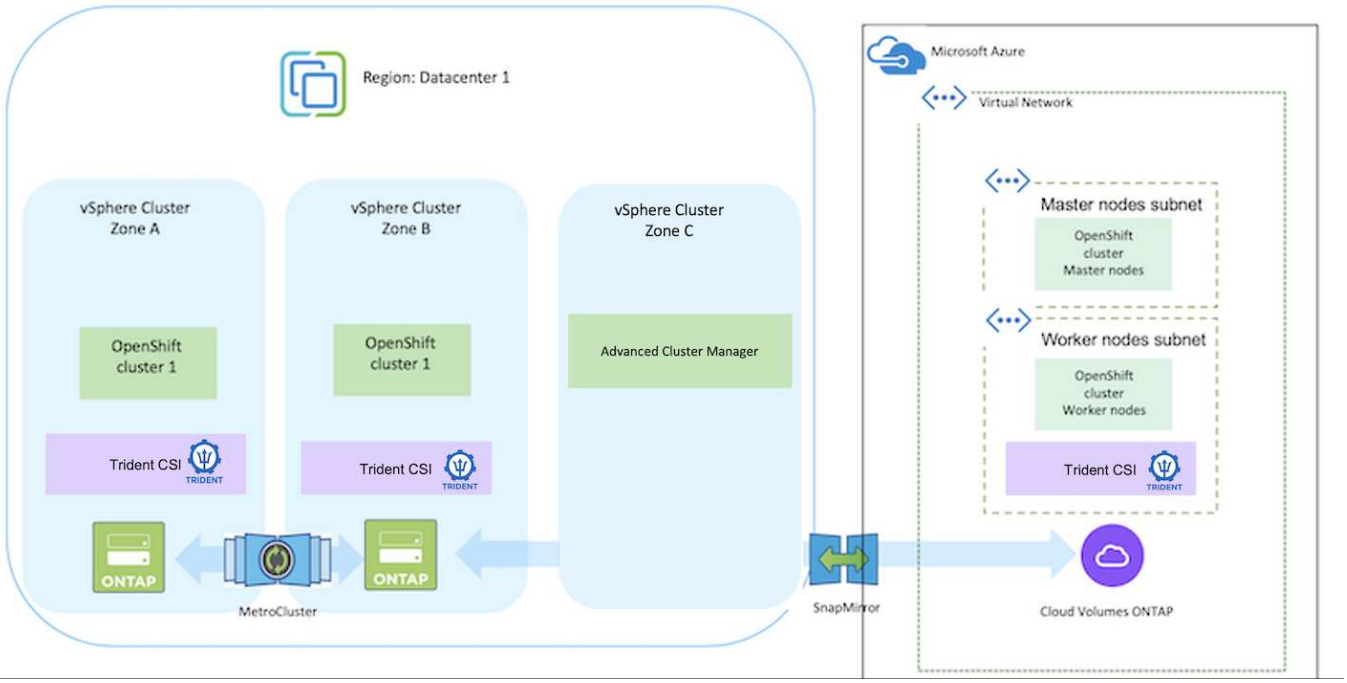


Para conocer las consideraciones al usar ONTAP en una configuración de MetroCluster , consulte"aquí" .

Escenario 5: Protección de datos y migración del entorno local al entorno de Azure mediante Trident Protect

En las instalaciones: clúster OpenShift autogestionado y almacenamiento autogestionado Azure Cloud: clúster OpenShift autogestionado y almacenamiento autogestionado

- Usa Trident Protect para proteger aplicaciones y apoyar la migración entre los clústeres locales y OpenShift en Azure.



Para conocer las consideraciones al usar ONTAP en una configuración de MetroCluster , consulte"aquí" .

Versiones de varios componentes utilizados en la validación de la solución

La solución prueba y valida la migración y la protección de datos centralizada con la plataforma de contenedores OpenShift, OpenShift Advanced Cluster Manager, NetApp ONTAP y NetApp Trident Protect.

Los escenarios 1, 2 y 3 de la solución se validaron utilizando las versiones que se muestran en la siguiente tabla:

Componente	Versión
VMware	Versión de cliente vSphere 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Clúster de concentradores	OpenShift 4.11.34
Clústeres de origen y destino	OpenShift 4.12.9 local y en AWS
* NetApp Trident*	Servidor y cliente Trident 23.04.0
* Protección Trident de NetApp *	Trident Protect 22.11.0-82

* NetApp ONTAP*	ONTAP 9.12.1
AWS FSx ONTAP	AZ único

El escenario 4 de la solución se validó utilizando las versiones que se muestran en la siguiente tabla:

Componente	Versión
VMware	Versión 8.0.2.00000 de vSphere Client VMware ESXi, 8.0.2, 22380479
Clúster de concentradores	OpenShift 4.13.13
Clústeres de origen y destino	OpenShift 4.13.12 local y en Google Cloud
* NetApp Trident*	Servidor y cliente Trident 23.07.0
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	AZ única, nodo único, 9.14.0

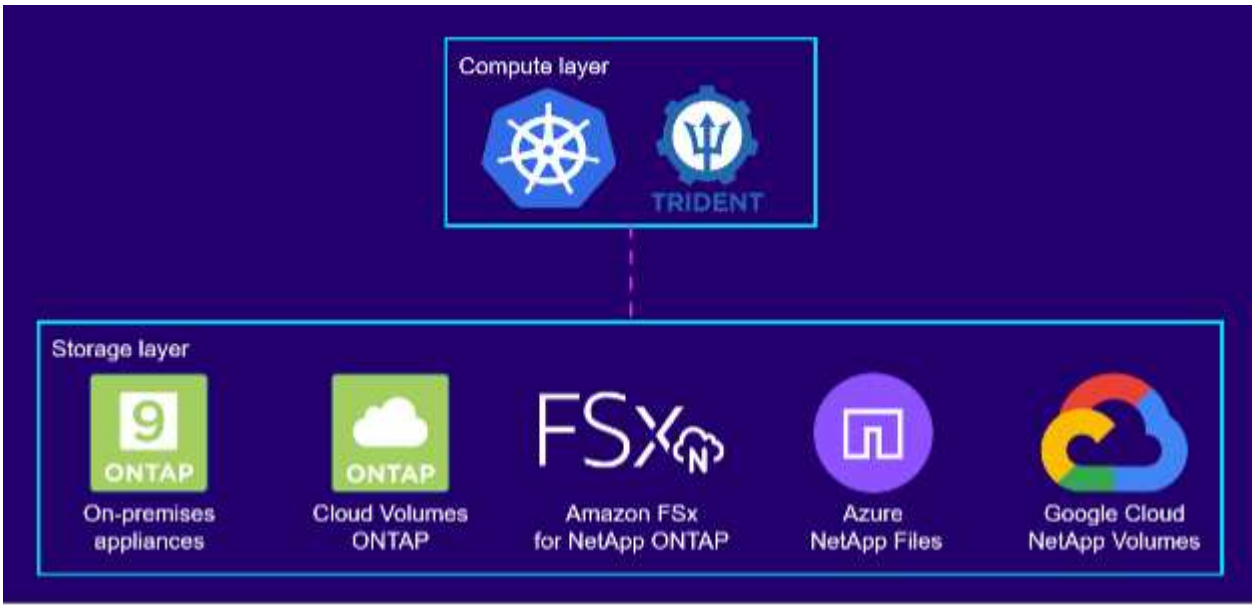
El escenario 5 de la solución se validó utilizando las versiones que se muestran en la siguiente tabla:

Componente	Versión
VMware	Versión 8.0.2.00000 de vSphere Client VMware ESXi, 8.0.2, 22380479
Clústeres de origen y destino	OpenShift 4.13.25 local y en Azure
* NetApp Trident*	Trident Server y Client 23.10.0
* Protección Trident de NetApp *	Trident Protect 23.10
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	AZ única, nodo único, 9.14.0

Integraciones de almacenamiento de NetApp compatibles con Red Hat OpenShift Containers

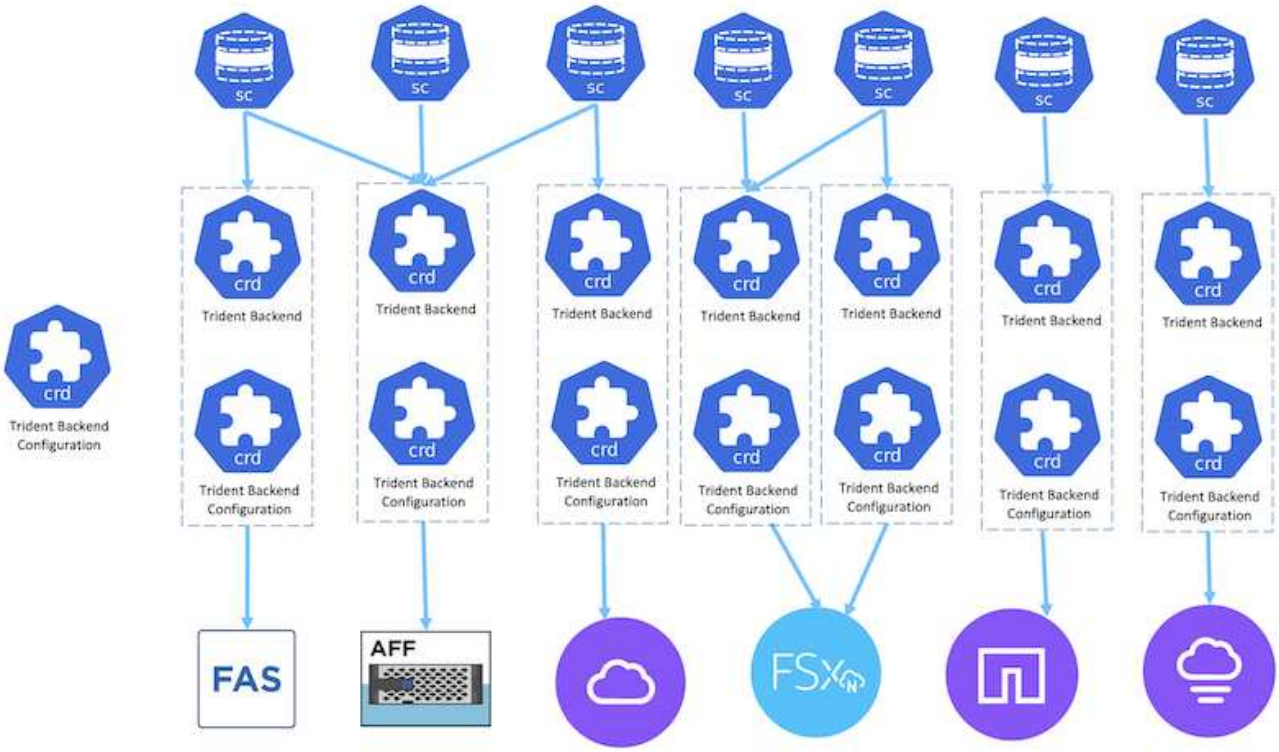
Independientemente de si los contenedores Red Hat OpenShift se ejecutan en VMware o en hiperescaladores, NetApp Trident se puede utilizar como aprovisionador de CSI para los distintos tipos de almacenamiento backend de NetApp que admite.

El siguiente diagrama muestra los distintos almacenamientos backend de NetApp que se pueden integrar con clústeres OpenShift mediante NetApp Trident.



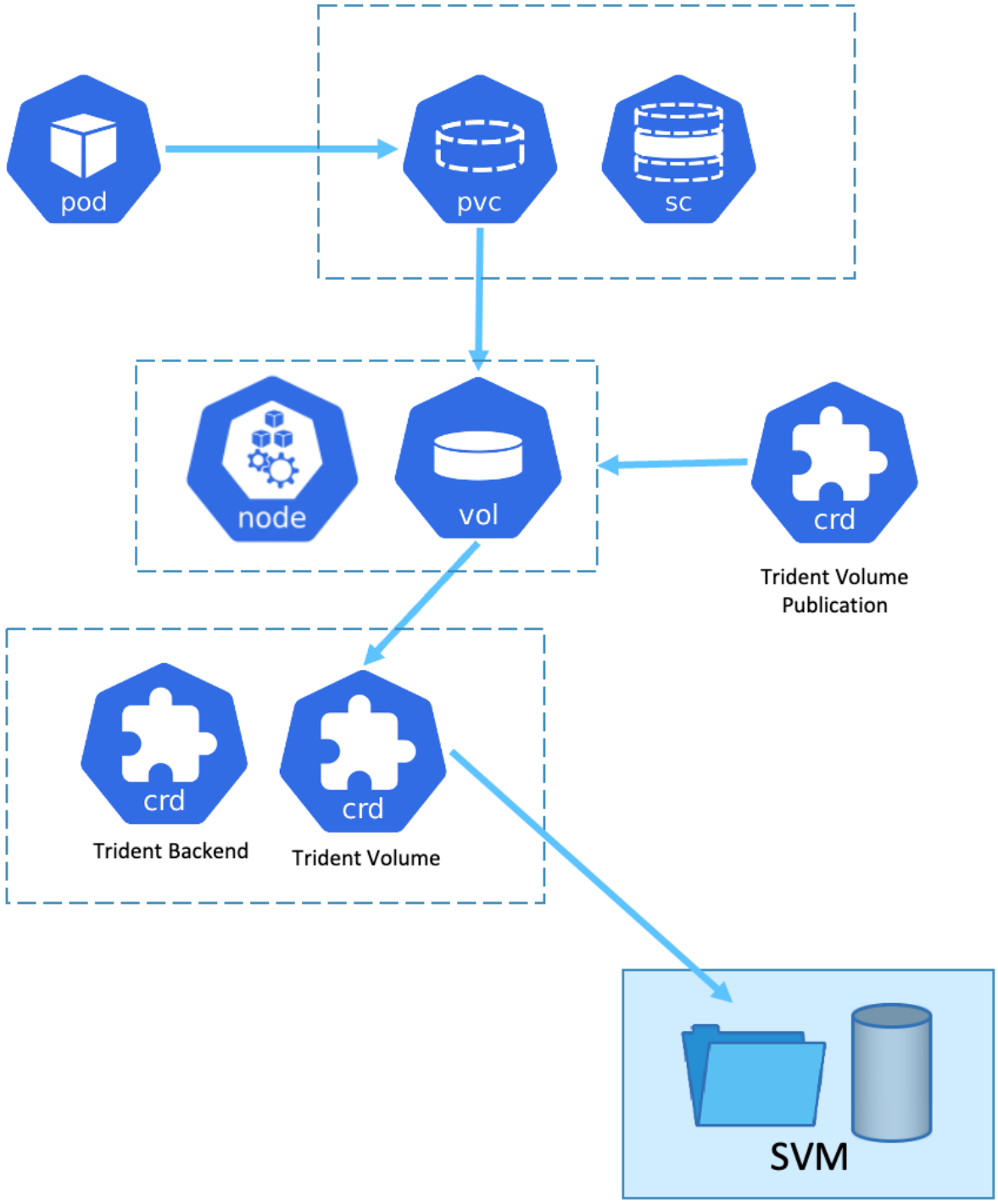
La máquina virtual de almacenamiento (SVM) de ONTAP proporciona multitenencia segura. Un solo clúster OpenShift puede conectarse a una sola SVM o a varias SVM o incluso a varios clústeres ONTAP . La clase de almacenamiento filtra el almacenamiento de backend según parámetros o etiquetas. Los administradores de almacenamiento definen los parámetros para conectarse al sistema de almacenamiento mediante la configuración del backend de Trident. Una vez establecida la conexión, se crea el backend trident y se completa la información que la clase de almacenamiento puede filtrar.

La relación entre la clase de almacenamiento y el backend se muestra a continuación.



El propietario de la aplicación solicita un volumen persistente mediante la clase de almacenamiento. La clase de almacenamiento filtra el almacenamiento del backend.

La relación entre el pod y el almacenamiento backend se muestra a continuación.



Opciones de interfaz de almacenamiento de contenedores (CSI)

En entornos vSphere, los clientes pueden elegir el controlador VMware CSI y/o Trident CSI para integrar con ONTAP. Con VMware CSI, los volúmenes persistentes se consumen como discos SCSI locales, mientras que con Trident, se consumen con la red.

Como VMware CSI no admite los modos de acceso RWX con ONTAP, las aplicaciones deben usar Trident CSI si se requiere el modo RWX. En las implementaciones basadas en FC, se prefiere VMware CSI y SnapMirror

Business Continuity (SMBC) proporciona alta disponibilidad a nivel de zona.

VMware CSI es compatible

- Almacenes de datos basados en bloques centrales (FC, FCoE, iSCSI, NVMeoF)
- Almacenes de datos basados en archivos principales (NFS v3, v4)
- Almacenes de datos vVol (bloques y archivos)

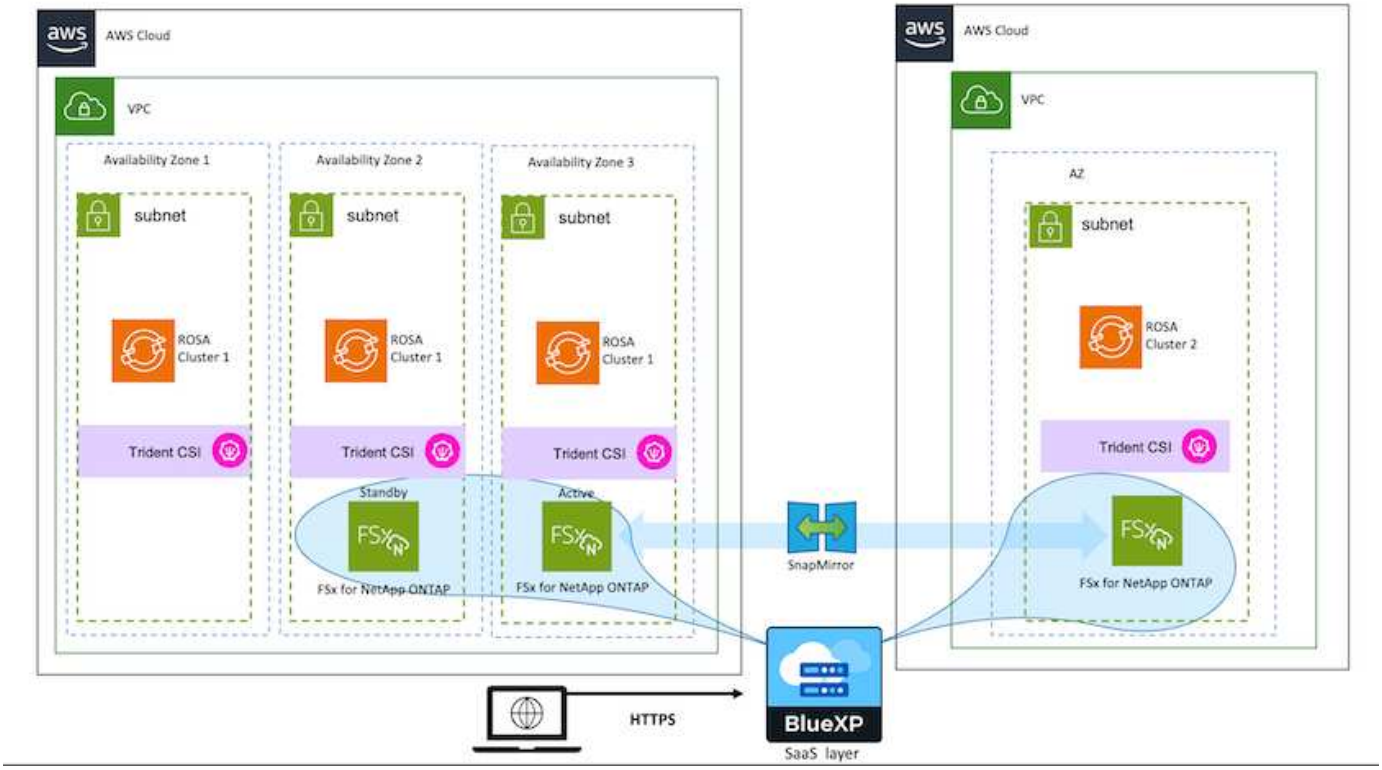
Trident cuenta con los siguientes controladores para apoyar a ONTAP

- ontap-san (volumen dedicado)
- ontap-san-economy (volumen compartido)
- ontap-nas (volumen dedicado)
- ontap-nas-economy (volumen compartido)
- ontap-nas-flexgroup (volumen dedicado a gran escala)

Tanto para VMware CSI como para Trident CSI, ONTAP admite nconnect, troncalización de sesión, kerberos, etc. para NFS y rutas múltiples, autenticación chap, etc. para protocolos de bloque.

En AWS, Amazon FSx for NetApp ONTAP (FSx ONTAP) se puede implementar en una sola zona de disponibilidad (AZ) o en varias AZ. Para cargas de trabajo de producción que requieren alta disponibilidad, multi-AZ brinda tolerancia a fallas a nivel zonal y tiene mejor caché de lectura NVMe en comparación con una sola AZ. Para más información, consulte"Pautas de rendimiento de AWS" .

Para ahorrar costos en el sitio de recuperación ante desastres, se puede utilizar un solo AZ FSx ONTAP
.



Para conocer la cantidad de SVM compatibles con FSx ONTAP, consulte"Administración de la máquina virtual de almacenamiento FSx ONTAP"

Documentación adicional

A continuación se muestra documentación adicional como referencia:

1. "VMware vSphere"
2. "Documentación del producto de la plataforma OpenShift Container"
3. "Instalación de clústeres de la plataforma de contenedores OpenShift"
4. "Documentación del producto de gestión avanzada de clústeres"
5. "Creación de un clúster mediante ACM"
6. "Implementación de Red Hat Quay en OpenShift"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda" - Verda (de código abierto) cuenta con una colección de hooks de ejecución de referencia para aplicaciones populares nativas de la nube que hacen un uso intensivo de datos
10. "NetApp servicios de datos"
11. "Red Hat OpenShift Service on AWS con arquitectura clásica"
12. "Amazon FSx ONTAP"
13. "Instalación de clústeres OpenShift en GCP"
14. "Instalación de clústeres de OpenShift en Azure"

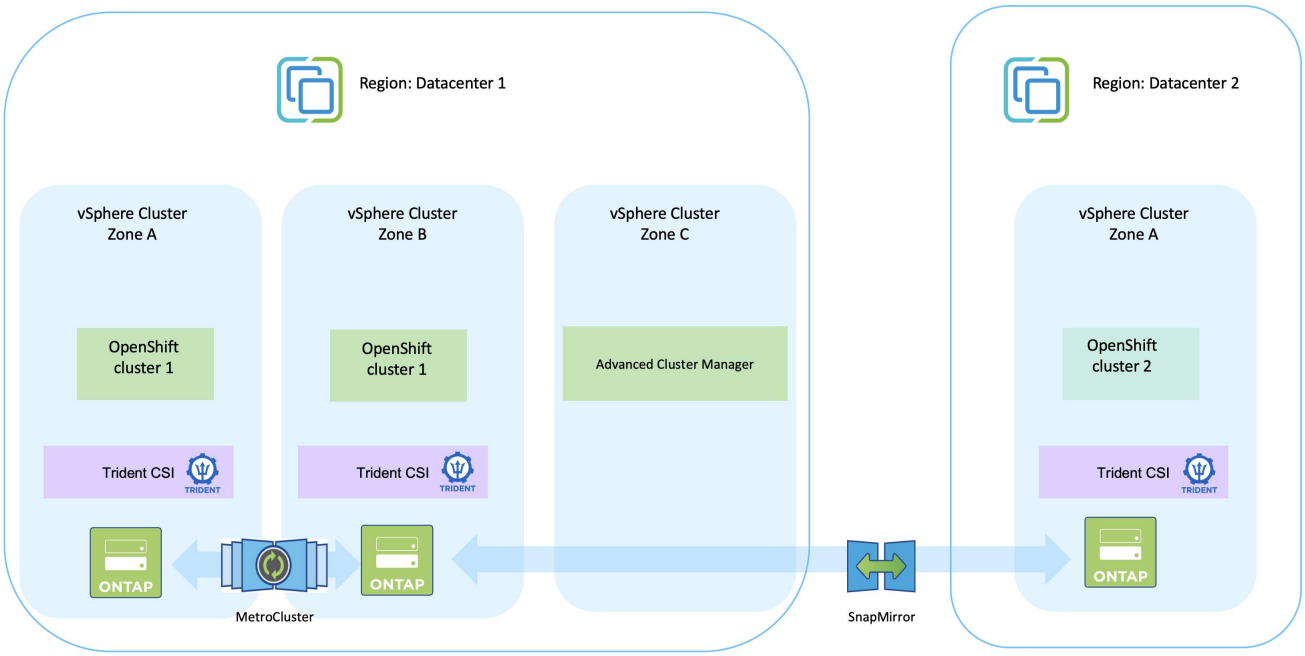
Openshift para instalaciones locales

Solución NetApp con cargas de trabajo de la plataforma Red Hat OpenShift Container en VMware

Si los clientes necesitan ejecutar sus modernas aplicaciones en contenedores en la infraestructura de sus centros de datos privados, pueden hacerlo. Deben planificar e implementar la plataforma de contenedores Red Hat OpenShift (OCP) para lograr un entorno exitoso y listo para producción para implementar sus cargas de trabajo de contenedores. Sus clústeres OCP se pueden implementar en VMware o en hardware real.

El almacenamiento NetApp ONTAP ofrece protección de datos, confiabilidad y flexibilidad para implementaciones de contenedores. Trident actúa como proveedor de almacenamiento dinámico para consumir almacenamiento ONTAP persistente para las aplicaciones con estado de los clientes. NetApp Trident Protect se puede utilizar para los numerosos requisitos de gestión de datos de aplicaciones con estado, como protección de datos, migración y continuidad empresarial.

Con VMware vSphere, las herramientas de NetApp ONTAP proporcionan un complemento vCenter que se puede utilizar para aprovisionar almacenes de datos. Aplique etiquetas y úselas con OpenShift para almacenar la configuración y los datos del nodo. El almacenamiento basado en NVMe proporciona menor latencia y alto rendimiento.

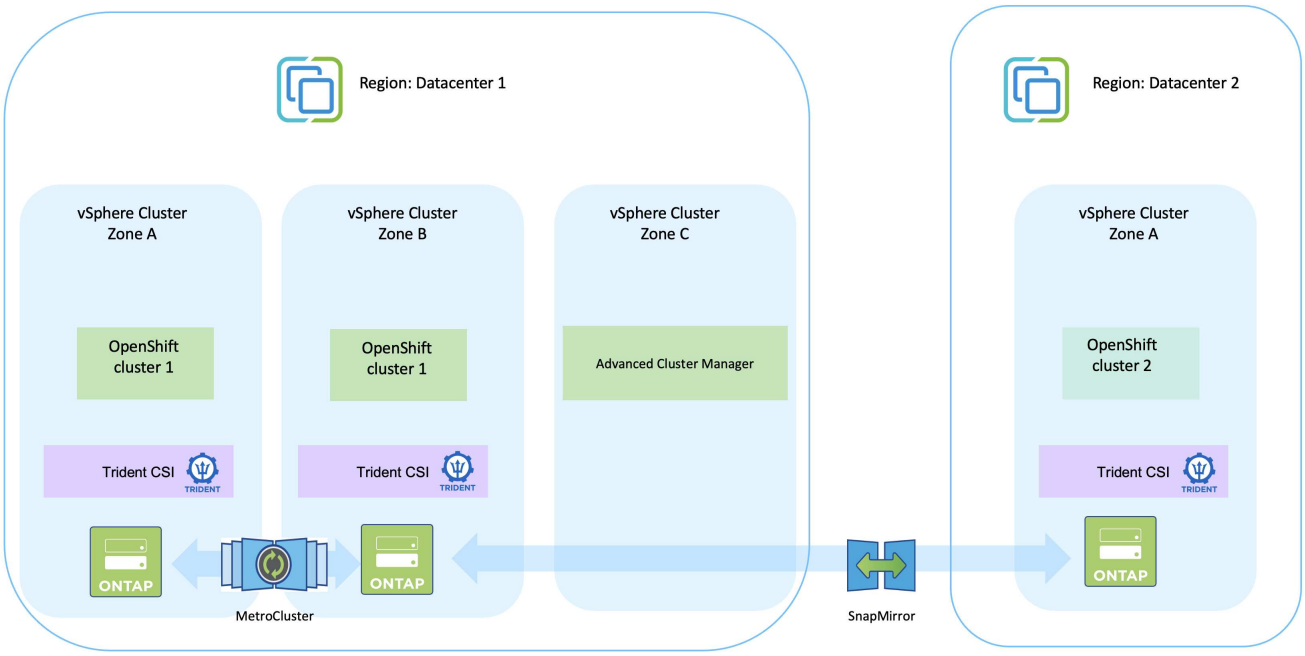


Implementar y configurar la plataforma Red Hat OpenShift Container en VMware

Esta sección describe un flujo de trabajo de alto nivel sobre cómo configurar y administrar clústeres de OpenShift y administrar aplicaciones con estado en ellos. Se muestra el uso de matrices de almacenamiento NetApp ONTAP con la ayuda de Trident para proporcionar volúmenes persistentes.

> Hay varias formas de implementar clústeres de la plataforma Red Hat OpenShift Container. Esta descripción de alto nivel de la configuración proporciona enlaces a la documentación para el método específico que se utilizó. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en el"sección de recursos" .

Aquí se muestra un diagrama que representa los clústeres implementados en VMware en un centro de datos.



El proceso de configuración se puede dividir en los siguientes pasos:

▼ **Implementar y configurar una máquina virtual CentOS**

- Se implementa en el entorno VMware vSphere.
- Esta máquina virtual se utiliza para implementar algunos componentes como NetApp Trident y NetApp Trident Protect para la solución.
- Se configura un usuario root en esta máquina virtual durante la instalación.

▼ **Implementar y configurar un clúster de OpenShift Container Platform en VMware vSphere (Hub Cluster)**

Consulta las instrucciones del método "Despliegue asistido" para implementar un clúster OCP.

Recuerde lo siguiente: - Crear una clave pública y privada ssh para proporcionarla al instalador. Estas claves se utilizarán para iniciar sesión en los nodos maestro y de trabajo si es necesario. - Descargue el programa instalador desde el instalador asistido. Este programa se utiliza para iniciar las máquinas virtuales que crea en el entorno VMware vSphere para los nodos maestro y de trabajo. - Las máquinas virtuales deben tener los requisitos mínimos de CPU, memoria y disco duro. (Consulte los comandos de creación de vm en"este" página para los nodos maestro y de trabajo que proporcionan esta información) - El diskUUID debe estar habilitado en todas las máquinas virtuales. - Cree un mínimo de 3 nodos para el maestro y 3 nodos para el trabajador. - Una vez que el instalador los descubra, active el botón de alternancia de integración de VMware vSphere.

▼ **Instalar la gestión avanzada de clústeres en el clúster del concentrador**

Esto se instala utilizando el Operador de administración de clúster avanzado en el clúster central. Consulte las instrucciones"aquí" .

▼ **Instalar dos clústeres OCP adicionales (origen y destino)**

- Los clústeres adicionales se pueden implementar mediante el ACM en el clúster central.
- Consulta las instrucciones "aquí".

▼ **Configurar el almacenamiento de NetApp ONTAP**

- Instalar un clúster ONTAP con conectividad a las máquinas virtuales OCP en el entorno VMWare.
- Crear un SVM.
- Configurar el almacenamiento de datos NAS para acceder al almacenamiento en SVM.

▼ **Instalar NetApp Trident en los clústeres OCP**

- Instalar NetApp Trident en los tres clústeres: concentrador, de origen y de destino
- Consulta las instrucciones "aquí".
- Cree un backend de almacenamiento para ontap-nas.
- Cree una clase de almacenamiento para ontap-nas.
- Consulte las instrucciones"aquí" .

▼ **Implementar una aplicación en el clúster de origen**

Utilice OpenShift GitOps para implementar una aplicación. (por ejemplo, Postgres, Ghost)

El siguiente paso es utilizar Trident Protect para la protección de datos y la migración de datos desde el clúster de origen al de destino. Referirse"aquí" para obtener instrucciones.

Protección de datos mediante Trident Protect

Esta página muestra las opciones de protección de datos para aplicaciones basadas en Red Hat OpenShift Container que se ejecutan en VMware vSphere usando Trident Protect.

A medida que los usuarios emprenden su viaje de modernización de aplicaciones con Red Hat OpenShift, debe haber una estrategia de protección de datos para protegerlos de un borrado accidental o cualquier otro error humano. A menudo también se requiere una estrategia de protección por motivos regulatorios o de cumplimiento para proteger sus datos de un desastre.

Los requisitos de protección de datos varían desde volver a una copia de un punto en el tiempo hasta conmutar automáticamente a un dominio de falla diferente sin ninguna intervención humana. Muchos clientes eligen ONTAP como su plataforma de almacenamiento preferida para sus aplicaciones Kubernetes debido a sus ricas características como multitenencia, multiprotocolo, alto rendimiento y ofertas de capacidad, replicación y almacenamiento en caché para ubicaciones de múltiples sitios, seguridad y flexibilidad.

Para obtener más información sobre cómo proteger y migrar cargas de trabajo de contenedores usando Trident Protect, revisa la siguiente sección: - "Protege y migra aplicaciones en contenedores usando Trident Protect"

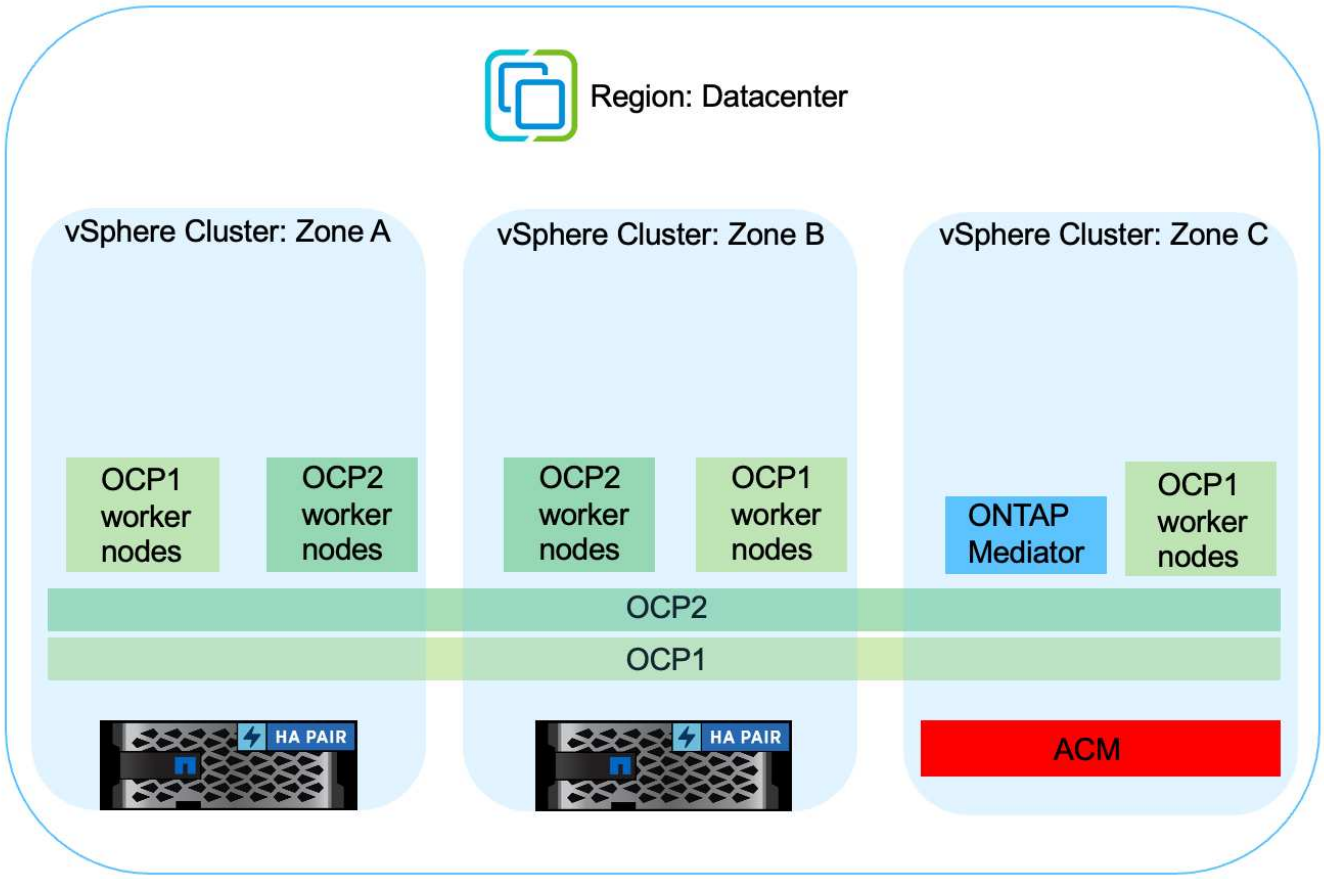
Continuidad de negocio con MetroCluster

La mayor parte de nuestra plataforma de hardware para ONTAP tiene características de alta disponibilidad para proteger contra fallas del dispositivo, evitando la necesidad de realizar recuperación ante desastres. Pero para protegerse de incendios o cualquier otro desastre y continuar el negocio con cero RPO y bajo RTO, a menudo se utiliza una solución MetroCluster .

Los clientes que actualmente cuentan con un sistema ONTAP pueden ampliarlo a MetroCluster agregando sistemas ONTAP compatibles dentro de las limitaciones de distancia para brindar recuperación ante desastres a nivel de zona. Trident, la CSI (interfaz de almacenamiento de contenedores) admite NetApp ONTAP, incluida la configuración de MetroCluster , así como otras opciones como Cloud Volumes ONTAP, Azure NetApp Files,

AWS FSx ONTAP, etc. Trident ofrece cinco opciones de controlador de almacenamiento para ONTAP y todas son compatibles con la configuración de MetroCluster . Referirse"aquí" para obtener detalles adicionales sobre los controladores de almacenamiento ONTAP compatibles con Trident.

La solución MetroCluster requiere una extensión de red de capa 2 o la capacidad de acceder a la misma dirección de red desde ambos dominios de falla. Una vez que la configuración de MetroCluster está en su lugar, la solución es transparente para los propietarios de las aplicaciones, ya que todos los volúmenes en el svm de MetroCluster están protegidos y obtienen los beneficios de SyncMirror (RPO cero).



Para la configuración de backend de Trident (TBC), no especifique dataLIF ni SVM cuando utilice la configuración de MetroCluster . Especifique la IP de administración de SVM para managementLIF y use las credenciales del rol vsadmin.

Detalles sobre las funciones de protección de datos de Trident Protect están disponibles "aquí".

Nube híbrida con componentes autogestionados

Solución NetApp con cargas de trabajo de la plataforma Red Hat OpenShift Container en la nube híbrida

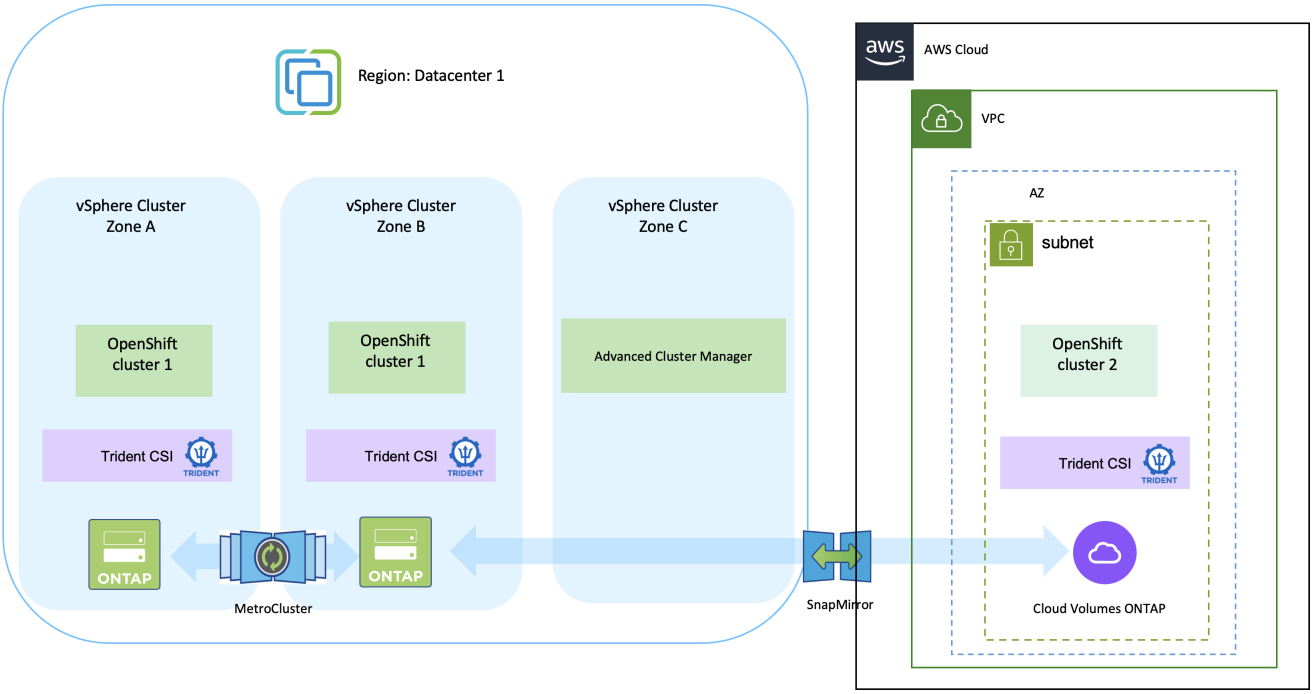
Los clientes pueden estar en un punto de su proceso de modernización en el que estén listos para trasladar algunas cargas de trabajo seleccionadas o todas las cargas de trabajo de sus centros de datos a la nube. Pueden optar por utilizar contenedores OpenShift autogestionados y almacenamiento NetApp autogestionado en la nube por

diversos motivos. Deben planificar e implementar la plataforma de contenedores Red Hat OpenShift (OCP) en la nube para lograr un entorno exitoso y listo para producción para migrar sus cargas de trabajo de contenedores desde sus centros de datos. Sus clústeres OCP se pueden implementar en VMware o Bare Metal en sus centros de datos y en AWS, Azure o Google Cloud en el entorno de la nube.

NetApp Cloud Volumes ONTAP ofrece protección de datos, fiabilidad y flexibilidad para implementaciones de contenedores en AWS, Azure y Google Cloud. Trident funciona como el aprovisionador de almacenamiento dinámico para consumir el almacenamiento persistente Cloud Volumes ONTAP para las aplicaciones con estado de los clientes. Trident Protect se puede usar para los requisitos de gestión de datos de aplicaciones con estado, como protección de datos, migración y continuidad del negocio.

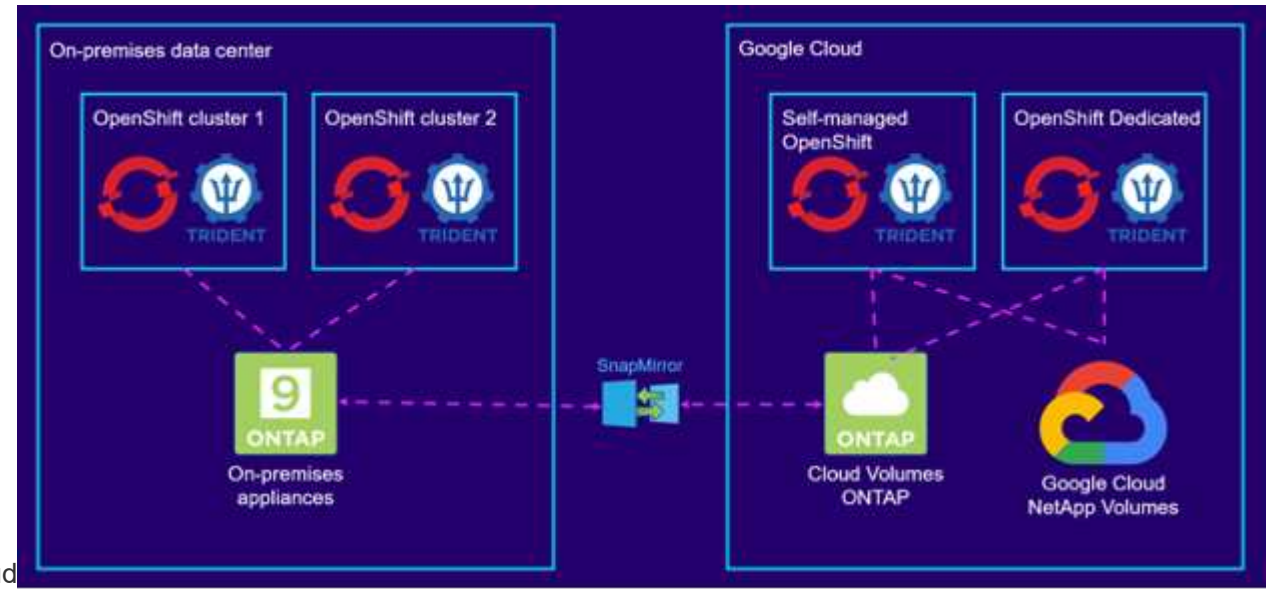
Solución de protección y migración de datos para cargas de trabajo de contenedores OpenShift en una nube híbrida utilizando Trident Protect

Local y
AWS

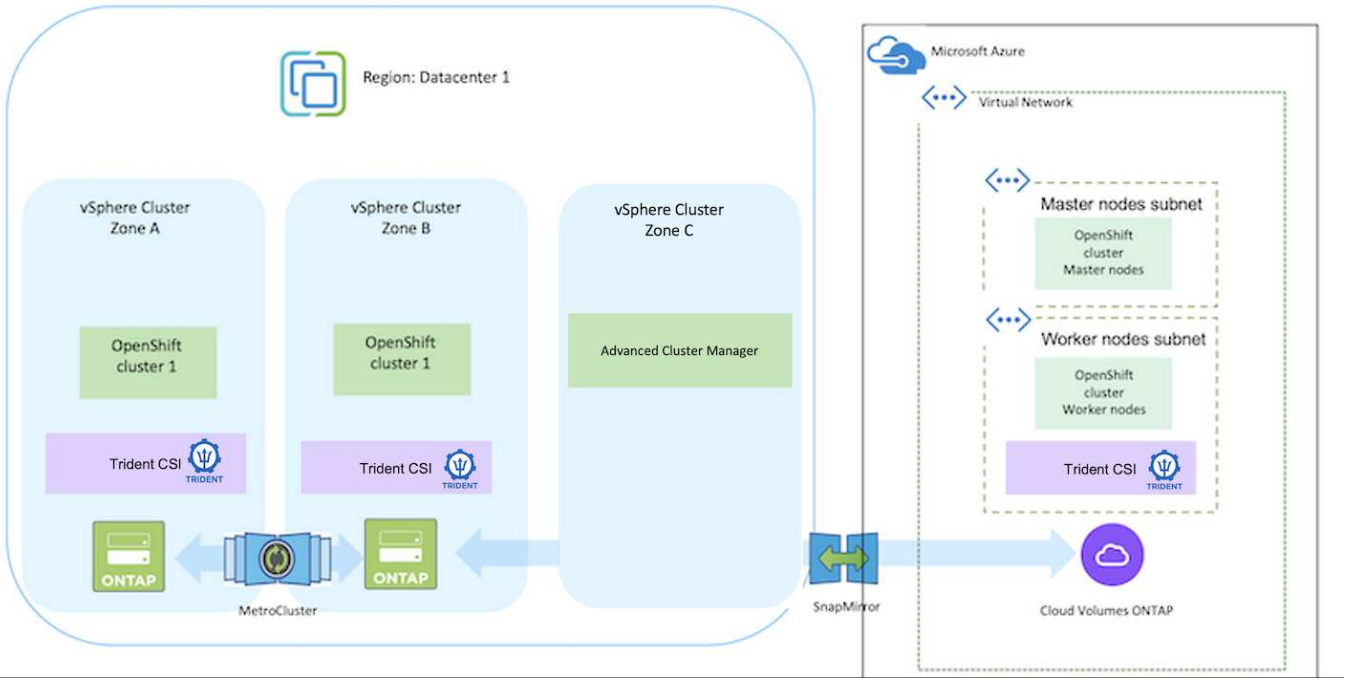


Local y Google

Cloud



Local y en la nube de Azure



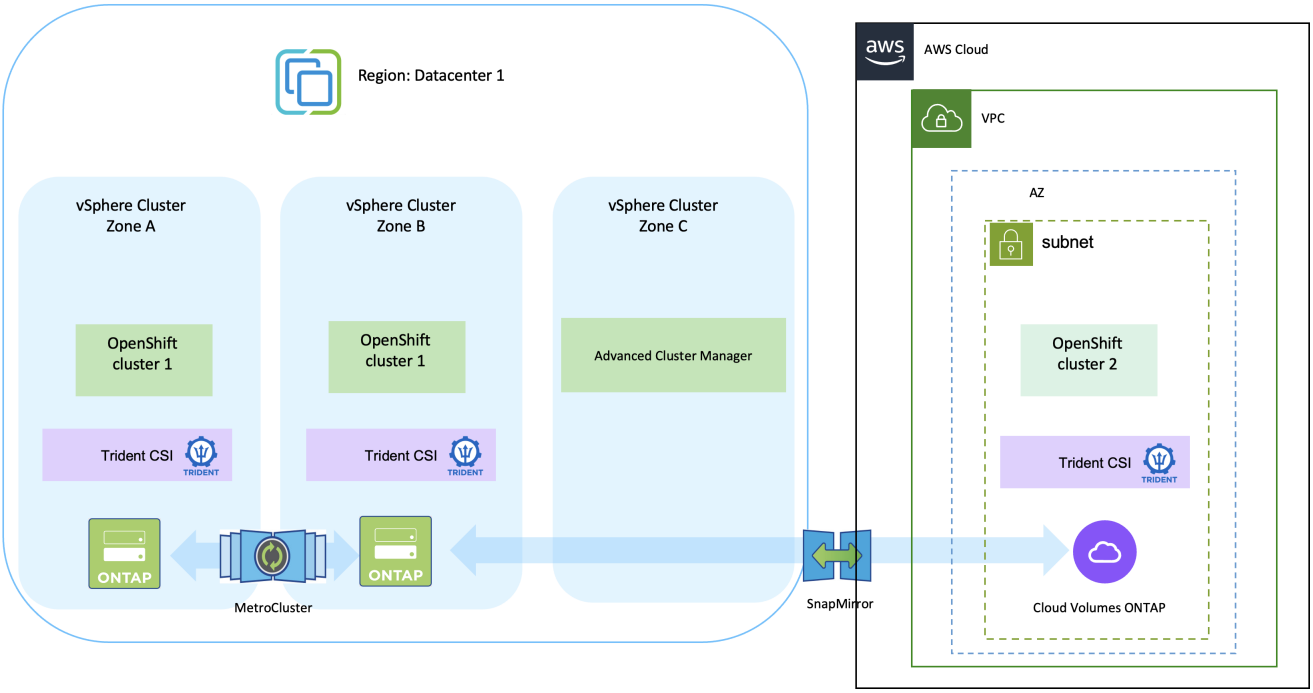
Implementar y configurar la plataforma Red Hat OpenShift Container en AWS

Esta sección describe un flujo de trabajo de alto nivel sobre cómo configurar y administrar clústeres OpenShift en AWS e implementar aplicaciones con estado en ellos. Se muestra el uso del almacenamiento NetApp Cloud Volumes ONTAP con la ayuda de Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Trident Protect para realizar actividades de migración y protección de datos para las aplicaciones con estado.

Hay varias formas de implementar clústeres de la plataforma Red Hat OpenShift Container en

AWS. Esta descripción de alto nivel de la configuración proporciona enlaces a la documentación para el método específico que se utilizó. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en el"sección de recursos" .

Aquí hay un diagrama que representa los clústeres implementados en AWS y conectados al centro de datos mediante una VPN.



El proceso de configuración se puede dividir en los siguientes pasos:

▼ **Instale un clúster OCP en AWS desde Administración avanzada de clústeres.**

- Cree una VPC con una conexión VPN de sitio a sitio (usando pfsense) para conectarse a la red local.
- La red local tiene conectividad a Internet.
- Cree 3 subredes privadas en 3 zonas de disponibilidad diferentes.
- Cree una zona alojada privada de Route 53 y un solucionador de DNS para la VPC.

Crea un clúster de OpenShift en AWS desde el asistente de Advanced Cluster Management (ACM). Consulta las instrucciones "aquí".

También puedes crear el clúster en AWS desde la consola de nube híbrida de OpenShift. Consulta "aquí" para obtener instrucciones.

Al crear el clúster utilizando ACM, tiene la posibilidad de personalizar la instalación editando el archivo yaml después de completar los detalles en la vista de formulario. Una vez creado el clúster, puede iniciar sesión mediante SSH en los nodos del clúster para solucionar problemas o realizar una configuración manual adicional. Utilice la clave ssh que proporcionó durante la instalación y el nombre de usuario core para iniciar sesión.

▼ **Implementa Cloud Volumes ONTAP en AWS con la consola de NetApp.**

- Instale el conector en el entorno VMware local. Consulte las instrucciones"aquí" .
- Implemente una instancia de CVO en AWS utilizando el conector. Consulte las instrucciones"aquí" .

> El conector también se puede instalar en el entorno de la nube. Referirse"aquí" Para obtener información adicional.

▼ **Instalar Trident en el clúster OCP**

- Implementa Trident Operator con Helm. Consulta las instrucciones "aquí"
- Crea un backend y una clase de almacenamiento. Consulte las instrucciones"aquí" .

Uso de la función de topología CSI de Trident para arquitecturas multizona

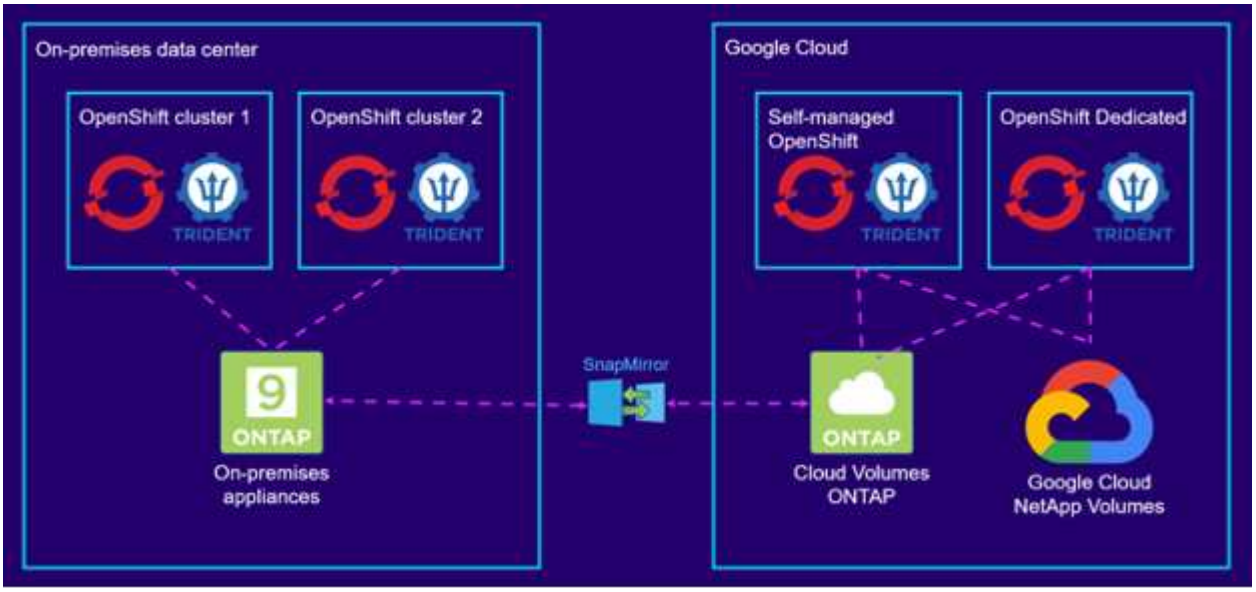
En la actualidad, los proveedores de nube permiten a los administradores de clústeres Kubernetes/OpenShift generar nodos de los clústeres que están basados en zonas. Los nodos pueden ubicarse en diferentes zonas de disponibilidad dentro de una región o en varias regiones. Para facilitar el aprovisionamiento de volúmenes para cargas de trabajo en una arquitectura multizona, Trident utiliza la topología CSI. Al utilizar la función de topología CSI, el acceso a los volúmenes se puede limitar a un subconjunto de nodos, según las regiones y las zonas de disponibilidad. Referirse"aquí" Para más detalles.

> Kubernetes admite dos modos de enlace de volumen: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Trident crea el volumen sin ningún conocimiento de topología. Los volúmenes persistentes se crean sin depender de los requisitos de programación del pod solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y el enlace de un volumen persistente para un PVC se retrasan hasta que se programa y crea un pod que usa el PVC. De esta manera, se crean volúmenes para cumplir con las restricciones de programación impuestas por los requisitos de topología. Los backends de almacenamiento Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (backend consciente de la topología). Para las StorageClasses que utilizan dicho backend, solo se creará un volumen si lo solicita una aplicación programada en una zona o región compatible. (Clase de almacenamiento que tiene en cuenta la topología) Consulte"aquí" Para más detalles.

Implementar y configurar Red Hat OpenShift Container Platform en Google Cloud

Esta sección describe un flujo de trabajo de alto nivel sobre cómo configurar y administrar clústeres OpenShift en GCP e implementar aplicaciones con estado en ellos. Se muestra el uso del almacenamiento Google Cloud NetApp Volumes y NetApp Cloud Volumes ONTAP con la ayuda de Trident para proporcionar volúmenes persistentes.

Aquí hay un diagrama que muestra los clústeres implementados en GCP y conectados al centro de datos mediante una VPN.



Hay varias formas de implementar clústeres de la plataforma Red Hat OpenShift Container en GCP. Esta descripción de alto nivel de la configuración proporciona enlaces a la documentación para el método específico que se utilizó. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en el"sección de recursos" .

El proceso de configuración se puede dividir en los siguientes pasos:

Instalar un clúster OCP en GCP desde la CLI

- Asegúrate de que cumples todos los requisitos previos indicados en "aquí".
- Para la conectividad VPN entre las instalaciones locales y GCP, se creó y configuró una máquina virtual pfsense. Para obtener instrucciones, consulte "aquí" .
  - La dirección de puerta de enlace remota en pfsense se puede configurar solo después de haber creado una puerta de enlace VPN en Google Cloud Platform.
  - Las direcciones IP de red remota para la Fase 2 se pueden configurar solo después de que el programa de instalación del clúster OpenShift se ejecute y cree los componentes de infraestructura para el clúster.
  - La VPN en Google Cloud solo se puede configurar después de que el programa de instalación haya creado los componentes de infraestructura para el clúster.
- Ahora instale el clúster OpenShift en GCP.
  - Descarga el programa de instalación y el pull secret y despliega el clúster siguiendo los pasos que se indican en la documentación "aquí".
  - La instalación crea una red VPC en Google Cloud Platform. También crea una zona privada en Cloud DNS y agrega registros A.
    - Utilice la dirección del bloque CIDR de la red VPC para configurar pfsense y establecer la conexión VPN. Asegúrese de que los firewalls estén configurados correctamente.
    - Agregue registros A en el DNS del entorno local utilizando la dirección IP en los registros A del DNS de Google Cloud.
  - La instalación del clúster se completa y proporcionará un archivo kubeconfig y un nombre de usuario y contraseña para iniciar sesión en la consola del clúster.

Implementar Google Cloud NetApp Volumes

- Los Google Cloud NetApp Volumes se pueden agregar a sus proyectos como se describe"aquí" .

Implementa Cloud Volumes ONTAP en GCP con NetApp Console

- Instala un agente de NetApp Console en Google Cloud. Consulta las instrucciones "aquí".
- Implementa una instancia de CVO en Google Cloud mediante el agente. Consulta las instrucciones "aquí".

Instalar Trident en el clúster OCP en GCP

- Hay muchos métodos para implementar Trident, tal y como se muestra "aquí".
- Para este proyecto, Trident se instaló implementando manualmente Trident Operator siguiendo las instrucciones "aquí".
- Crear un backend y clases de almacenamiento. Consulte las instrucciones"aquí" .

Uso de la función de topología CSI de Trident para arquitecturas multizona

En la actualidad, los proveedores de nube permiten a los administradores de clústeres Kubernetes/OpenShift generar nodos de los clústeres que están basados en zonas. Los nodos pueden ubicarse en diferentes zonas de disponibilidad dentro de una región o en varias regiones. Para facilitar el aprovisionamiento de volúmenes para cargas de trabajo en una arquitectura multizona, Trident utiliza la topología CSI. Al utilizar la función de topología CSI, el acceso a los volúmenes se puede limitar a un subconjunto de nodos, según las regiones y las zonas de disponibilidad. Referirse"aquí" Para más detalles.

> Kubernetes admite dos modos de enlace de volumen: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Trident crea el volumen sin ningún conocimiento de topología. Los volúmenes persistentes se crean sin depender de los requisitos de programación del pod solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y el enlace de un volumen persistente para un PVC se retrasan hasta que se programa y crea un pod que usa el PVC. De esta manera, se crean volúmenes para cumplir con las restricciones de programación impuestas por los requisitos de topología. Los backends de almacenamiento Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (backend consciente de la topología). Para las StorageClasses que utilizan dicho backend, solo se creará un volumen si lo solicita una aplicación programada en una zona o región compatible. (Clase de almacenamiento que tiene en cuenta la topología) Consulte"aquí" Para más detalles.

Video de demostración

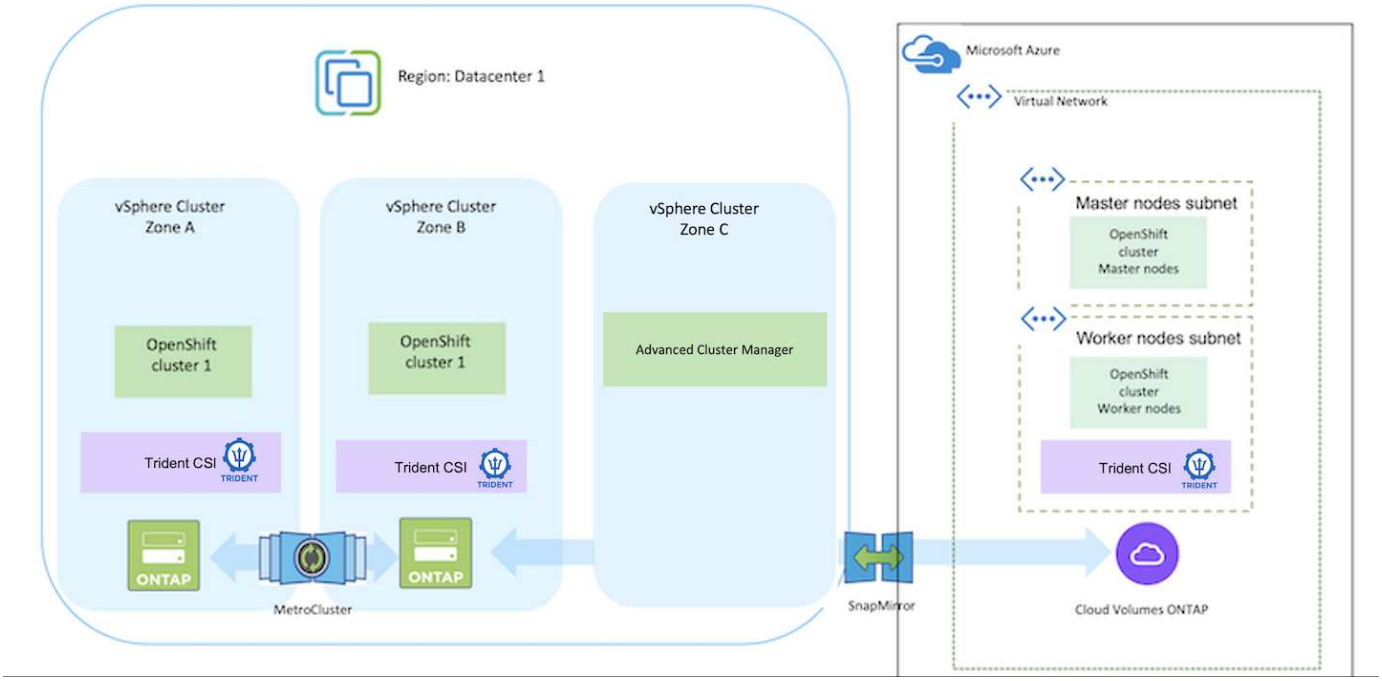
Instalación de OpenShift Cluster en Google Cloud Platform

Importación de clústeres de OpenShift a Trident Protect

Implementar y configurar la plataforma Red Hat OpenShift Container en Azure

Esta sección describe un flujo de trabajo de alto nivel sobre cómo configurar y administrar clústeres OpenShift en Azure e implementar aplicaciones con estado en ellos. Se muestra el uso del almacenamiento NetApp Cloud Volumes ONTAP con la ayuda de Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Trident Protect para realizar actividades de migración y protección de datos para las aplicaciones con estado.

Aquí hay un diagrama que muestra los clústeres implementados en Azure y conectados al centro de datos mediante una VPN.



Hay varias formas de implementar clústeres de la plataforma Red Hat OpenShift Container en Azure. Esta descripción de alto nivel de la configuración proporciona enlaces a la documentación para el método específico que se utilizó. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en el"sección de recursos" .

El proceso de configuración se puede dividir en los siguientes pasos:

▼ **Instalar un clúster OCP en Azure desde la CLI.**

- Asegúrate de que cumples todos los requisitos previos indicados en "aquí".
- Cree una VPN, subredes y grupos de seguridad de red y una zona DNS privada. Cree una puerta de enlace VPN y una conexión VPN de sitio a sitio.
- Para la conectividad VPN entre las instalaciones locales y Azure, se creó y configuró una máquina virtual pfsense. Para obtener instrucciones, consulte"aquí" .
- Descarga el programa de instalación y el pull secret e implementa el clúster siguiendo los pasos que se indican en la documentación "aquí".
- La instalación del clúster se completa y proporcionará un archivo kubeconfig y un nombre de usuario y contraseña para iniciar sesión en la consola del clúster.

A continuación se muestra un archivo install-config.yaml de muestra.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
```

```
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
```

```
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

▼ **Implementa Cloud Volumes ONTAP en Azure mediante la NetApp Console.**

- Instala un agente de NetApp Console en Azure. Consulta las instrucciones "aquí".
- Implementa una instancia de CVO en Azure mediante el agente. Consulta las instrucciones "aquí".

Uso de la función de topología CSI de Trident para arquitecturas multizona

En la actualidad, los proveedores de nube permiten a los administradores de clústeres Kubernetes/OpenShift generar nodos de los clústeres que están basados en zonas. Los nodos pueden ubicarse en diferentes zonas de disponibilidad dentro de una región o en varias regiones. Para facilitar el aprovisionamiento de volúmenes para cargas de trabajo en una arquitectura multizona, Trident utiliza la topología CSI. Al utilizar la función de topología CSI, el acceso a los volúmenes se puede limitar a un subconjunto de nodos, según las regiones y las zonas de disponibilidad. Referirse"aquí" Para más detalles.

> Kubernetes admite dos modos de enlace de volumen: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Trident crea el volumen sin ningún conocimiento de topología. Los volúmenes persistentes se crean sin depender de los requisitos de programación del pod solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y el enlace de un volumen persistente para un PVC se retrasan hasta que se programa y crea un pod que usa el PVC. De esta manera, se crean volúmenes para cumplir con las restricciones de programación impuestas por los requisitos de topología. Los backends de almacenamiento Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (backend consciente de la topología). Para las StorageClasses que utilizan dicho backend, solo se creará un volumen si lo solicita una aplicación programada en una zona o región compatible. (Clase de almacenamiento que tiene en cuenta la topología) Consulte"aquí" Para más detalles.

Protección de datos mediante Trident Protect

Para obtener más información sobre cómo proteger y migrar cargas de trabajo de contenedores usando Trident Protect, revisa la siguiente sección: - "Protege y migra aplicaciones en contenedores usando Trident Protect"

Nube híbrida con componentes administrados por el proveedor

Solución NetApp con cargas de trabajo de la plataforma de contenedores Red Hat OpenShift administradas

Los clientes pueden "nacer en la nube" o pueden estar en un punto de su proceso de

modernización en el que estén listos para trasladar algunas cargas de trabajo seleccionadas o todas las cargas de trabajo de sus centros de datos a la nube. Pueden optar por utilizar contenedores OpenShift administrados por el proveedor y almacenamiento NetApp administrado por el proveedor en la nube para ejecutar sus cargas de trabajo. Deben planificar e implementar los clústeres de contenedores Red Hat OpenShift administrados en la nube para lograr un entorno exitoso y listo para producción para sus cargas de trabajo de contenedores. NetApp ofrece ofertas de almacenamiento totalmente administradas para soluciones Red Hat administradas en las tres nubes públicas líderes.

- Amazon FSx for NetApp ONTAP (FSx ONTAP)*

FSx ONTAP ofrece protección de datos, confiabilidad y flexibilidad para implementaciones de contenedores en AWS. Trident actúa como aprovisionador de almacenamiento dinámico para consumir el almacenamiento persistente de FSx ONTAP para las aplicaciones con estado de los clientes.

Como ROSA se puede implementar en modo HA con nodos del plano de control distribuidos en múltiples zonas de disponibilidad, FSx ONTAP también se puede aprovisionar con la opción Multi-AZ que brinda alta disponibilidad y protección contra fallas de AZ.

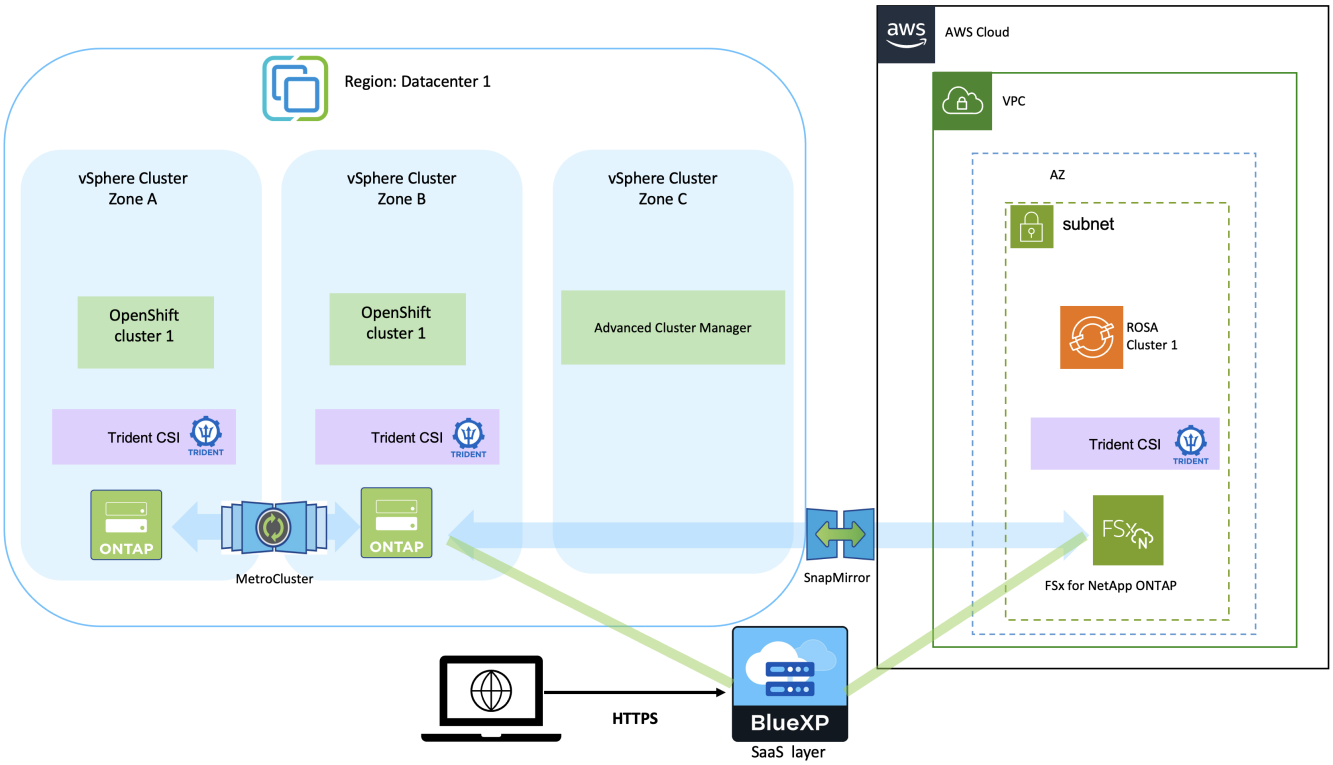
- Google Cloud NetApp Volumes*

Red Hat OpenShift Dedicated es una plataforma de aplicaciones totalmente administrada que le permite crear, implementar y escalar aplicaciones rápidamente en la nube híbrida. Google Cloud NetApp Volumes proporciona volúmenes persistentes que incorporan el conjunto completo de capacidades de gestión de datos empresariales de ONTAP a las implementaciones de OpenShift en Google Cloud.

Implementar y configurar la plataforma Managed Red Hat OpenShift Container en AWS

Esta sección describe, a grandes rasgos, un flujo de trabajo para configurar clústeres de Red Hat OpenShift gestionados en AWS(ROSA). Muestra el uso de Amazon FSx for NetApp ONTAP (FSx ONTAP) gestionado como backend de almacenamiento de Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre la implementación de FSx ONTAP en AWS mediante NetApp Console. Además, se proporcionan detalles sobre el uso de NetApp Console y OpenShift GitOps (Argo CD) para realizar actividades de protección y migración de datos para las aplicaciones con estado en clústeres ROSA.

Aquí hay un diagrama que representa los clústeres ROSA implementados en AWS y que utilizan FSx ONTAP como almacenamiento de backend.



Esta solución se verificó utilizando dos clústeres ROSA en dos VPC en AWS. Cada clúster ROSA se integró con FSx ONTAP mediante Trident. Hay varias formas de implementar clústeres ROSA y FSx ONTAP en AWS. Esta descripción de alto nivel de la configuración proporciona enlaces a la documentación para el método específico que se utilizó. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en el"sección de recursos" .

El proceso de configuración se puede dividir en los siguientes pasos:

Instalar clústeres ROSA

- Cree dos VPC y configure la conectividad de emparejamiento de VPC entre las VPC.
- Consulta "aquí" para ver instrucciones para instalar clústeres ROSA.

Instalar FSx ONTAP

- Instala FSx ONTAP en las VPC desde NetApp Console. Consulta "aquí" para crear una cuenta de NetApp Console y empezar. Consulta "aquí" para instalar FSx ONTAP. Consulta "aquí" para crear un conector en AWS para gestionar FSx ONTAP.
- Implemente FSx ONTAP mediante AWS. Referirse"aquí" para implementación mediante la consola de AWS.

Instalar Trident en clústeres ROSA (usando el gráfico Helm)

- Utiliza el chart de Helm para instalar Trident en clústeres ROSA. Consulta el enlace a la documentación: aquí.

Integración de FSx ONTAP con Trident para clústeres ROSA

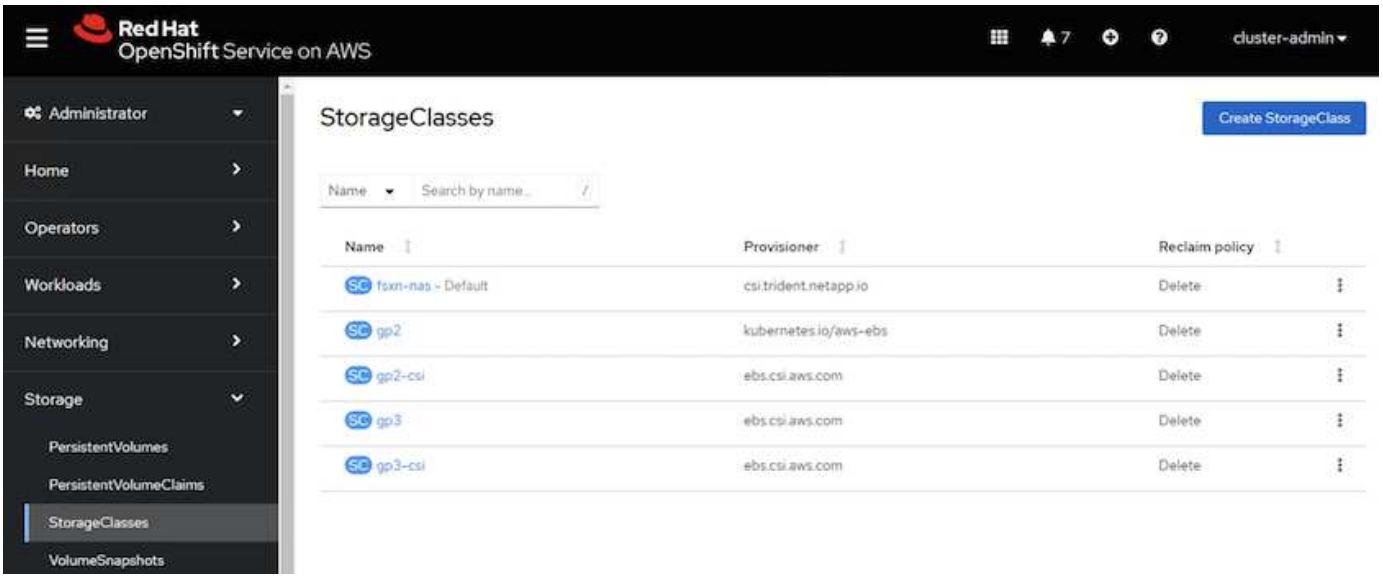
OpenShift GitOps se puede utilizar para implementar Trident CSI en todos los clústeres administrados a medida que se registran en ArgoCD mediante ApplicationSet.

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```



Crear clases de almacenamiento y backend usando Trident (para FSx ONTAP)

- Referirse"aquí" Para obtener detalles sobre la creación de clases de almacenamiento y backend.
- Haga que la clase de almacenamiento creada para FsxN con Trident CSI sea predeterminada desde OpenShift Console. Vea la captura de pantalla a continuación:



Implementar una aplicación usando OpenShift GitOps (Argo CD)

- Instala el operador OpenShift GitOps en el clúster. Consulta las instrucciones "aquí".
- SetUp una nueva instancia de Argo CD para el clúster. Consulta las instrucciones "aquí".

Abre la consola de Argo CD e implementa una aplicación. Como ejemplo, puedes implementar una aplicación de Jenkins con Argo CD usando un Helm Chart. Al crear la aplicación, se proporcionaron los siguientes

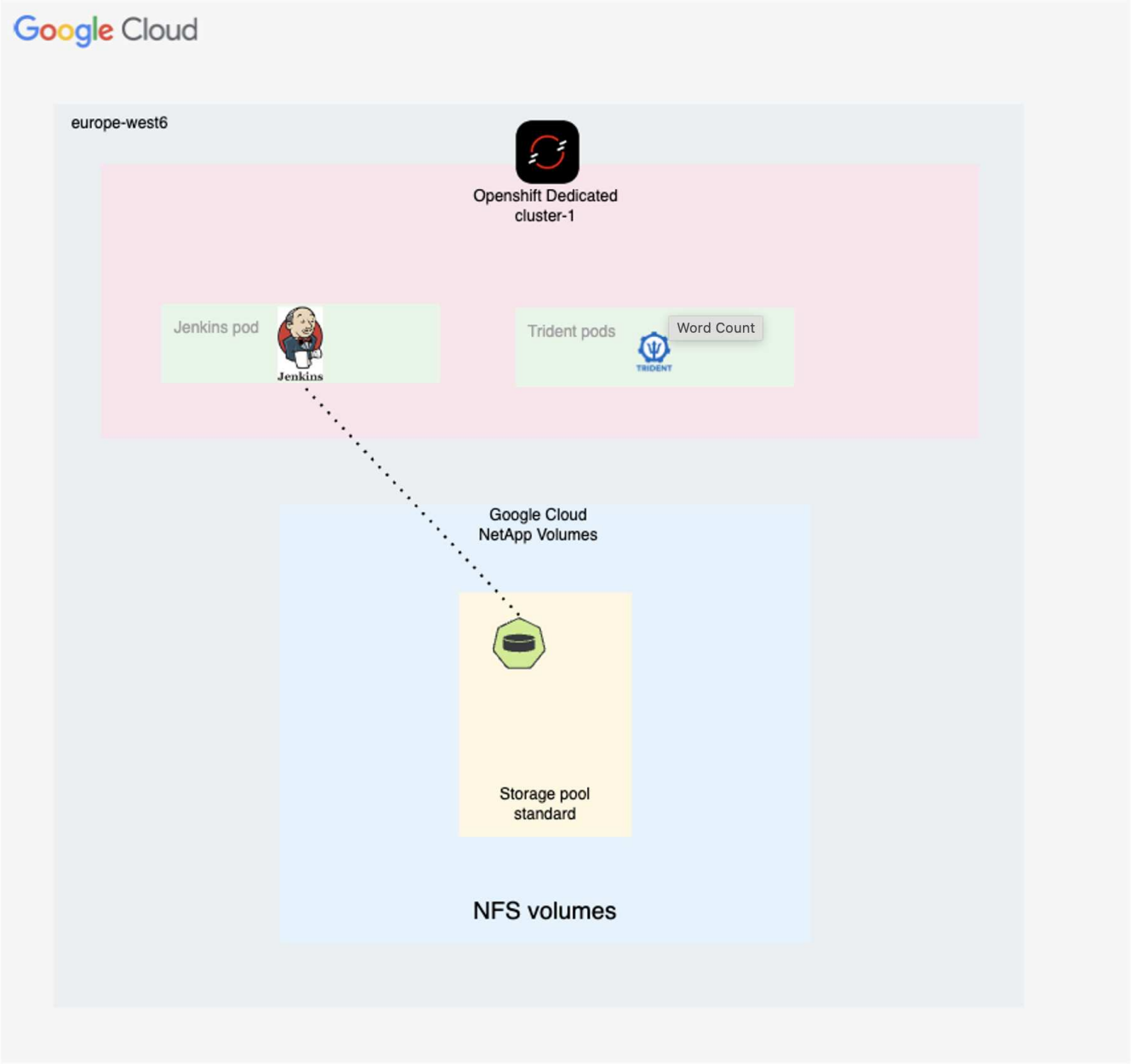
detalles: Project: default cluster: 'https://kubernetes.default.svc'[] (sin las comillas) Namespace: Jenkins la url del Helm Chart: 'https://charts.bitnami.com/bitnami'[] (sin las comillas)

Parámetros de Helm: global.storageClass: fsxn-nas

Implemente y configure OpenShift Dedicated en Google Cloud con Google Cloud NetApp Volumes

Esta sección describe un flujo de trabajo de alto nivel para configurar clústeres OpenShift Dedicated (OSD) en la plataforma Google Cloud. Muestra NetApp Trident usando Google Cloud NetApp Volumes como back-end de almacenamiento para proporcionar volúmenes persistentes para aplicaciones con estado que se ejecutan con Kubernetes.

Aquí se muestra un diagrama que representa un clúster OSD implementado en Google Cloud y que utiliza NetApp Volumes como almacenamiento de backend.



El proceso de configuración se puede dividir en los siguientes pasos:

Instalar clústeres OSD en Google Cloud

- Si desea utilizar una VPC existente para el clúster, debe crear la VPC, dos subredes, un enrutador en la nube y dos NAT en la nube de GCP para el clúster OSD. Referirse"aquí" para obtener instrucciones.
- Consulta "aquí" para ver las instrucciones sobre cómo instalar clústeres de OSD en GCP con el modelo de facturación Customer Cloud Subscription (CCS). OSD también está incluido en Google Cloud Marketplace. Hay un vídeo que muestra cómo instalar OSD con la solución de Google Cloud Marketplace "aquí".

Habilitar Google Cloud NetApp Volumes

- Referirse"aquí" para obtener información sobre cómo configurar el acceso a Google Cloud NetApp Volumes. Siga todos los pasos hasta el momento inclusive
- Crear un grupo de almacenamiento. Referirse"aquí" para obtener información sobre cómo configurar un grupo de almacenamiento en Google Cloud NetApp Volumes. Los volúmenes para las aplicaciones Kubernetes con estado que se ejecutan en OSD se crearán dentro del grupo de almacenamiento.

Instalar Trident en clústeres OSD (usando el gráfico Helm)

- Usa un Helm chart para instalar Trident en clusters OSD. Consulta "aquí" para ver instrucciones sobre cómo instalar el Helm chart.

Integración de NetApp Volumes con NetApp Trident para clústeres OSD

Cree clases de almacenamiento y backend con Trident (para Google Cloud NetApp Volumes)

- Consulte aquí para obtener detalles sobre la creación del backend.
- Si alguna de las clases de almacenamiento actuales en Kubernetes está marcada como predeterminada, elimine esa anotación editando la clase de almacenamiento.
- Cree al menos una clase de almacenamiento para volúmenes NetApp con el aprovisionador Trident CSI. Convierte exactamente una de las clases de almacenamiento en predeterminada mediante una anotación. Esto permitirá que una PVC utilice esta clase de almacenamiento cuando no se la llame explícitamente en el manifiesto de PVC. A continuación se muestra un ejemplo con la anotación.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

Implementar una aplicación usando OpenShift GitOps (Argo CD)

- Instala el operador OpenShift GitOps en el clúster. Consulta las instrucciones "aquí".
- SetUp una nueva instancia de Argo CD para el clúster. Consulta las instrucciones "aquí".

Abre la consola de Argo CD e implementa una aplicación. Como ejemplo, puedes implementar una aplicación

de Jenkins con Argo CD usando un Helm Chart. Al crear la aplicación, se proporcionaron los siguientes detalles: Project: default cluster: 'https://kubernetes.default.svc'[] (sin las comillas) Namespace: Jenkins la url del Helm Chart: 'https://charts.bitnami.com/bitnami'[] (sin las comillas)

Protección de datos

Para obtener más información sobre cómo proteger y migrar cargas de trabajo de contenedores usando Trident Protect, revisa la siguiente sección: - "Protege y migra aplicaciones en contenedores usando Trident Protect"

Soluciones multicloud híbridas adicionales de NetApp para cargas de trabajo de Red Hat OpenShift

Consulta las siguientes soluciones adicionales:

- "Solución de contenedores Red Hat OpenShift para entornos locales"
- "Solución de contenedores de Red Hat OpenShift Service on AWS"
- "Solución de virtualización de Red Hat OpenShift para entornos locales"
- "Solución de virtualización de Red Hat OpenShift Service on AWS"

Proteja sus datos con Trident Protect

Protección de datos para Container Apps en OpenShift Container Platform usando Trident Protect

Esta sección del documento de referencia proporciona detalles para crear instantáneas y copias de seguridad de Container Apps usando Trident Protect. NetApp Trident Protect proporciona capacidades avanzadas de gestión de datos de aplicaciones que mejoran la funcionalidad y la disponibilidad de aplicaciones Kubernetes con estado respaldadas por sistemas de almacenamiento NetApp ONTAP y el aprovisionador de almacenamiento NetApp Trident CSI. Trident Protect crea instantáneas y copias de seguridad de aplicaciones. Esto significa que las instantáneas y copias de seguridad se crean no solo para los datos de la aplicación en volúmenes persistentes, sino también para los metadatos de la aplicación. Las instantáneas y copias de seguridad creadas por Trident Protect pueden almacenarse en cualquiera de los siguientes almacenes de objetos y restaurarse desde ellos más adelante.

- AWS S3
- Almacenamiento de blobs de Azure
- Almacenamiento en la nube de Google
- ONTAP S3
- StorageGrid
- Cualquier otro almacenamiento compatible con S3

Trident Protect utiliza el modelo de control de acceso basado en roles (RBAC) de Kubernetes. Por defecto, Trident Protect proporciona un único espacio de nombres del sistema llamado trident-protect y su cuenta de

servicio predeterminada asociada. Si tienes una organización con muchos usuarios o necesidades de seguridad específicas, puedes usar las funciones de RBAC de Trident Protect para tener un control más granular sobre el acceso a los recursos y espacios de nombres.

Puedes encontrar información adicional sobre RBAC en Trident Protect en el "Documentación de Trident Protect"

> El administrador del clúster tiene acceso a los recursos en el espacio de nombres trident-protect predeterminado y también puede acceder a los recursos en todos los demás espacios de nombres. Los usuarios no pueden crear recursos personalizados (CR) de gestión de datos de aplicaciones, como CR de instantáneas y de copia de seguridad, en el espacio de nombres trident-protect. Como práctica recomendada, los usuarios deberán crear esas CR en el espacio de nombres de la aplicación.

Trident Protect puede instalarse siguiendo las instrucciones proporcionadas en la documentación "aquí". Esta sección te va a mostrar el flujo de trabajo para la protección de datos de aplicaciones en contenedores y la restauración de las aplicaciones usando Trident Protect. 1. Creación de instantáneas (bajo demanda o programada) 2. Restaurar desde una instantánea (restaurar en el mismo o en otro espacio de nombres) 3. Creación de copias de seguridad 4. Restaurar desde una copia de seguridad

▼ **Requisito previo**

Antes de crear las instantáneas y las copias de seguridad de una aplicación, se debe configurar el almacenamiento de objetos en Trident Protect para almacenar las instantáneas y las copias de seguridad. Esto se hace usando el bucket CR. Solo los administradores pueden crear un bucket CR y configurarlo. El bucket CR se conoce como AppVault en Trident Protect. Los objetos AppVault son la representación declarativa del flujo de trabajo de Kubernetes de un bucket de almacenamiento. Un CR AppVault contiene las configuraciones necesarias para que un bucket se use en operaciones de protección, como copias de seguridad, instantáneas, operaciones de restauración y replicación SnapMirror.

En este ejemplo, mostraremos el uso de ONTAP S3 como almacenamiento de objetos. Aquí está el flujo de trabajo para crear AppVault CR para ONTAP S3: 1. Crea un servidor de almacén de objetos S3 en el SVM en el clúster ONTAP. 2. Crea un bucket en el servidor de almacén de objetos. 3. Crea un usuario S3 en el SVM. Guarda la clave de acceso y la clave secreta en un lugar seguro. 4. En OpenShift, crea un secreto para almacenar las credenciales de ONTAP S3. 5. Crea un objeto AppVault para ONTAP S3

Configura Trident Protect AppVault para ONTAP S3

Archivo YAML de ejemplo para configurar Trident Protect con ONTAP S3 como AppVault

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
```

```
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

Archivo yaml de muestra para instalar la aplicación postgresql

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
```

```
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ **Crear instantáneas**

Creación de una instantánea a pedido

```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+-----------------+--------------+-----------+-----+-------+
|      NAME       |   APP REF    |   STATE   | AGE | ERROR |
+-----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+-----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```

```
[root@localhost DataProtection]# oc get all,pvc,volumesnapshot -n postgres
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
Warning: kubevirt.io/v1 VirtualMachineInstancePresets is now deprecated and will be removed in v2.
NAME                        READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-jfx49   1/1     Running   0          3h47m

NAME               TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/postgres   ClusterIP   172.30.132.112   <none>        5432/TCP   3h47m

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/postgres   1/1     1            1           3h47m

NAME                                  DESIRED   CURRENT   READY   AGE
replicaset.apps/postgres-cd9d6ccb   1         1         1       3h47m

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAG
ECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   8Gi        RWO            sc-zon
ea-nas   <unset>                 4h40m
persistentvolumeclaim/postgres-pvc                 Bound    pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   5Gi        RWO            sc-zon
ea-nas   <unset>                 3h47m

NAME                                                                                                                                READYTO
USE   SOURCEPVC                  SOURCESNAPSHOTCONTENT   RESTORESIZE   SNAPSHOTCLASS          SNAPSHOTCONTENT
          CREATIONTIME   AGE
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true
      postgres-pvc                                      53676Ki       trident-snapshotclass   snapcontent-796ea7f8-59a0-493e-bbd8-3a
e76fe9036c   13m            13m
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true
      data-postgres-postgresql-0                        368Ki         trident-snapshotclass   snapcontent-86a464d4-ffd8-4279-9cf7-88
88a097c001   13m            13m
```

Creación de una programación Con el siguiente comando, se crearán instantáneas diariamente a las 15:33 y se conservarán dos instantáneas y copias de seguridad.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily --hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+---------------------+---------+-------+-----+-------+
|   NAME    |     APP     |       SCHEDULE      | ENABLED | STATE | AGE | ERROR |
+-----------+-------------+---------------------+---------+-------+-----+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 17s |       |
+-----------+-------------+---------------------+---------+-------+-----+-------+
[root@localhost DataProtection]#
```

Creación de un cronograma usando yaml

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+---------------------+---------+-------+------+-------+
|   NAME    |     APP     |       SCHEDULE      | ENABLED | STATE | AGE  | ERROR |
+-----------+-------------+---------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+-------------+---------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

Puedes ver las instantáneas creadas según este cronograma.

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

También se crean instantáneas de volumen.

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                  READYTOUSE   SOURCEPVC
                                CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ Eliminar la aplicación para simular la pérdida de la aplicación

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ Restaurar desde una instantánea al mismo espacio de nombres

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

La aplicación y su PVC se restauran al mismo espacio de nombres.

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ **Restaurar desde una instantánea a un espacio de nombres diferente**

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |      APPVAULT      |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

Puedes ver que la aplicación ha sido restaurada a un nuevo espacio de nombres.

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                  Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ **Crear copias de seguridad**

Creación de una copia de seguridad a pedido

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1             | postgres-app | Completed | 6m19s  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Creación de un cronograma para la copia de seguridad

Las copias de seguridad diarias y horarias de la lista anterior se crean a partir de la programación configurada previamente.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ **Restaurar desde una copia de seguridad**

Elimine la aplicación y los PVC para simular una pérdida de datos.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Restaurar al mismo espacio de nombres #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir" creado.

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

La aplicación y los PVC se restauran en el mismo espacio de nombres.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w   1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                 Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

Restaurar a un espacio de nombres diferente Crea un nuevo espacio de nombres. Restaurar desde una copia de seguridad al nuevo espacio de nombres.

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p   1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                 Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ Migrar aplicaciones

Para clonar o migrar una aplicación a un clúster diferente (realizar un clon entre clústeres), crea una copia de seguridad en el clúster de origen y luego restaura la copia de seguridad en un clúster diferente. Asegúrate de que Trident Protect está instalado en el clúster de destino.

En el clúster de origen, realice los pasos como se muestra en la siguiente imagen:

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

Desde el clúster de origen, cambie el contexto al clúster de destino. Luego, asegúrese de que se pueda acceder a AppVault desde el contexto del clúster de destino y obtenga el contenido de AppVault del clúster de destino.

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+------------------+----------+-----------+------+-------+
|       NAME       | PROVIDER |   STATE   | AGE  | ERROR |
+------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+--------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-----------------------------------------------------------------------------+
|    CLUSTER   |     APP     |  TYPE  |            NAME             |        TIMESTAMP        |
                    PATH                                                     |
+--------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-----------------------------------------------------------------------------+
| ocp-cluster11 | bbox        | backup | bboxbackup1                 | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                |
| ocp-cluster11 | postgres-app | backup | backup1                     | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3            |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300  | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd  |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300  | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d  |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031 |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1    | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3    |
```

Utilice la ruta de respaldo de la lista y cree un objeto CR de respaldo y restauración como se muestra en el siguiente comando.

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|          NAME            |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

Ahora puedes ver que los pods de aplicación y los PVC se crean en el clúster de destino.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                  READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                        STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                 Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Protege las máquinas virtuales en Red Hat OpenShift Virtualization usando Trident Protect

Protege las máquinas virtuales en OpenShift Virtualization usando instantáneas y copias de seguridad. Este procedimiento incluye crear un AppVault usando el almacén de objetos S3 de ONTAP, configurar Trident Protect para capturar datos de máquinas virtuales, incluidos los objetos de recursos de Kubernetes, volúmenes persistentes e imágenes internas, y restaurar los datos cuando sea necesario.

Las máquinas virtuales en el entorno de virtualización OpenShift son aplicaciones en contenedores que se ejecutan en los nodos de trabajo de su plataforma OpenShift Container. Es importante proteger los metadatos de las máquinas virtuales, así como los discos persistentes de las máquinas virtuales, para que cuando se pierdan o se dañen, se puedan recuperar.

Los discos persistentes de las VMs de OpenShift Virtualization pueden ser respaldados por almacenamiento ONTAP integrado al clúster de OpenShift usando "Trident CSI". En esta sección usamos "Trident Protect" para crear snapshots y backups de VMs, incluyendo sus volúmenes de datos, en el almacén de objetos ONTAP.

Luego restauramos desde una instantánea o una copia de seguridad cuando sea necesario.

Trident Protect permite realizar instantáneas, copias de seguridad, restauraciones y recuperación ante desastres de aplicaciones y VMs en un clúster de OpenShift. Para las VMs de OpenShift Virtualization, los datos que se pueden proteger con Trident Protect incluyen objetos de recursos de Kubernetes asociados con las VMs, volúmenes persistentes e imágenes internas.

Las siguientes son las versiones de los distintos componentes utilizados para los ejemplos de esta sección

- "Clúster OpenShift 4.17"
- "OpenShift Virtualization instalado a través del operador de virtualización OpenShift proporcionado por Red Hat"
- "Trident 25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

Crea AppVault para almacenamiento de objetos

▼ **Crear AppVault**

Antes de crear las instantáneas y las copias de seguridad de una aplicación o una máquina virtual, se debe configurar el almacenamiento de objetos en Trident Protect para almacenar las instantáneas y las copias de seguridad. Esto se hace usando el bucket CR. Solo los administradores pueden crear un bucket CR y configurarlo. El bucket CR se conoce como AppVault en Trident Protect. Los objetos AppVault son la representación declarativa del flujo de trabajo de Kubernetes de un bucket de almacenamiento. Un CR AppVault contiene las configuraciones necesarias para que un bucket se utilice en operaciones de protección, como copias de seguridad, instantáneas, operaciones de restauración y replicación SnapMirror.

En este ejemplo, te mostraremos el uso de ONTAP S3 como almacén de objetos. Aquí tienes el flujo de trabajo para crear AppVault CR para ONTAP S3: 1. Crea un servidor de almacén de objetos S3 en el SVM en ONTAP Cluster. 2. Crea un bucket en el servidor de almacén de objetos. 3. Crea un usuario S3 en el SVM. Guarda la clave de acceso y la clave secreta en un lugar seguro. 4. En OpenShift, crea un secreto para guardar las credenciales de ONTAP S3. 5. Crea un objeto AppVault para ONTAP S3

Configura Trident Protect AppVault para ONTAP S3

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
```

```
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+-------------------+----------+-----------+-------+---------+-------+
|       NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+-------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault | OntapS3  | Available |       |         | 8d17h |
+-------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

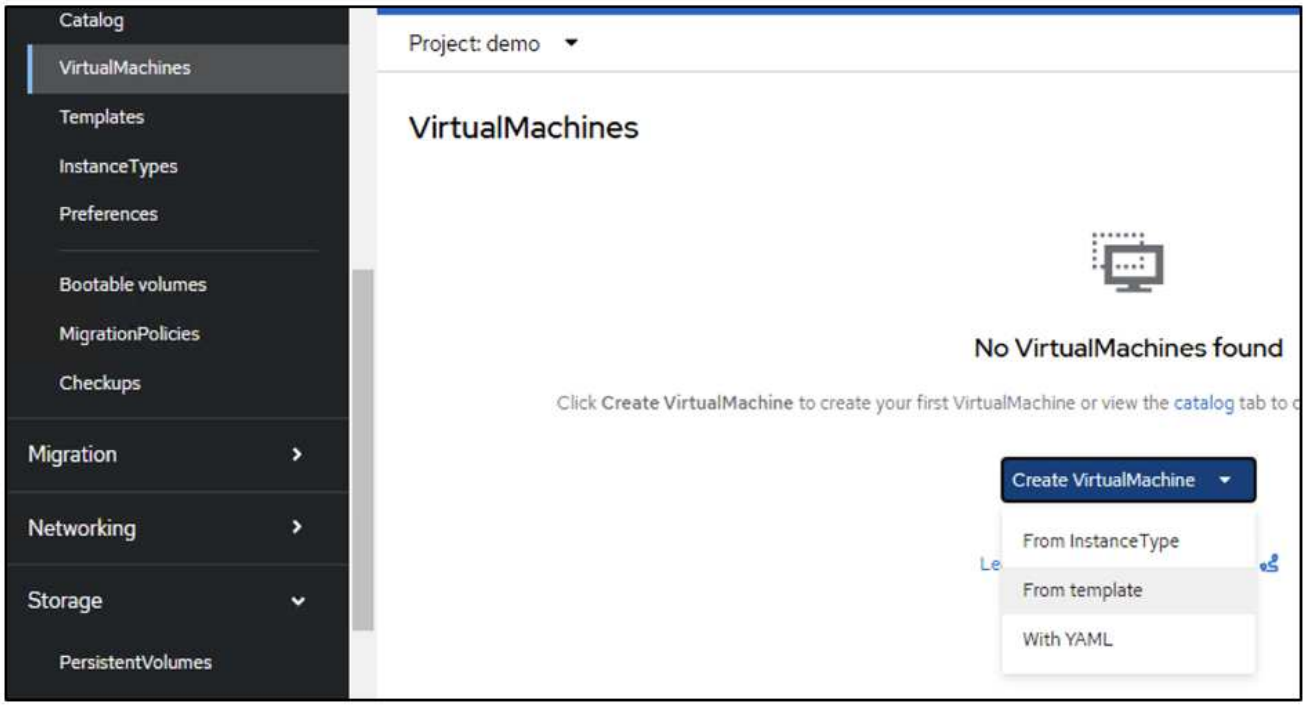
Crear una máquina virtual en OpenShift Virtualization

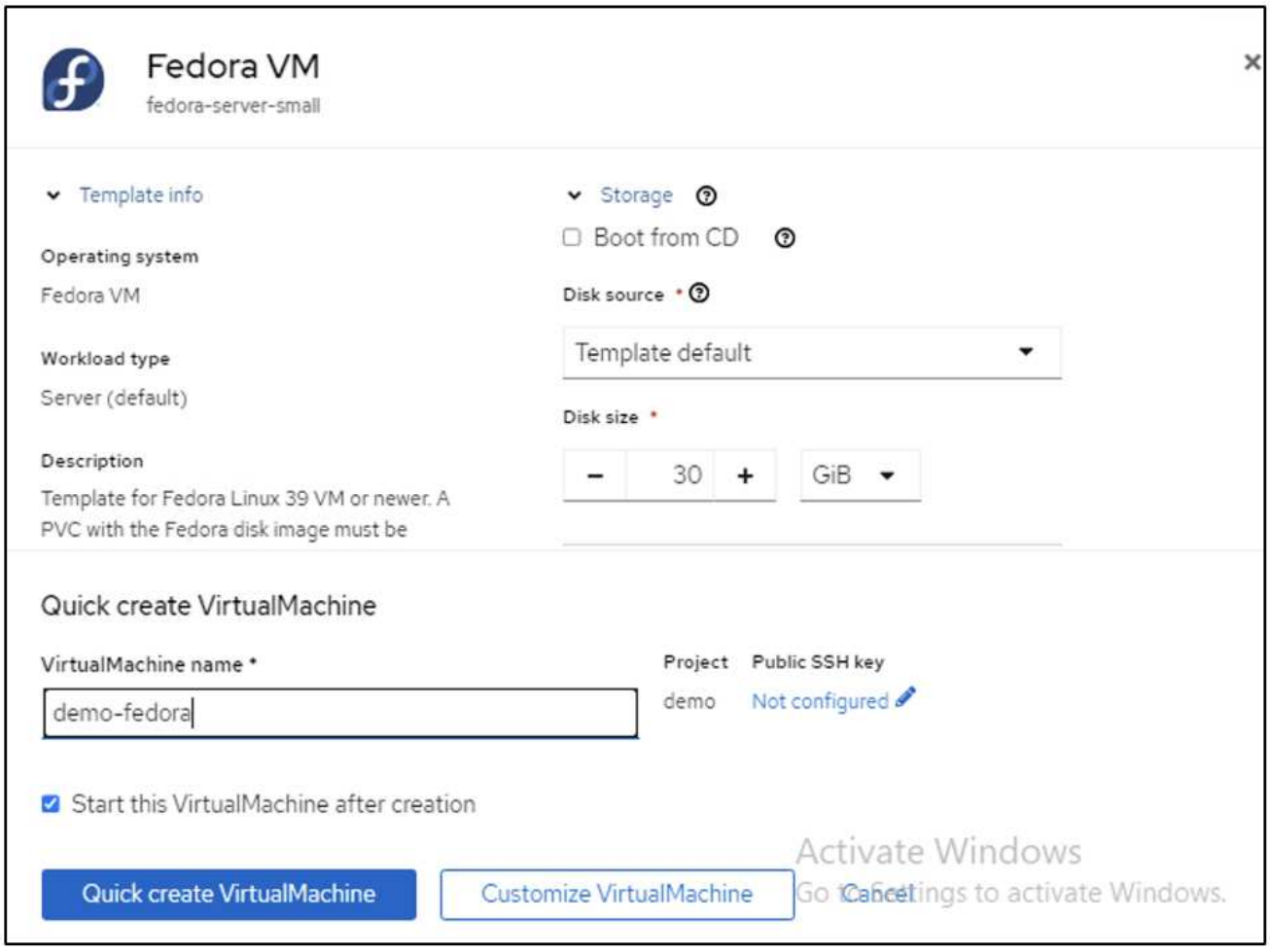
▼ **Crear una máquina virtual en OpenShift Virtualization**

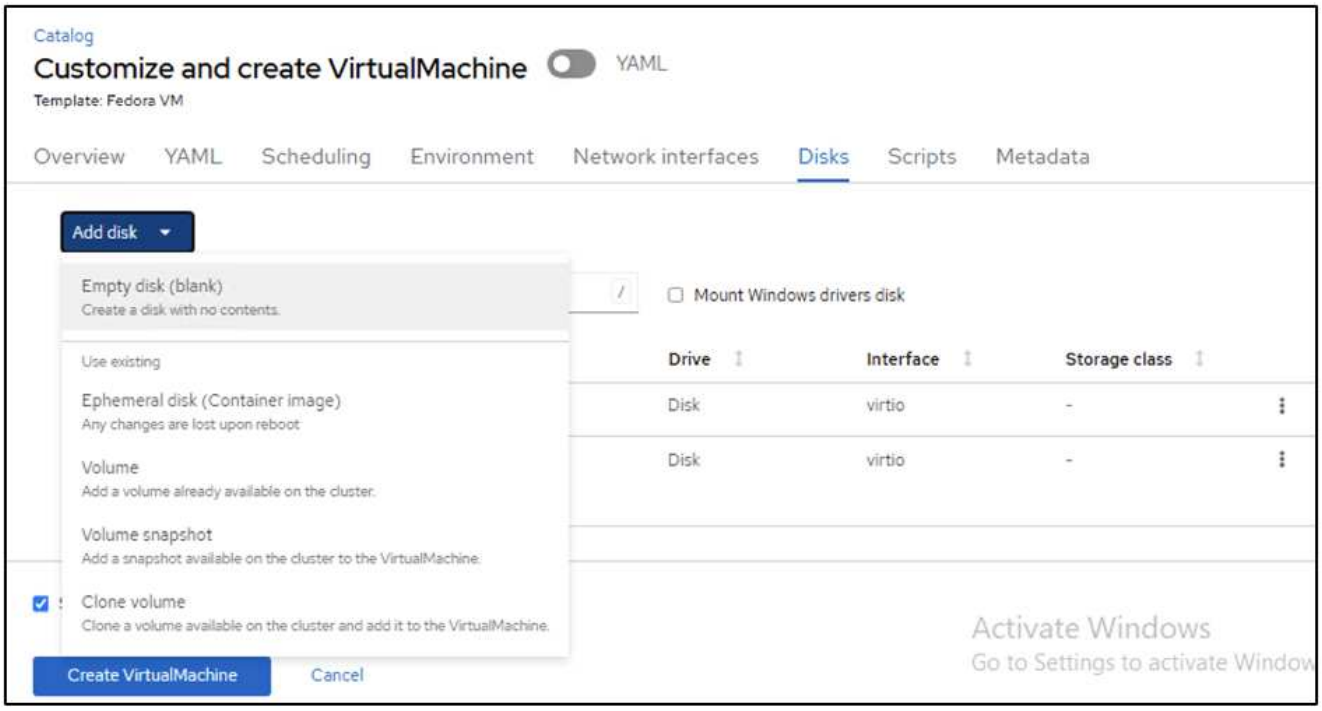
Las siguientes capturas de pantalla muestran la creación de la VM (demo-fedora en el espacio de nombres demo) desde la consola usando la plantilla. El disco raíz elige automáticamente la clase de almacenamiento predeterminada, por lo tanto, verifique que la clase de almacenamiento predeterminada esté configurada adecuadamente. En esta configuración, la clase de almacenamiento predeterminada es **sc-zonea-san**. Asegúrese de que cuando cree el disco adicional, elija la clase de almacenamiento sc-zonea-san y marque la casilla de verificación "**Aplicar configuración de almacenamiento optimizada**". Esto establecerá los modos de acceso en RWX y el modo de volumen en Bloquear.

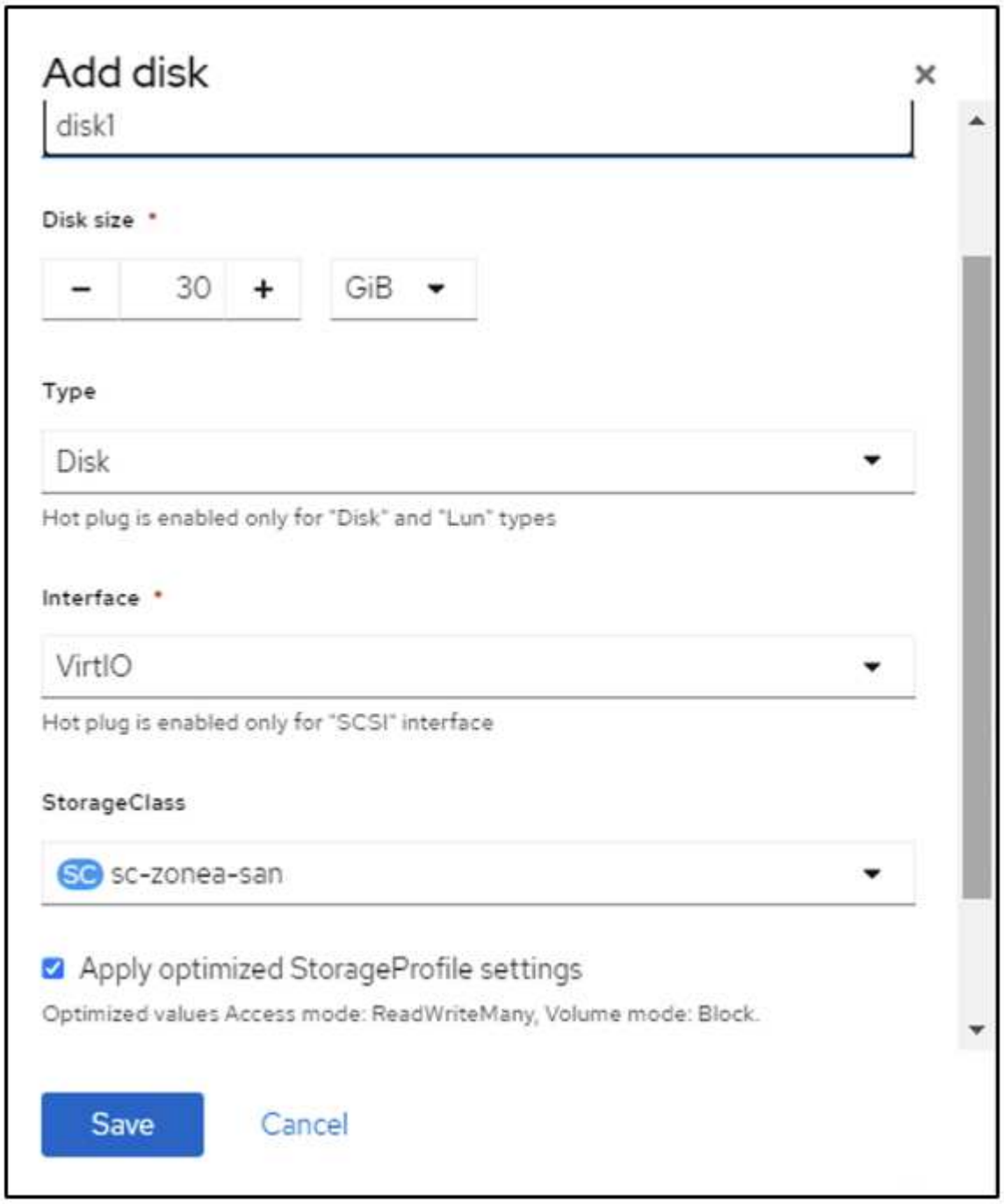
Trident admite el modo de acceso RWX en el modo de volumen de bloque para SAN (iSCSI, NVMe/TCP y FC). (Es el modo de acceso predeterminado para NAS). El modo de acceso RWX es necesario si necesita realizar una migración en vivo de las máquinas virtuales en un momento posterior.

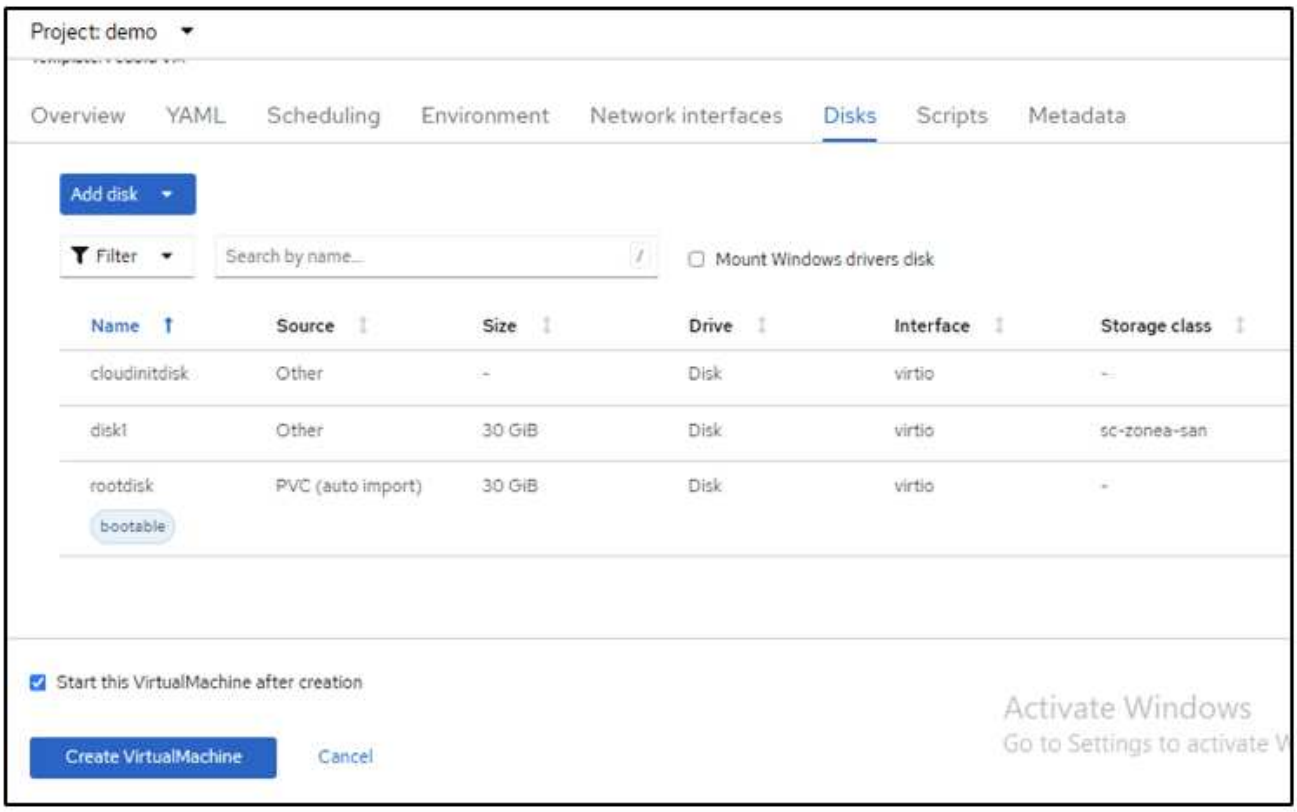



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Activate Windows
Go to Settings to activate Windows.
Quick create VirtualMachine
Customize VirtualMachine
Cancel


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Crear una aplicación

▼ Crear aplicación

Crea una aplicación Trident Protect para la máquina virtual

En el ejemplo, el espacio de nombres demo tiene una VM y todos los recursos del espacio de nombres se incluyen cuando creas la app.

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
```

```
  namespace: demo
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

Proteja la aplicación creando una copia de seguridad

▼ **Crear copias de seguridad**

Crear una copia de seguridad a pedido

Cree una copia de seguridad de la aplicación (demo-vm) creada anteriormente que incluya todos los recursos en el espacio de nombres de demostración. Proporcione el nombre de la bóveda de aplicaciones donde se almacenarán las copias de seguridad.

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Crear copias de seguridad según un cronograma

Cree un cronograma para las copias de seguridad especificando la granularidad y la cantidad de copias de seguridad a conservar.

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
```

```
schedule.protect.trident.netapp.io/backup-schedule1 created

#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+------------------------------+---------+----------------+-----------+-------+--------+
|             NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+------------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand     | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Restaurar desde una copia de seguridad

▼ **Restaurar desde copias de seguridad**

Restaurar la máquina virtual al mismo espacio de nombres

En el ejemplo, la copia de seguridad demo-vm-backup-on-demand contiene la copia de seguridad con la aplicación demo para la máquina virtual Fedora.

Primero, elimine la máquina virtual y asegúrese de que los PVC, el pod y los objetos de la máquina virtual se eliminen del espacio de nombres "demo".

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                  STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

Ahora, cree un objeto de restauración de copia de seguridad en el lugar.

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Verifique que la máquina virtual, los pods y los PVC se hayan restaurado

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Restaurar la máquina virtual a un espacio de nombres diferente

Primero, cree un nuevo espacio de nombres en el que desea restaurar la aplicación, en este ejemplo demo2. A continuación, cree un objeto de restauración de copia de seguridad

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
```

```
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

Verifique que la VM, los pods y los PVC se creen en el nuevo espacio de nombres demo2.

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Proteger la aplicación usando instantáneas

▼ Crear instantáneas

Crear una instantánea a pedido Cree una instantánea para la aplicación y especifique el almacén de aplicaciones donde debe almacenarse.

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
```

```
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Crear un cronograma para las instantáneas Crea un cronograma para las instantáneas. Especifique la granularidad y la cantidad de instantáneas que se conservarán.

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-------------------------------------------+---------+----------------+-----------+-------+--------+
|                   NAME                    |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand                 | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000               | demo-vm | Delete         | Completed |       | 1m29s  |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Restaurar desde una instantánea

▼ Restaurar desde una instantánea

Restaurar la VM desde la instantánea al mismo espacio de nombres Eliminar la VM demo-fedora del espacio de nombres demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

Cree un objeto de restauración de instantánea en el lugar a partir de la instantánea de la máquina virtual.

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
```

```
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+----------------------------------+-------------------+-----------+-------+--------+
|               NAME               |     APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Verifique que la VM y sus PVC se creen en el espacio de nombres de demostración.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                STATUS   VOLUME
persistentvolumeclaim/demo-fedora                   Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

Restaurar la máquina virtual desde la instantánea a un espacio de nombres diferente

Eliminar la máquina virtual en el espacio de nombres demo2 previamente restaurada desde la copia de seguridad.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                                    Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                                    Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

Cree el objeto de restauración de instantánea a partir de la instantánea y proporcione la asignación del espacio de nombres.

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-------------------------------------+--------------------+-----------+-------+--------+
|                NAME                 |      APPVAULT      |   STATE   | ERROR |  AGE   |
+-------------------------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-------------------------------------+--------------------+-----------+-------+--------+
```

Verifique que la VM y sus PVC se restauren en el nuevo espacio de nombres demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   29h   Running   True

NAME                                                  STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san   <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san   <unset>                 29h
[root@localhost RedHat]#
```

Restaurar una máquina virtual específica

▼ Seleccionar máquinas virtuales específicas en un espacio de nombres para crear instantáneas/copias de seguridad y restaurar

En el ejemplo anterior, teníamos una sola VM dentro de un espacio de nombres. Al incluir todo el espacio de nombres en la copia de seguridad, se capturaron todos los recursos asociados con esa máquina virtual. En el siguiente ejemplo, agregamos otra VM al mismo espacio de nombres y creamos una aplicación solo para esta nueva VM usando un selector de etiquetas.

Crear una nueva VM (demo-centos vm) en el espacio de nombres demo

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora   81m     Running   True

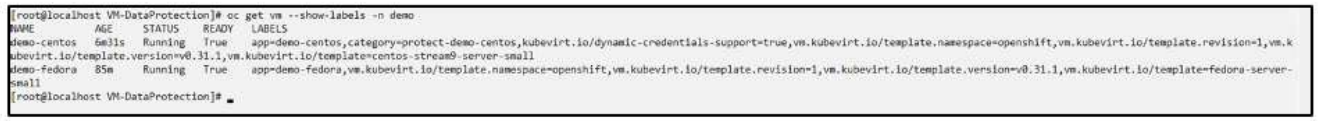
NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g   1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          81m

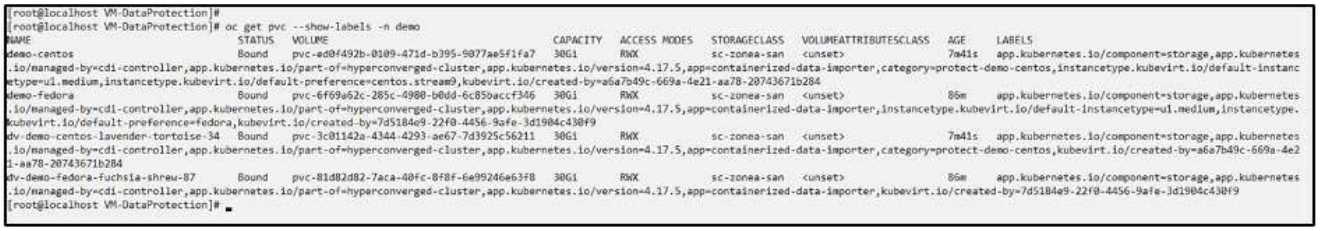
NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                     Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                     Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Etiquete la máquina virtual demo-centos y sus recursos asociados

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

Verifique que la máquina virtual demo-centos y los pvc tengan las etiquetas





Cree una aplicación solo para una VM específica (demo-centos) usando el selector de etiquetas

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+------------------+------------+-------+------+
|      NAME        | NAMESPACES | STATE | AGE  |
+------------------+------------+-------+------+
| demo-centos-app  | demo       | Ready | 56s  |
| demo-vm          | demo       | Ready | 4h6m |
+------------------+------------+-------+------+
```

El método para crear copias de seguridad e instantáneas a pedido y según un cronograma es el mismo que se mostró anteriormente. Dado que la aplicación trident-protect que se utiliza para crear las instantáneas o las copias de seguridad solo contiene la VM específica del espacio de nombres, la restauración desde ellas solo restaura una VM específica. A continuación se muestra un ejemplo de una operación de copia de seguridad y restauración.

Crear una copia de seguridad de una máquina virtual específica en un espacio de nombres utilizando su aplicación correspondiente

En los pasos anteriores, se creó una aplicación utilizando selectores de etiquetas para incluir solo la máquina virtual centos en el espacio de nombres de demostración. Cree una copia de seguridad (copia de seguridad a pedido, en este ejemplo) para esta aplicación.

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+------------------------------+-----------------+----------------+-----------+-------+--------+
|             NAME             |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand     | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500  | demo-vm         | Retain         | Completed |       | 56m17s |
+------------------------------+-----------------+----------------+-----------+-------+--------+
```

Restaurar una VM específica en el mismo espacio de nombres La copia de seguridad de una VM específica (centos) se creó usando la aplicación correspondiente. Si se crea una copia de seguridad en el lugar y una restauración a partir de esto, solo se restaura esta máquina virtual específica. Eliminar la máquina virtual Centos.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora   4m27s   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                  STATUS   VOLUME
persistentvolumeclaim/demo-fedora                     Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87 Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

Cree una copia de seguridad y restauración en el lugar desde demo-centos-backup-on-demand y verifique que la máquina virtual centos se haya recreado.

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore  | ontap-s3-appvault  | Completed |       | 57m9s |
| demo-fedora-restore  | ontap-s3-appvault  | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

Activate
Go to Sett

Restaurar una VM específica en un espacio de nombres diferente Cree una restauración de copia de seguridad en un espacio de nombres diferente (demo3) desde demo-centos-backup-on-demand y verifique que la VM centos se haya recreado.

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-
demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |     APPVAULT       |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                  AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

Demostración en video

El siguiente video muestra una demostración de cómo proteger una máquina virtual mediante instantáneas

Protegiendo una máquina virtual

Proteja las aplicaciones de contenedores mediante herramientas de terceros

Protección de datos para aplicaciones de contenedores en OpenShift Container Platform mediante la API de OpenShift para la protección de datos (OADP)

Esta sección del documento de referencia proporciona detalles para crear copias de seguridad de aplicaciones de contenedores utilizando la API de OpenShift para protección de datos (OADP) con Velero en NetApp ONTAP S3 o NetApp StorageGRID S3. Las copias de seguridad de los recursos con alcance de espacio de nombres, incluidos los volúmenes persistentes (PV), de la aplicación, se crean mediante instantáneas de CSI Trident .

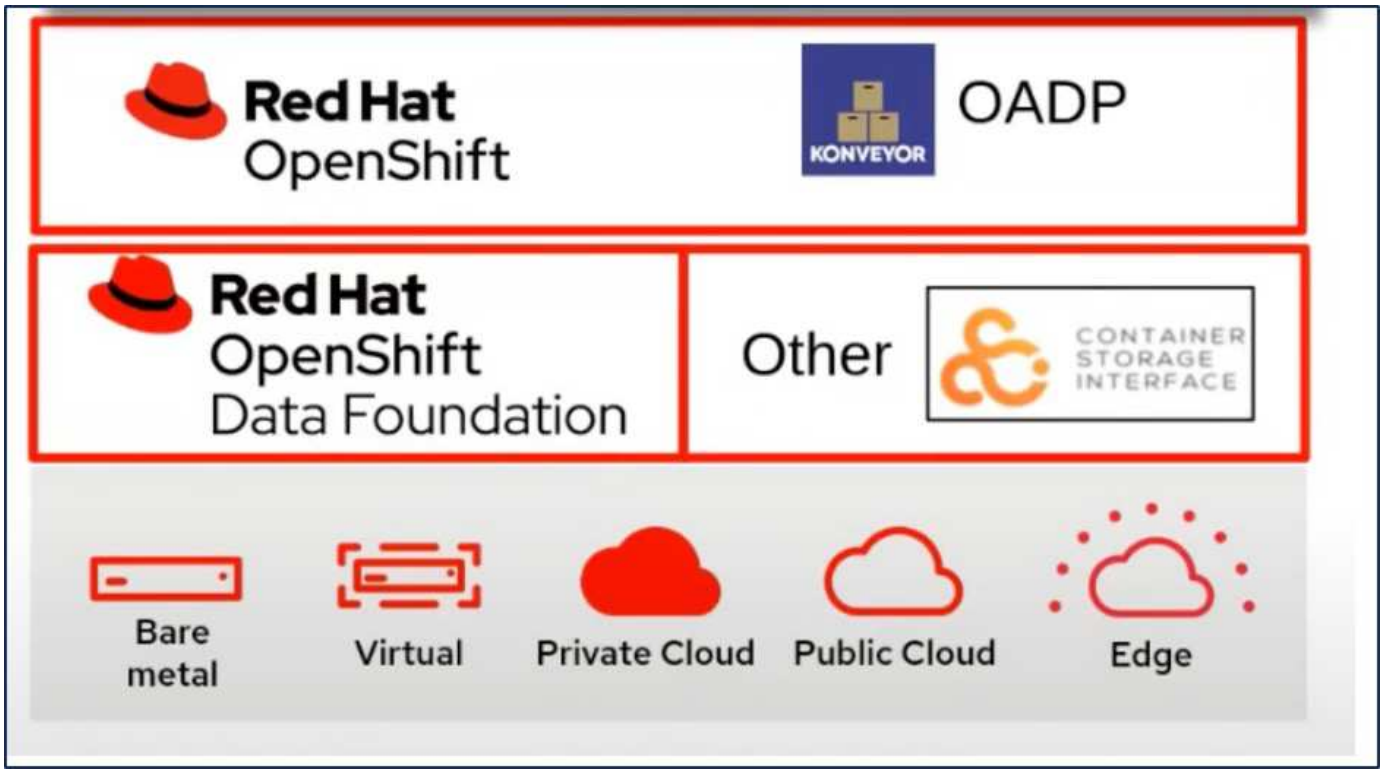
El almacenamiento persistente para las aplicaciones en contenedores puede basarse en el almacenamiento

ONTAP integrado en el clúster de OpenShift mediante "Trident CSI". En esta sección utilizamos "API de OpenShift para la protección de datos (OADP)" para realizar copias de seguridad de las aplicaciones incluidos sus volúmenes de datos en

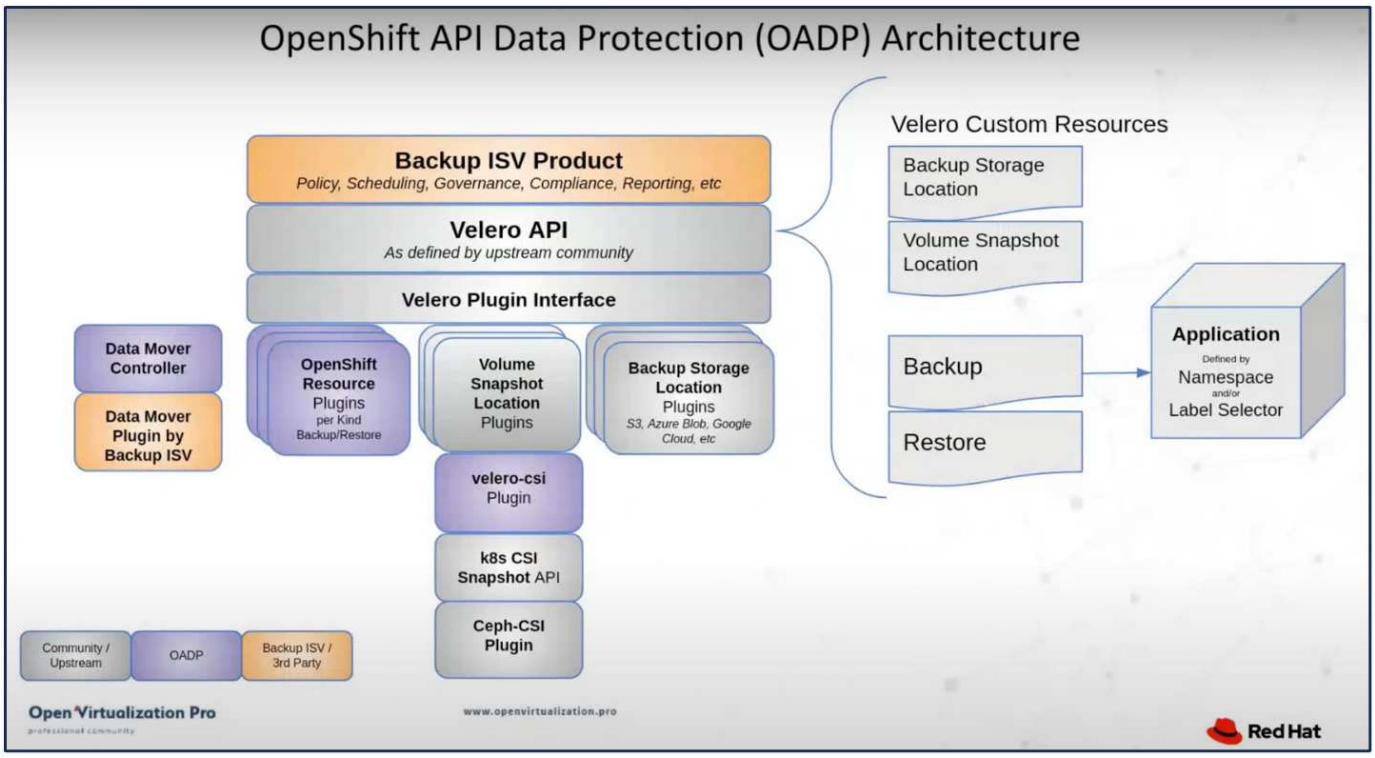
- Almacenamiento de objetos ONTAP
- StorageGrid

Luego restauramos desde la copia de seguridad cuando sea necesario. Tenga en cuenta que la aplicación solo se puede restaurar en el clúster desde donde se creó la copia de seguridad.

OADP permite la copia de seguridad, la restauración y la recuperación ante desastres de aplicaciones en un clúster OpenShift. Los datos que se pueden proteger con OADP incluyen objetos de recursos de Kubernetes, volúmenes persistentes e imágenes internas.



Red Hat OpenShift ha aprovechado las soluciones desarrolladas por las comunidades OpenSource para la protección de datos. "Velero" es una herramienta de código abierto para realizar copias de seguridad y restaurar de forma segura, realizar recuperación ante desastres y migrar recursos de clústeres de Kubernetes y volúmenes persistentes. Para utilizar Velero fácilmente, OpenShift ha desarrollado el operador OADP y el complemento Velero para integrarlo con los controladores de almacenamiento CSI. El núcleo de las API de OADP que se exponen se basan en las API de Velero. Después de instalar el operador OADP y configurarlo, las operaciones de copia de seguridad y restauración que se pueden realizar se basan en las operaciones expuestas por la API de Velero.



OADP 1.3 está disponible en el centro de operadores del clúster OpenShift 4.12 y posteriores. Tiene un Data Mover incorporado que puede mover instantáneas de volumen CSI a un almacén de objetos remoto. Esto proporciona portabilidad y durabilidad al mover instantáneas a una ubicación de almacenamiento de objetos durante la copia de seguridad. Las instantáneas estarán luego disponibles para su restauración después de un desastre.

Las siguientes son las versiones de los distintos componentes utilizados para los ejemplos de esta sección

- Clúster OpenShift 4.14
- Operador OADP 1.13 proporcionado por Red Hat
- Velero CLI 1.13 para Linux
- Trident 24.02
- ONTAP 9.12
- PostgreSQL instalado usando Helm.

"Trident CSI" "API de OpenShift para la protección de datos (OADP)" "Velero"

Instalación del operador de API de OpenShift para protección de datos (OADP)

En esta sección se describe la instalación del operador OpenShift API for Data Protection (OADP).

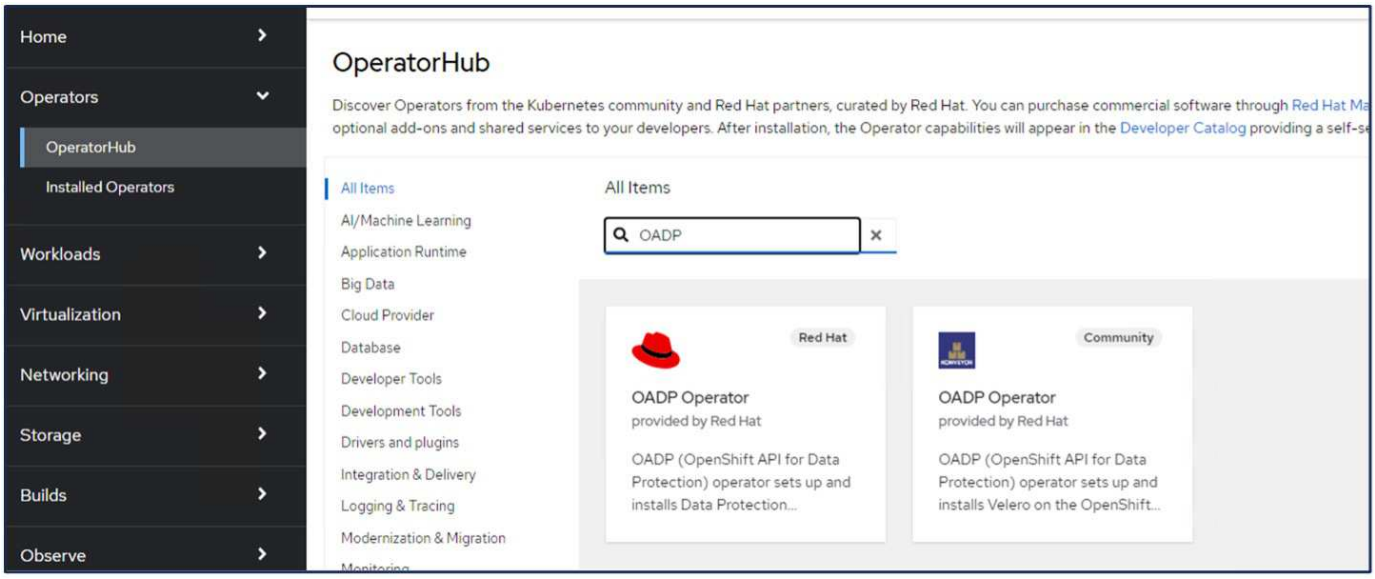
Prerrequisitos

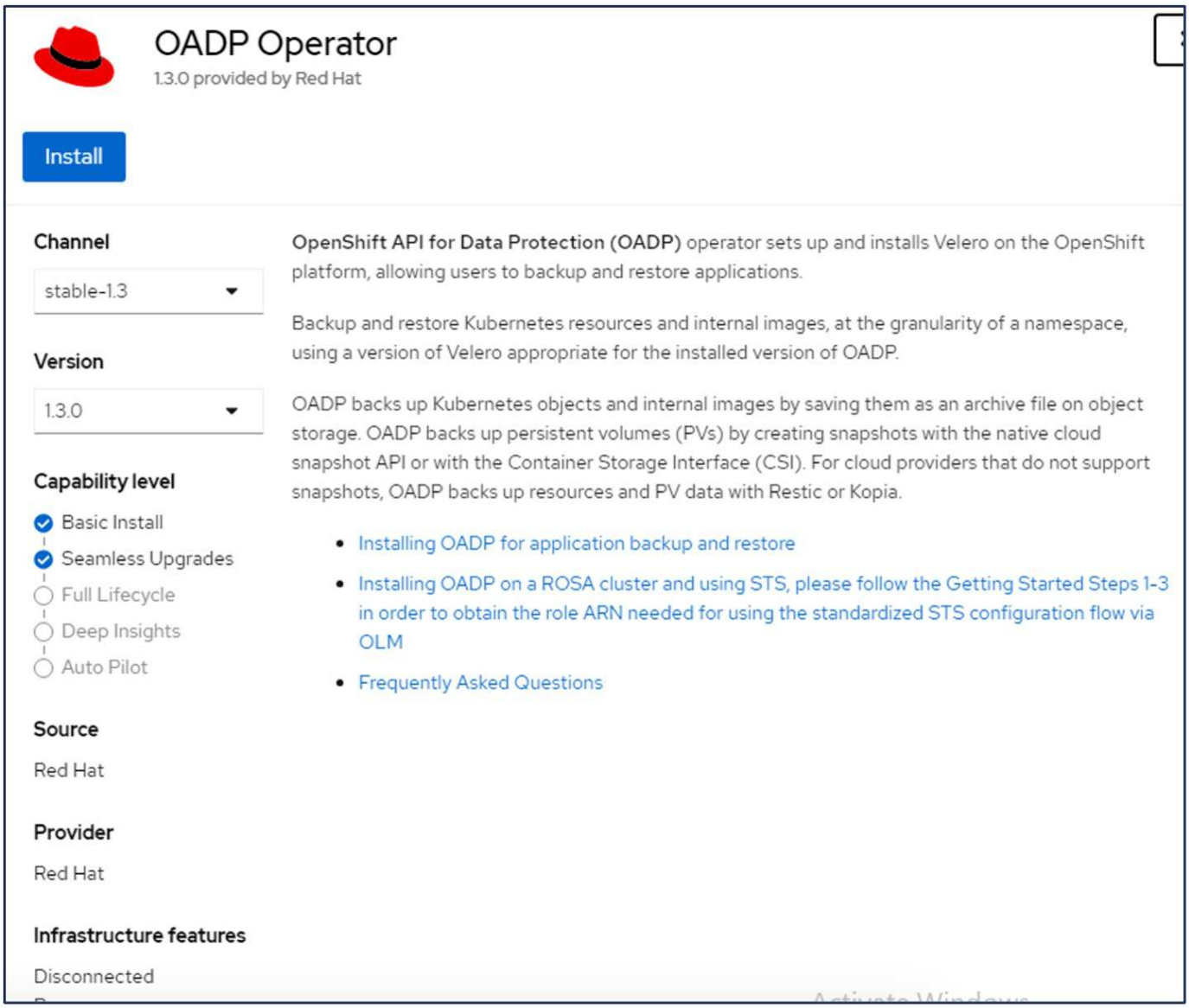
- Un clúster Red Hat OpenShift (posterior a la versión 4.12) instalado en una infraestructura física con nodos de trabajo RHCOS
- Un clúster NetApp ONTAP integrado con el clúster mediante Trident

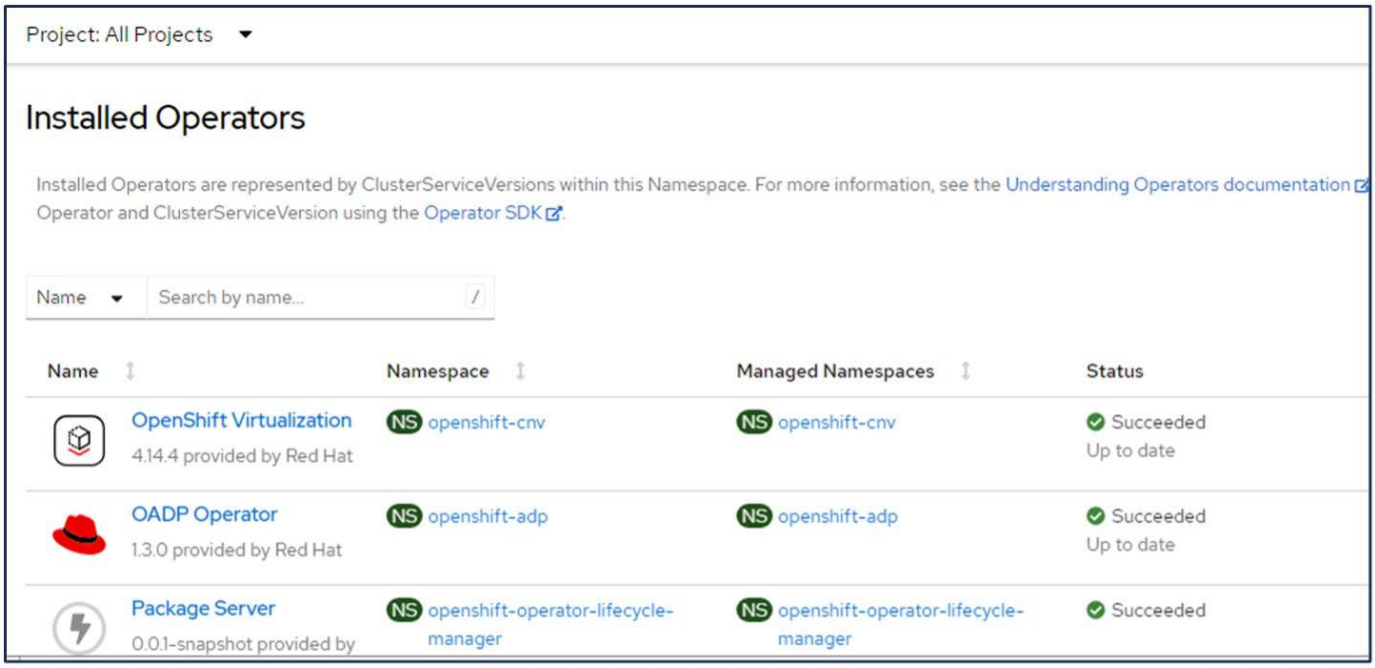
- Un backend Trident configurado con un SVM en un clúster ONTAP
- Una StorageClass configurada en el clúster OpenShift con Trident como aprovisionador
- Clase Trident Snapshot creada en el clúster
- Acceso de administrador de clúster al clúster Red Hat OpenShift
- Acceso de administrador al clúster NetApp ONTAP
- Una aplicación, por ejemplo, postgresql implementada en el clúster
- Una estación de trabajo de administrador con herramientas tridentctl y oc instaladas y agregadas a $PATH

Pasos para instalar el operador OADP

1. Vaya al Centro de operadores del clúster y seleccione el operador Red Hat OADP. En la página Instalar, utilice todas las selecciones predeterminadas y haga clic en instalar. En la página siguiente, utilice nuevamente todos los valores predeterminados y haga clic en Instalar. El operador OADP se instalará en el espacio de nombres openshift-adp.




OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions


Project: All Projects
Installed Operators
Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation
Operator and ClusterServiceVersion using the Operator SDK
Name
Search by name...
Name
Namespace
Managed Namespaces
Status
OpenShift Virtualization
4.14.4 provided by Red Hat
openshift-cnv
openshift-cnv
Succeeded
Up to date
OADP Operator
1.3.0 provided by Red Hat
openshift-adp
openshift-adp
Succeeded
Up to date
Package Server
0.0.1-snapshot provided by
openshift-operator-lifecycle-manager
openshift-operator-lifecycle-manager
Succeeded

Requisitos previos para la configuración de Velero con detalles de Ontap S3

Una vez realizada la instalación del operador, configure la instancia de Velero. Velero se puede configurar para utilizar almacenamiento de objetos compatible con S3. Configure ONTAP S3 utilizando los procedimientos que se muestran en la"Sección de gestión de almacenamiento de objetos de la documentación de ONTAP" . Necesitará la siguiente información de su configuración de ONTAP S3 para integrarse con Velero.

- Una interfaz lógica (LIF) que se puede utilizar para acceder a S3
- Credenciales de usuario para acceder a S3 que incluyen la clave de acceso y la clave de acceso secreta
- Un nombre de depósito en S3 para copias de seguridad con permisos de acceso para el usuario
- Para obtener un acceso seguro al almacenamiento de objetos, se debe instalar un certificado TLS en el servidor de almacenamiento de objetos.

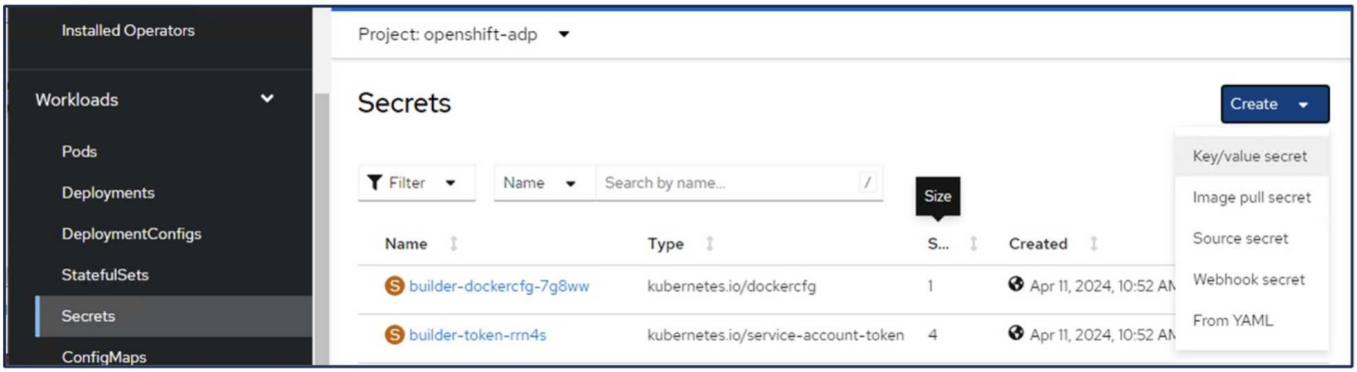
Requisitos previos para la configuración de Velero con detalles de StorageGrid S3

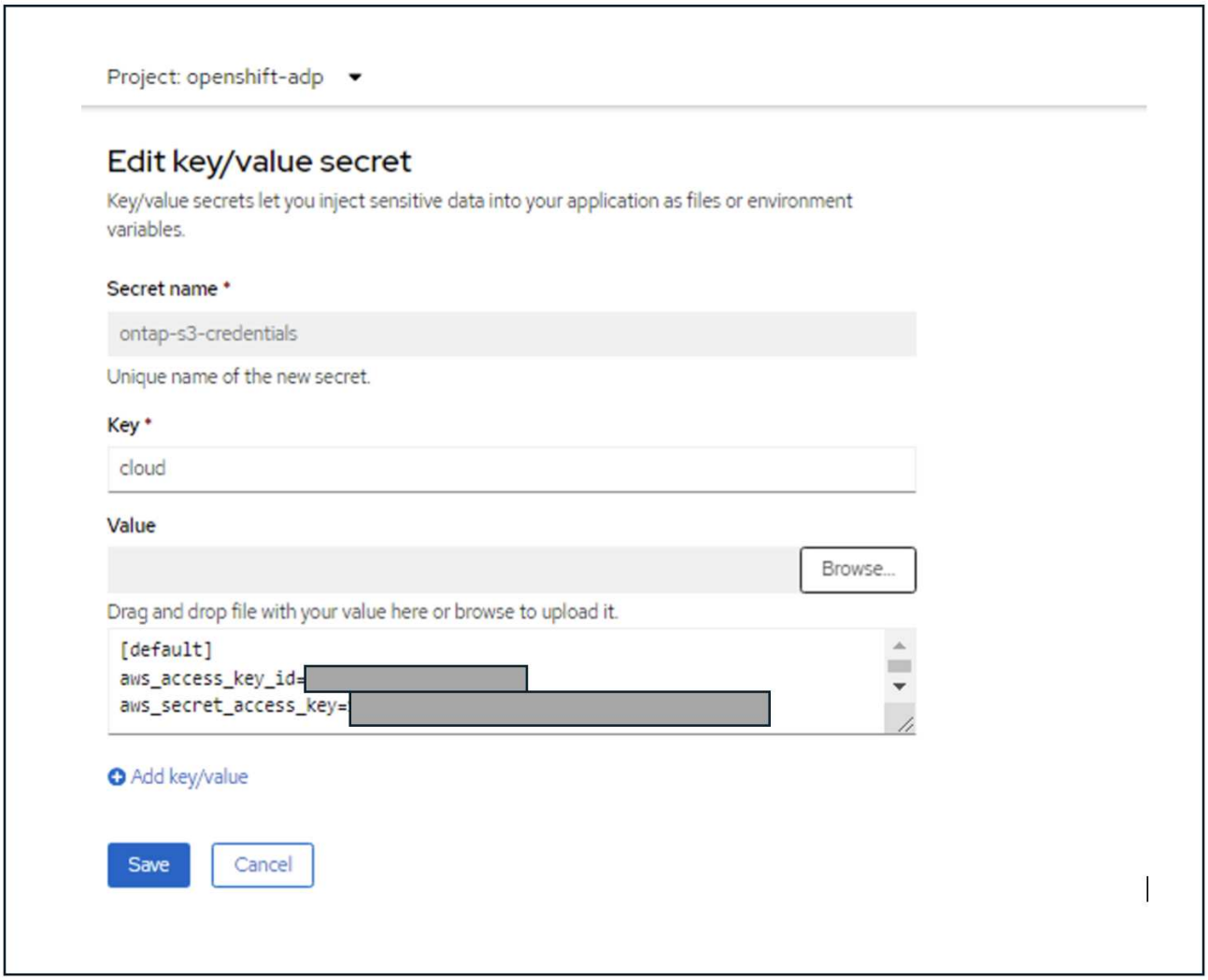
Velero se puede configurar para utilizar almacenamiento de objetos compatible con S3. Puede configurar StorageGrid S3 mediante los procedimientos que se muestran en la"Documentación de StorageGrid" . Necesitará la siguiente información de su configuración de StorageGrid S3 para integrarse con Velero.

- El punto final que se puede utilizar para acceder a S3
- Credenciales de usuario para acceder a S3 que incluyen la clave de acceso y la clave de acceso secreta
- Un nombre de depósito en S3 para copias de seguridad con permisos de acceso para el usuario
- Para obtener un acceso seguro al almacenamiento de objetos, se debe instalar un certificado TLS en el servidor de almacenamiento de objetos.

Pasos para configurar Velero

- Primero, cree un secreto para una credencial de usuario de ONTAP S3 o una credencial de usuario de StorageGrid Tenant. Esto se utilizará para configurar Velero más adelante. Puede crear un secreto desde la CLI o desde la consola web. Para crear un secreto desde la consola web, seleccione Secretos y luego haga clic en Secreto de clave/valor. Proporcione los valores para el nombre de la credencial, la clave y el valor como se muestra. Asegúrese de utilizar el Id. de clave de acceso y la clave de acceso secreta de su usuario S3. Nombra el secreto apropiadamente En el siguiente ejemplo, se crea un secreto con credenciales de usuario de ONTAP S3 llamado ontap-s3-credentials.





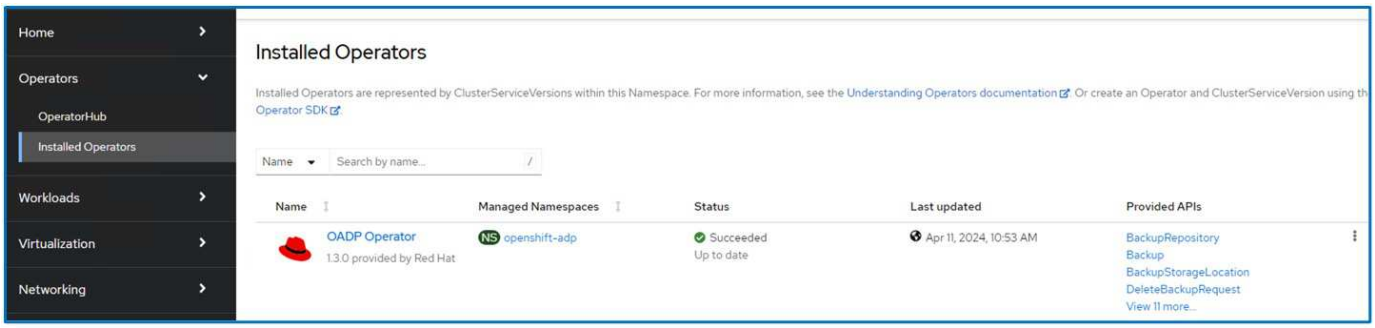
Para crear un secreto llamado sg-s3-credentials desde la CLI, puede utilizar el siguiente comando.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

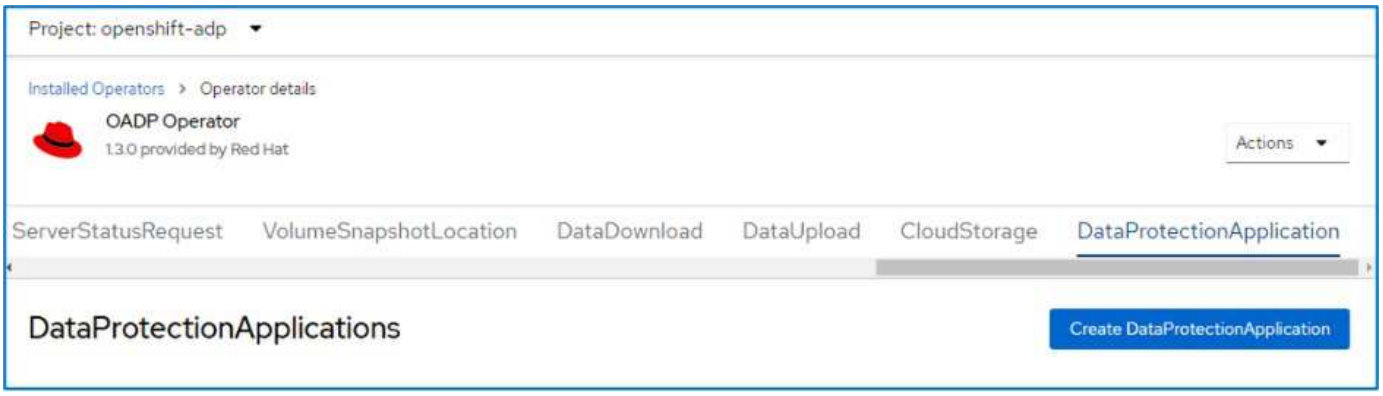
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- A continuación, para configurar Velero, seleccione Operadores instalados en el elemento de menú bajo Operadores, haga clic en el operador OADP y luego seleccione la pestaña **DataProtectionApplication**.



Haga clic en Crear aplicación de protección de datos. En la vista de formulario, proporcione un nombre para la aplicación de protección de datos o utilice el nombre predeterminado.



Ahora vaya a la vista YAML y reemplace la información de especificación como se muestra en los ejemplos de archivos YAML a continuación.

Archivo yaml de muestra para configurar Velero con ONTAP S3 como ubicación de respaldo

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
```

```
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

Archivo yaml de muestra para configurar Velero con StorageGrid S3 como ubicación de respaldo

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
```

```
        - kubevirt
```

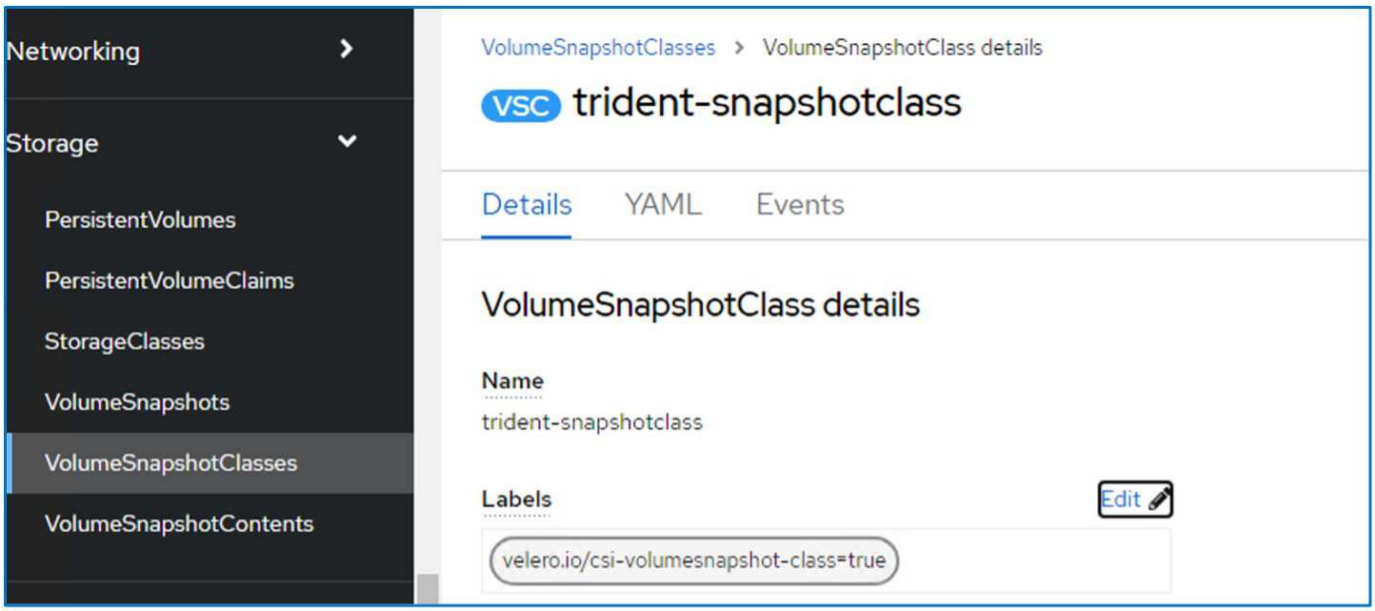
La sección de especificaciones del archivo yaml debe configurarse adecuadamente para los siguientes parámetros, de forma similar al ejemplo anterior.

backupLocations ONTAP S3 o StorageGrid S3 (con sus credenciales y otra información como se muestra en el yaml) está configurado como BackupLocation predeterminado para velero.

snapshotLocations Si usa instantáneas de la Interfaz de almacenamiento de contenedores (CSI), no necesita especificar una ubicación de instantánea porque creará un CR VolumeSnapshotClass para registrar el controlador CSI. En nuestro ejemplo, utiliza Trident CSI y previamente ha creado VolumeSnapShotClass CR utilizando el controlador Trident CSI.

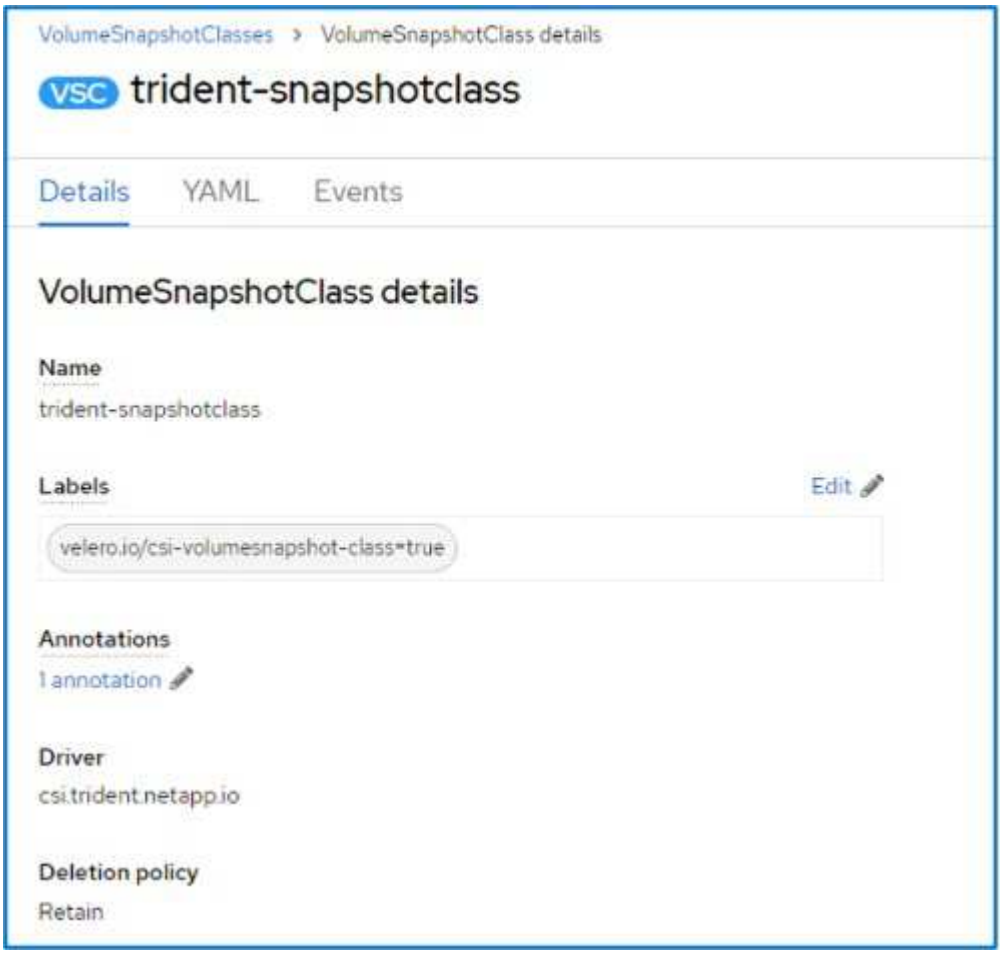
Habilitar complemento CSI Agregue csi a los complementos predeterminados para Velero para realizar copias de seguridad de volúmenes persistentes con instantáneas CSI. Los complementos CSI de Velero, para realizar copias de seguridad de los PVC respaldados por CSI, elegirán VolumeSnapshotClass en el clúster que tenga establecida la etiqueta **velero.io/csi-volumesnapshot-class**. Para esto

- Debe tener creada la clase VolumeSnapshotClass de tridente.
- Edite la etiqueta de trident-snapshotclass y configúrela en **velero.io/csi-volumesnapshot-class=true** como se muestra a continuación.

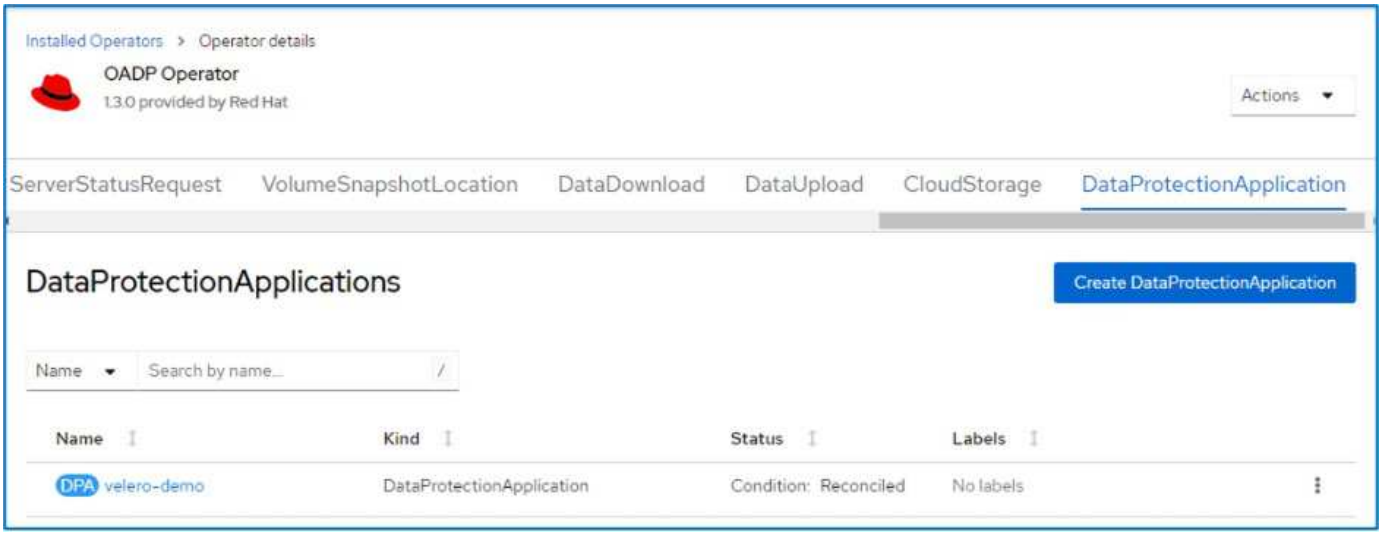


Asegúrese de que las instantáneas puedan persistir incluso si se eliminan los objetos VolumeSnapshot. Esto se puede hacer configurando **deletionPolicy** en Retener. De lo contrario, al eliminar un espacio de nombres se perderán por completo todos los PVC respaldados en él.

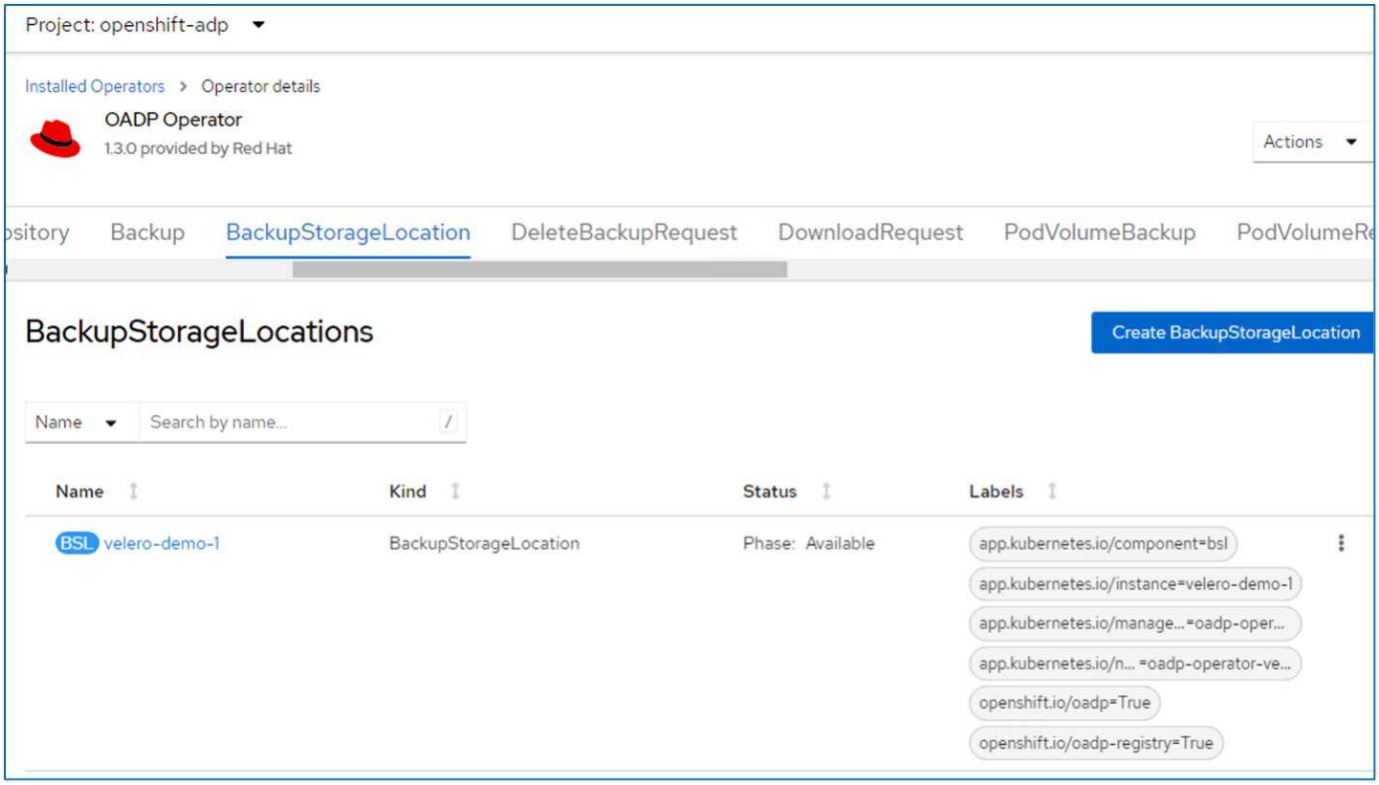
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Asegúrese de que la aplicación DataProtectionApplication se haya creado y esté en condición: Reconciliada.



El operador OADP creará un BackupStorageLocation correspondiente. Este se utilizará al crear una copia de seguridad.



Creación de copias de seguridad a pedido para aplicaciones en OpenShift Container Platform

En esta sección se describe cómo crear copias de seguridad a pedido para máquinas virtuales en OpenShift Virtualization.

Pasos para crear una copia de seguridad de una aplicación

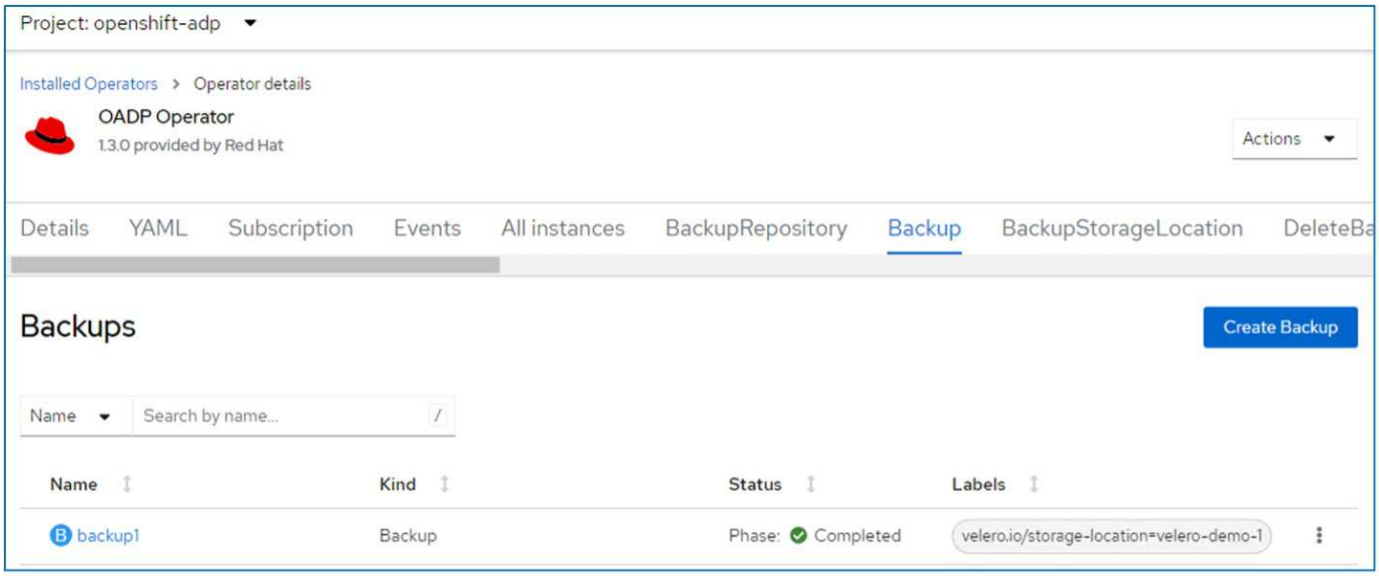
Para crear una copia de seguridad bajo demanda de una aplicación (metadatos de la aplicación y volúmenes persistentes de la aplicación), haz clic en la pestaña **Backup** para crear un Backup Custom Resource (CR). Se proporciona un ejemplo de yaml para crear el Backup CR. Con este yaml, harás una copia de seguridad de la aplicación y de su almacenamiento persistente en el namespace especificado. Puedes configurar parámetros adicionales, como se muestra en "documentación".

El CSI creará una instantánea de los volúmenes persistentes y de los recursos de la aplicación en el espacio de nombres especificado. Esta instantánea se almacenará en la ubicación de respaldo especificada en el yaml. La copia de seguridad permanecerá en el sistema durante 30 días según lo especificado en el TTL.

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
```

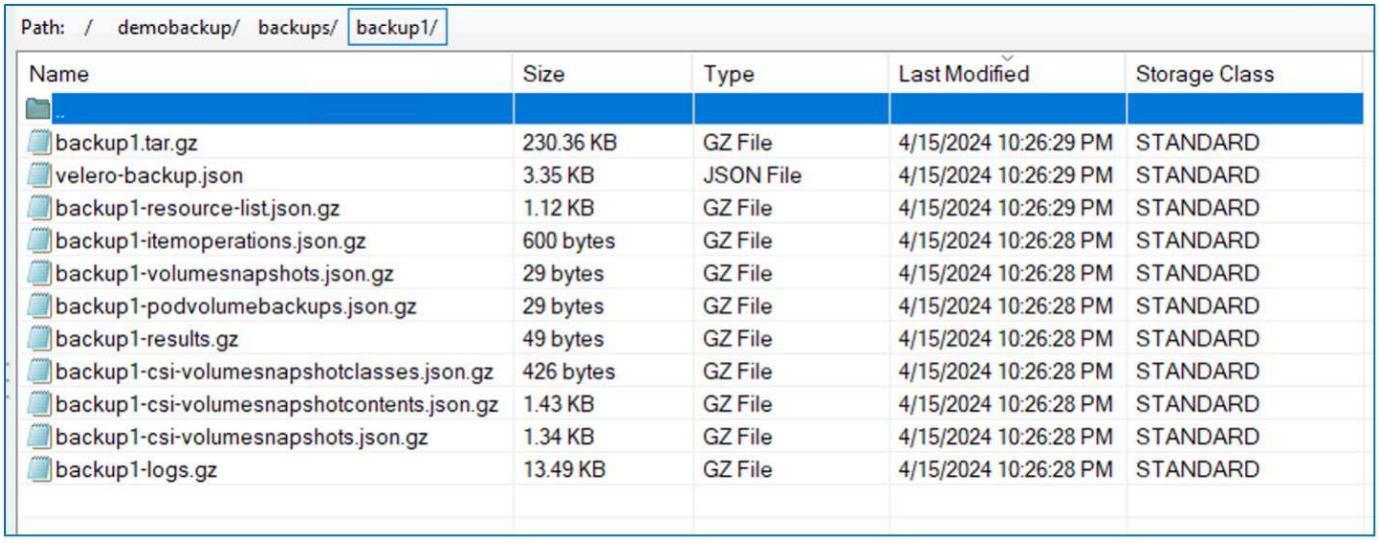
```
  ttl: 720h0m0s
```

Una vez que se complete la copia de seguridad, su fase se mostrará como completada.



Puede inspeccionar la copia de seguridad en el almacenamiento de objetos con la ayuda de una aplicación de navegador S3. La ruta de la copia de seguridad aparece en el depósito configurado con el nombre de prefijo (velero/container-demo-backup). Puede ver que el contenido de la copia de seguridad incluye las instantáneas de volumen, los registros y otros metadatos de la aplicación.

En StorageGrid, también puede utilizar la consola S3 que está disponible en el Administrador de inquilinos para ver los objetos de respaldo.



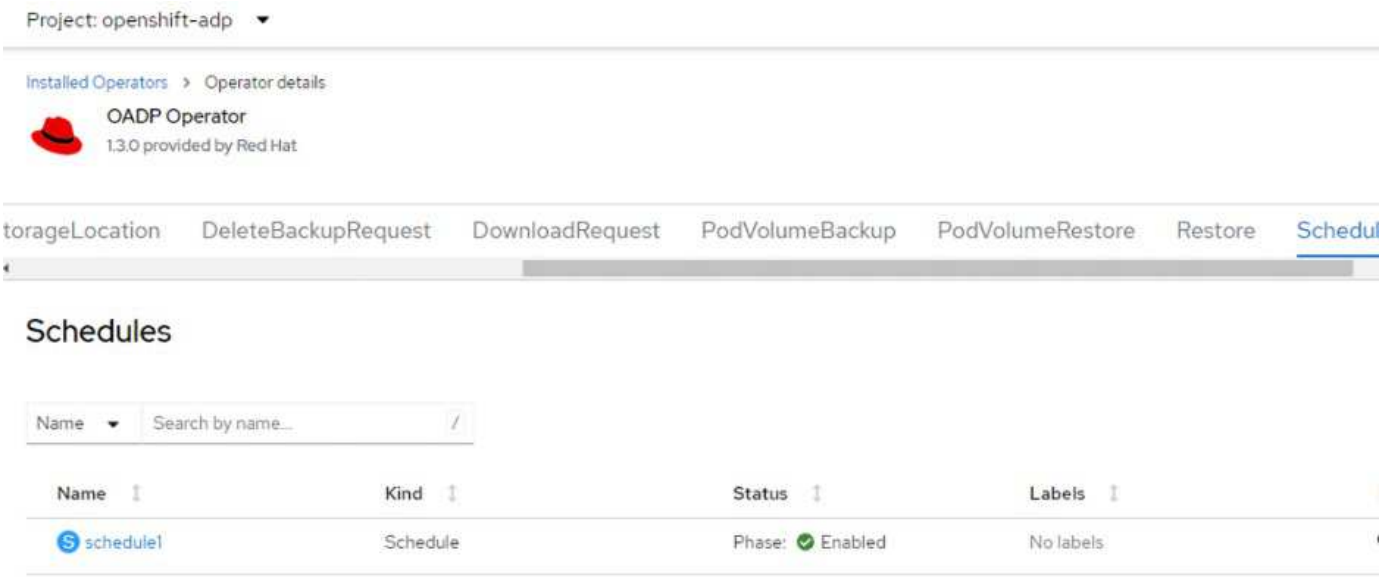
Creación de copias de seguridad programadas para aplicaciones

Para crear copias de seguridad según un cronograma, debe crear una CR programada. La programación es simplemente una expresión Cron que le permite especificar la hora en la que desea crear la copia de seguridad. A continuación se muestra un ejemplo de yaml para crear un CR de programación.

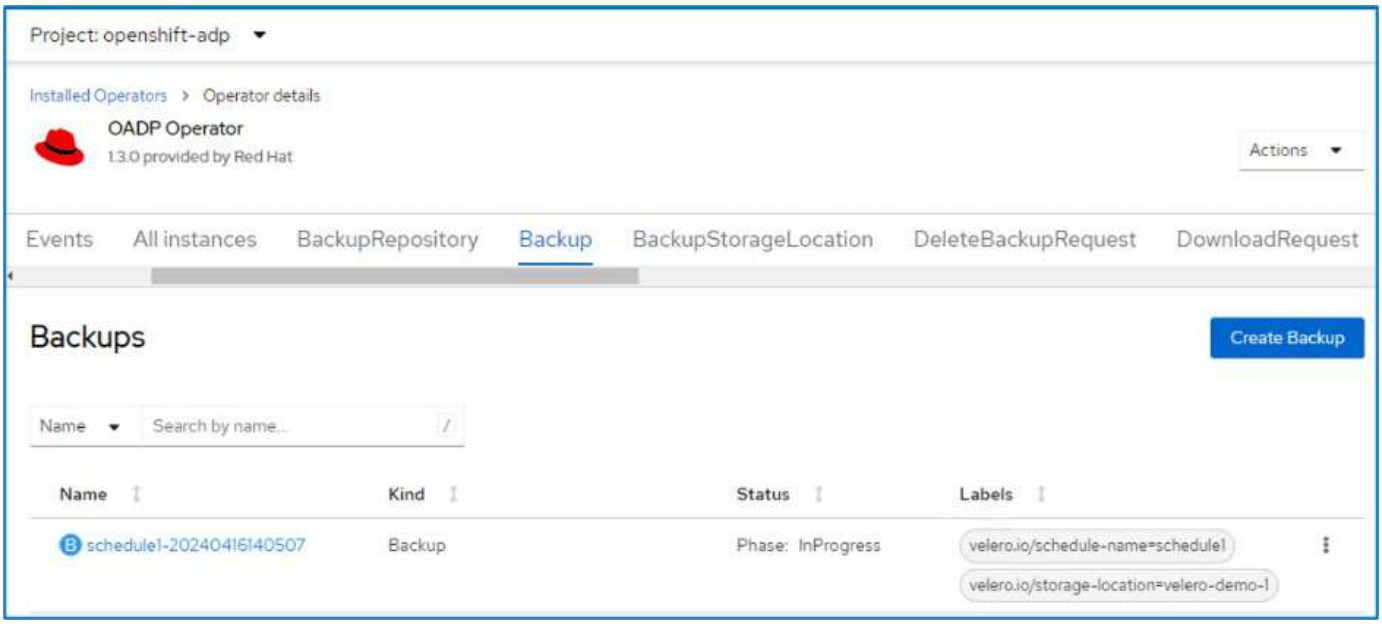
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

La expresión Cron 0 7 * * * significa que se creará una copia de seguridad a las 7:00 todos los días. También se especifican los espacios de nombres que se incluirán en la copia de seguridad y la ubicación de almacenamiento para la copia de seguridad. Entonces, en lugar de una CR de respaldo, se utiliza una CR programada para crear una copia de seguridad en el momento y frecuencia especificados.

Una vez creado el cronograma, se habilitará.



Se crearán copias de seguridad según este cronograma y se podrán ver desde la pestaña Copia de seguridad.



Migrar una aplicación de un clúster a otro

Las capacidades de respaldo y restauración de Velero lo convierten en una herramienta valiosa para migrar sus datos entre clústeres. Esta sección describe cómo migrar aplicaciones de un clúster a otro creando una copia de seguridad de la aplicación en el almacenamiento de objetos de un clúster y luego restaurando la aplicación desde el mismo almacenamiento de objetos a otro clúster. .

▼ **Copia de seguridad del primer clúster**

Requisitos previos del clúster 1

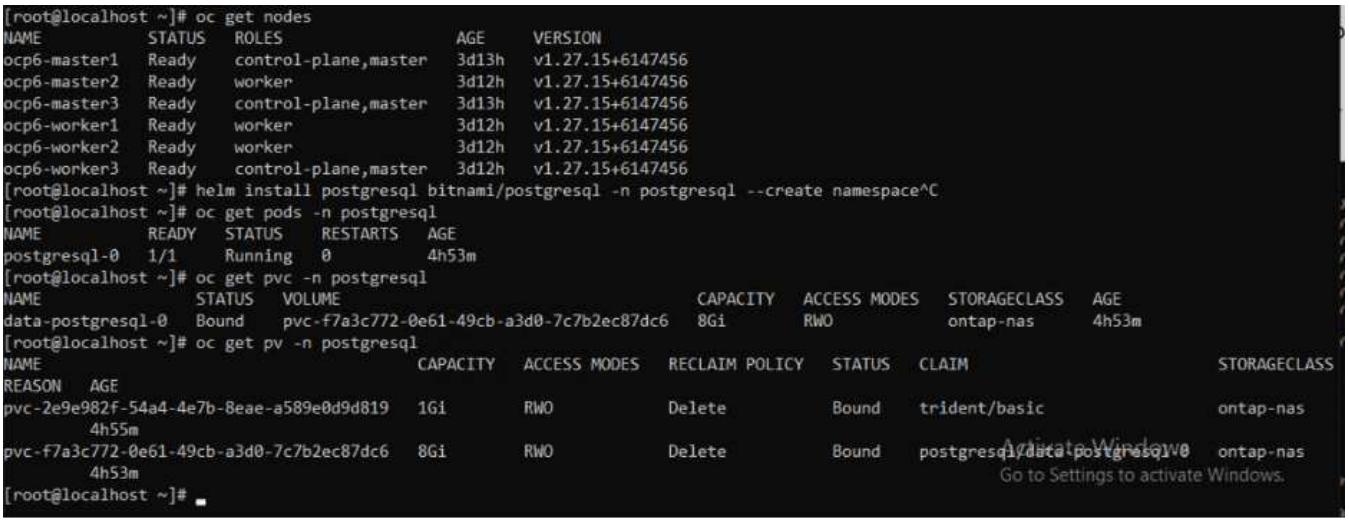
- Trident debe estar instalado en el clúster.
- Se debe crear un backend trident y una clase de almacenamiento.
- El operador OADP debe estar instalado en el clúster.
- La aplicación DataProtectionApplication debe estar configurada.

Utilice la siguiente especificación para configurar el objeto DataProtectionApplication.

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
```

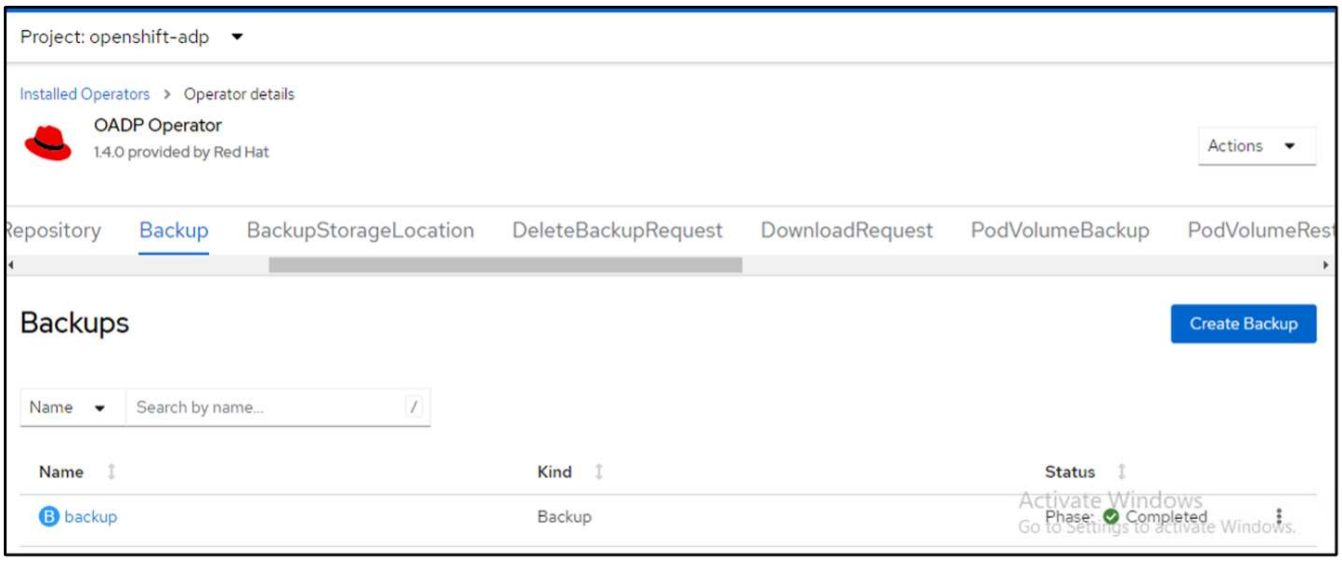
```
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

- Cree una aplicación en el clúster y realice una copia de seguridad de esta aplicación. A modo de ejemplo, instale una aplicación postgres.



- Utilice la siguiente especificación para la CR de respaldo:

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



Puede hacer clic en la pestaña **Todas las instancias** para ver los diferentes objetos que se están creando y pasando por diferentes fases para finalmente llegar a la fase de copia de seguridad **completada**.

Se almacenará una copia de seguridad de los recursos en el espacio de nombres postgresql en la ubicación de almacenamiento de objetos (ONTAP S3) especificada en backupLocation en la especificación OADP.

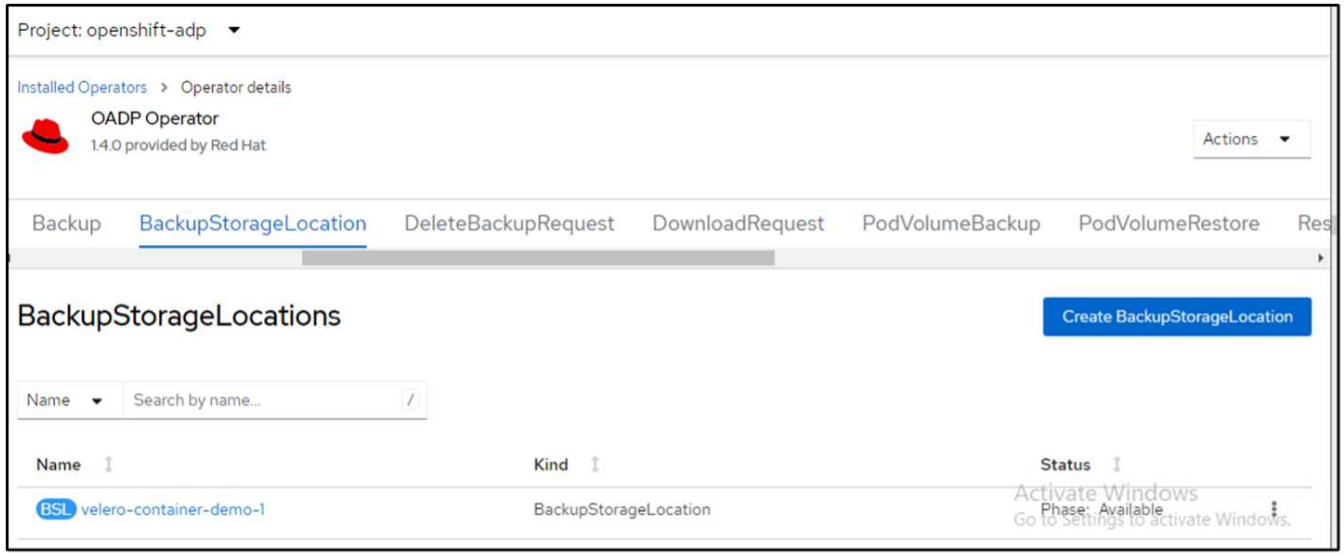
▼ **Restaurar a un segundo clúster**

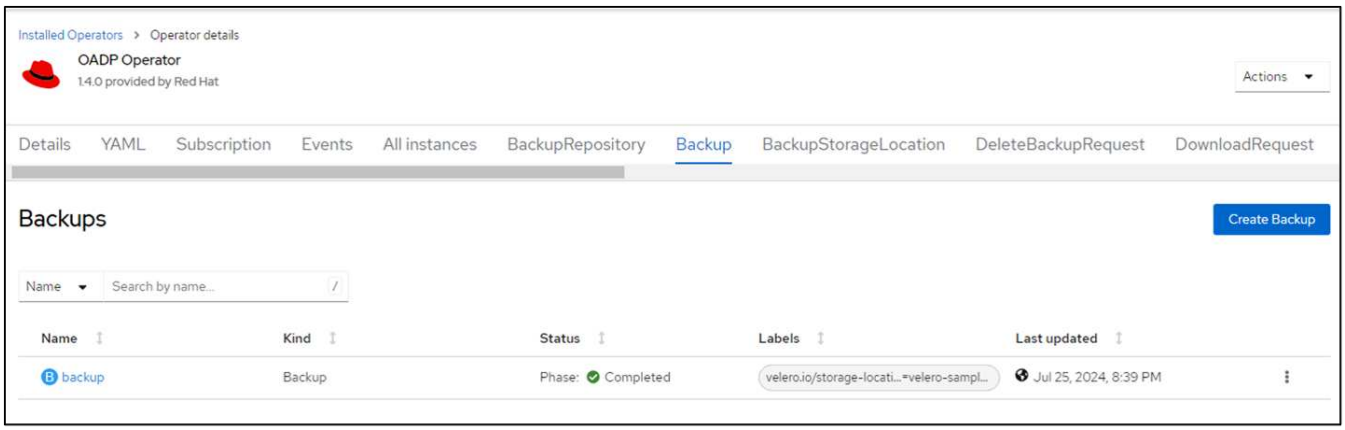
Requisitos previos del clúster 2

- Trident debe estar instalado en el clúster 2.
- La aplicación postgresql NO debe estar ya instalada en el espacio de nombres postgresql.
- El operador OADP debe estar instalado en el clúster 2, y la ubicación de BackupStorage debe apuntar a la misma ubicación de almacenamiento de objetos donde se almacenó la copia de seguridad del primer clúster.
- El CR de respaldo debe ser visible desde el segundo clúster.

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic        ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc     vsphere-sc              2d7
h
[root@localhost ~]#
```



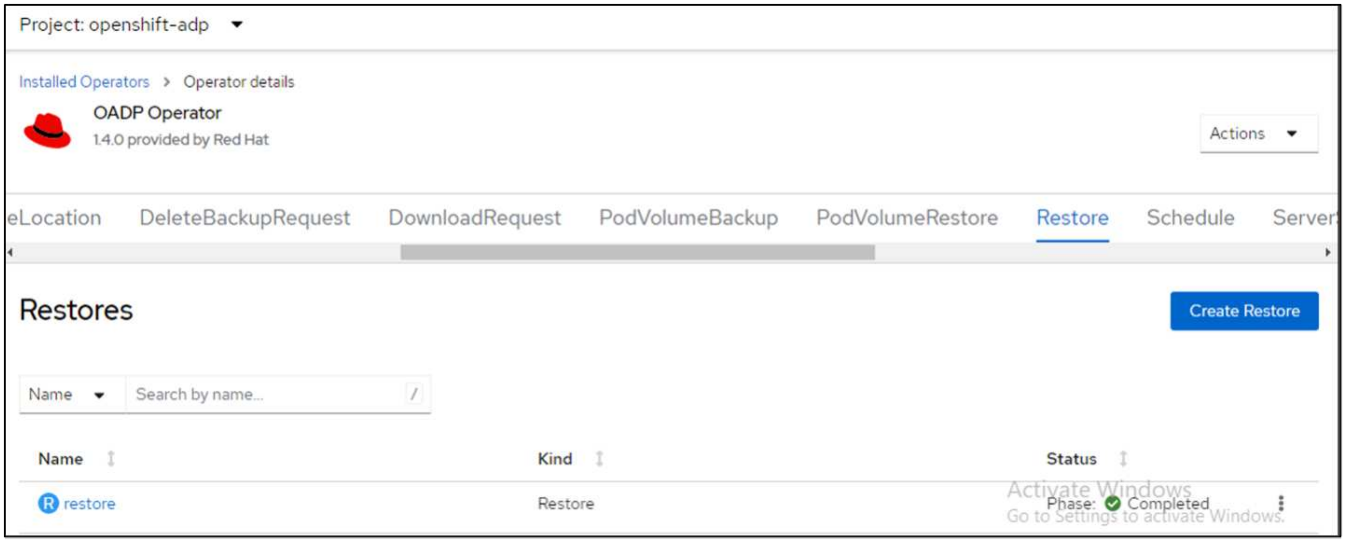


Restaurar la aplicación en este clúster desde la copia de seguridad. Utilice el siguiente yaml para crear el CR de restauración.

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
```

```
spec:
  backupName: backup
  restorePVs: true
```

Cuando se complete la restauración, verá que la aplicación postgresql se está ejecutando en este clúster y está asociada con el pvc y un pv correspondiente. El estado de la aplicación es el mismo que cuando se realizó la copia de seguridad.




```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                  AGE    VERSION
ocp7-master1  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3  Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME              STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                           STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                   ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0    ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc                vsphere-sc
         2d10h
[root@localhost ~]#
```

Restaurar una aplicación desde una copia de seguridad

Esta sección describe cómo restaurar aplicaciones desde una copia de seguridad.

Prerrequisitos

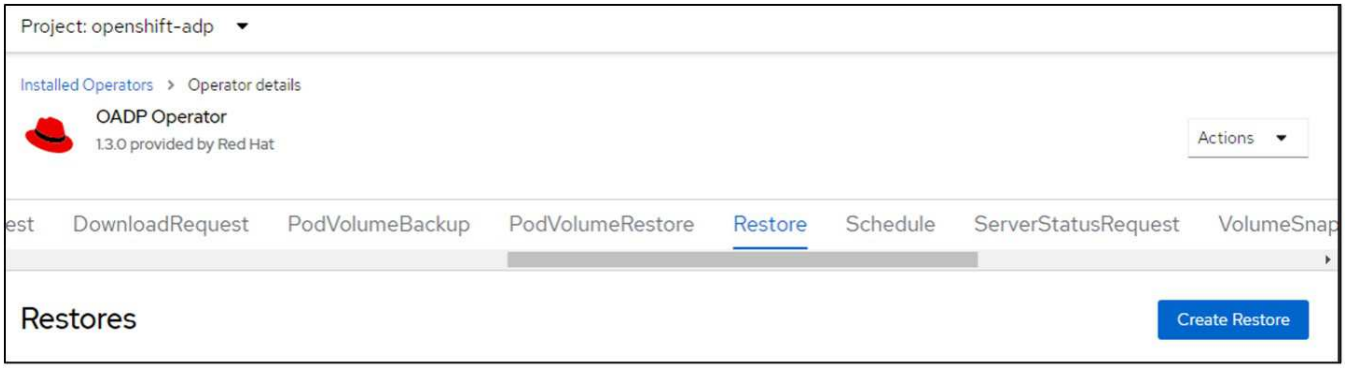
Para restaurar desde una copia de seguridad, supongamos que el espacio de nombres donde existía la aplicación se eliminó accidentalmente.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

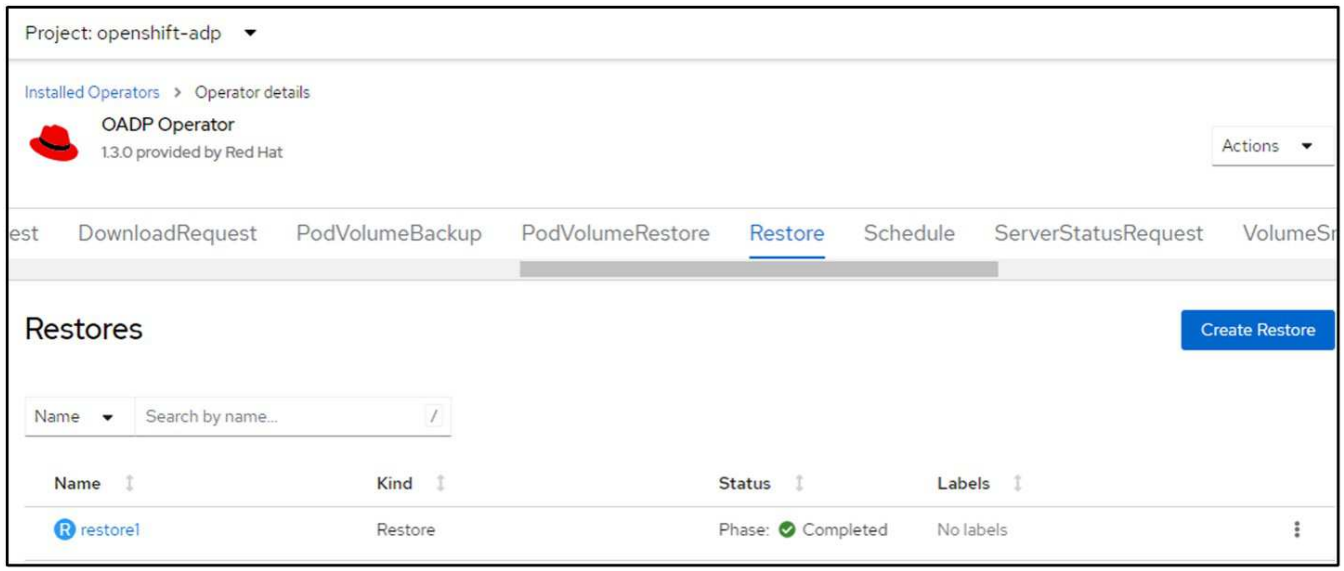
▼ **Restaurar al mismo espacio de nombres**

Para restaurar desde la copia de seguridad que acabamos de crear, tienes que crear un Restore Custom Resource (CR). Tienes que darle un nombre, indicar el nombre de la copia de seguridad desde la que quieres restaurar y establecer restorePVs en true. Puedes configurar parámetros adicionales como se muestra en "documentación". Haz clic en el botón Create.




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

Cuando la fase se muestra completada, puedes ver que la aplicación se ha restaurado al estado en el que se tomó la instantánea. La aplicación se restaura al mismo espacio de nombres.




```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

▼ **Restaurar a un espacio de nombres diferente**

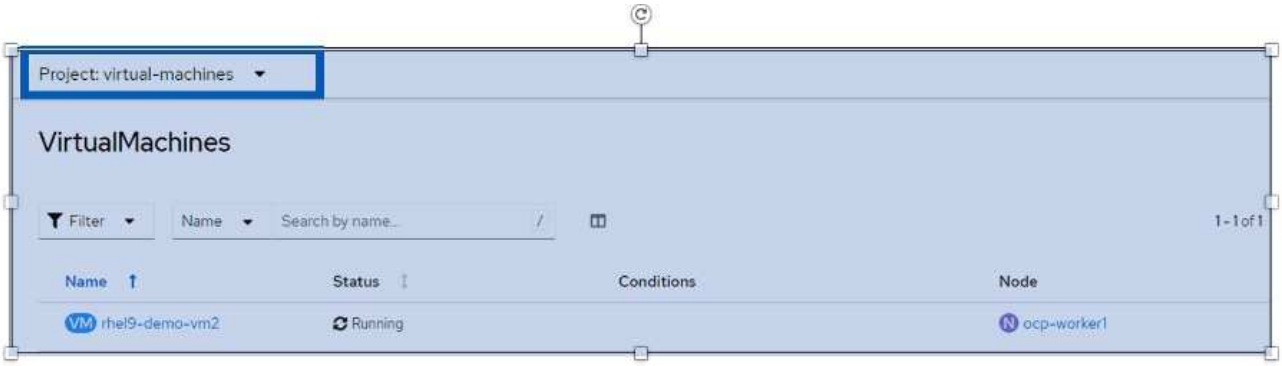
Para restaurar la aplicación a un espacio de nombres diferente, puedes proporcionar un namespaceMapping en la definición yaml del CR de restauración.

El siguiente archivo yaml de muestra crea un CR de restauración para restaurar una aplicación y su almacenamiento persistente desde el espacio de nombres postgresql al nuevo espacio de nombres postgresql-restored.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
```

```
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

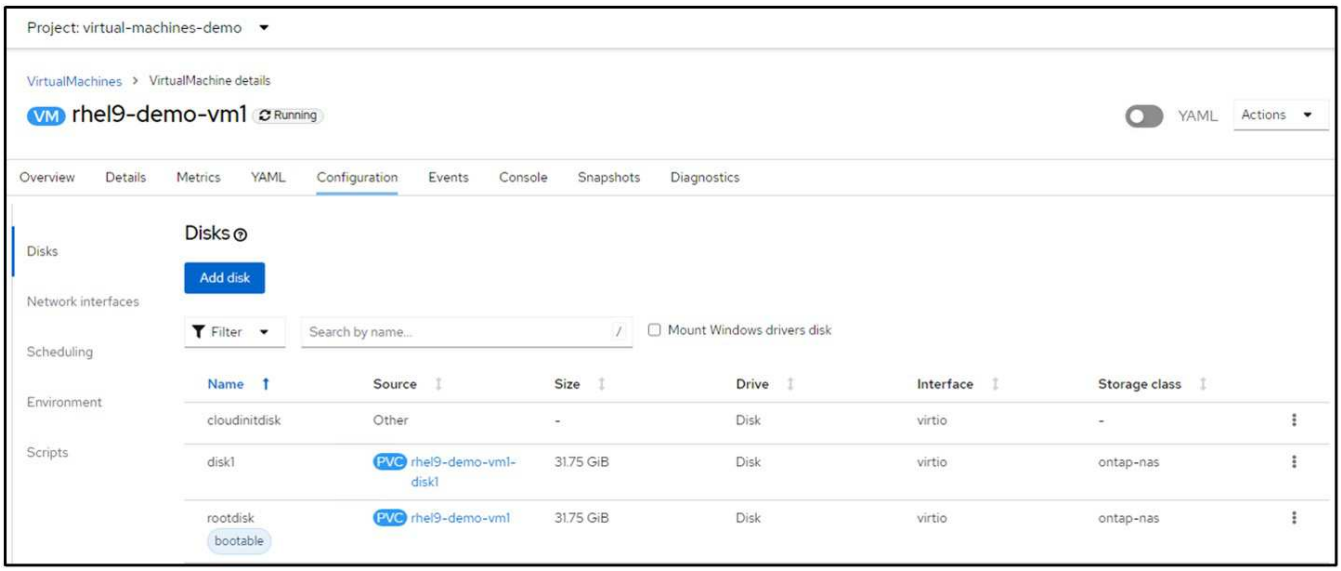
Cuando la fase se muestra completada, puedes ver que la aplicación se ha restaurado al estado en el que se tomó la instantánea. La aplicación se restaura a un espacio de nombres diferente según lo especificado en el yaml.

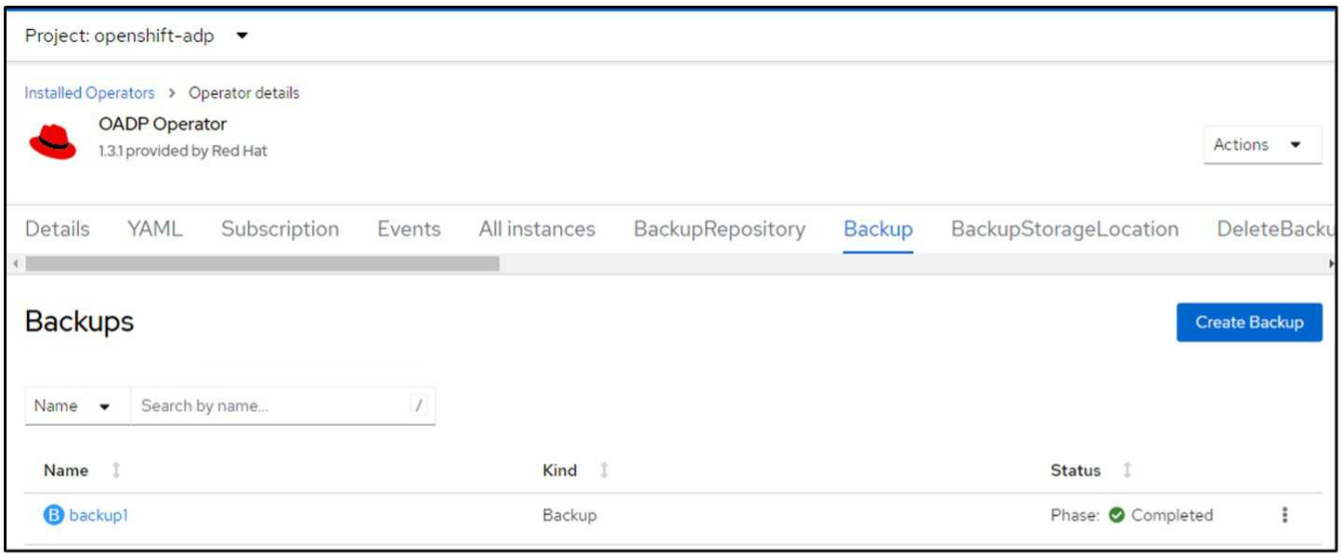


▼ **Restaurar a una clase de almacenamiento diferente**

Velero proporciona una capacidad genérica para modificar los recursos durante la restauración especificando parches json. Los parches json se aplican a los recursos antes de restaurarlos. Los parches json se especifican en un mapa de configuración y el mapa de configuración se referencia en el comando de restauración. Esta función le permite restaurar utilizando diferentes clases de almacenamiento.

En el siguiente ejemplo, la aplicación, durante la implementación, utiliza ontap-nas como clase de almacenamiento para sus volúmenes persistentes. Se crea una copia de seguridad de la aplicación llamada backup-postgresql-ontaps3.





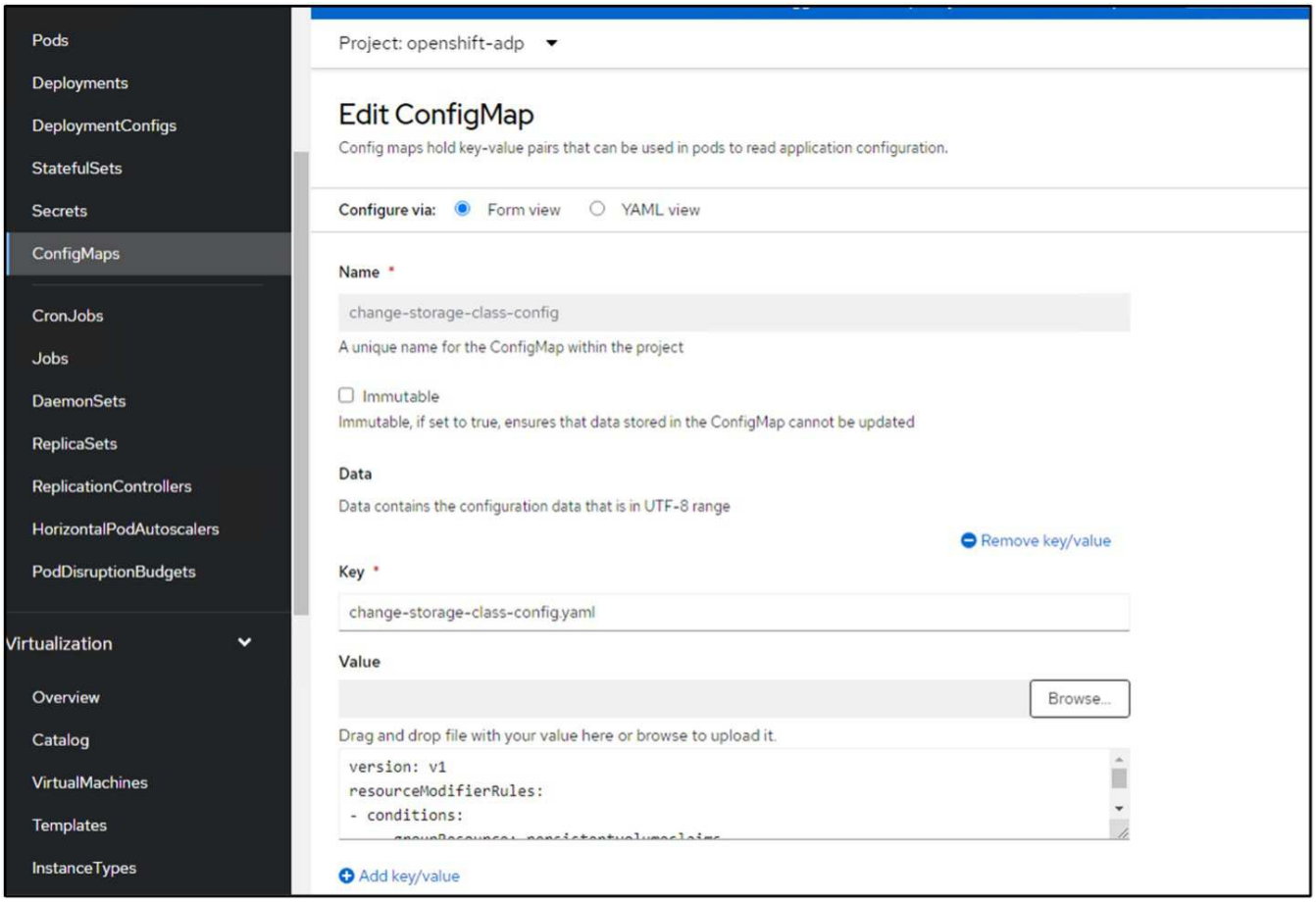
Simular una pérdida de la aplicación desinstalándola.

Para restaurar la máquina virtual utilizando una clase de almacenamiento diferente, por ejemplo, la clase de almacenamiento ontap-nas-eco, debe realizar los siguientes dos pasos:

Paso 1

Cree un mapa de configuración (consola) en el espacio de nombres openshift-adp de la siguiente manera: Complete los detalles como se muestra en la captura de pantalla: Seleccione el espacio de nombres: openshift-adp Nombre: change-ontap-sc (puede ser cualquier nombre) Clave: change-ontap-sc-config.yaml: Valor:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



El objeto de mapa de configuración resultante debería verse así (CLI):

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"


BinaryData
====

Events:  <none>
```

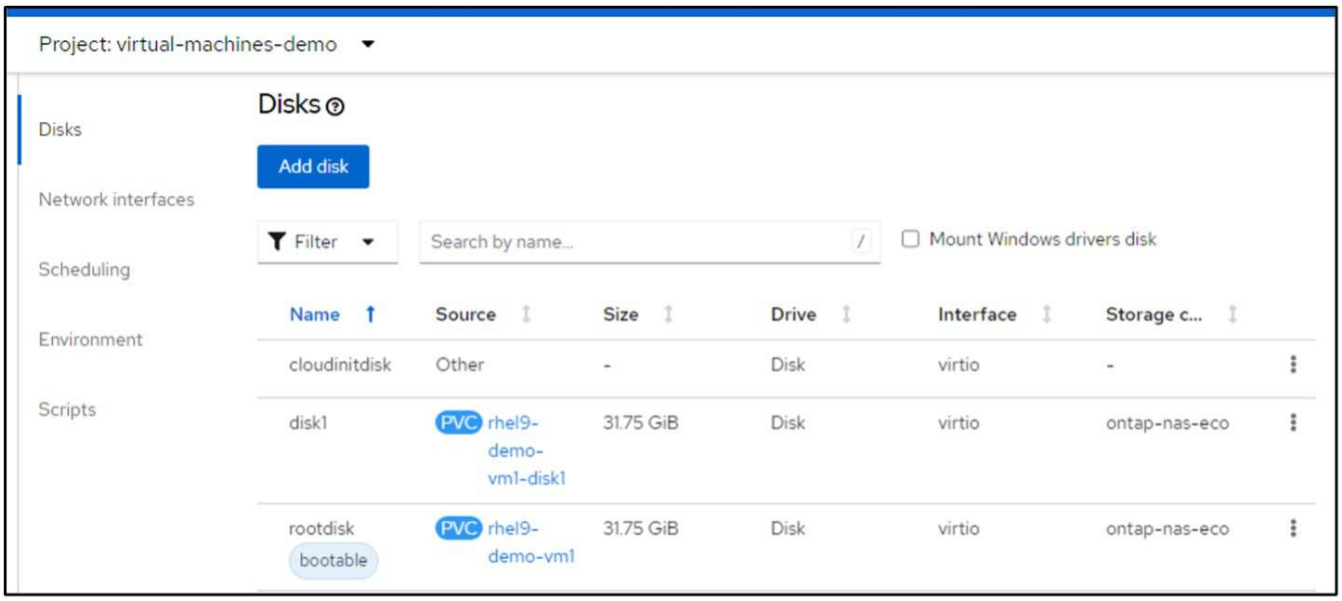
Este mapa de configuración aplicará la regla de modificación de recursos cuando se cree la restauración. Se aplicará un parche para reemplazar el nombre de la clase de almacenamiento a ontap-nas-eco para todos los reclamos de volumen persistente que comiencen con rhel.

Paso 2

Para restaurar la máquina virtual, utilice el siguiente comando desde la CLI de Velero:

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

La aplicación se restaura en el mismo espacio de nombres con las reclamaciones de volumen persistentes creadas utilizando la clase de almacenamiento ontap-nas-eco.



Eliminar copias de seguridad y restauraciones al usar Velero

Esta sección describe cómo eliminar copias de seguridad y restauraciones de aplicaciones en la plataforma de contenedores OpenShift usando Velero.

Listar todas las copias de seguridad

Puede enumerar todos los CR de respaldo mediante la herramienta CLI de OC o la herramienta CLI de Velero. Descargue Velero CLI como se indica en las instrucciones en el"Documentación de Velero" .

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Eliminar una copia de seguridad

Puede eliminar un CR de respaldo sin eliminar los datos de almacenamiento de objetos mediante la herramienta CLI de OC. La copia de seguridad se eliminará de la salida de CLI/Consola. Sin embargo, dado que la copia de seguridad correspondiente no se elimina del almacenamiento de objetos, volverá a aparecer en la salida de la CLI/consola.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

Si desea eliminar la copia de seguridad CR y los datos de almacenamiento de objetos asociados, puede hacerlo utilizando la herramienta CLI de Velero.

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                       Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Eliminar la restauración

Puede eliminar el objeto CR de restauración mediante la CLI de OC o la CLI de Velero

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

Vea videos y demostraciones sobre soluciones multicloud híbridas con NetApp

Vea videos sobre soluciones multicloud híbridas para Amazon Web Services con NetApp

Explore la completa videoteca de NetApp que presenta soluciones multicloud híbridas para AWS con NetApp. Mire videos sobre almacenamiento conectado para invitados, ahorros en TCO, almacenes de datos complementarios y flujos de trabajo de migración para VMware Cloud on AWS y Amazon FSx para ONTAP, incluidos escenarios de Windows y Linux.

Almacenamiento conectado para invitados

Almacenamiento conectado invitado de Windows con FSx ONTAP mediante iSCSI

Almacenamiento invitado conectado de Linux con FSx ONTAP mediante NFS

TCO y almacenes de datos complementarios

Ahorros en el TCO de VMware Cloud on AWS con Amazon FSx ONTAP

Almacén de datos complementario de VMware Cloud on AWS con Amazon FSx ONTAP

Flujos de trabajo de migración (HCX)

Configuración e implementación de VMware HCX para VMC

Demostración de migración de vMotion con VMware HCX para VMC y FSx ONTAP

Demostración de migración en frío con VMware HCX para VMC y FSx ONTAP

Vea videos sobre soluciones multicloud híbridas para Azure VMware Cloud con NetApp

Explore la completa biblioteca de videos de NetApp que presenta soluciones multicloud híbridas para Azure VMware Solution (AVS) con NetApp. Esta colección incluye videos sobre almacenes de datos complementarios, recuperación ante desastres y flujos de trabajo de migración.

Almacenes de datos complementarios

Descripción general del almacén de datos complementario de Azure VMware Solution con Azure NetApp Files

Recuperación ante desastres

Azure VMware Solution DR con Cloud Volumes ONTAP, SnapCenter y JetStream

Flujos de trabajo de migración (HCX)

Demostración de migración en frío con VMware HCX para AVS y ANF

Demostración de vMotion con VMware HCX para AVS y ANF

Demostración de migración masiva con VMware HCX para AVS y ANF

Vea videos sobre soluciones multicloud híbridas para Red Hat OpenShift con NetApp

Explore la completa videoteca de NetApp que presenta soluciones multicloud híbridas para Red Hat OpenShift con NetApp. Esta colección incluye demostraciones sobre instantáneas y restauración para OpenShift en AWS (ROSA) con FSx ONTAP, integración con Trident, conmutación por error y recuperación para aplicaciones, e implementación automatizada de Oracle RAC en FlexPod con Ansible.

Instantáneas y restauración

Instantánea/restauración para aplicaciones en clústeres de Red Hat OpenShift Service en AWS (ROSA) con almacenamiento de Amazon FSx ONTAP

Integración de almacenamiento

Integración de FSx ONTAP con Trident

Conmutación por error y recuperación

Conmutación por error y recuperación de aplicaciones en ROSA con FSx ONTAP

Automatización de soluciones



Implementación automatizada de Oracle 19c RAC en FlexPod con Ansible

Lea blogs de soluciones en la nube de expertos de NetApp

Lea los blogs que ofrecen orientación práctica y mejores prácticas para integrar el almacenamiento ONTAP con las soluciones de nube de NetApp .

Integración de VMware con AWS y Amazon FSx para ONTAP

- "Migre máquinas virtuales de VMware a AWS mediante el protocolo iSCSI de Amazon EC2 y Amazon FSx ONTAP"
- "Amazon EVS ahora se integra con FSx para ONTAP"
- "Amazon EVS anuncia compatibilidad con FSx para ONTAP"
- "Configurar la nube híbrida con FSx ONTAP y VMware Cloud en AWS SDDC mediante VMware HCX"

Solución VMware de Azure

- "Optimiza el almacenamiento y las cargas de trabajo de VMware con uso intensivo de datos en cualquier cloud"
- "¿VMware workloads to Azure VMware Solution? Lee esto primero."

Motor VMware de Google Cloud

- "Compatibilidad del almacén de datos de Google Cloud NetApp Volumes con Google Cloud VMware Engine (NetApp)"
- "Cómo usar NetApp Volumes como almacenes de datos para Google Cloud VMware Engine (Google)"
- "Blog de NetApp : Una mejor manera de migrar sus aplicaciones con gran capacidad de almacenamiento a Google Cloud"

Protección y gestión de datos

- "3-2-1 protección de datos para VMware con SnapCenter Plug-in y NetApp Backup and Recovery para las VM"
- "Observabilidad para el centro de datos moderno con NetApp Cloud Insights"

NetApp para cargas de trabajo de contenedores OpenShift

- "NetApp ONTAP también funciona como almacenamiento de registros en la plataforma de contenedores Red Hat OpenShift"

Nube soberana de VMware

- "Presentamos la nueva iniciativa Sovereign Cloud"

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de Marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Puede encontrar una lista actualizada de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Información de copyright

Copyright © 2026 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.