Cloud público e híbrido

NetApp Solutions

NetApp
May 10, 2024

Tabla de contenidos

Cloud público e híbrido 1
Multicloud híbrido de NetApp con soluciones de VMware 1
Nube soberana de VMware 500
Multicloud híbrido de NetApp con cargas de trabajo de contenedores de Red Hat OpenShift 502

Cloud público e híbrido

Multicloud híbrido de NetApp con soluciones de VMware

VMware para el cloud público

Información general del multicloud híbrido de NetApp con VMware

La mayoría de las organizaciones DE TECNOLOGÍA siguen el enfoque de «cloud híbrido primero». Estas organizaciones se encuentran en una fase de transformación, y los clientes evalúan su entorno TECNOLÓGICO actual y, posteriormente, migran sus cargas de trabajo al cloud según el proceso de evaluación y detección.

Los factores para que los clientes migren a la nube pueden ser la elasticidad y la ráfaga, la salida del centro de datos, la consolidación del centro de datos, escenarios de fin de la vida útil, las fusiones, adquisiciones, etc. El motivo de esta migración puede variar en función de cada organización y sus respectivas prioridades empresariales. A la hora de trasladarse al cloud híbrido, elegir el almacenamiento adecuado en el cloud es muy importante para aprovechar el poder de la implementación y la elasticidad del cloud.

Opciones de cloud de VMware en el cloud público

En esta sección se describe cómo cada uno de los proveedores de cloud admite una pila de centro de datos definido por software (SDDC) de VMware y/o Cloud Foundation (VCF) en sus respectivas ofertas de cloud público.

Solución Azure VMware

La solución de VMware para Azure es un servicio de cloud híbrido que permite centros de datos SDDC de VMware completamente funcionales dentro del cloud público de Microsoft Azure. Azure VMware Solution es una solución de primera parte totalmente gestionada y con soporte de Microsoft, verificada por VMware aprovechando la infraestructura de Azure. Esto significa que, cuando se pone en marcha la solución VMware para Azure, el cliente obtiene ESXi de VMware para virtualización informática, VSAN para almacenamiento hiperconvergente NSX y NSX para redes y seguridad, todo ello al tiempo que aprovecha la presencia global de Microsoft Azure, las mejores instalaciones de los centros de datos de su clase y la proximidad al amplio ecosistema de servicios y soluciones de Azure nativos.

VMware Cloud en AWS

VMware Cloud en AWS aporta el software SDDC empresarial de VMware al cloud de AWS con acceso optimizado a los servicios nativos de AWS. Con la tecnología de VMware Cloud Foundation, VMware Cloud en AWS integra los productos de virtualización de redes, almacenamiento e informática de VMware (vSphere de VMware, VSAN de VMware y NSX de VMware) junto con la gestión de VMware vCenter Server, optimizada para ejecutarse en una infraestructura de AWS dedicada, elástica y con configuración básica.

Motor de Google Cloud VMware

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 de VMware Cloud Foundation: VMware vSphere, vCenter, VSAN y NSX-T. Este servicio posibilita una ruta rápida al cloud, que migra o amplía sin problemas las cargas de trabajo de VMware existentes de entornos en las instalaciones a Google Cloud Platform sin los costes, el esfuerzo o el riesgo de volver a crear la arquitectura de aplicaciones o cambiar las herramientas. Se trata de un servicio que vende y recibe soporte de Google, en estrecha colaboración con VMware.

El cloud privado SDDC y la colocación de Cloud Volumes de NetApp proporcionan el mejor rendimiento con una latencia de red mínima.

¿Sabía esto?

Independientemente del cloud utilizado, cuando se pone en marcha un SDDC de VMware, el clúster inicial incluye los siguientes productos:

- Hosts VMware ESXi para virtualización de recursos informáticos con un dispositivo vCenter Server para gestión
- Almacenamiento hiperconvergente VSAN de VMware que incorpora los activos de almacenamiento físico de cada host ESXi
- NSX de VMware para redes virtuales y seguridad con un clúster de NSX Manager para la gestión

Configuración del almacenamiento

Para los clientes que planean alojar cargas de trabajo intensivas del almacenamiento y escalar horizontalmente en cualquier solución VMware alojada en el cloud, la infraestructura hiperconvergente predeterminada dicta que la expansión se haga en los recursos de computación y almacenamiento.

Al integrarse con NetApp Cloud Volumes, como Azure NetApp Files, Amazon FSX para NetApp ONTAP, Cloud Volumes ONTAP (disponible en los tres principales proveedores a hiperescala) y Cloud Volumes Service para Google Cloud, los clientes ahora tienen opciones para escalar su almacenamiento de forma independiente, Y solo añada nodos de computación al clúster SDDC según sea necesario.

Notas:

- VMware no recomienda configuraciones de clúster desequilibradas, por lo que ampliar el almacenamiento significa añadir más hosts, lo que implica más 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 una opción para proporcionar varios niveles de rendimiento con el fin de alinear los requisitos de las aplicaciones, el rendimiento y el coste.
- Es muy fácil llegar a los límites de la capacidad de almacenamiento de VSAN creada sobre los hosts del clúster. Utilice Cloud Volumes de NetApp para escalar el almacenamiento para alojar conjuntos de datos activos o organizar los datos en niveles en el almacenamiento persistente.

Azure NetApp Files, Amazon FSX para NetApp ONTAP, Cloud Volumes ONTAP (disponible en los tres

principales proveedores a hiperescala) y Cloud Volumes Service para Google Cloud se pueden utilizar en combinación con las máquinas virtuales invitadas. Esta arquitectura de almacenamiento híbrido consta de un almacén de datos VSAN que contiene el sistema operativo invitado y datos binarios de aplicaciones. Los datos de la aplicación se conectan a la máquina virtual a través de un iniciador iSCSI basado en invitados o los montajes NFS/SMB que se comunican directamente con Amazon FSX para ONTAP de NetApp, Cloud Volume ONTAP, Azure NetApp Files y Cloud Volumes Service para Google Cloud respectivamente. Esta configuración le permite superar con facilidad los retos que plantea la capacidad de almacenamiento, al igual que VSAN, el espacio libre disponible depende de las políticas de almacenamiento y espacio de Slack utilizadas.

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

- La capacidad bruta total para un SDDC de tres nodos = 31,1 TB (aproximadamente 10 TB para cada nodo).
- El espacio de demora que se debe mantener antes de que se añadan hosts adicionales = 25% = (.25 x 31,1 TB) = 7,7 TB.
- La capacidad bruta utilizable tras la deducción de espacio libre = 23,4 TB
- El espacio libre efectivo disponible depende de la normativa 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 útil/2)
  - RAID 5 = espacio libre efectivo = 17,5 TB (capacidad bruta utilizable/1.33)

Por este motivo, el uso de Cloud Volumes de NetApp como almacenamiento conectado al invitado ayudaría a ampliar el almacenamiento y optimizar el TCO cumpliendo con los requisitos de rendimiento y protección de datos.

El almacenamiento en invitado era la única opción disponible en el momento de escribir este documento. A medida que esté disponible la compatibilidad complementaria con almacenes de datos NFS, estará disponible la documentación adicional "aquí".

Puntos que hay que recordar

- En los modelos de almacenamiento híbrido, coloque cargas de trabajo de nivel 1 o de alta prioridad en un almacén de datos VSAN para satisfacer cualquier requisito de latencia específica, ya que forman parte del host en sí y cerca de él. Utilice mecanismos «guest» para cualquier equipo virtual de carga de trabajo para el que se pueda aceptar latencias transaccionales.
- Utilice la tecnología SnapMirror® de NetApp para replicar los datos de la carga de trabajo del sistema ONTAP local en Cloud Volumes ONTAP o Amazon FSX para ONTAP de NetApp con el fin de facilitar la migración mediante mecanismos de nivel de bloque. Esto no se aplica a Azure NetApp Files y Cloud Volumes Services. Para migrar datos a Azure NetApp Files o Cloud Volumes Services, utilice NetApp XCP, la copia y sincronización de BlueXP, rysnc o robocopy en función del protocolo de archivo utilizado.
- Las pruebas demuestran una latencia adicional de entre 2 y 4 ms al acceder al almacenamiento desde los respectivos centros de datos de dominio completo. Tenga en cuenta esta latencia adicional en los requisitos de las aplicaciones al asignar el almacenamiento.
- En el caso del montaje de almacenamiento conectado «guest» durante la conmutación por error de prueba y la conmutación en caso de recuperación en caso de fallo real, asegúrese de que los iniciadores iSCSI se vuelven a configurar, DNS se actualiza para los recursos compartidos SMB y los puntos de montaje NFS se actualizan en fstab.

- Asegúrese de que la configuración del registro de E/S multivía (MPIO), firewall y tiempo de espera de disco de Microsoft en invitado esté configurada correctamente dentro de la máquina virtual.

Esto solo se aplica al almacenamiento conectado como invitado.

Ventajas del almacenamiento en cloud de NetApp

El almacenamiento en cloud de NetApp ofrece las siguientes ventajas:

- Mejora la densidad de computación a almacenamiento escalando el almacenamiento con independencia de la capacidad de computación.
- Permite reducir el número de hosts, con lo que se reduce el TCO general.
- El fallo del nodo de computación no afecta al rendimiento de almacenamiento.
- La reformulación del volumen y la funcionalidad de nivel de servicio dinámica de Azure NetApp Files le permiten optimizar los costes ajustando el tamaño de las cargas de trabajo de estado constante y evitando, por tanto, el sobreaprovisionamiento.
- Las eficiencias del almacenamiento, la organización en niveles del cloud y las funcionalidades de modificación del tipo de instancia de Cloud Volumes ONTAP permiten formas óptimas de añadir y escalar almacenamiento.
- Evita el sobreaprovisionamiento de recursos de almacenamiento solo se añaden cuando es necesario.
- Le permiten crear copias y clones Snapshot eficientes sin que el rendimiento se vea afectado.
- Ayuda a gestionar los ataques de ransomware mediante una recuperación rápida de copias Snapshot.
- Proporciona una recuperación ante desastres regional, basada en la transferencia de bloques incremental y el nivel de bloque de backup integrado en las regiones proporciona un mejor RPO y RTO.

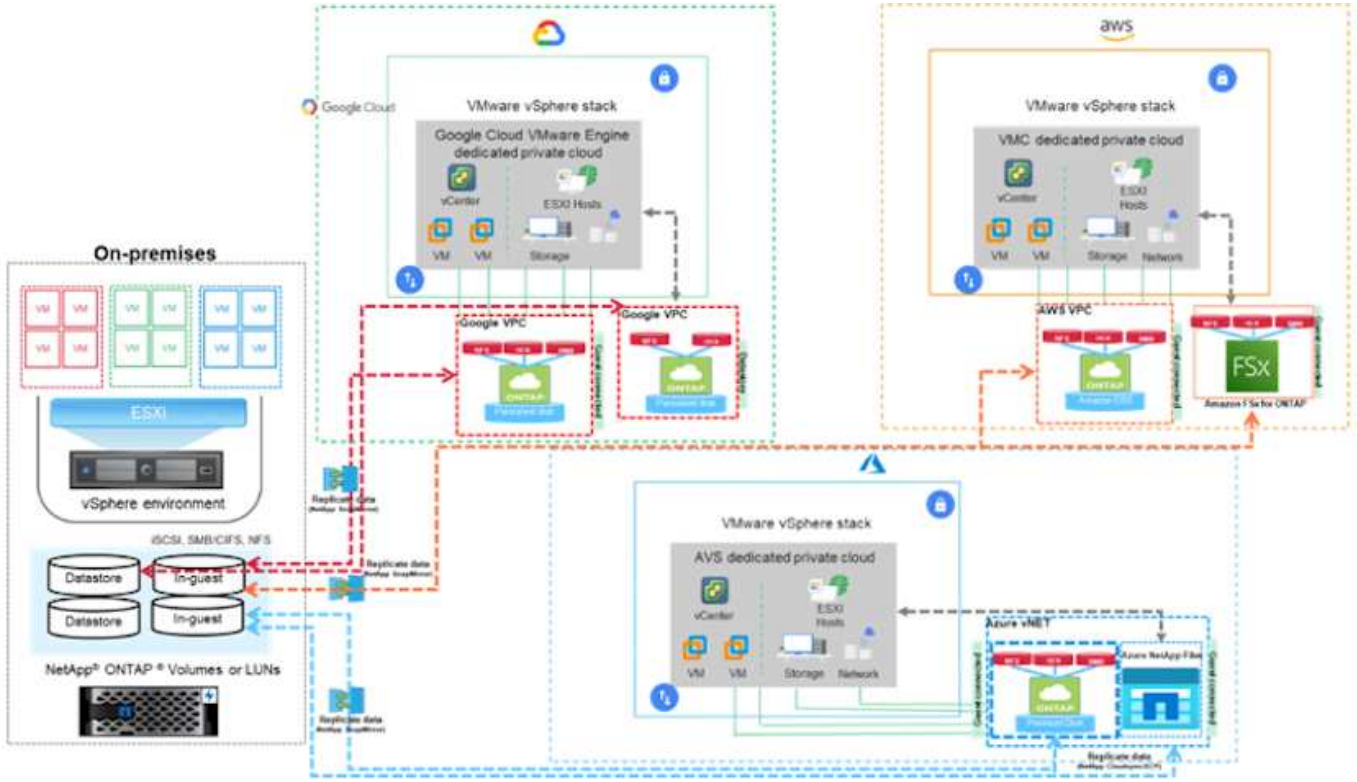
Supuestos

- Se habilita la tecnología SnapMirror u otros mecanismos de migración de datos relevantes. Hay muchas opciones de conectividad, desde las instalaciones hasta cualquier cloud a hiperescala. Utilice la ruta adecuada y trabaje con los equipos de redes pertinentes.
- El almacenamiento en invitado era la única opción disponible en el momento de escribir este documento. A medida que esté disponible la compatibilidad complementaria con almacenes de datos NFS, estará disponible la documentación adicional "aquí".

Involucre a los arquitectos de soluciones de NetApp y a los respectivos arquitectos de cloud a hiperescala para planificar y ajustar el tamaño del almacenamiento y al número necesario de hosts. NetApp recomienda identificar los requisitos de rendimiento del almacenamiento antes de utilizar el dimensionador Cloud Volumes ONTAP para finalizar el tipo de instancia de almacenamiento o el nivel de servicio adecuado con el rendimiento adecuado.

Arquitectura detallada

Desde el punto de vista más alto, esta arquitectura (que se muestra en la siguiente figura) aborda cómo lograr una conectividad multicloud híbrida y portabilidad de aplicaciones en múltiples proveedores de cloud utilizando Cloud Volumes ONTAP de NetApp, Cloud Volumes Service para Google Cloud y Azure NetApp Files como opción de almacenamiento en invitado adicional.



Soluciones de NetApp para VMware en proveedores a hiperescala

Obtenga más información acerca de las funcionalidades que NetApp aporta a los tres (3) proveedores a hiperescala principales, desde NetApp como dispositivo de almacenamiento conectado a invitado o un almacén de datos NFS complementario, para la migración de flujos de trabajo, para ampliar o bursting al cloud, backup/restauración y recuperación ante desastres.

Elija su cloud y deje que NetApp haga el resto.

Para ver las funcionalidades de un proveedor a hiperescala específico, haga clic en la pestaña adecuada para ese proveedor a hiperescala.

Para ir a la sección del contenido deseado, seleccione una de las siguientes opciones:

- "VMware en la configuración de proveedores a hiperescala"
- "Opciones de almacenamiento de NetApp"
- "Soluciones cloud de NetApp/VMware"

VMware en la configuración de proveedores a hiperescala

Al igual que en las instalaciones, la planificación de un entorno de virtualización basado en cloud es crucial para tener un entorno preparado para la producción con éxito a la hora de crear equipos virtuales y migración.

AWS/VMC

En esta sección se describe cómo configurar y gestionar VMware Cloud en AWS SDDC y utilizarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

> El almacenamiento invitado es el único método compatible para conectar Cloud Volumes ONTAP a VMC de AWS.

El proceso de configuración puede dividirse en los siguientes pasos:

- Poner en marcha y configurar VMware Cloud para AWS
- Conecte VMware Cloud a FSX ONTAP

Vea el detalles "Pasos de configuración para VMC".

Azure / AVS

En esta sección se describe cómo configurar y gestionar la solución VMware de Azure y utilizarla en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

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

El proceso de configuración puede dividirse en los siguientes pasos:

- Registre el proveedor de recursos y cree un cloud privado
- Conéctese a una puerta de enlace de red virtual ExpressRoute nueva o existente
- Validar la conectividad de red y acceder al cloud privado

Vea el detalles "Pasos de configuración para AVS".

GCP/GCVE

En esta sección se describe cómo configurar y gestionar GCVE y cómo utilizarlo junto con las opciones disponibles para conectar el almacenamiento de NetApp.

> El almacenamiento invitado es el único método compatible para conectar Cloud Volumes ONTAP y Cloud Volumes Services a GCVE.

El proceso de configuración puede dividirse en los siguientes pasos:

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

Vea el detalles "Pasos de configuración para GCVE".

Opciones de almacenamiento de NetApp

El almacenamiento NetApp se puede utilizar de varias maneras, ya sea como almacén de datos NFS «guest» o como almacén de datos NFS complementario, en cada uno de los 3 proveedores a hiperescala más importantes.

Visite "Opciones de almacenamiento de NetApp admitidas" si quiere más información.

AWS/VMC

AWS admite almacenamiento de NetApp con las siguientes configuraciones:

- FSX ONTAP como almacenamiento conectado como invitado
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado
- FSX ONTAP como almacén de datos NFS complementario

Vea el detalles "Opciones de almacenamiento de conexión para invitado para VMC". Vea el detalles "Opciones suplementarias de almacén de datos de NFS para VMC".

Azure / AVS

Azure admite almacenamiento de NetApp en las siguientes configuraciones:

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

Vea el detalles "Opciones de almacenamiento de Guest Connect para AVS". Vea el detalles "Opciones complementarias de almacén de datos NFS para AVS".

GCP/GCVE

Google Cloud es compatible con almacenamiento de NetApp en las siguientes configuraciones:

- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado
- Cloud Volumes Service (CVS) como almacenamiento conectado como invitado
- Cloud Volumes Service (CVS) como almacén de datos NFS complementario

Vea el detalles "Opciones de almacenamiento de Guest Connect para GCVE".

Más información acerca de "Soporte de almacén de datos de Cloud Volumes Service de NetApp para Google Cloud VMware Engine (blog de NetApp)" o. "Cómo usar CVS de NetApp como almacenes de datos para Google Cloud VMware Engine (blog de Google)"

Soluciones cloud de NetApp/VMware

Con las soluciones de cloud de NetApp y VMware, muchos casos de uso son fáciles de poner en marcha en el proveedor a hiperescala que elija. VMware define los casos de uso de cargas de trabajo en el cloud principal como:

- Protect (incluye recuperación ante desastres y backup/restauración)
- Migración
- Extender

AWS/VMC

"Examine las soluciones de NetApp para AWS/VMC"

Azure / AVS

"Examine las soluciones de NetApp para Azure / AVS"

GCP/GCVE

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

Configuraciones compatibles para el multicloud híbrido de NetApp con VMware

Comprender las combinaciones para el soporte del almacenamiento de NetApp en los principales proveedores a hiperescala.

	Invitado conectado	Datastore NFS suplementario
AWS	ONTAP FSM de CVO"Detalles"	FSX ONTAP"Detalles"
Azure	CVO ANF"Detalles"	ANF"Detalles"
GCP	CLOUD VOLUMES ONTAP"Detalles"	CVS"Detalles"

Configuración del entorno de virtualización en el proveedor de cloud

Aquí se ofrece información sobre cómo configurar el entorno de virtualización en cada uno de los proveedores a hiperescala compatibles.

AWS/VMC

En esta sección se describe cómo configurar y gestionar VMware Cloud en AWS SDDC y utilizarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

> El almacenamiento invitado es el único método compatible para conectar Cloud Volumes ONTAP a VMC de AWS.

El proceso de configuración puede dividirse en los siguientes pasos:

- Poner en marcha y configurar VMware Cloud para AWS
- Conecte VMware Cloud a FSX ONTAP

Vea el detalles "Pasos de configuración para VMC".

Azure / AVS

En esta sección se describe cómo configurar y gestionar la solución VMware de Azure y utilizarla en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

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

El proceso de configuración puede dividirse en los siguientes pasos:

- Registre el proveedor de recursos y cree un cloud privado
- Conéctese a una puerta de enlace de red virtual ExpressRoute nueva o existente
- Validar la conectividad de red y acceder al cloud privado

Vea el detalles "Pasos de configuración para AVS".

GCP/GCVE

En esta sección se describe cómo configurar y gestionar GCVE y cómo utilizarlo junto con las opciones disponibles para conectar el almacenamiento de NetApp.

> El almacenamiento invitado es el único método compatible para conectar Cloud Volumes ONTAP y Cloud Volumes Services a GCVE.

El proceso de configuración puede dividirse en los siguientes pasos:

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

Vea el detalles "Pasos de configuración para GCVE".

Implemente y configure el entorno de virtualización en AWS

Al igual que en las instalaciones, la planificación de VMware Cloud en AWS es crucial para tener un entorno preparado para la producción con éxito a la hora de crear máquinas virtuales y migración.

En esta sección se describe cómo configurar y gestionar VMware Cloud en AWS SDDC y utilizarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

> El almacenamiento invitado es actualmente el único método compatible para conectar Cloud Volumes ONTAP (CVO) a AWS VMC.

El proceso de configuración puede dividirse en los siguientes pasos:

Ponga en marcha y configure VMware Cloud para AWS

"VMware Cloud en AWS" Ofrece una experiencia nativa del cloud para cargas de trabajo basadas en VMware en el ecosistema de AWS. Cada centro de datos definido por software (SDDC) de VMware se ejecuta en un cloud privado virtual de Amazon (VPC) y proporciona una pila completa de VMware (incluido vCenter Server), las redes definidas por software NSX-T, el almacenamiento definido por software VSAN y uno o más hosts ESXi que proporcionan recursos informáticos y de almacenamiento a sus cargas de trabajo.

En esta sección se describe cómo configurar y gestionar VMware Cloud en AWS y cómo utilizarlo en combinación con Amazon FSX para ONTAP de NetApp y/o Cloud Volumes ONTAP en AWS con el almacenamiento invitado.

> ⓘ El almacenamiento invitado es actualmente 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 en para ver un "Cuenta de Amazon Web Services".

Se necesita una cuenta de AWS para empezar, suponiendo que no se haya creado ya. Nuevo o existente, necesita privilegios administrativos en la cuenta para muchos pasos de este procedimiento. Vea esto "enlace" Para obtener más información acerca de las credenciales de AWS.

Regístrese para obtener una cuenta de My VMware

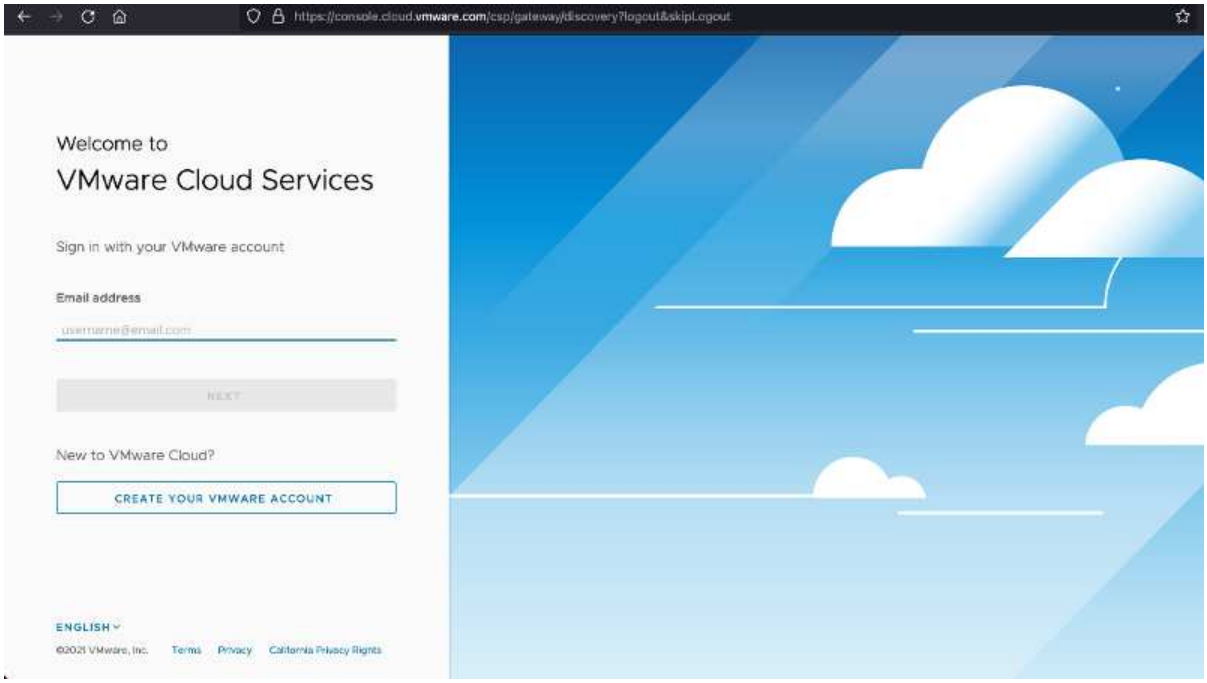
Regístrese en "Mi VMware" cuenta.

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

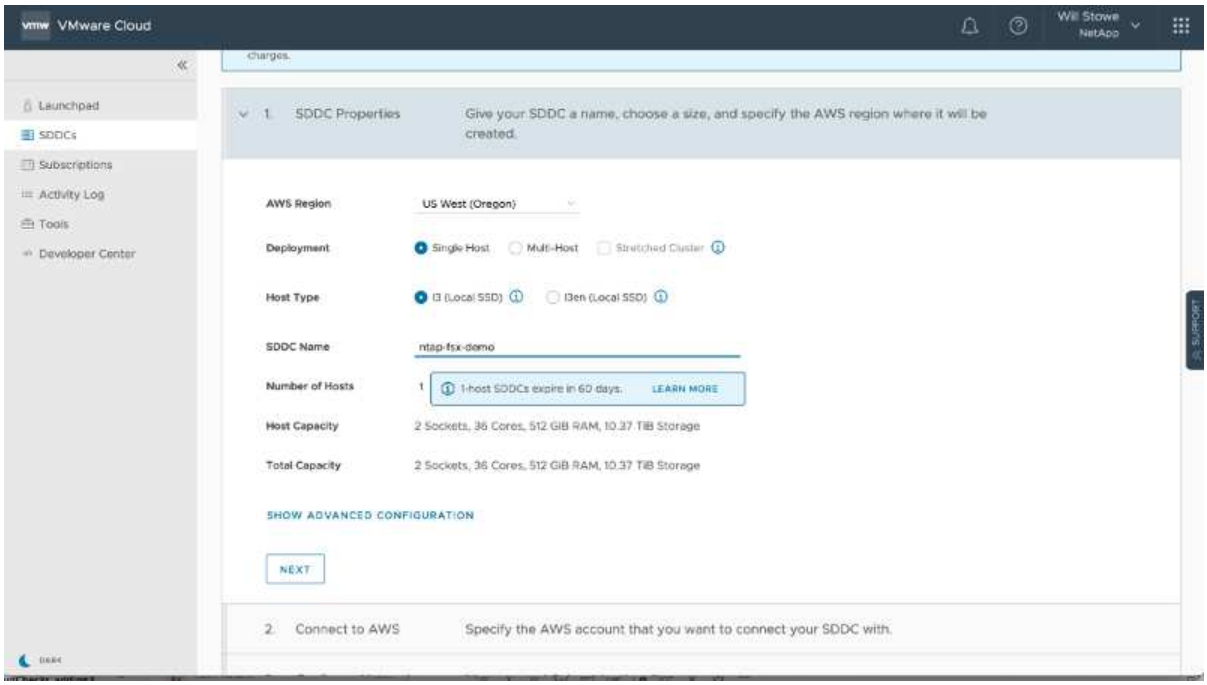
Aprovisione SDDC en VMware Cloud

Una vez que se ha configurado la cuenta de VMware y se ha realizado el ajuste de tamaño adecuado, la puesta en marcha de un centro de datos definido por software es el siguiente paso obvio para usar el servicio VMware Cloud en AWS. Para crear un SDDC, elija una región AWS para alojarlo, proporcione un nombre al SDDC y especifique cuántos hosts ESXi desea que contenga el SDDC. Si todavía no tiene una cuenta de AWS, puede crear un SDDC de configuración de inicio que contenga un único host ESXi.

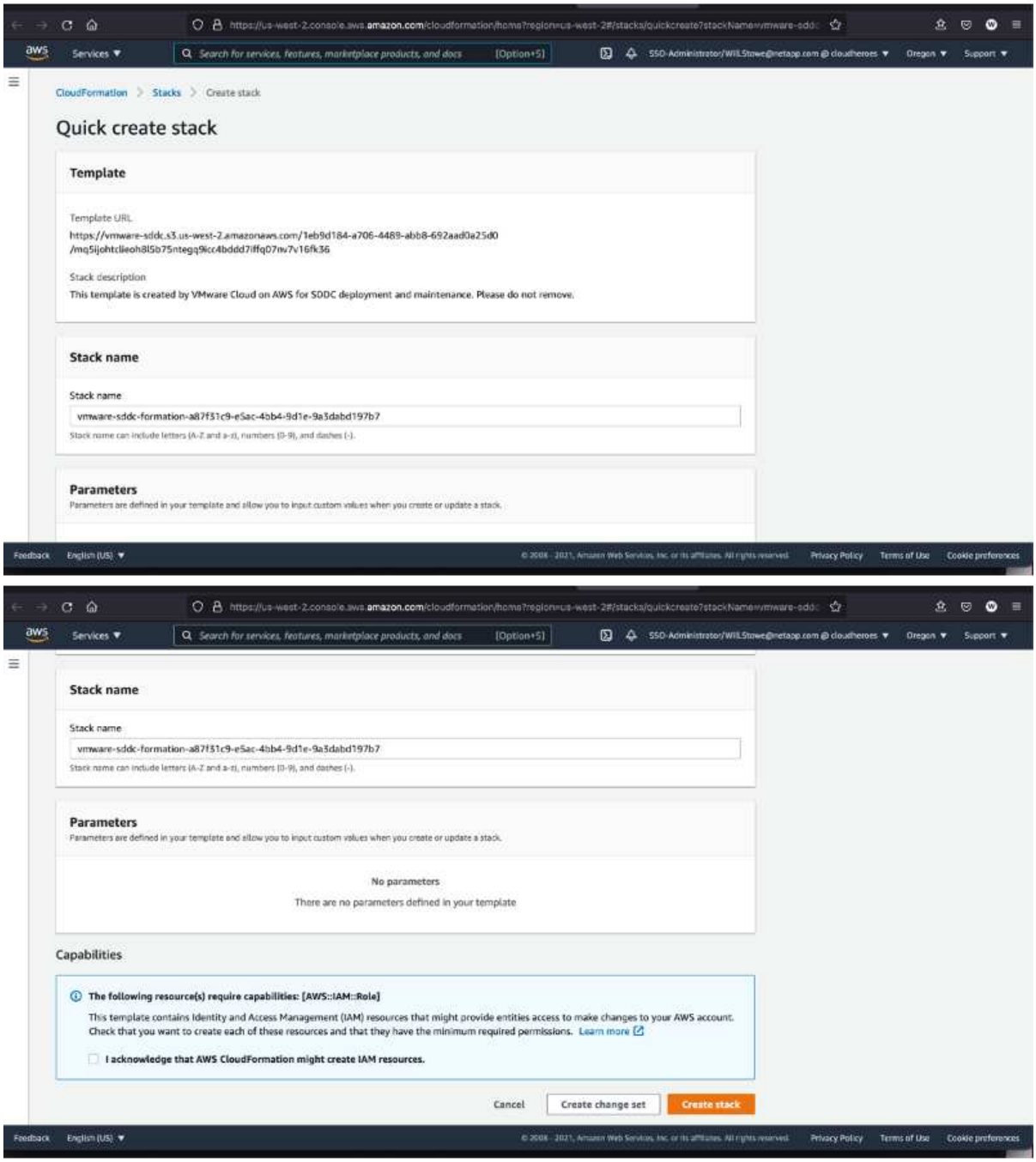
1. Inicie sesión en VMware Cloud Console con sus credenciales de VMware existentes o creadas recientemente.

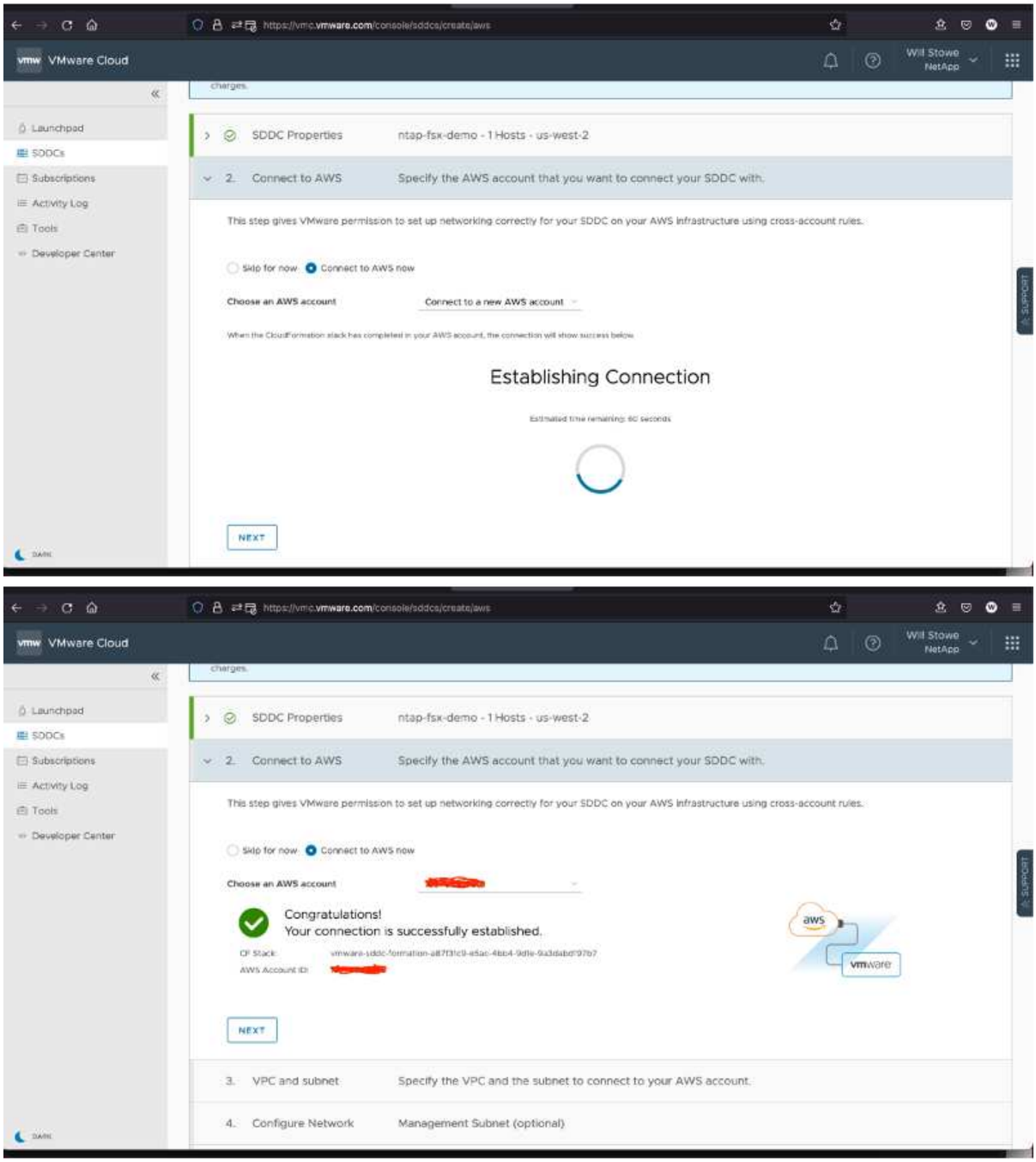


2. Configure la región, la puesta en marcha y el tipo de host de AWS y el nombre del SDDC:



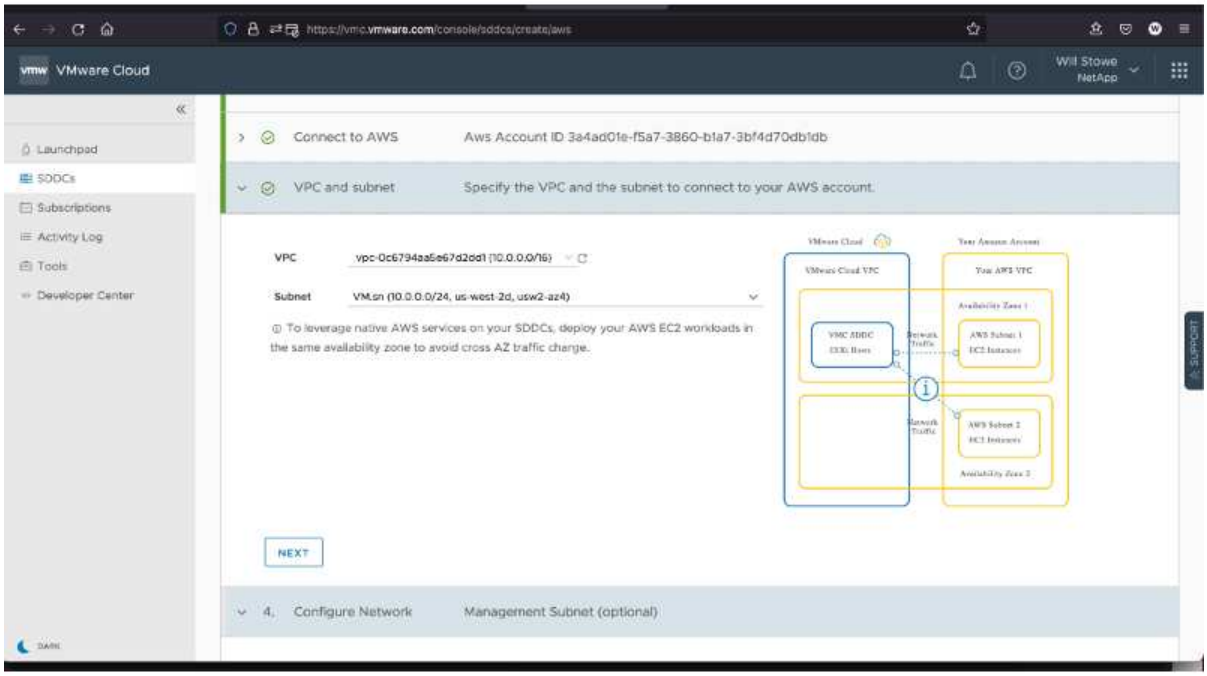
3. Conéctese a la cuenta de AWS deseada y ejecute la pila AWS Cloud Formation.



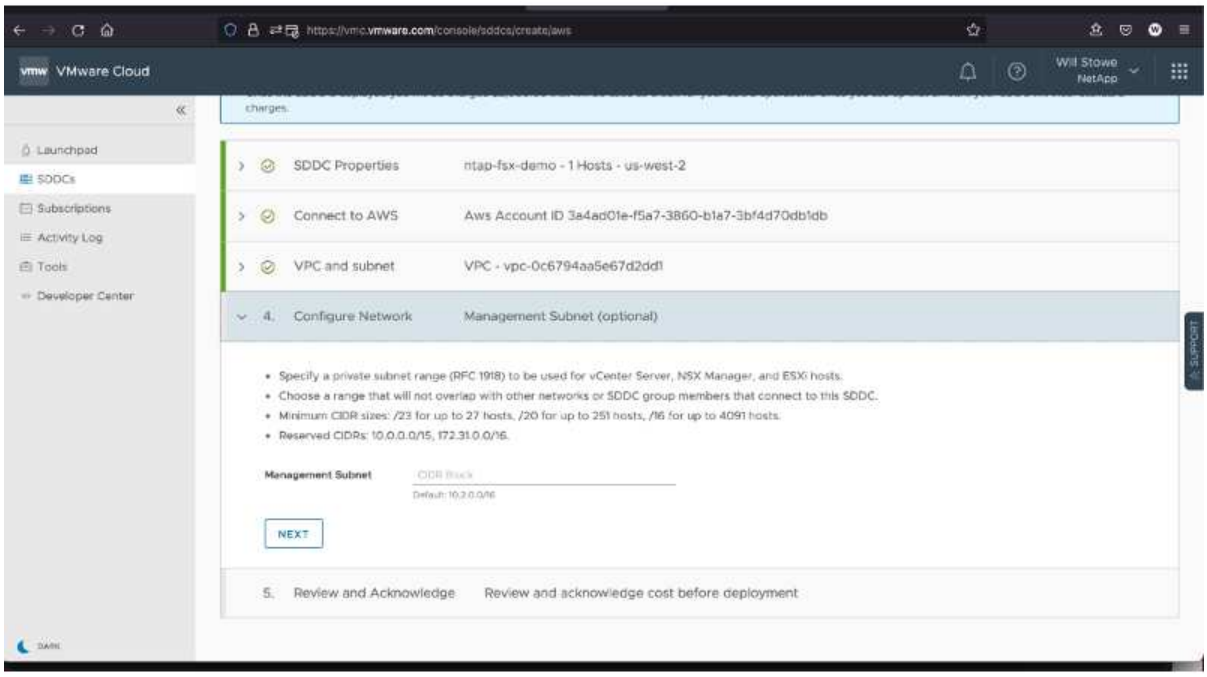


En esta validación se utiliza la configuración de un solo host.

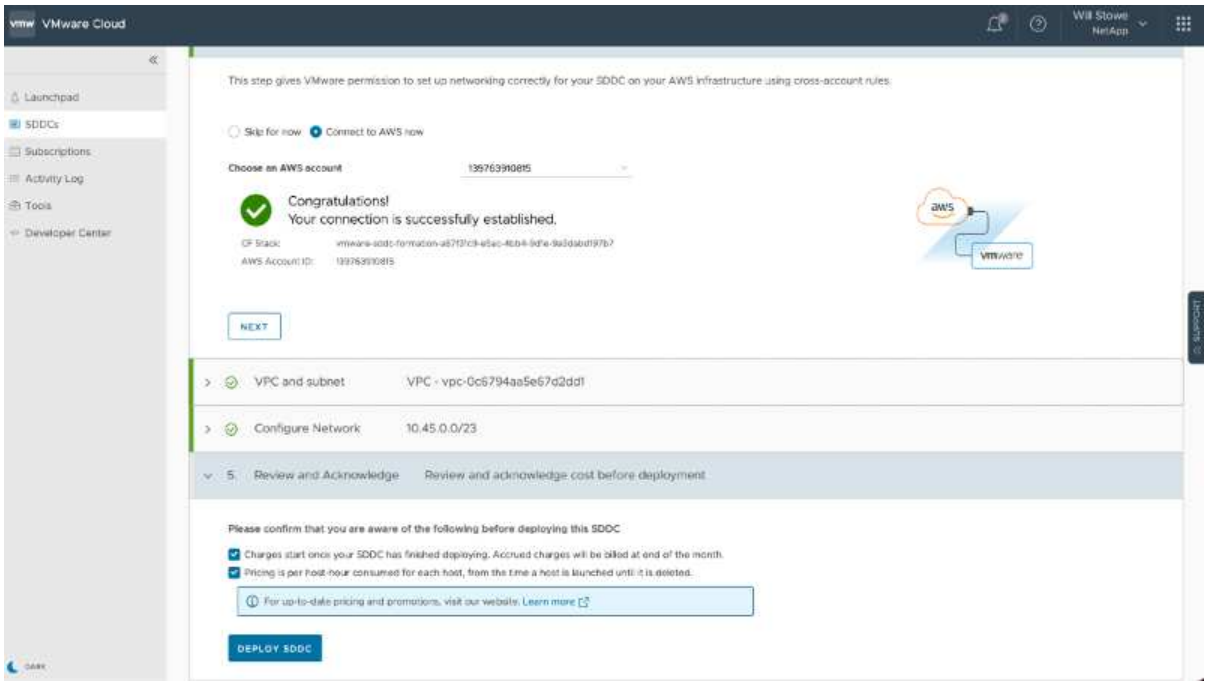
4. Seleccione el VPC de AWS que desee para conectar el entorno de VMC con.



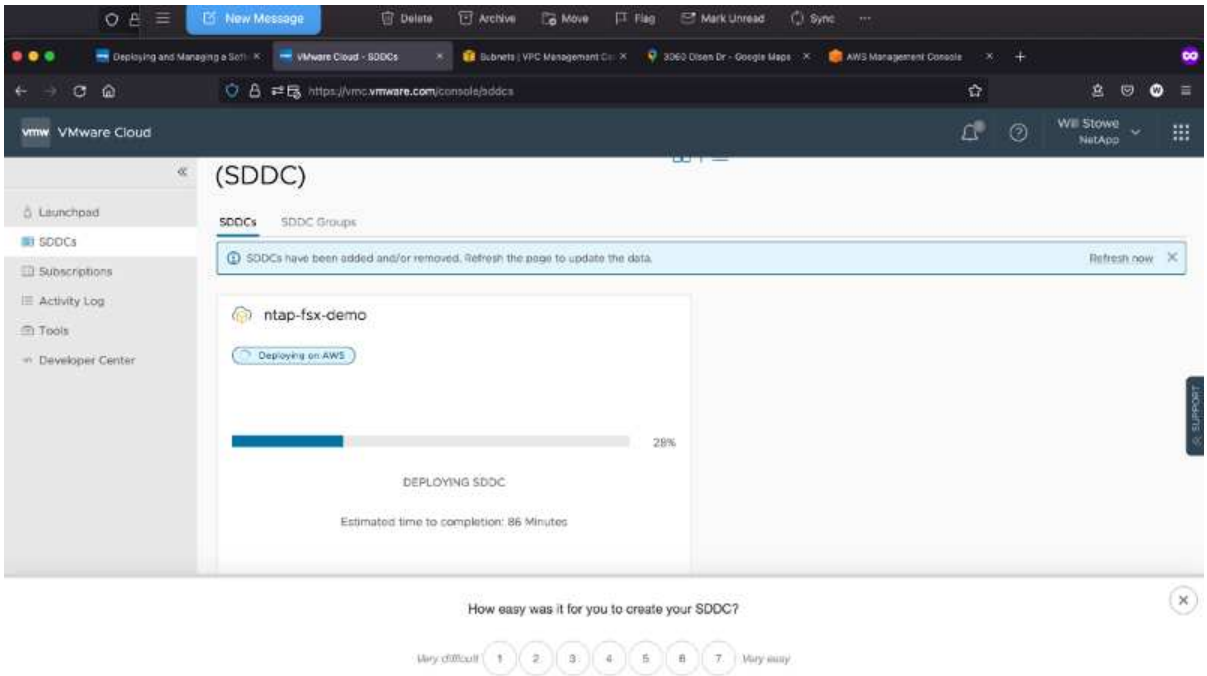
5. Configure la subred de gestión de VMC; esta subred contiene servicios gestionados por VMC como vCenter, NSX, etc. No elija un espacio de direcciones superpuesto con ninguna otra red que necesite conectividad con el entorno SDDC. Por último, siga las recomendaciones para el tamaño CIDR anotado a continuación.



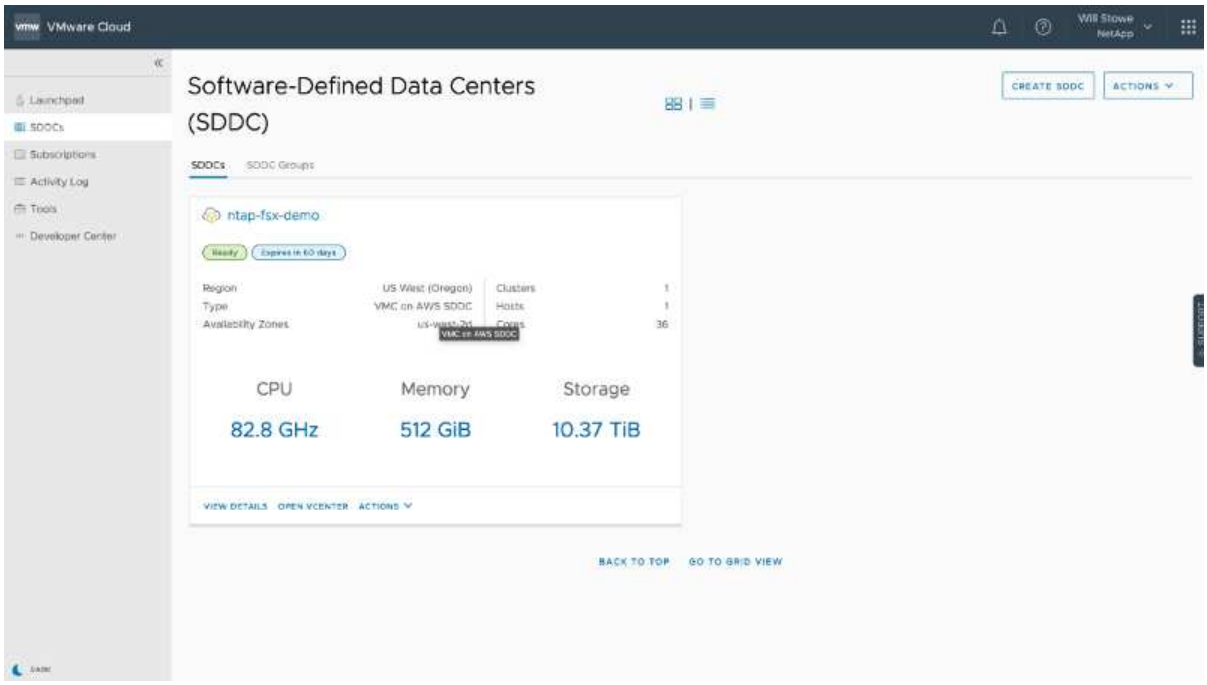
6. Revise y reconozca la configuración del SDDC y, a continuación, haga clic en Deploy the SDDC.



Normalmente, el proceso de puesta en marcha tarda aproximadamente dos horas en completarse.



7. Tras la finalización, el SDDC está listo para su uso.

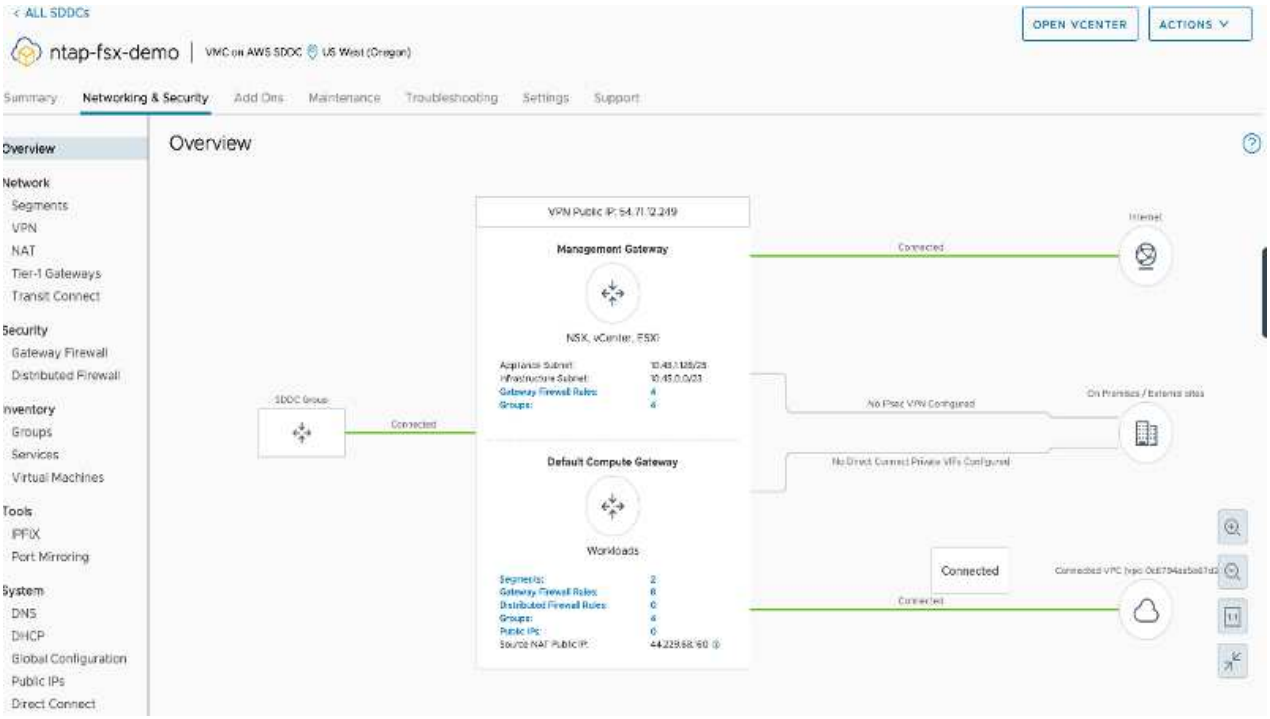


Para obtener una guía paso a paso sobre la puesta en marcha de SDDC, consulte "Implemente un SDDC a partir de la consola VMC".

Conecte VMware Cloud a FSX ONTAP

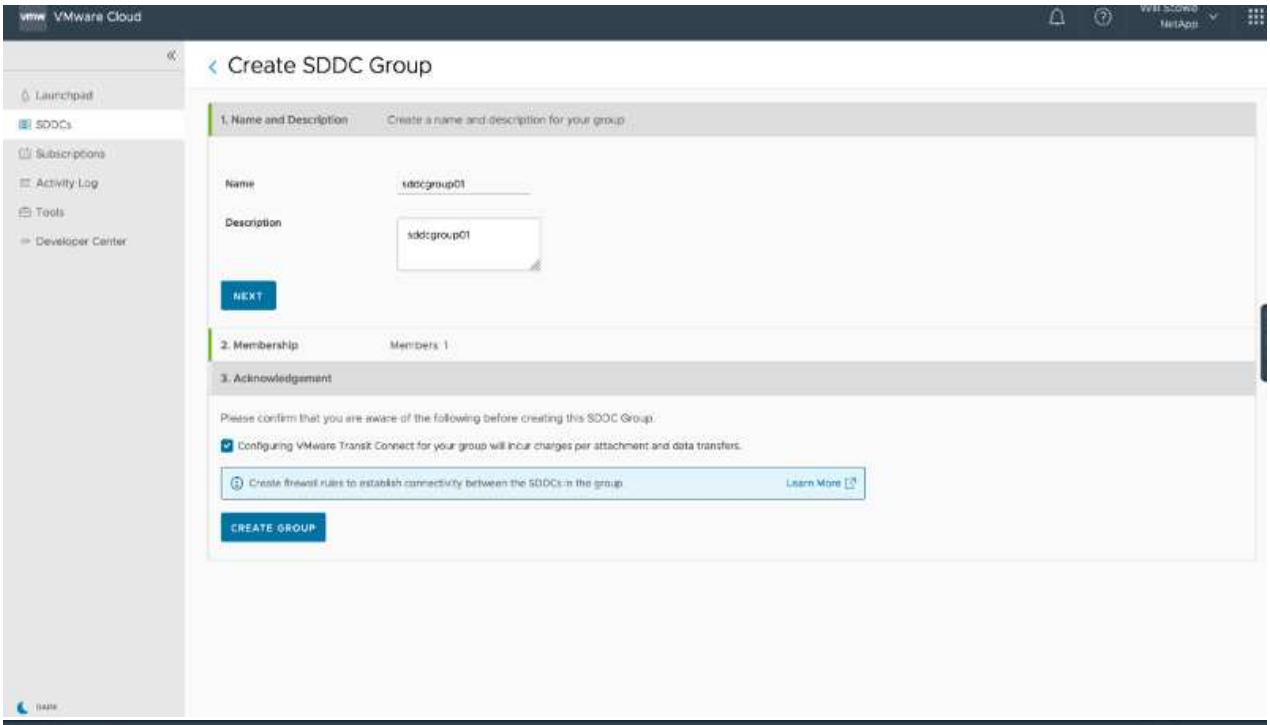
Para conectar VMware Cloud a FSX ONTAP, lleve a cabo los siguientes pasos:

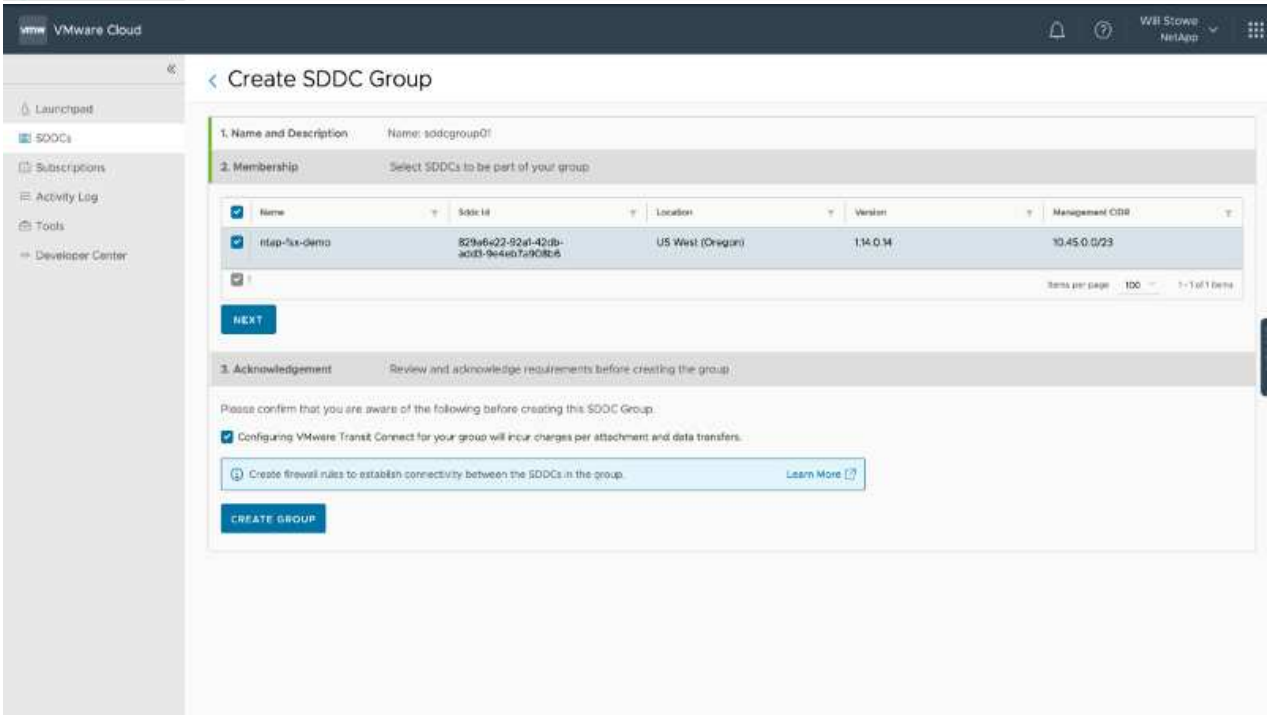
1. Con la puesta en marcha de VMware Cloud completada y conectada a AWS VPC, debe poner en marcha Amazon FSX para ONTAP de NetApp en un nuevo VPC, en lugar de hacerlo en el VPC conectado original (consulte la captura de pantalla de abajo). No se puede acceder a FSX (IP flotantes de NFS y SMB) si se ha implementado en el VPC conectado. Tenga en cuenta que los extremos DE ISCSI como Cloud Volumes ONTAP funcionan muy bien con el VPC conectado.

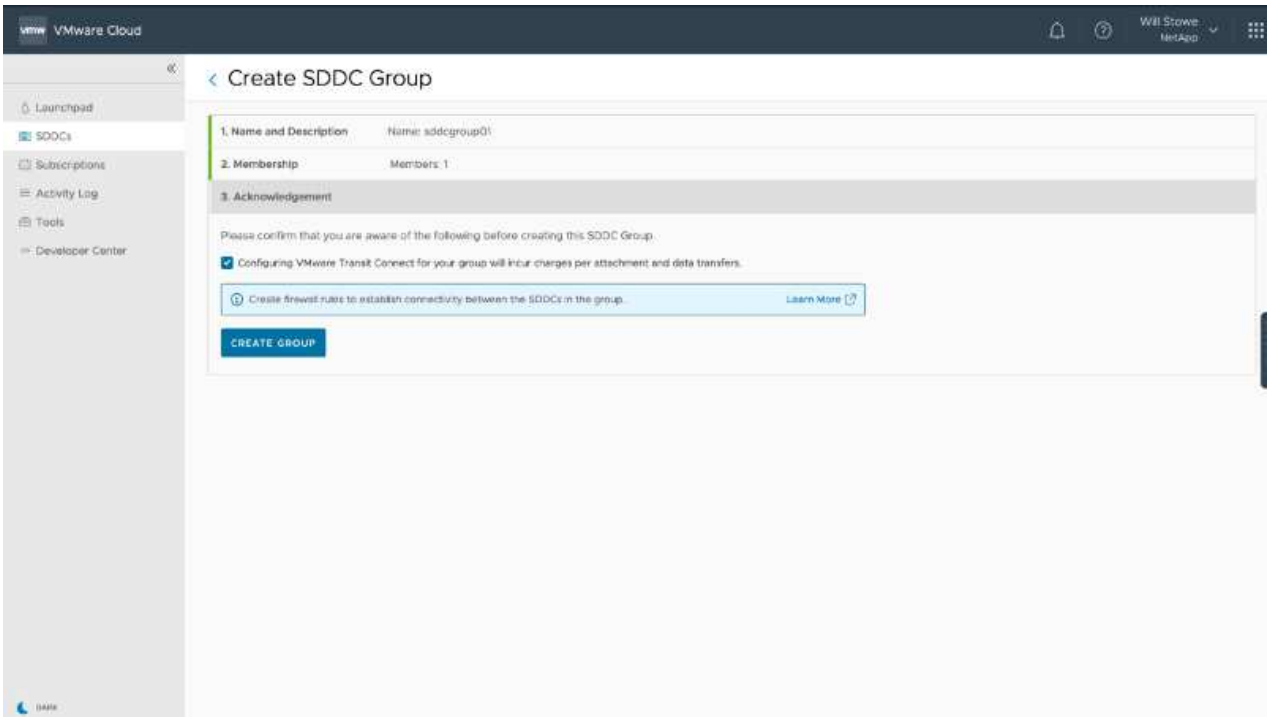


2. Ponga en marcha un VPC adicional en la misma región y, a continuación, ponga en marcha Amazon FSX para ONTAP de NetApp en el nuevo VPC.

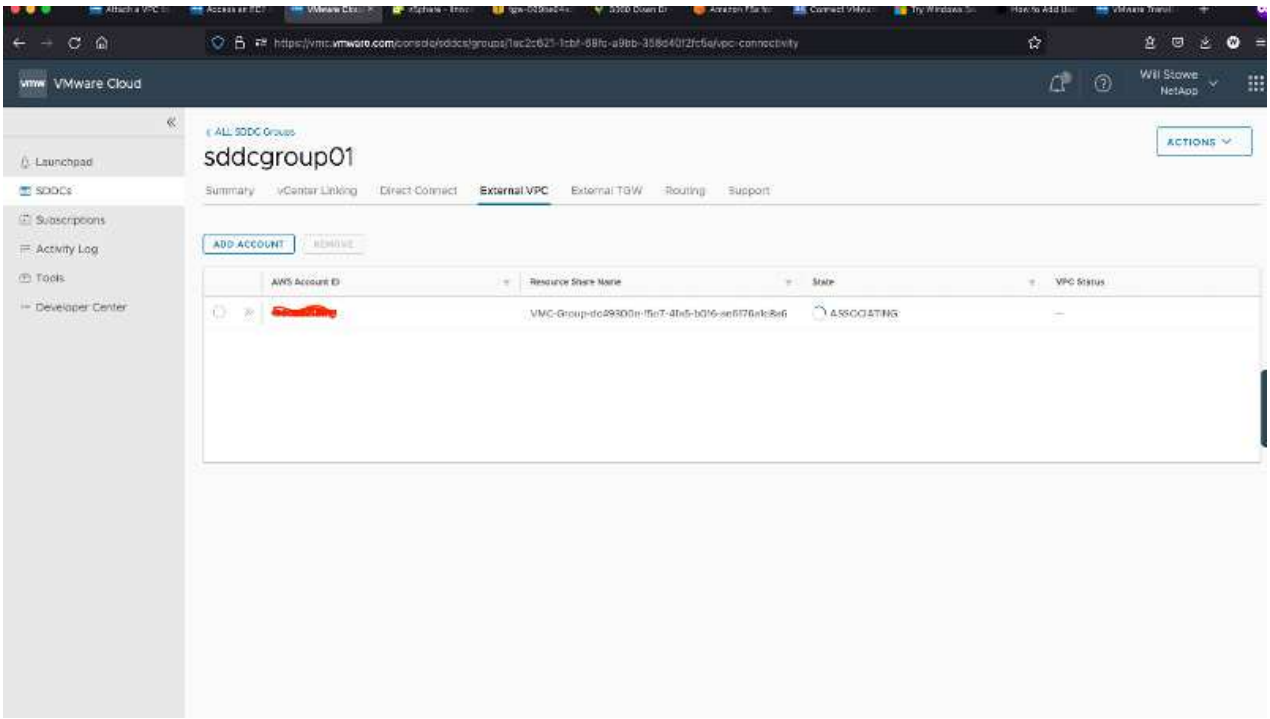
   La configuración de un grupo SDDC en la consola VMware Cloud permite las opciones de configuración de red necesarias para conectarse al nuevo VPC, en el que se pone en marcha FSX. En el paso 3, compruebe que “Configuración de VMware Transit Connect para su grupo incurrirá en cargos por archivo adjunto y transferencia de datos” y, a continuación, seleccione Crear grupo. El proceso puede tardar unos minutos en completarse.

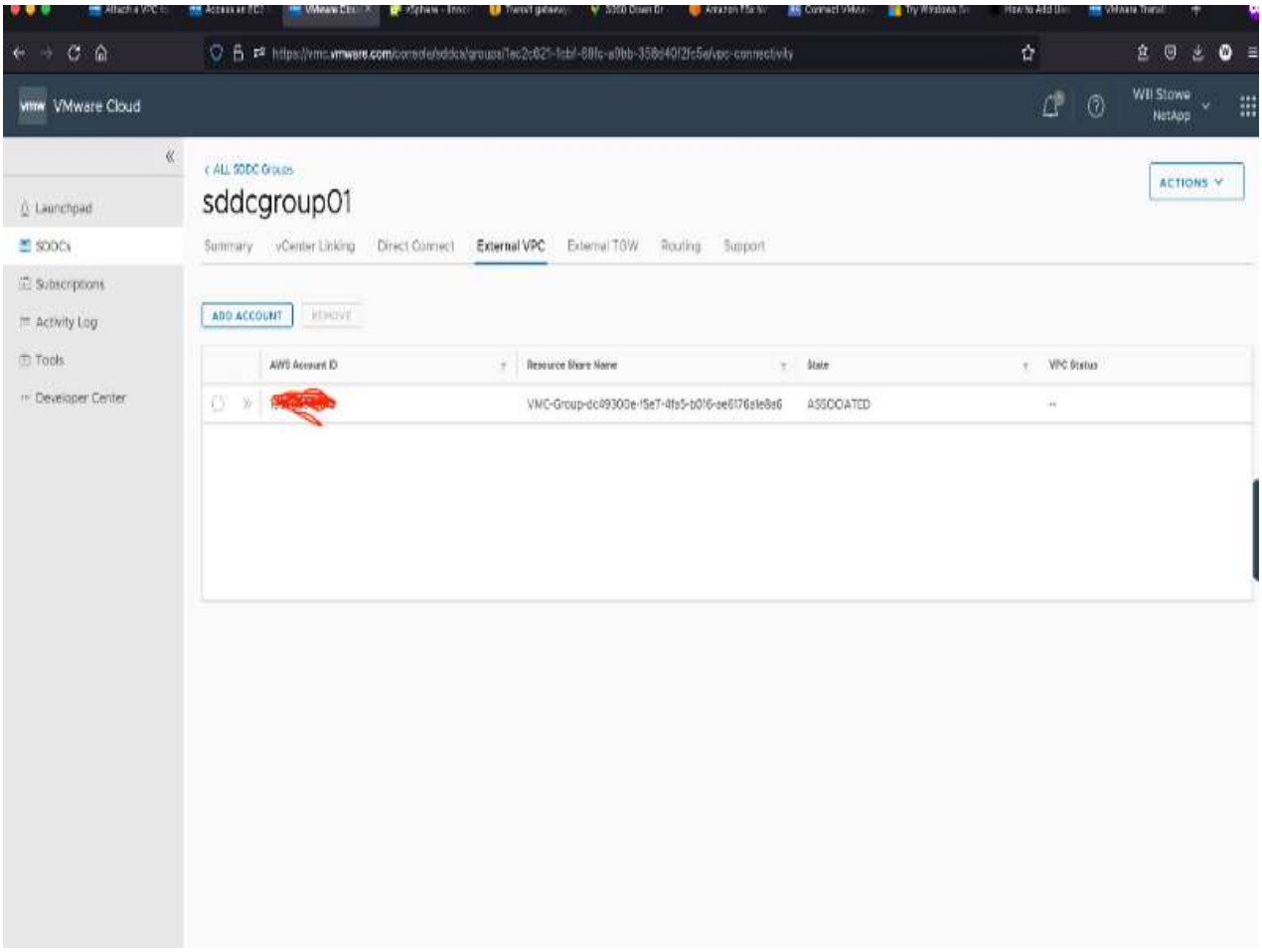

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP


VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6e22-92a1-42db-acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page
100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

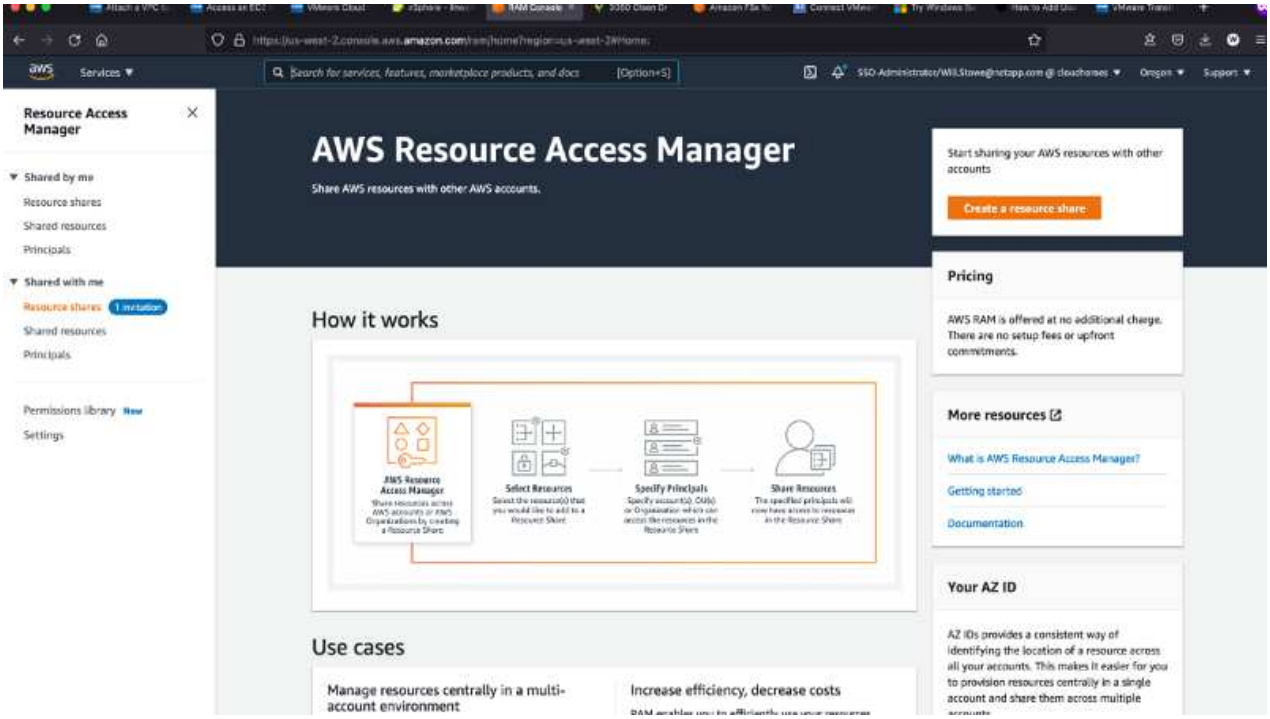


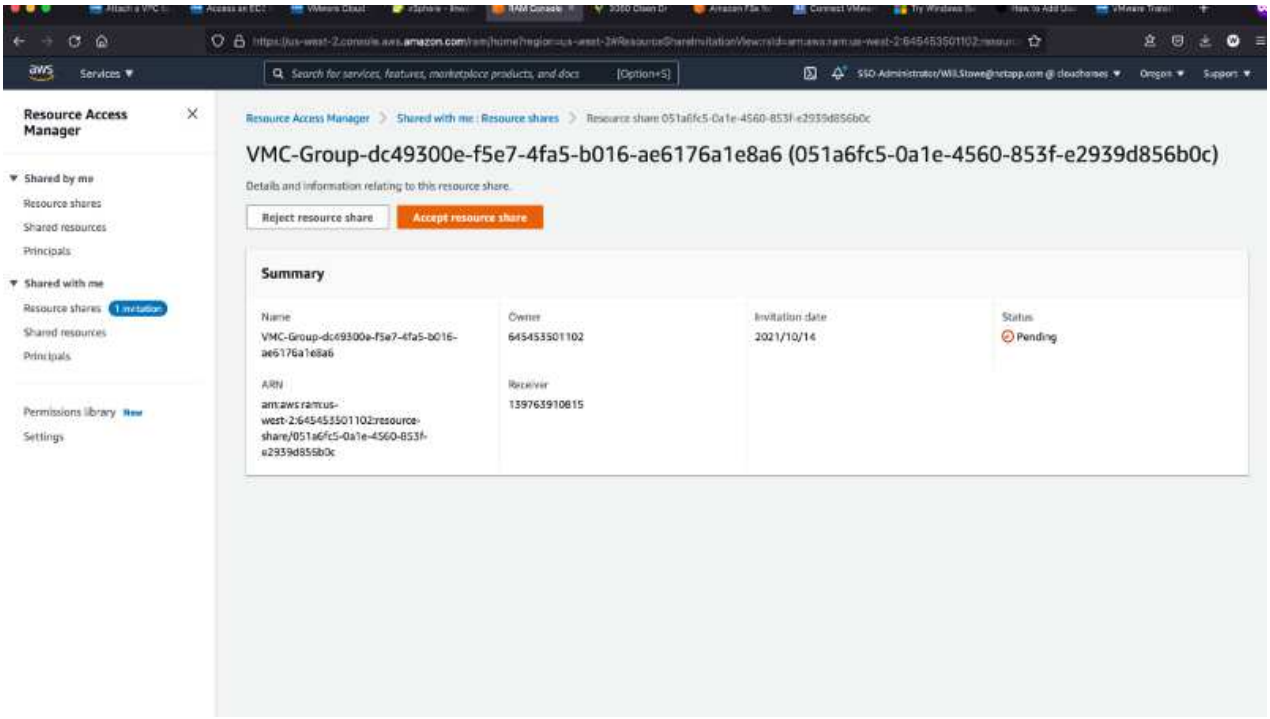
3. Conecte el VPC recién creado al grupo de SDDC recién creado. Seleccione la pestaña External VPC y siga el "Instrucciones para añadir un VPC externo" al grupo. Este proceso puede tardar entre 10 y 15 minutos en completarse.



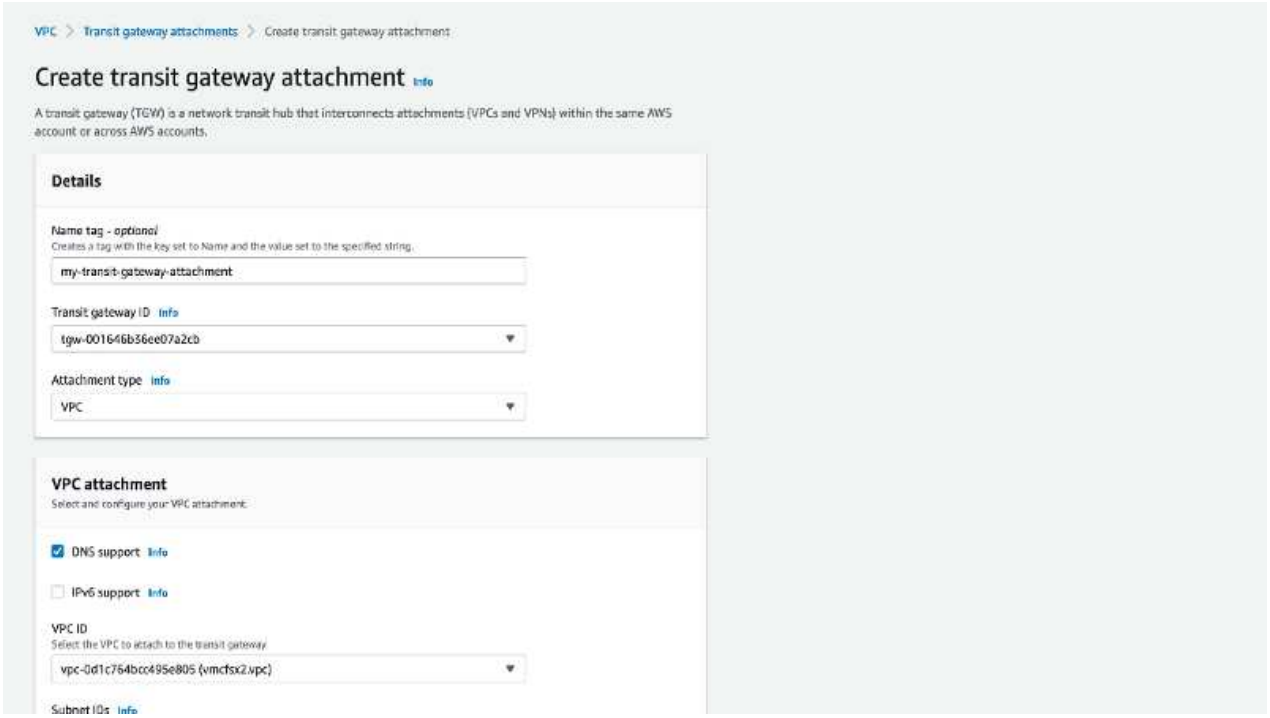


4. Como parte del proceso VPC externo, se le pedirá a través de la consola de AWS que un nuevo recurso compartido a través de Resource Access Manager. El recurso compartido es el "Puerta de enlace de tránsito de AWS" Gestionado por VMware Transit Connect.

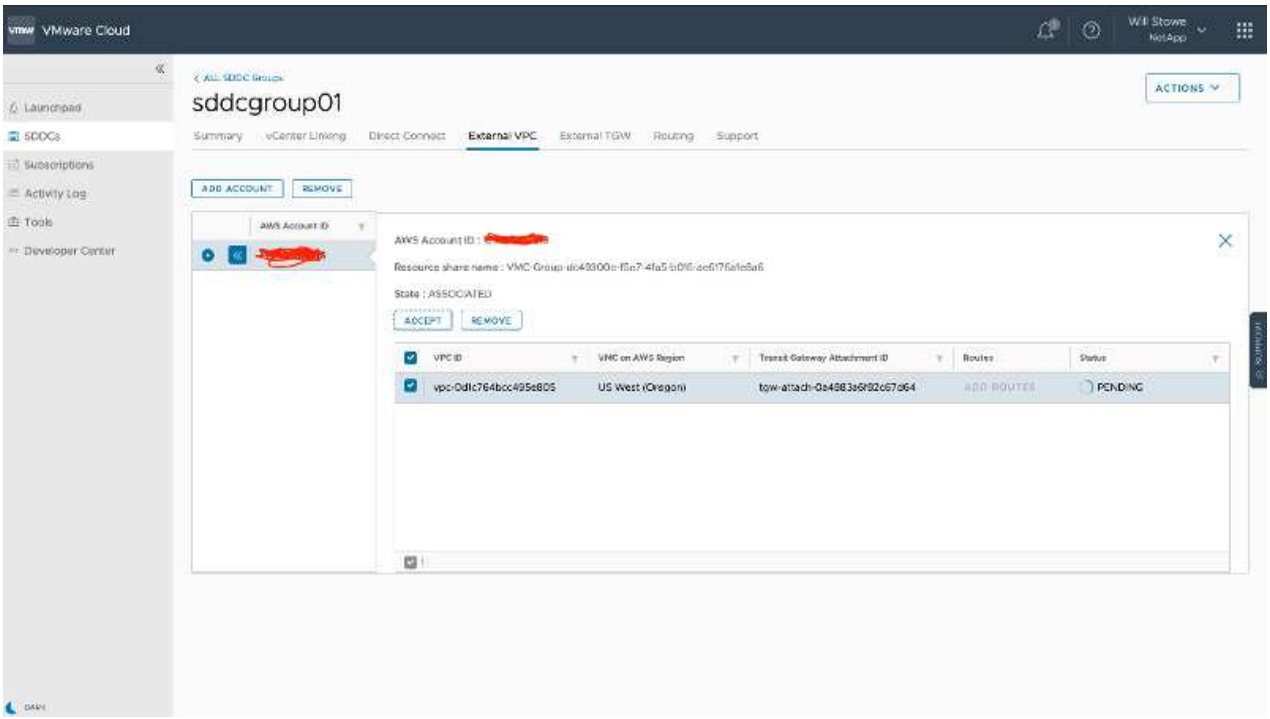




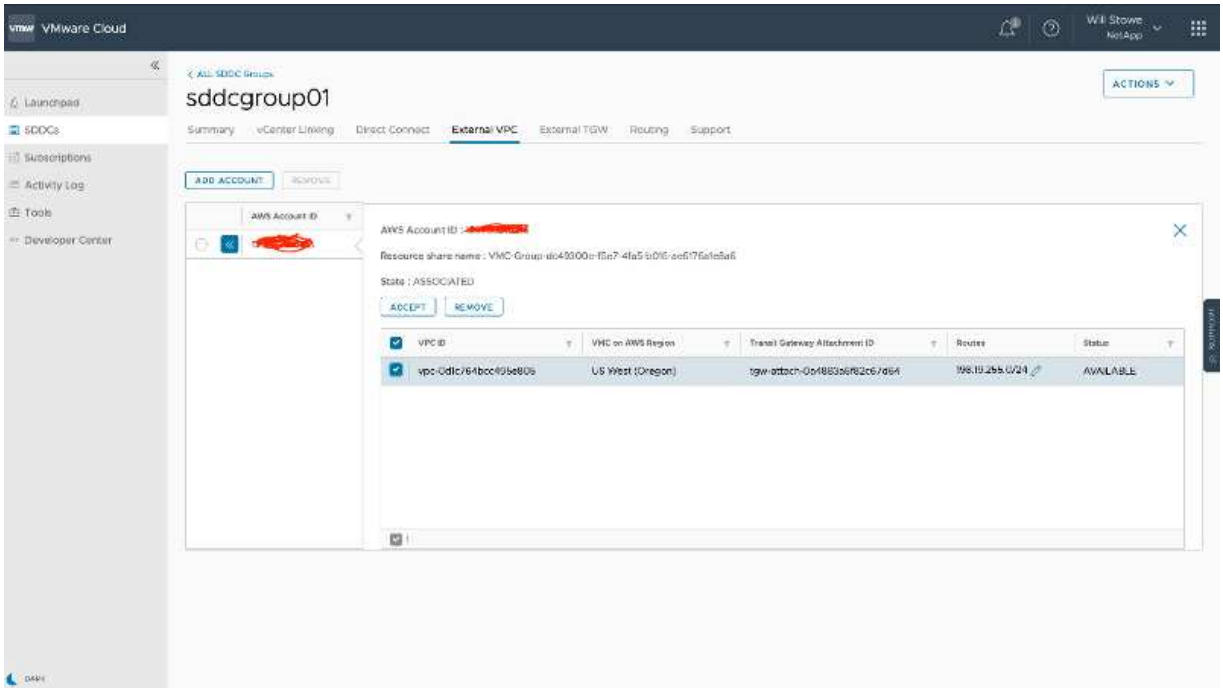
5. Cree el adjunto de puerta de enlace de tránsito.



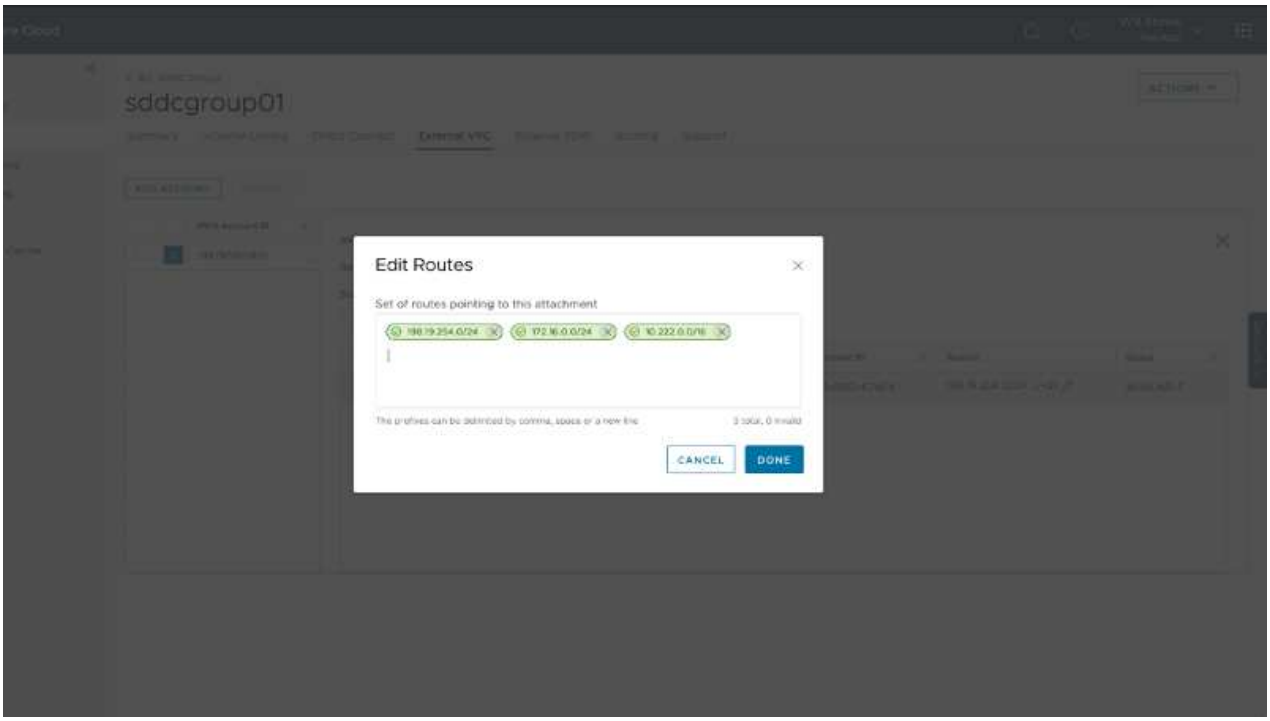
6. De nuevo en la consola VMC, acepte el archivo adjunto VPC. Este proceso puede tardar aproximadamente 10 minutos en completarse.



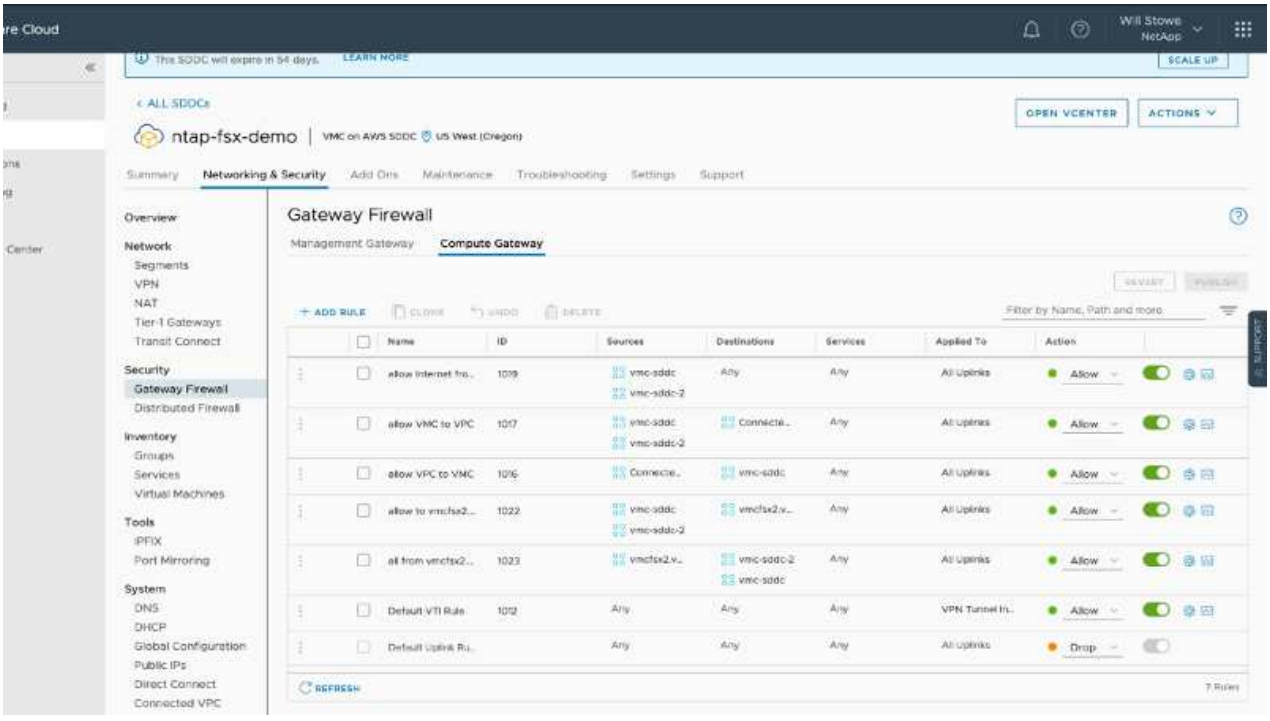
7. En la ficha VPC externo, haga clic en el icono de edición de la columna rutas y añádase las siguientes rutas requeridas:
   - Una ruta para el intervalo IP flotante para Amazon FSX para ONTAP de NetApp "IP flotantes".
   - Ruta para el intervalo IP flotante para Cloud Volumes ONTAP (si procede).
   - Una ruta para el espacio de direcciones VPC externo recién creado.



8. Por último, permita el tráfico bidireccional "reglas del firewall" Para acceder a FSX/CVO. Siga estas "pasos detallados" Para reglas de firewall de puerta de enlace de computación para conectividad de carga de trabajo SDDC.



9. Una vez configurados los grupos de firewall para la puerta de enlace de gestión y computación, es posible acceder al para vCenter de la siguiente manera:



El siguiente paso es verificar que Amazon FSX ONTAP o Cloud Volumes ONTAP está configurado en función de sus requisitos y que los volúmenes se aprovisionan para descargar componentes de almacenamiento de VSAN para optimizar la implementación.

Ponga en marcha y configure el entorno de virtualización en Azure

Como en las instalaciones, la planificación de la solución VMware para Azure es crucial para tener un entorno listo para la producción con éxito a la hora de crear máquinas virtuales y migraciones.

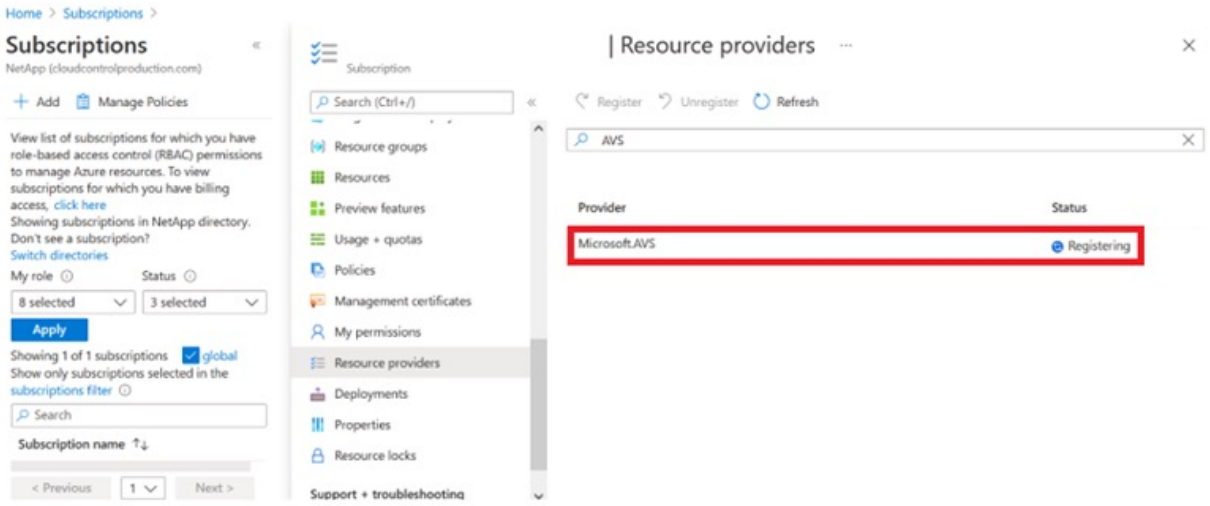
En esta sección se describe cómo configurar y gestionar la solución VMware de Azure y utilizarla en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

El proceso de configuración puede dividirse en los siguientes pasos:

Registre el proveedor de recursos y cree un cloud privado

Para usar la solución VMware de Azure, registre primero el proveedor de recursos dentro de la suscripción identificada:

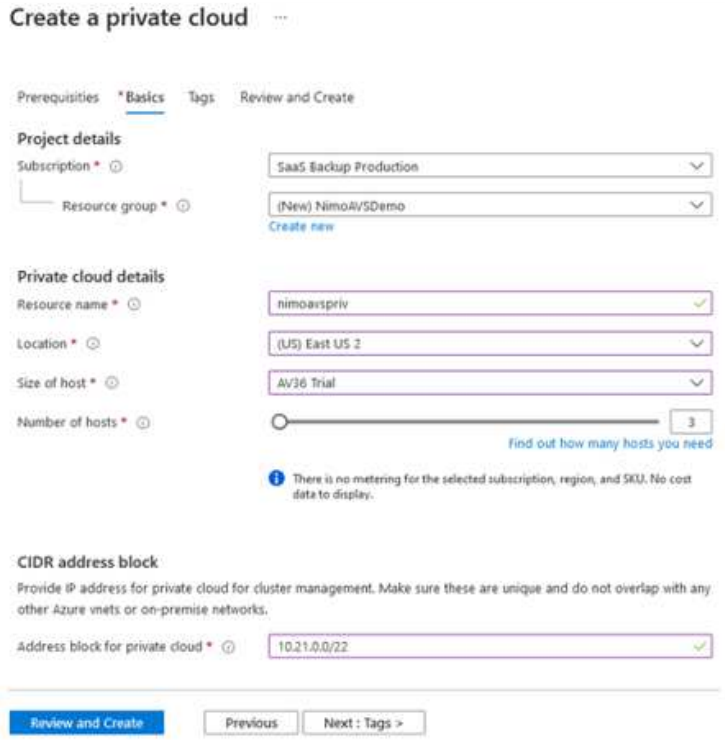
1. Inicie sesión en el portal de Azure.
2. En el menú del portal de Azure, seleccione todos los servicios.
3. En el cuadro de diálogo todos los servicios, introduzca la suscripción y, a continuación, seleccione Suscripciones.
4. Para verlo, seleccione la suscripción en la lista de suscripciones.
5. Seleccione proveedores de recursos e introduzca Microsoft.AVS en la búsqueda.
6. Si el proveedor de recursos no está registrado, seleccione Register.



7. Una vez registrado el proveedor de recursos, cree un cloud privado de Azure VMware Solution mediante el portal de Azure.
8. Inicie sesión en el portal de Azure.
9. Seleccione Crear un nuevo recurso.
10. En el cuadro de texto Buscar en el mercado, introduzca la solución VMware para Azure y selecciónela de los resultados.
11. En la página Azure VMware Solution, seleccione Create.
12. En la ficha conceptos básicos, introduzca los valores en los campos y seleccione revisar + Crear.

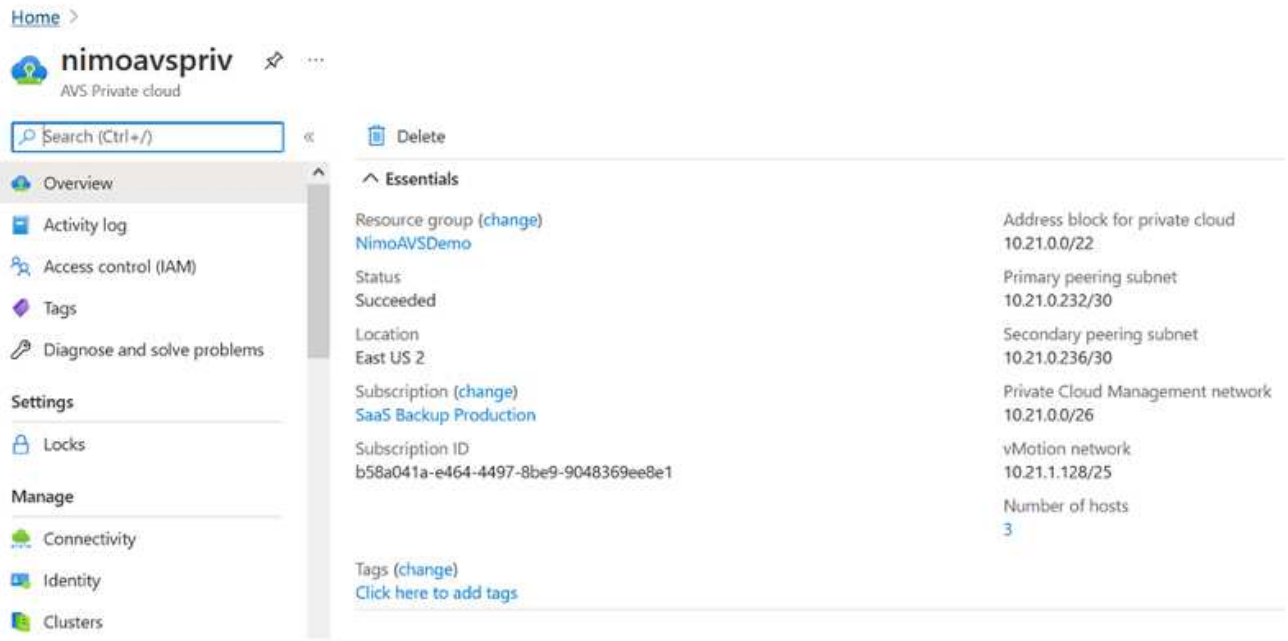
Notas:

- Para un inicio rápido, reúna la información necesaria durante la fase de planificación.
- Seleccione un grupo de recursos existente o cree un nuevo grupo de recursos para el cloud privado. Un grupo de recursos es un contenedor lógico en el que se implementan y gestionan los recursos de Azure.
- Asegúrese de que la dirección CIDR sea única y no se superponga con otras redes virtuales de Azure o en las instalaciones. CIDR representa la red de gestión de nube privada y se utiliza para los servicios de gestión de clúster, como vCenter Server y NSX-T Manager. NetApp recomienda utilizar el espacio de direcciones /22. En este ejemplo, se utiliza 10.21.0.0/22.



El proceso de aprovisionamiento dura entre 4 y 5 horas, aproximadamente. Una vez completado el proceso, compruebe que la implementación se realizó correctamente accediendo a la nube privada desde el portal de Azure. Se muestra el estado correcto cuando se completa la implementación.

Un cloud privado de una solución VMware Azure requiere una red virtual de Azure. Como la solución VMware Azure no es compatible con vCenter en las instalaciones, se requieren pasos adicionales para integrarse con un entorno local existente. También es necesario configurar un circuito ExpressRoute y una puerta de enlace de red virtual. Mientras se espera a que finalice el aprovisionamiento del clúster, cree una red virtual nueva o utilice una existente para conectarse a la solución VMware Azure.



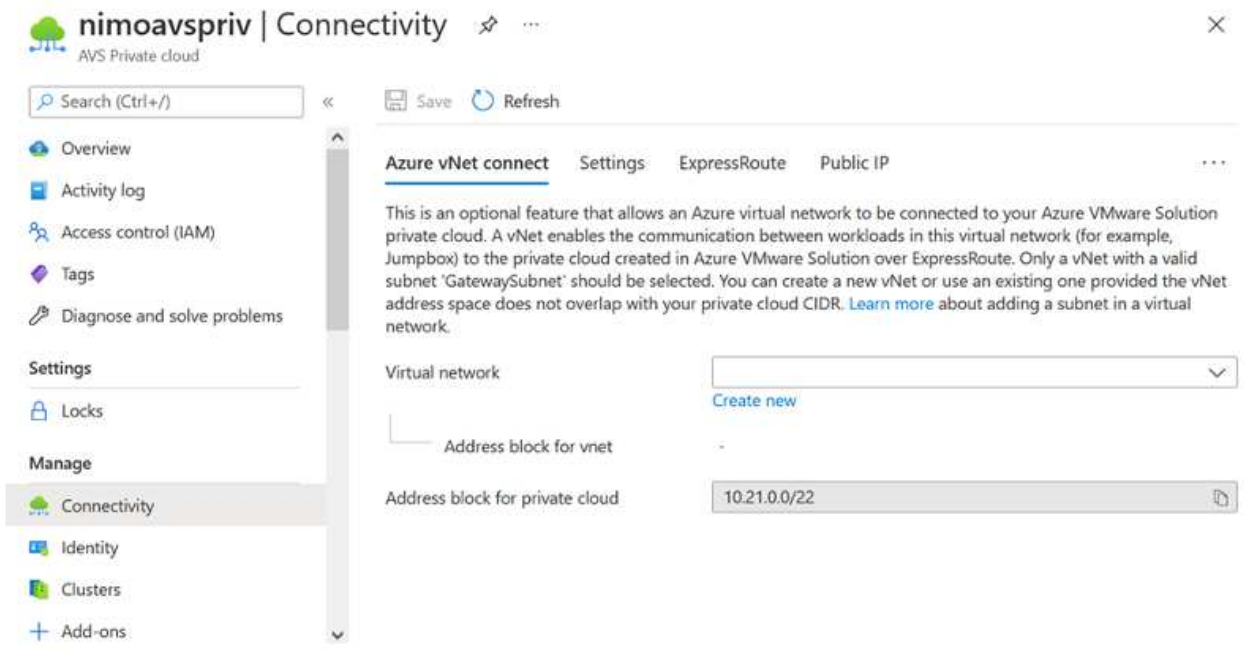
Conéctese a una puerta de enlace de red virtual ExpressRoute nueva o existente

Para crear una nueva red virtual de Azure (vnet), seleccione la pestaña Azure vnet Connect. Como alternativa, puede crear una manualmente desde el portal de Azure mediante el asistente Create Virtual Network:

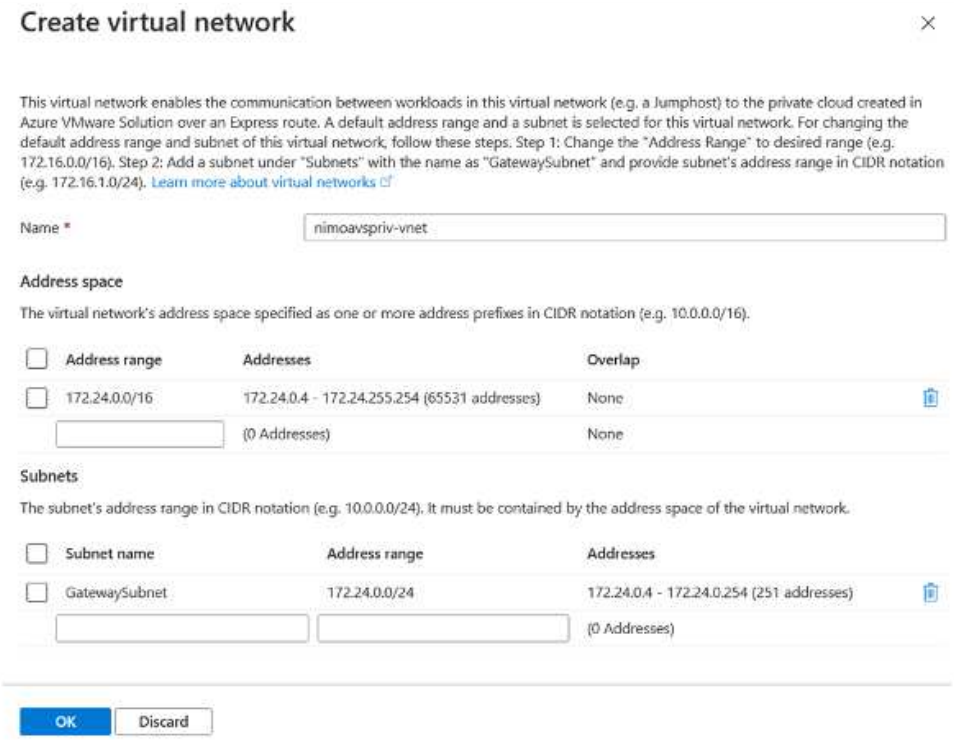
1. Acceda a Azure VMware Solution Private Cloud y acceda a Connectivity en la opción Manage.
2. Seleccione Azure vnet Connect.
3. Para crear un nuevo vnet, seleccione la opción Crear nuevo.

   Esta función permite conectar una vnet al cloud privado de la solución VMware para Azure. Vnet permite la comunicación entre cargas de trabajo en esta red virtual mediante la creación automática de los componentes necesarios (por ejemplo, buzón de entrada, servicios compartidos como Azure NetApp Files y Cloud Volume ONTAP) al cloud privado creado en la solución Azure VMware sobre ExpressRoute.

   Nota: el espacio de dirección vnet no debe superponerse con la nube privada CIDR.



4. Proporcione o actualice la información del nuevo vnet y seleccione Aceptar.

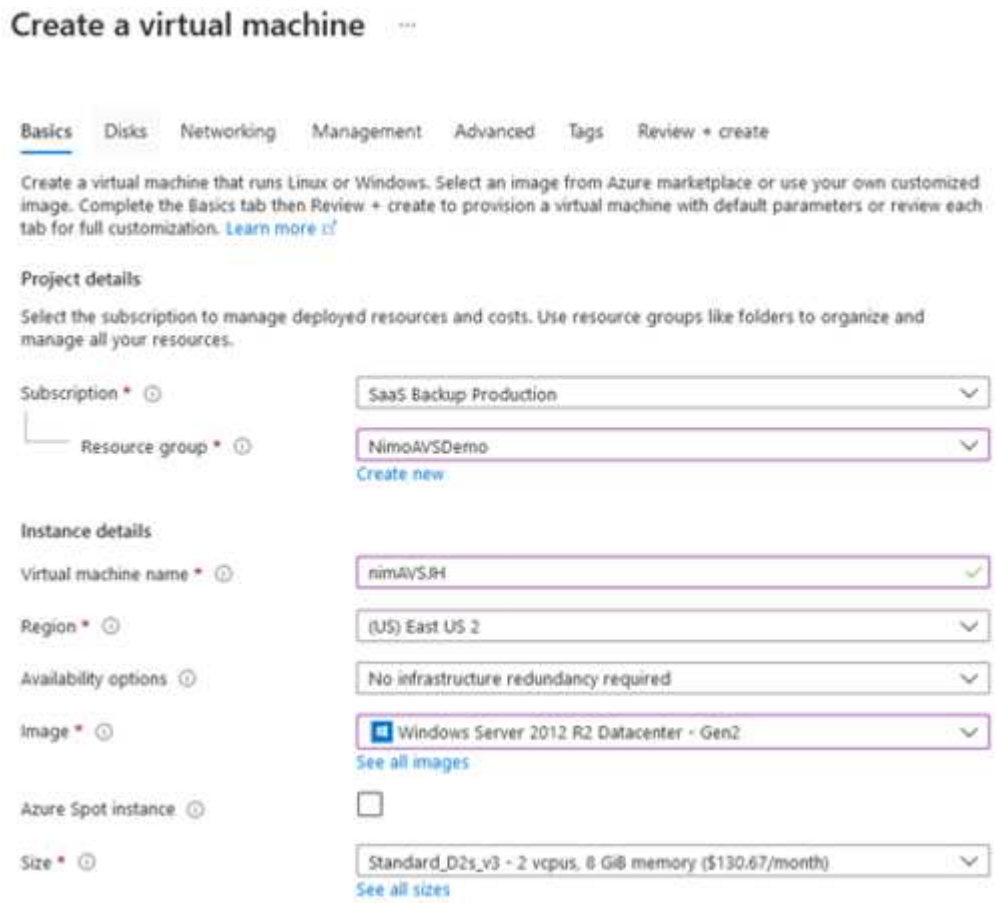


El vnet con el intervalo de direcciones y la subred de puerta de enlace proporcionados se crea en la suscripción designada y el grupo de recursos.

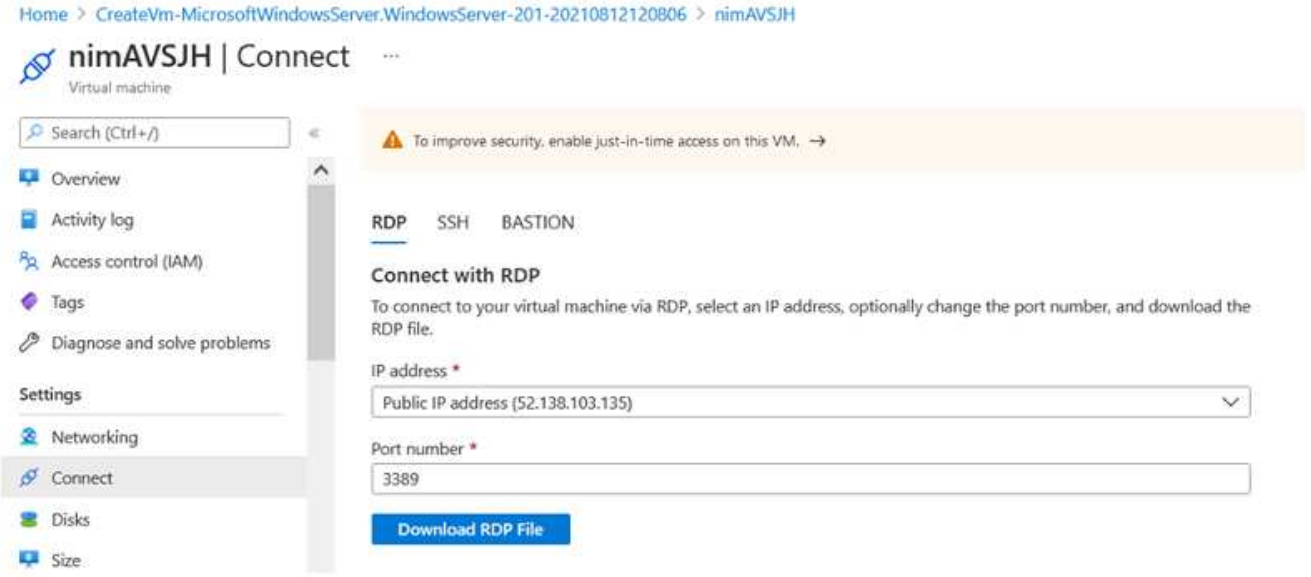
Si crea un vnet manualmente, cree un gateway de red virtual con el SKU y ExpressRoute adecuados como tipo de gateway. Una vez completada la puesta en marcha, conecte la conexión de ExpressRoute a la puerta de enlace de red virtual que contiene el cloud privado de la solución VMware de Azure mediante la clave de autorización. Para obtener más información, consulte "Configure las redes para su cloud privado de VMware en Azure".

Validar la conexión de la red y acceso al cloud privado de la solución VMware Azure

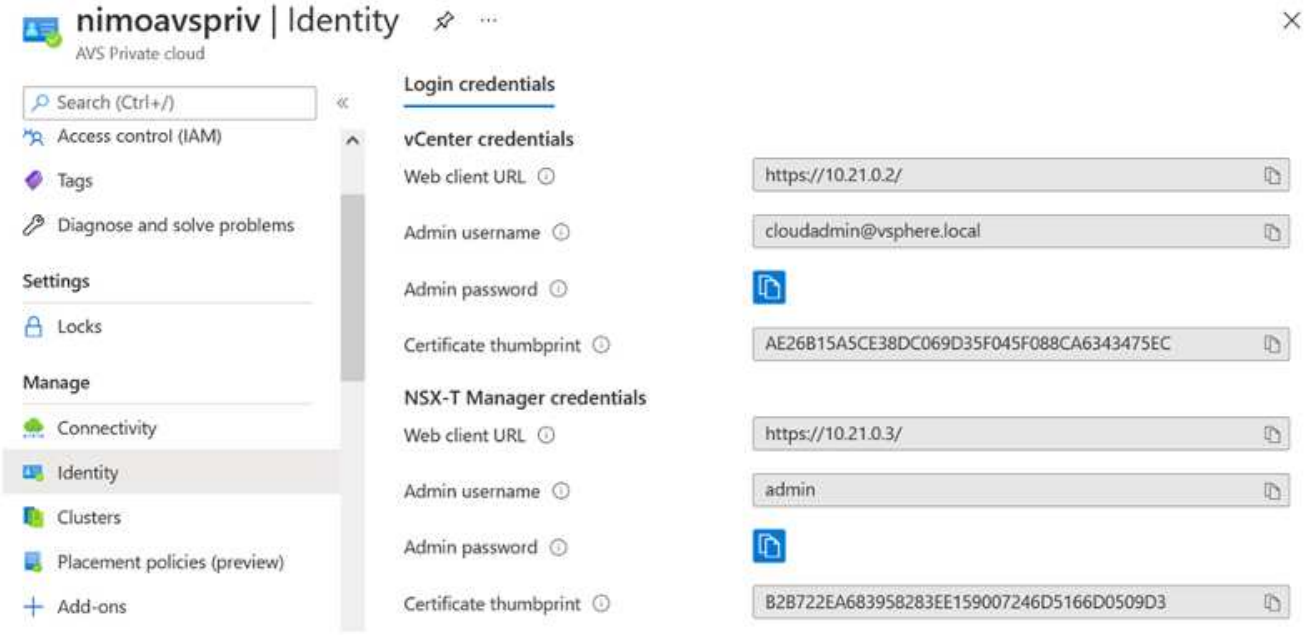
La solución para VMware Azure no le permite gestionar un cloud privado con VMware vCenter en las instalaciones. En su lugar, se requiere el host de salto para conectarse a la instancia de Azure VMware Solution vCenter. Cree un host de salto en el grupo de recursos designado e inicie sesión en Azure VMware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



Después de aprovisionar la máquina virtual, utilice la opción Connect para acceder a RDP.

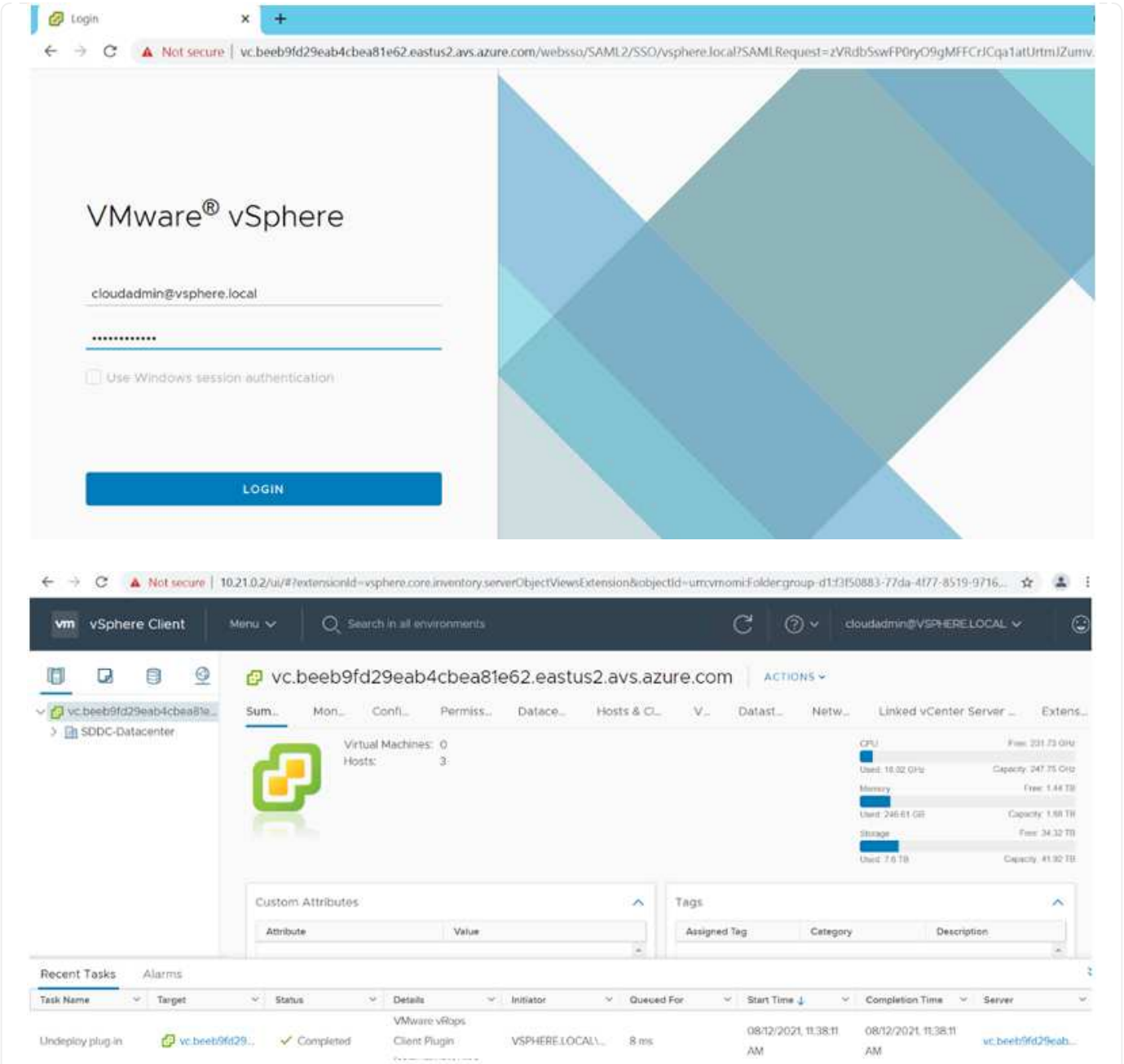


Inicie sesión en vCenter desde esta máquina virtual de host de salto recién creada mediante el usuario administrador de la nube . Para acceder a las credenciales, vaya al portal de Azure y vaya a Identity (en la opción Manage dentro de la nube privada). Desde aquí, se pueden copiar las URL y las credenciales de usuario del cloud privado vCenter y NSX-T Manager.



En la máquina virtual Windows, abra un explorador y desplácese hasta la URL del cliente web de vCenter y utilice el nombre de usuario admin como **cloudadmin@vsphere.locloc l** y pegue la contraseña copiada. De igual modo, también es posible acceder al administrador de NSX-T mediante la URL del cliente web utilice el nombre de usuario admin y pegue la contraseña copiada para crear segmentos nuevos o modificar las puertas de enlace del nivel existente.

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



Ahora se pone en marcha y configura el SDDC de la solución para Azure VMware. Aproveche ExpressRoute Global REACH para conectar el entorno local al cloud privado de la solución VMware para Azure. Para obtener más información, consulte "Configurar de forma conjunta los entornos locales en la solución Azure VMware".

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

Al igual que en las instalaciones, la planificación de Google Cloud VMware Engine (GCVE) es crucial para un entorno listo para la producción con éxito para la creación de equipos virtuales y la migración.

En esta sección se describe cómo configurar y gestionar GCVE y cómo utilizarlo junto con las opciones disponibles para conectar el almacenamiento de NetApp.

El proceso de configuración puede dividirse en los siguientes pasos:

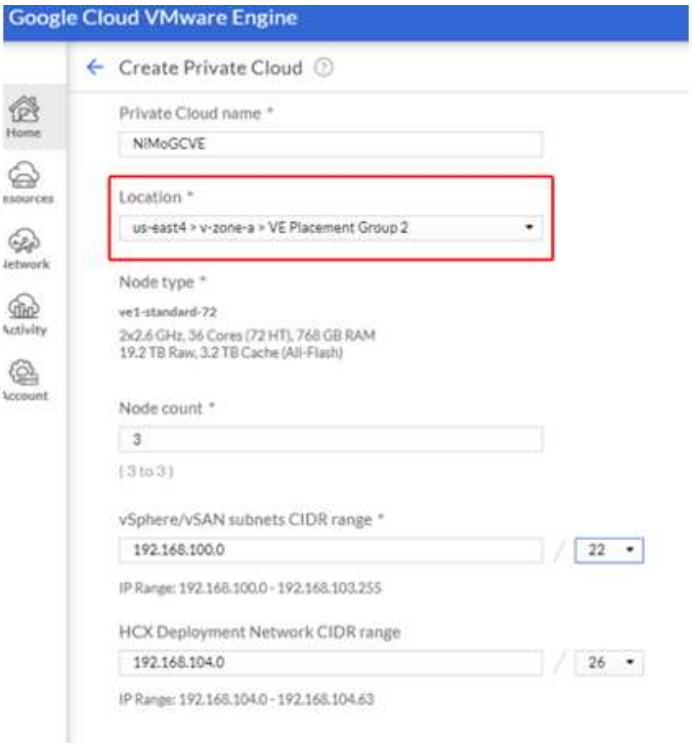
Implementar y configurar GCVE

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

Haga clic en el botón “New Private Cloud” e introduzca la configuración deseada para GCVE Private Cloud. En “ubicación”, asegúrese de poner en marcha el cloud privado en la misma región/zona donde se pone en marcha CVS/CVO, para garantizar el mejor rendimiento y la menor latencia.

Requisitos previos:

- Configurar el rol del IAM de administración de servicio del motor VMware
- "Habilite el acceso a la API de VMware Engine y la cuota de nodo"
- Asegúrese de que la gama CIDR no se superpone con ninguna de las subredes en las instalaciones o en la nube. El rango CIDR debe ser /27 o superior.



Nota: La creación de clouds privados puede tardar entre 30 minutos y 2 horas.

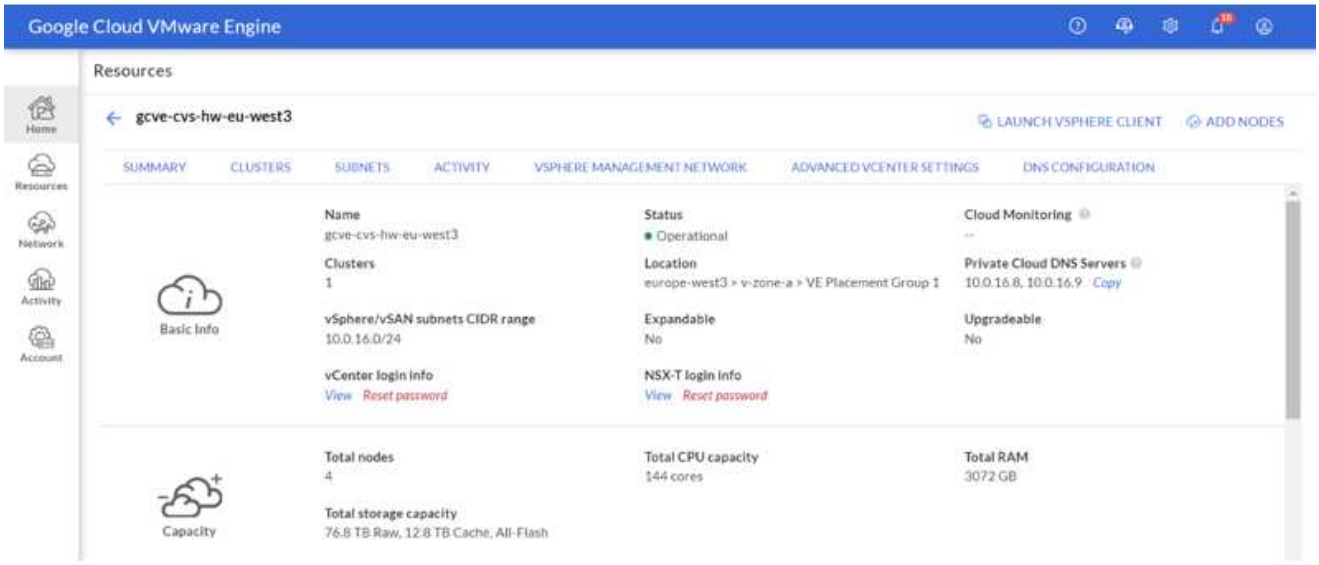
Active el acceso privado a GCVE

Una vez aprovisionado el cloud privado, configure el acceso privado al cloud privado para obtener una conexión de ruta de datos de alto rendimiento y baja latencia.

De este modo, se asegurará de que la red VPC en la que se ejecutan las instancias de Cloud Volumes ONTAP pueda comunicarse con la nube privada de GCVE. Para ello, siga la "Documentación para GCP". Para Cloud Volume Service, establezca una conexión entre VMware Engine y Cloud Volumes Service mediante la ejecución de un par de tiempo único entre los proyectos de host de inquilinos. Siga estos pasos para obtener más información "enlace".

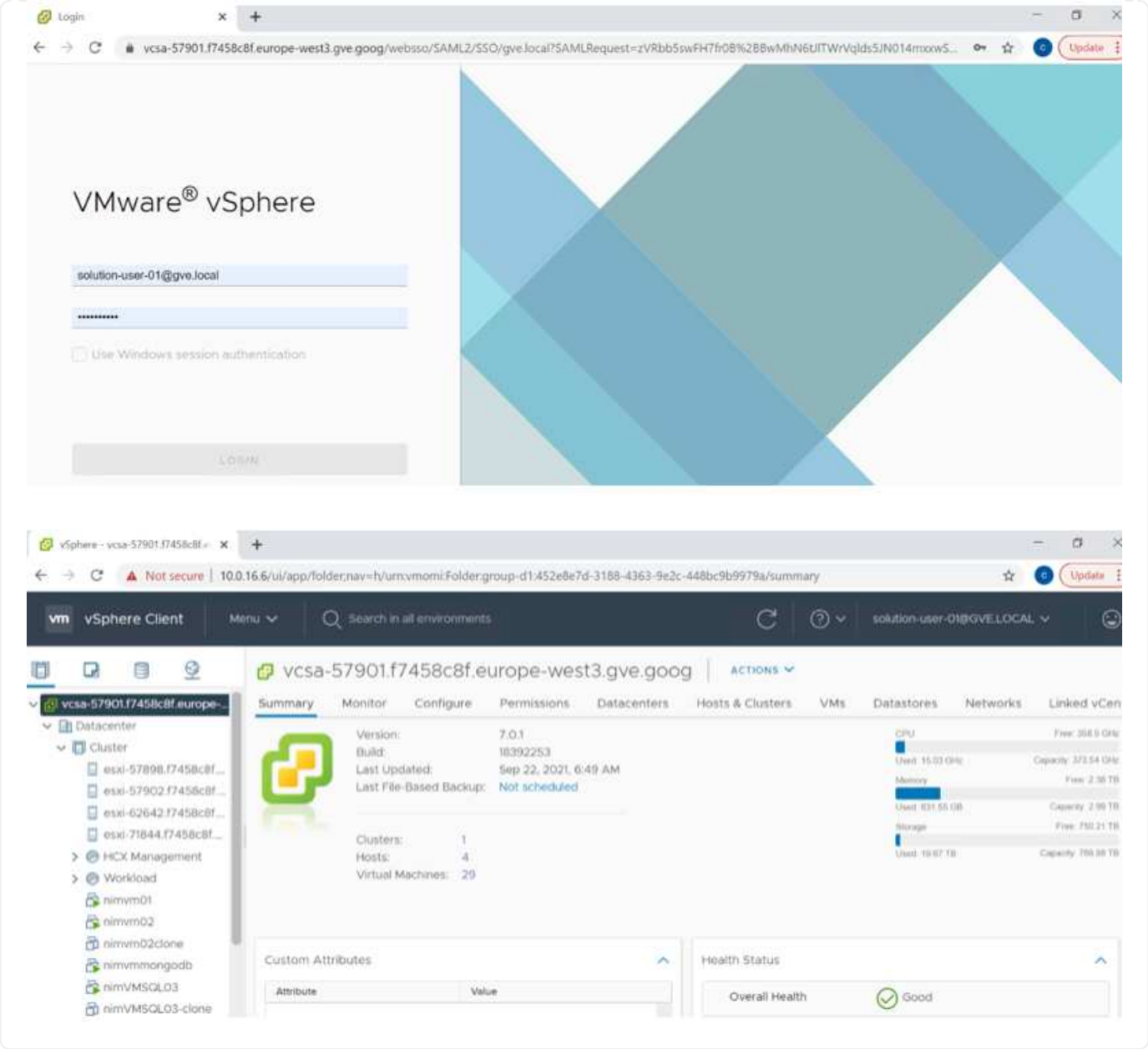
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

Inicie sesión en vcenter con el usuario CloudOwner@gve.loc/. Para acceder a las credenciales, vaya al portal VMware Engine, vaya a Resources y seleccione la nube privada adecuada. En la sección Basic info, haga clic en el enlace View para 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 Windows, abra un explorador y desplácese hasta la URL del cliente web de vCenter Y utilice el nombre de usuario admin como CloudOwner@gve.locloc l y pegue la contraseña copiada. De igual modo, también es posible acceder al administrador de NSX-T mediante la URL del cliente web utilice el nombre de usuario admin y pegue la contraseña copiada para crear segmentos nuevos o modificar las puertas de enlace del nivel existente.

Para conectar desde una red local a un cloud privado con motor de VMware, aproveche la VPN de cloud o la interconexión de cloud para obtener la conectividad adecuada y asegúrese de que los puertos necesarios estén abiertos. Siga estos pasos para obtener más información "enlace".



Implemente el almacén de datos complementario del servicio de volúmenes de cloud de NetApp en GCVE

Consulte "Procedimiento para implementar un almacén de datos NFS complementario con NetApp CVS en GCVE"

Opciones de almacenamiento de NetApp para proveedores de cloud público

Explore las opciones para NetApp como almacenamiento en los tres principales proveedores a hiperescala.

AWS/VMC

AWS admite almacenamiento de NetApp con las siguientes configuraciones:

- FSX ONTAP como almacenamiento conectado como invitado
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado
- FSX ONTAP como almacén de datos NFS complementario

Vea el detalles "Opciones de almacenamiento de conexión para invitado para VMC". Vea el detalles "Opciones suplementarias de almacén de datos de NFS para VMC".

Azure / AVS

Azure admite almacenamiento de NetApp en las siguientes configuraciones:

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

Vea el detalles "Opciones de almacenamiento de Guest Connect para AVS". Vea el detalles "Opciones complementarias de almacén de datos NFS para AVS".

GCP/GCVE

Google Cloud es compatible con almacenamiento de NetApp en las siguientes configuraciones:

- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado
- Cloud Volumes Service (CVS) como almacenamiento conectado como invitado
- Cloud Volumes Service (CVS) como almacén de datos NFS complementario

Vea el detalles "Opciones de almacenamiento de Guest Connect para GCVE".

Más información acerca de "Soporte de almacén de datos de Cloud Volumes Service de NetApp para Google Cloud VMware Engine (blog de NetApp)" o. "Cómo usar CVS de NetApp como almacenes de datos para Google Cloud VMware Engine (blog de Google)"

TR-4938: Monte Amazon FSX para ONTAP como almacén de datos NFS con VMware Cloud en AWS

Niyaz Mohamed, NetApp

Introducción

Todas las organizaciones exitosas se encuentran en el camino de la transformación y la modernización. Como parte de este proceso, las empresas suelen usar sus inversiones existentes en VMware para aprovechar las ventajas de la nube y explorar cómo migrar, aumentar, ampliar y ofrecer recuperación tras desastres a los procesos de la manera más fluida posible. Los clientes que migran al cloud deben evaluar los casos de uso de elasticidad y ráfaga, salida del centro de datos, consolidación del centro de datos, escenarios de fin de la vida útil, fusiones, adquisiciones, etc.

Aunque VMware Cloud en AWS es la opción preferida para la mayoría de los clientes, ya que ofrece funcionalidades híbridas únicas a los clientes, las opciones de almacenamiento nativo limitadas han restringido su utilidad para organizaciones con cargas de trabajo con un gran volumen de almacenamiento.

Debido a que el almacenamiento está directamente ligado a los hosts, la única forma de escalar el almacenamiento es añadir más hosts, lo cual puede aumentar los costes entre un 35 % y un 40 % o más para cargas de trabajo con un uso intensivo del almacenamiento. Estas cargas de trabajo necesitan almacenamiento adicional y rendimiento segregado, no una potencia adicional, pero esto implica pagar por hosts adicionales. Aquí es donde el "integración reciente" El de FSX para ONTAP resulta muy útil para cargas de trabajo con un uso intensivo del almacenamiento y el rendimiento con VMware Cloud en AWS.

Consideremos el siguiente caso: Un cliente requiere ocho hosts para la potencia (vCPU/vmem), pero también tienen un requisito fundamental para el almacenamiento. Tras su evaluación, necesitan 16 hosts para satisfacer los requisitos de almacenamiento. Esto aumenta el TCO general porque deben comprar toda la capacidad adicional cuando todo lo que realmente necesitan es más almacenamiento. Esto es aplicable en cualquier caso de uso, incluidos la migración, la recuperación ante desastres, bursting, prueba/desarrollo, y así sucesivamente.

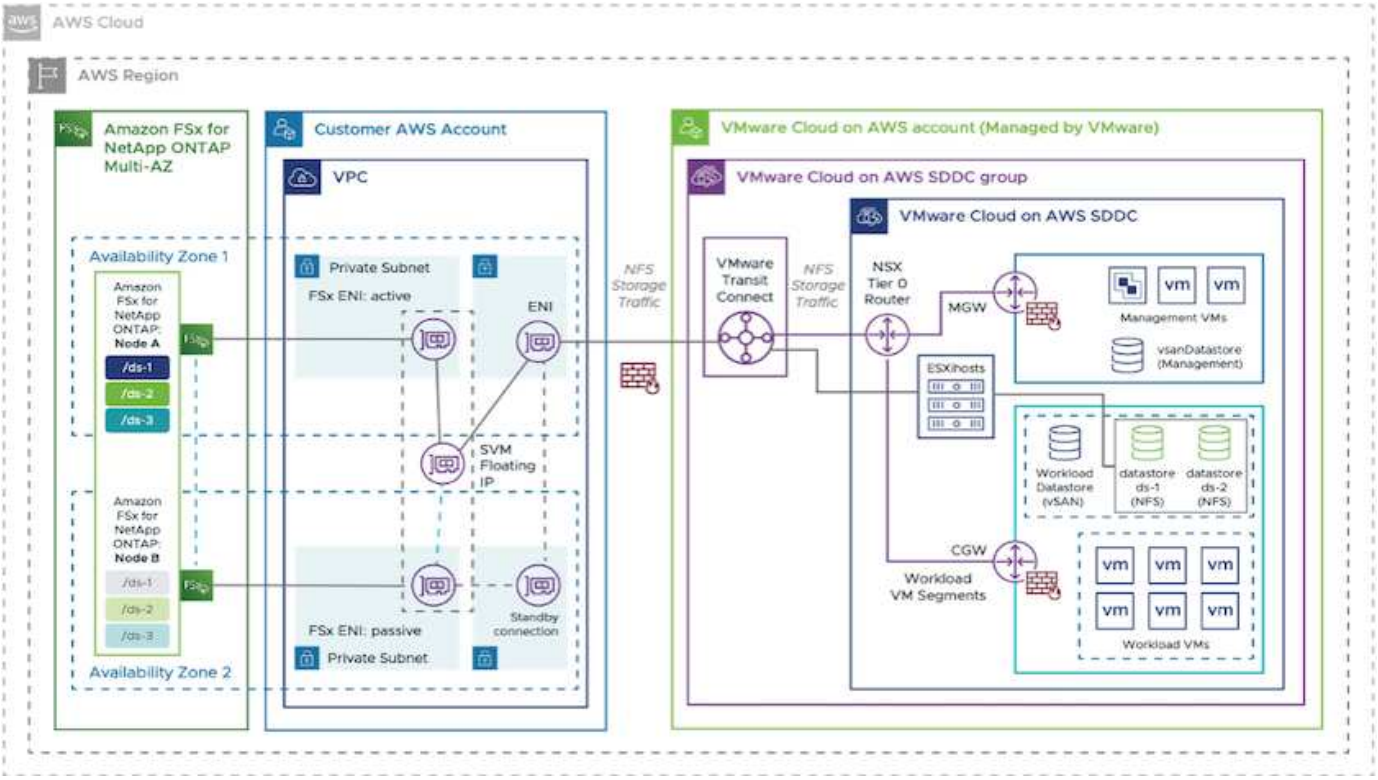
Este documento le guía por los pasos necesarios para aprovisionar y conectar FSX para ONTAP como almacén de datos NFS para VMware Cloud en AWS.

Esta solución también está disponible en VMware. Visite la "Cloud Tech Zone de VMware" si quiere más información.

Opciones de conectividad

VMware Cloud en AWS es compatible con las puestas en marcha de FSX para ONTAP, tanto de Multi-AZ como de Single-AZ.

En esta sección se describe la arquitectura de conectividad de alto nivel junto con los pasos necesarios para implementar la solución para ampliar el almacenamiento en un clúster SDDC sin la necesidad de añadir hosts adicionales.



Los pasos de puesta en marcha de alto nivel son los siguientes:

1. Cree Amazon FSX para ONTAP en un VPC designado nuevo.
2. Cree un grupo SDDC.
3. Cree VMware Transit Connect y un accesorio TGW.
4. Configurar enrutamiento (AWS VPC y SDDC) y grupos de seguridad.
5. Conecte un volumen NFS como almacén de datos al clúster SDDC.

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

FSX para ONTAP no es compatible actualmente con clústeres extendidos.

Conclusión

Este documento abarca los pasos necesarios para configurar Amazon FSX para ONTAP con el cloud de VMware en AWS. Amazon FSX para ONTAP proporciona opciones excelentes para poner en marcha y gestionar las cargas de trabajo de aplicaciones junto con servicios de archivos y reducir el TCO, ya que hace que los requisitos de datos sean fluido en la capa de la aplicación. Sea cual sea el caso práctico, elija VMware Cloud en AWS junto con Amazon FSX para ONTAP para obtener la rápida comprensión de las ventajas del cloud, una infraestructura consistente y operaciones desde las instalaciones a AWS, la portabilidad bidireccional de cargas de trabajo, y la capacidad y el rendimiento de clase empresarial. Es el mismo proceso y procedimientos que ya conoce y que se utilizan para conectar el almacenamiento. Recuerde que solo la posición de los datos ha cambiado con nuevos nombres, las herramientas y los procesos siguen siendo los mismos y Amazon FSX para ONTAP ayuda a optimizar la implementación general.

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

Amazon FSx para VMware Cloud de ONTAP

Opciones de almacenamiento conectado invitado de NetApp para AWS

AWS admite almacenamiento de NetApp conectado como invitado con el servicio FSX nativo (FSX ONTAP) o Cloud Volumes ONTAP (CVO).

FSX ONTAP

Amazon FSX para ONTAP de NetApp es un servicio completamente gestionado que ofrece un almacenamiento de archivos muy fiable, escalable, de alto rendimiento y con numerosas funciones integrado en el popular sistema de archivos ONTAP de NetApp. FSX para ONTAP combina las funciones, el rendimiento, las funcionalidades y las operaciones API de los sistemas de archivos de NetApp con la agilidad, la escalabilidad y la simplicidad de un servicio AWS totalmente gestionado.

FSX para ONTAP proporciona un almacenamiento de archivos compartido con gran diversidad de funciones, rápido y flexible, al que se puede acceder ampliamente desde instancias informáticas de Linux, Windows y MacOS que se ejecutan en AWS o en las instalaciones. FSX para ONTAP ofrece un almacenamiento en unidades de estado sólido (SSD) de alto rendimiento con latencias inferiores a milisegundos. Con FSX para ONTAP, puede obtener niveles de SSD de rendimiento de su carga de trabajo a la vez que paga el almacenamiento SSD por una pequeña fracción de sus datos.

La gestión de los datos con FSX para ONTAP es más sencilla porque puede crear copias Snapshot, clonar y replicar los archivos con solo hacer clic en un botón. Además, FSX para ONTAP ordena automáticamente los datos en niveles para un almacenamiento elástico de menor coste, reduciendo así la necesidad de

aprovisionar o gestionar capacidad.

FSX para ONTAP también proporciona un almacenamiento duradero y de alta disponibilidad con backups totalmente gestionados y soporte para la recuperación ante desastres en toda la región. Para facilitar la protección y seguridad de sus datos, FSX para ONTAP admite la seguridad de datos y aplicaciones antivirus más conocidas.

FSX ONTAP como almacenamiento conectado como invitado

Configure Amazon FSX para ONTAP de NetApp con VMware Cloud en AWS

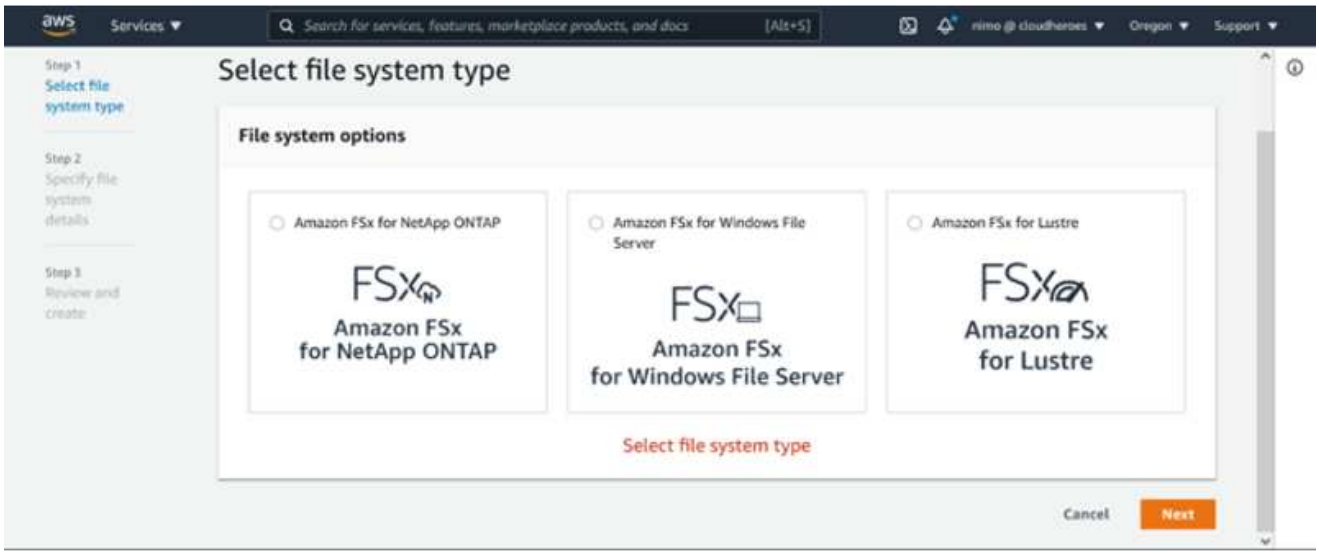
Se pueden montar LUN y recursos compartidos de archivos de Amazon FSX para ONTAP de NetApp a partir de máquinas virtuales creadas dentro del entorno VMware SDDC en VMware Cloud en AWS. Los volúmenes también pueden montarse en el cliente Linux y asignarse en el cliente Windows mediante el protocolo NFS o SMB, y se puede acceder A LAS LUN en clientes Linux o Windows como dispositivos de bloque cuando se montan mediante iSCSI. Amazon FSX para el sistema de archivos ONTAP de NetApp puede configurarse rápidamente con los siguientes pasos.

Amazon FSX para ONTAP de NetApp y VMware Cloud en AWS debe estar en la misma zona de disponibilidad para conseguir un mejor rendimiento y evitar cargos por transferencia de datos entre zonas de disponibilidad.

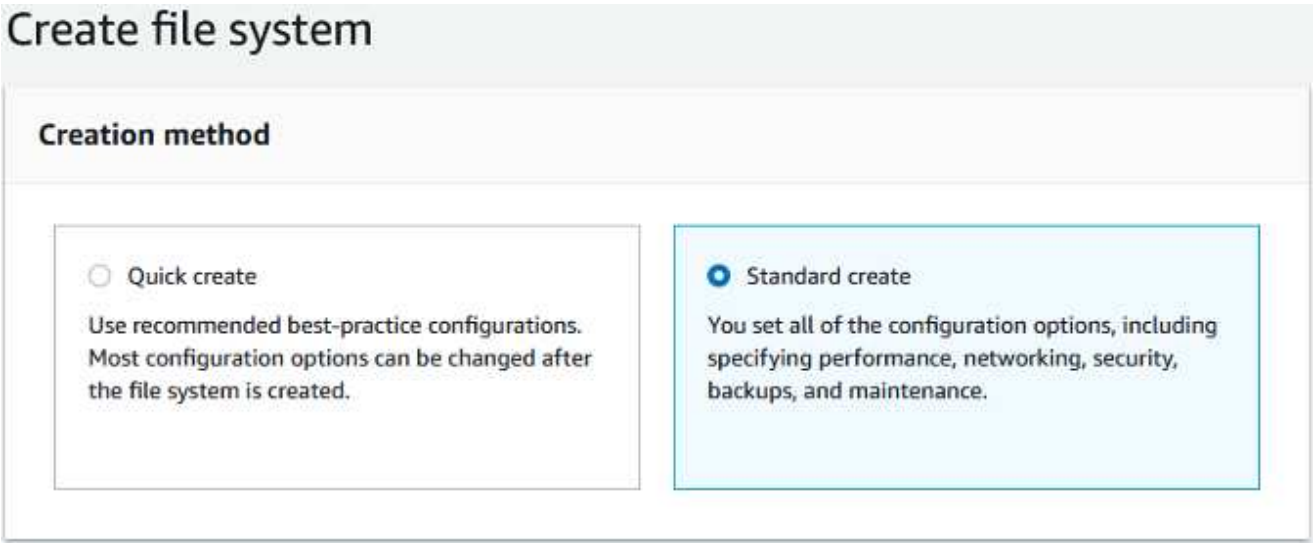
Cree y monte Amazon FSX para volúmenes de ONTAP

Para crear y montar el sistema de archivos Amazon FSX para ONTAP de NetApp, lleve a cabo los siguientes pasos:

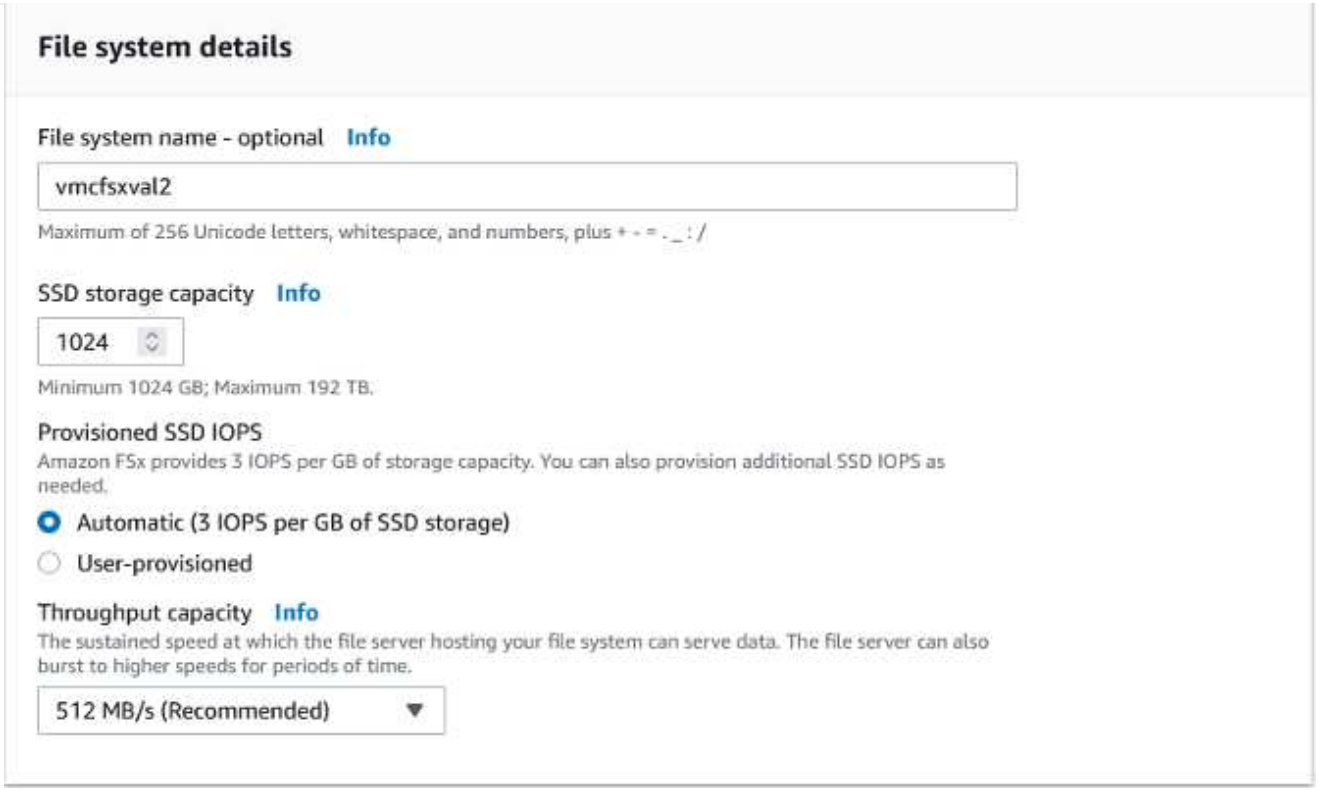
1. Abra el "Consola de Amazon FSX" Y elija Crear sistema de archivos para iniciar el asistente de creación del sistema de archivos.
2. En la página Select File System Type, seleccione Amazon FSX para ONTAP de NetApp y, a continuación, seleccione Next. Aparece la página Crear sistema de archivos.



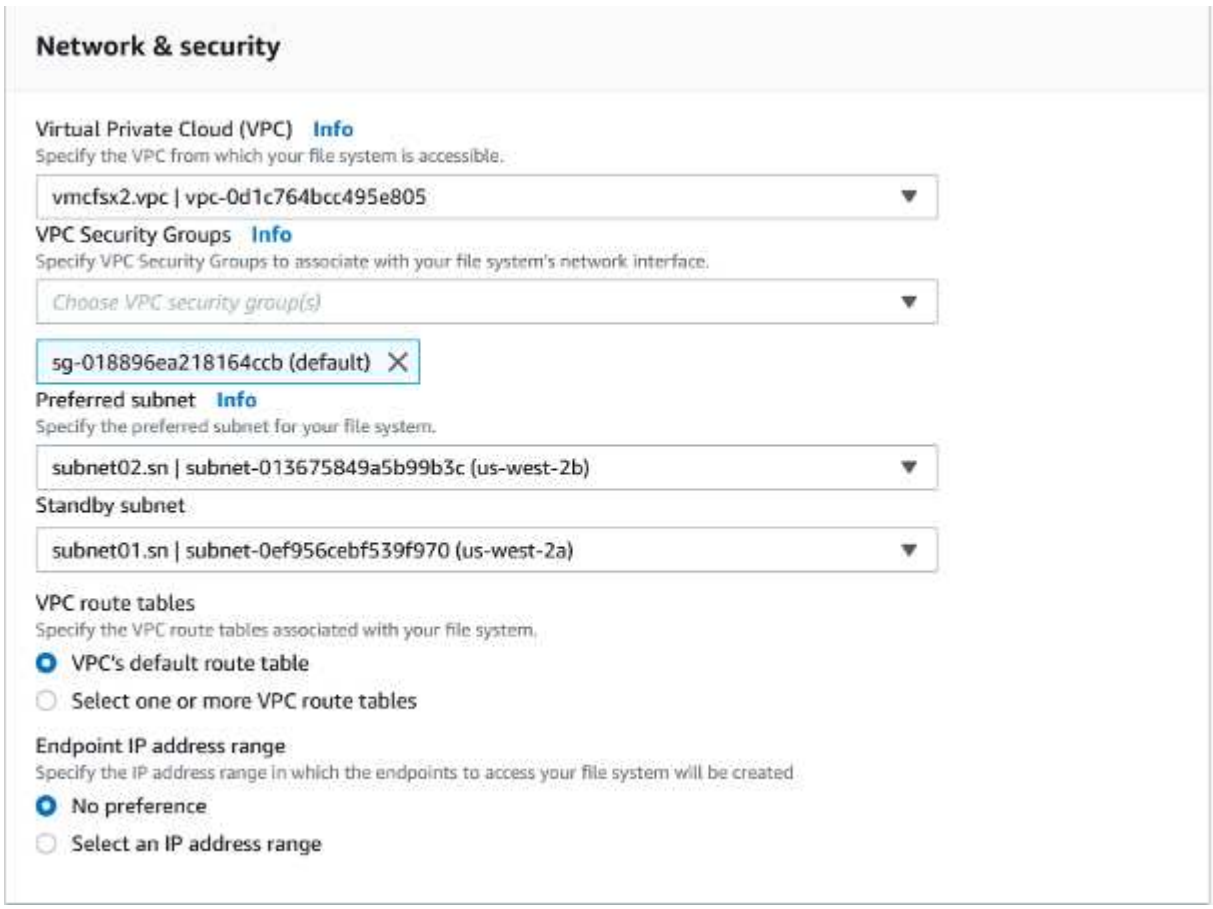
1. En la sección Networking, para la nube privada virtual (VPC), elija el VPC adecuado y las subredes preferidas junto con la tabla de rutas. En este caso, se selecciona vmcfsx2.vpc en la lista desplegable.



1. Para el método de creación, seleccione creación estándar. También puede seleccionar creación rápida, pero este documento utiliza la opción creación estándar.

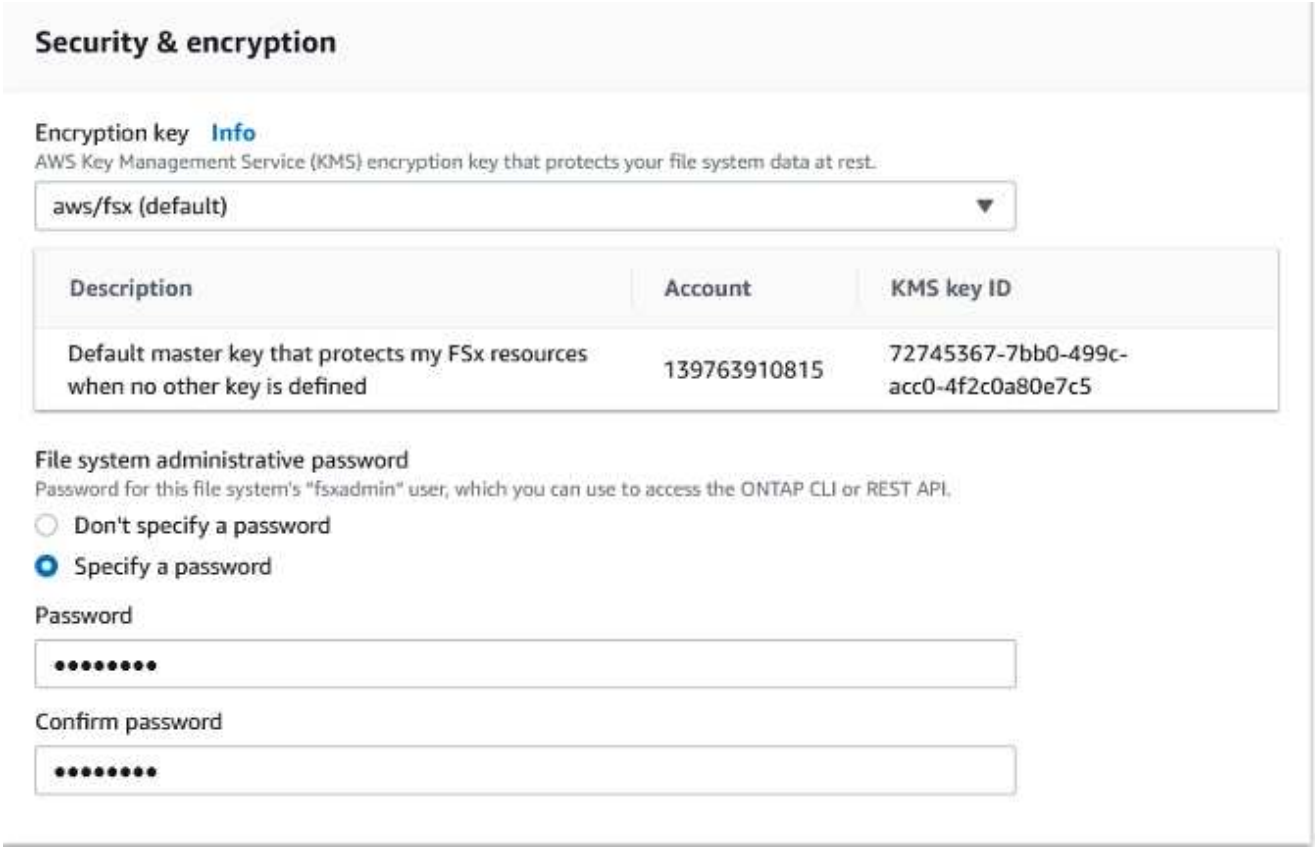


1. En la sección Networking, para la nube privada virtual (VPC), elija el VPC adecuado y las subredes preferidas junto con la tabla de rutas. En este caso, se selecciona vmcfsx2.vpc en la lista desplegable.

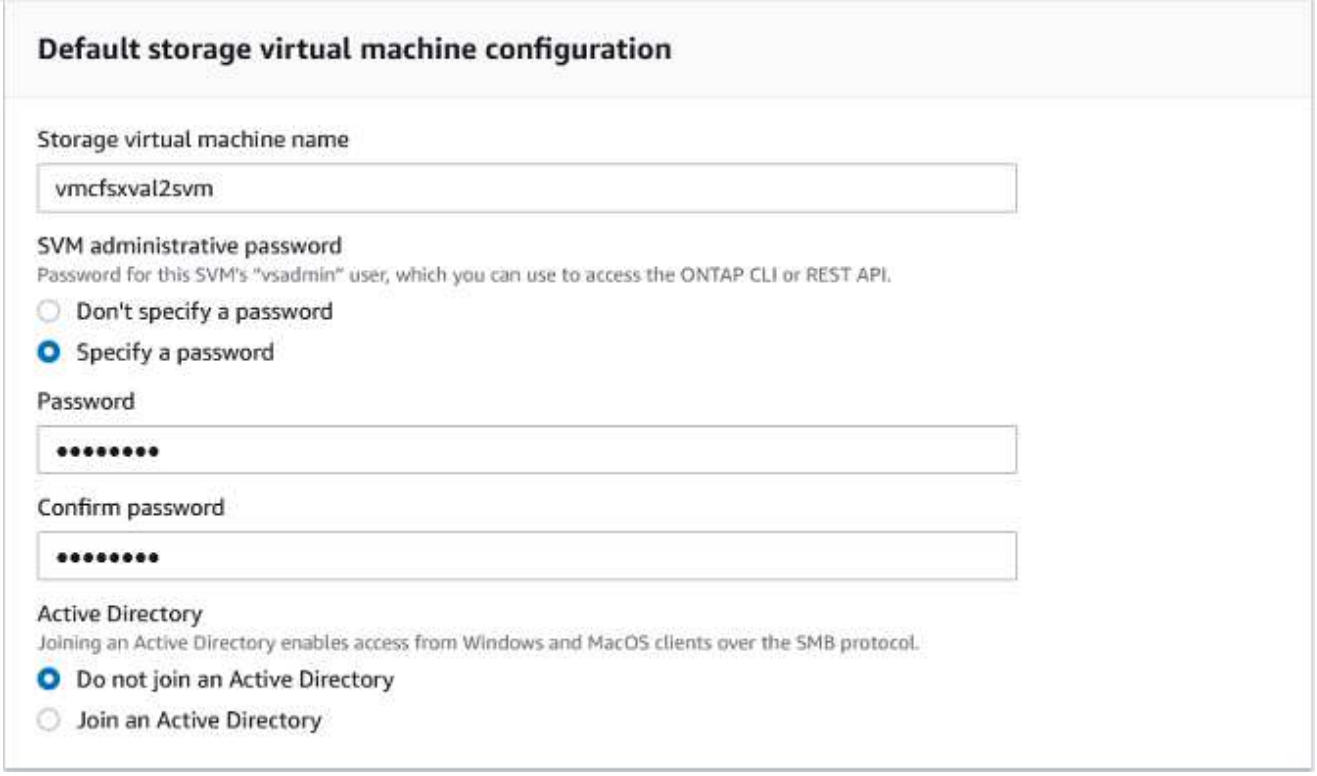


En la sección Networking, para la nube privada virtual (VPC), elija el VPC adecuado y las subredes preferidas junto con la tabla de rutas. En este caso, se selecciona vmcfsx2.vpc en la lista desplegable.

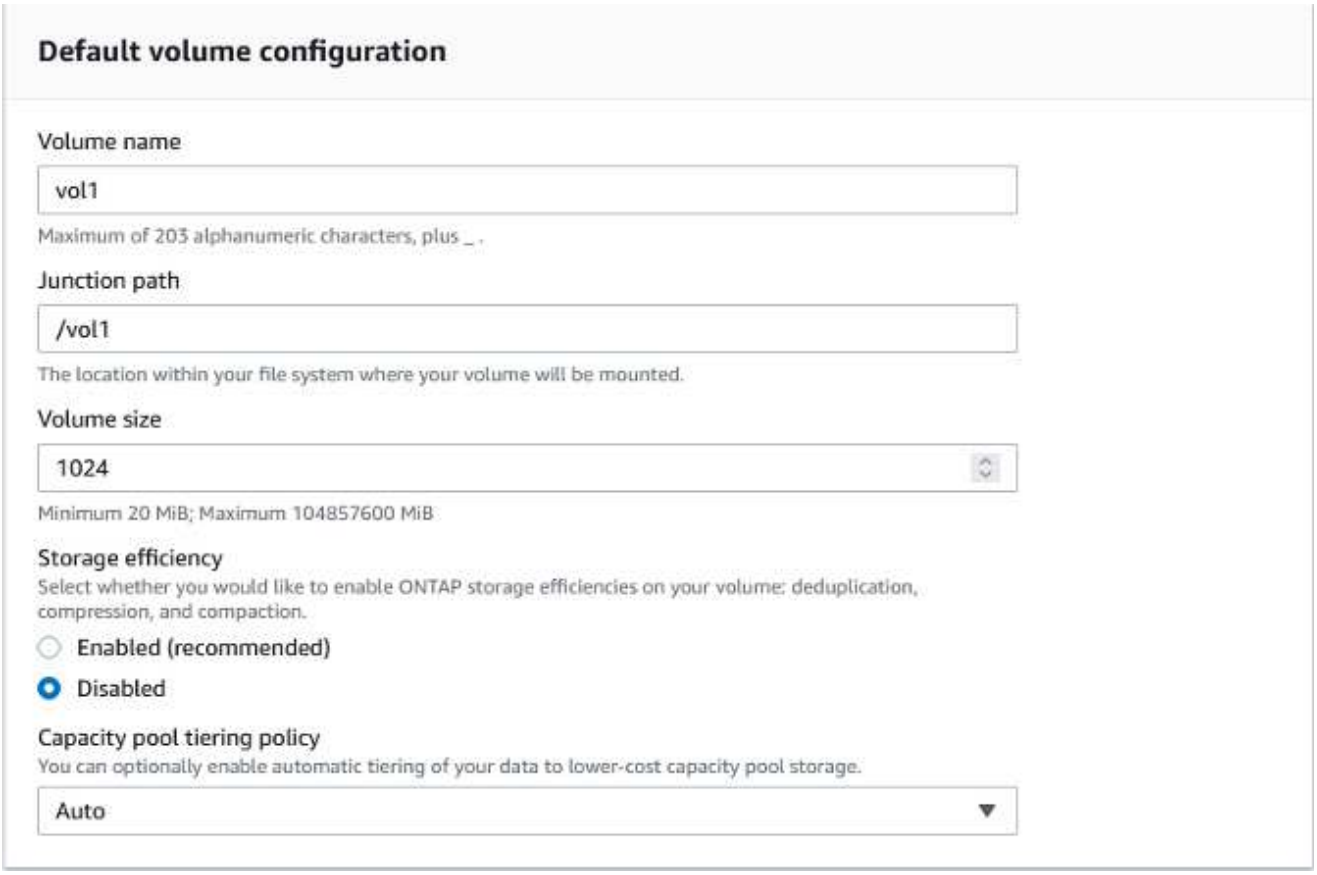
1. En la sección Security & Encryption, en la clave de cifrado, elija la clave de cifrado del servicio de gestión de claves de AWS (AWS KMS) que protege los datos del sistema de archivos en reposo. Para la contraseña administrativa del sistema de archivos, introduzca una contraseña segura para el usuario fsxadmin.



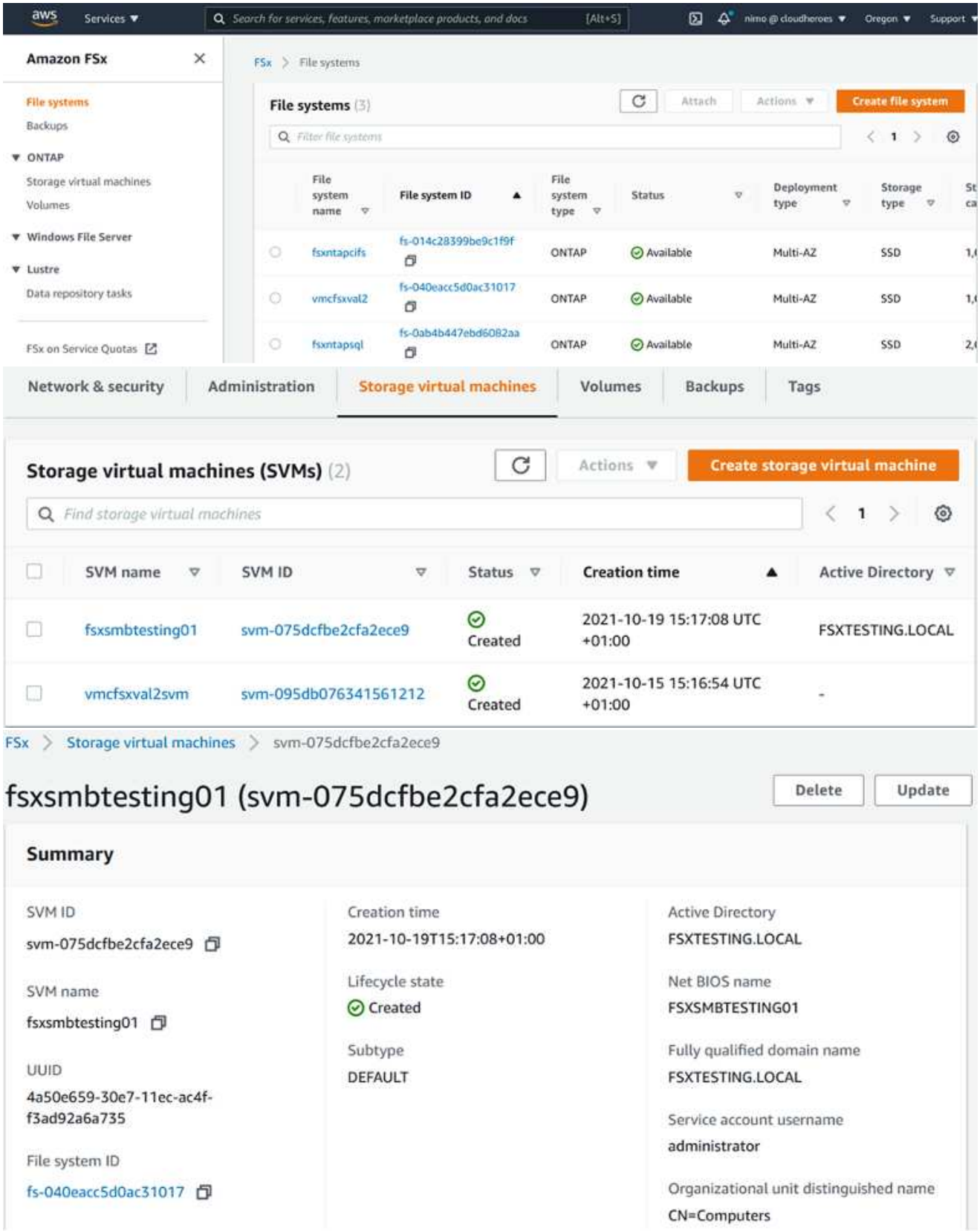
1. En la máquina virtual y especifique la contraseña para su uso con vsadmin para administrar ONTAP mediante las API DE REST o la CLI. Si no se especifica ninguna contraseña, se puede utilizar un usuario fsxadmin para administrar la SVM. En la sección Active Directory, asegúrese de unirse a Active Directory a la SVM para aprovisionar los recursos compartidos de SMB. En la sección Default Storage Virtual Machine Configuration, proporcione un nombre para el almacenamiento en esta validación, los recursos compartidos de SMB se aprovisionan mediante un dominio de Active Directory autogestionado.



1. En la sección Default Volume Configuration, especifique el nombre y el tamaño del volumen. Este es un volumen NFS. Para la eficiencia del almacenamiento, elija Activado para activar las funciones de eficiencia del almacenamiento de ONTAP (compresión, deduplicación y compactación) o Desactivado 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.

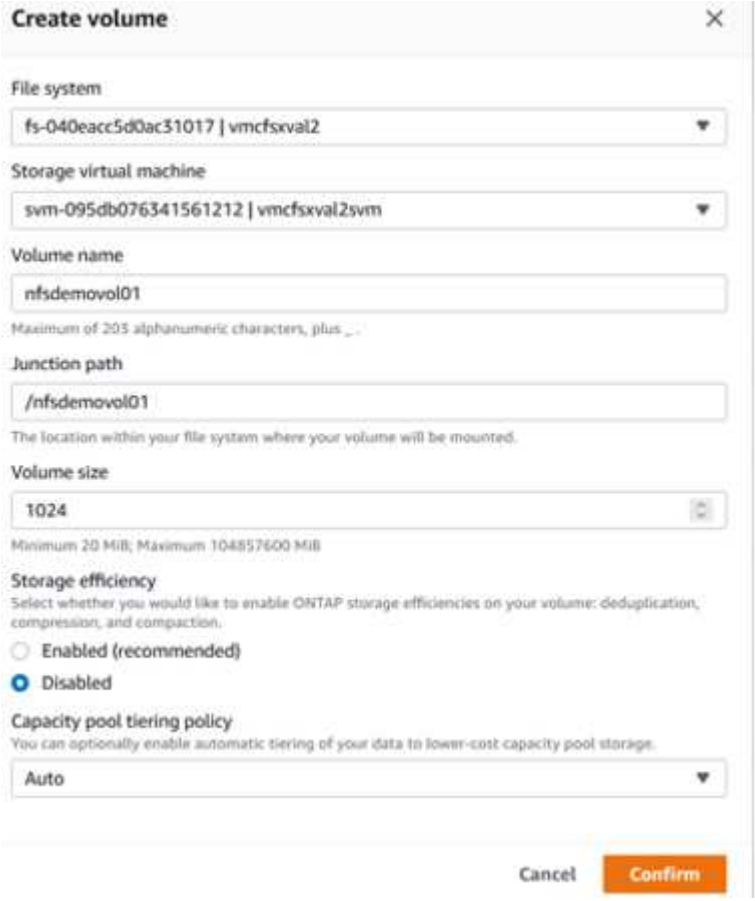


Para obtener información detallada, consulte "Introducción a Amazon FSX para ONTAP de NetApp".

Después de crear el sistema de archivos como se ha mencionado anteriormente, cree el volumen con el tamaño y el protocolo necesarios.

1. Abra el "Consola de Amazon FSX".
2. En el panel de navegación de la izquierda, elija 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. Se muestra el cuadro de diálogo Crear volumen.

Por motivos de demostración, se crea un volumen NFS en esta sección que se puede montar fácilmente en máquinas virtuales que se ejecuten en el cloud de VMware en AWS. nfsdemovol01 se crea como se muestra a continuación:



Montaje del volumen ONTAP FSX en el cliente Linux

Para montar el volumen ONTAP FSX creado en el paso anterior. A partir de los equipos virtuales de Linux dentro de VMC en AWS SDDC, complete los pasos siguientes:

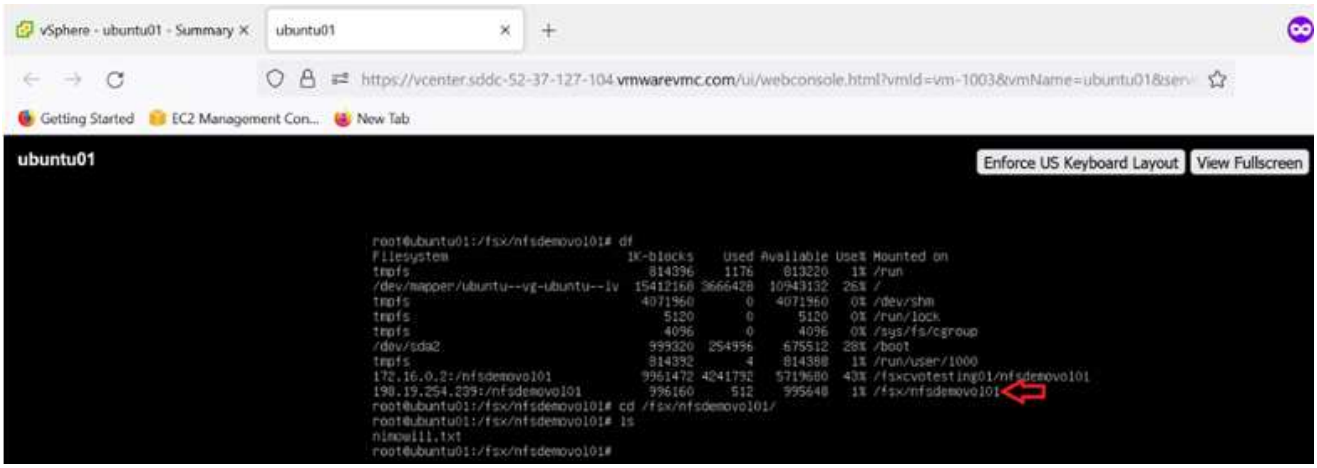
1. Conéctese a la instancia de Linux designada.
2. Abra un terminal en la instancia mediante Secure Shell (SSH) e inicie sesión con las credenciales adecuadas.
3. Cree un directorio para el punto de montaje del volumen con el comando siguiente:

```
 $ sudo mkdir /fsx/nfsdemovol01
. Monte el volumen NFS de Amazon FSX para ONTAP de NetApp en el
directorio creado 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.



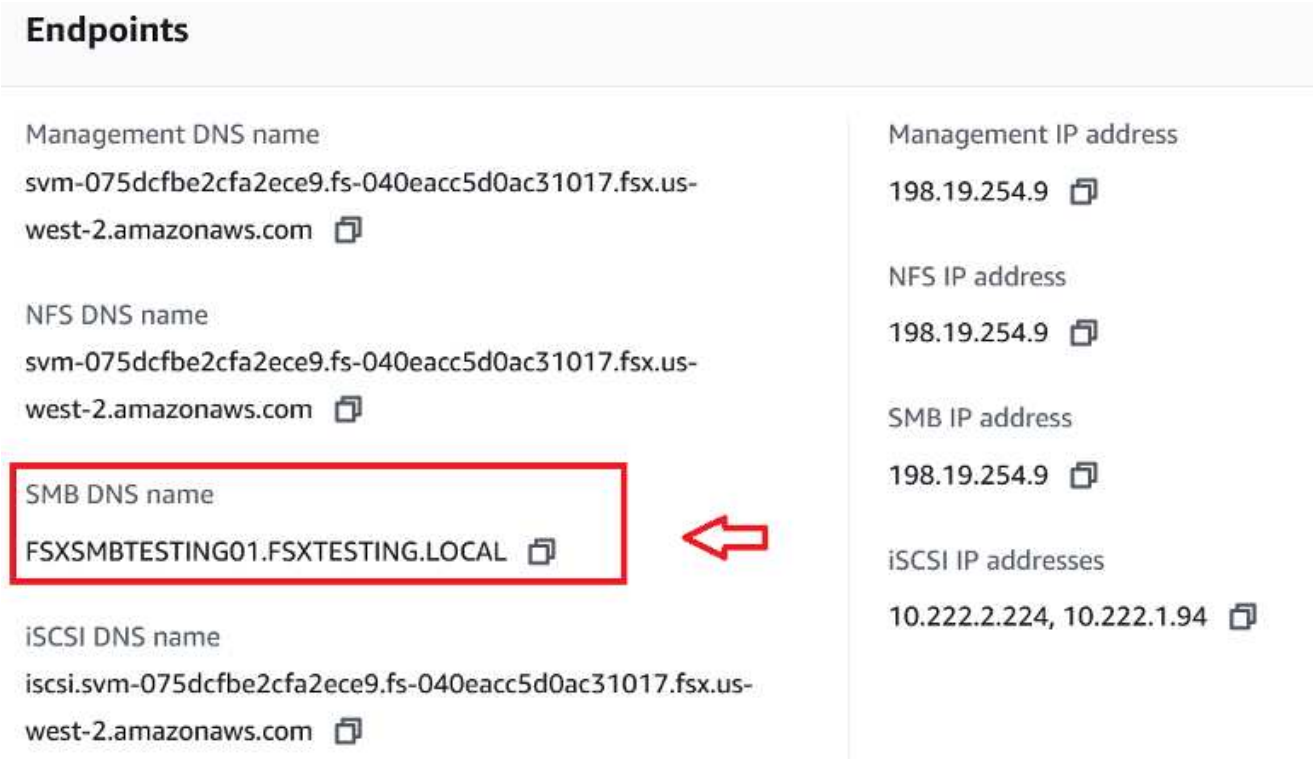
Montaje del volumen ONTAP FSX en el cliente Linux

Conecte volúmenes ONTAP FSX a clientes de Microsoft Windows

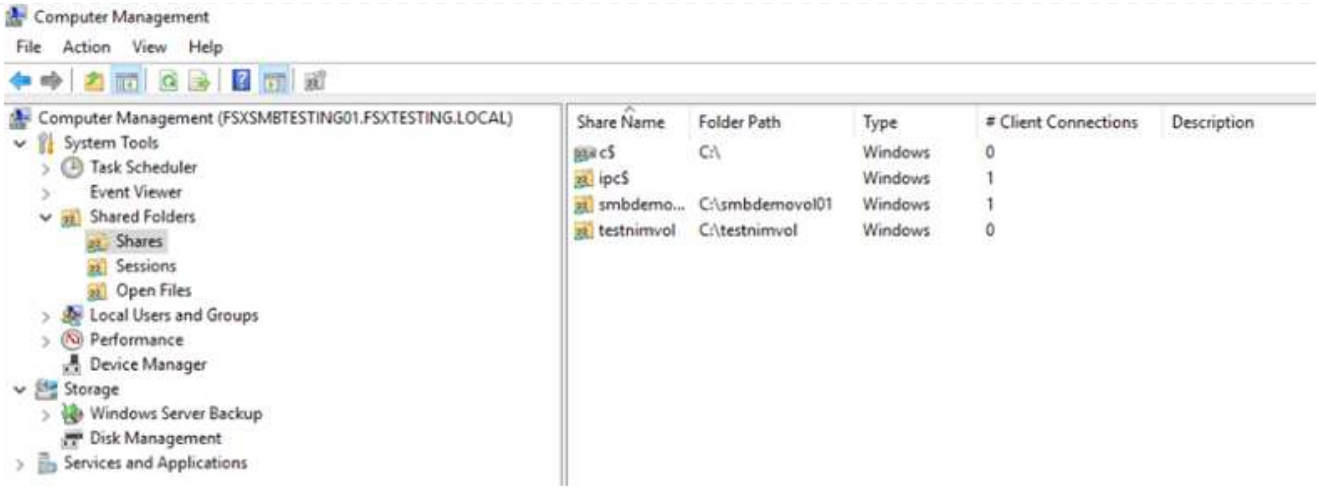
Para administrar y asignar recursos compartidos de archivos en un sistema de archivos Amazon FSX, se debe utilizar la GUI de carpetas compartidas.

1. Abra el menú Inicio y ejecute fsgmt.msc mediante Ejecutar como administrador. Al hacerlo, se abre la herramienta GUI de carpetas compartidas.
2. Haga clic en Acción > todas las tareas y elija conectar a otro equipo.
3. En otro equipo, introduzca el nombre de DNS de la máquina virtual de almacenamiento (SVM). Por ejemplo, se utiliza FSXSMBTESTING01.FSXTESTING.LOCAL en este ejemplo.

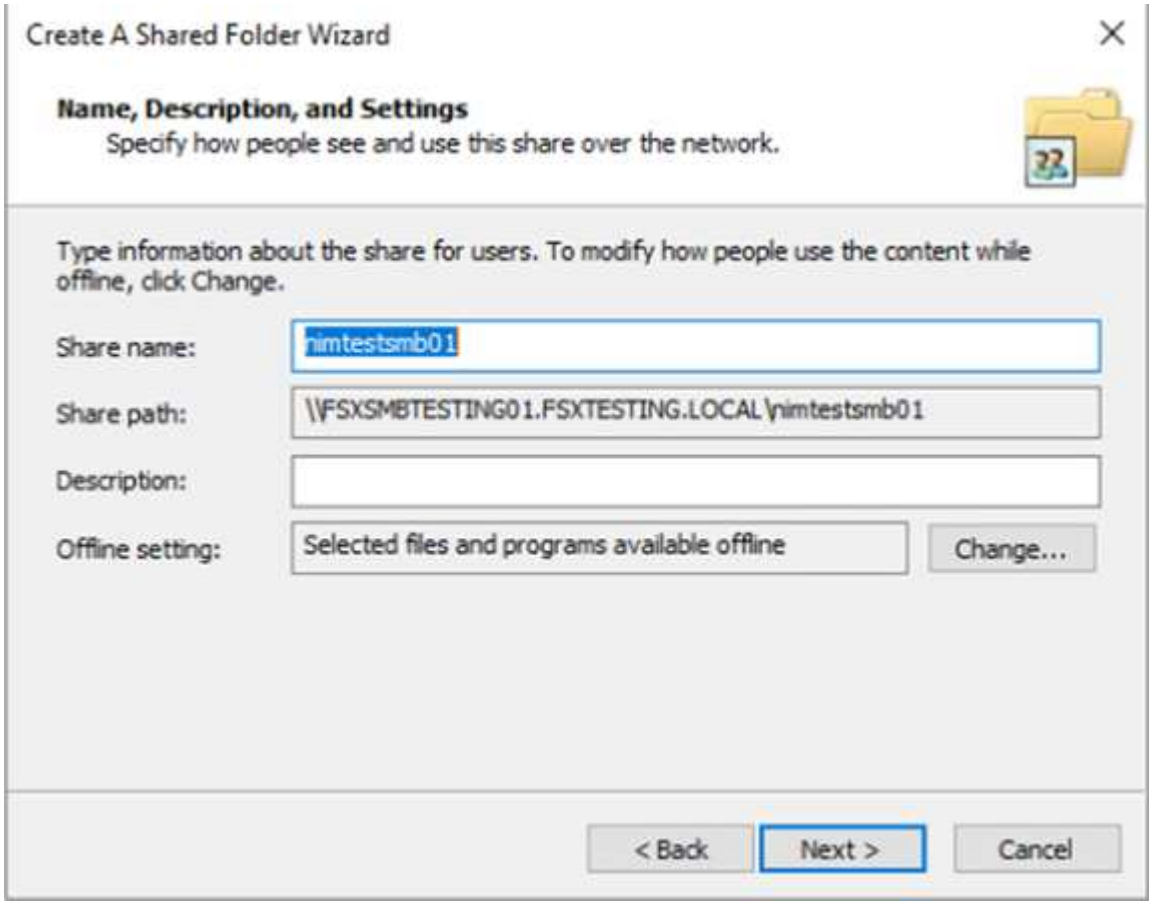
TP encuentra el nombre de DNS de la SVM en la consola de Amazon FSX, elige Storage Virtual Machines, selecciona SVM y, a continuación, desplácese hacia abajo hasta extremos para encontrar el nombre DNS del SMB. Haga clic en Aceptar. El sistema de archivos Amazon FSX aparece en la lista de carpetas compartidas.



1. En la herramienta carpetas compartidas, seleccione recursos compartidos en el panel izquierdo para ver los recursos compartidos activos del sistema de archivos Amazon FSX.

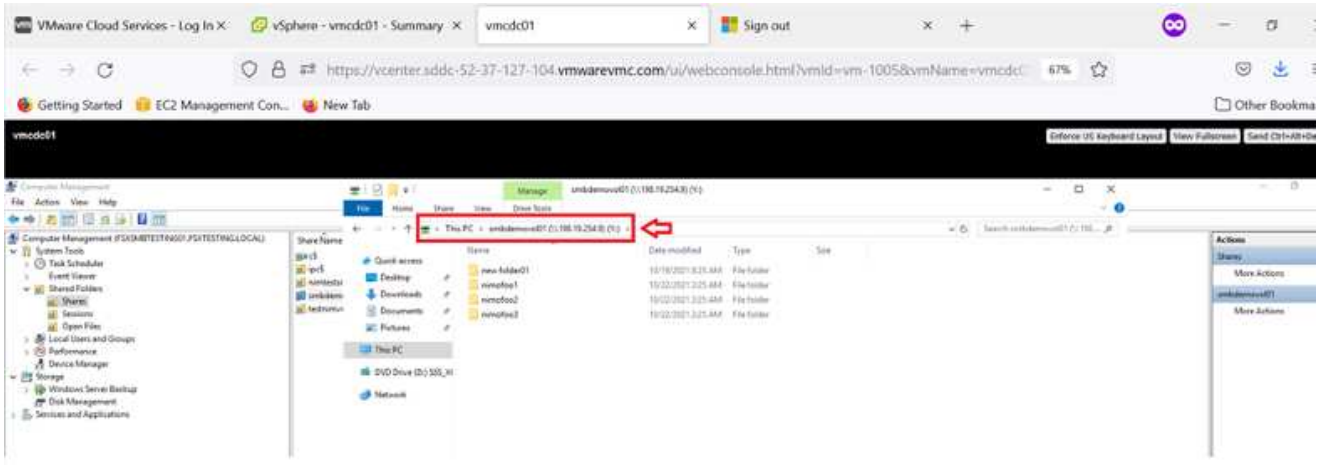


1. Ahora elija un nuevo recurso compartido y complete el asistente Crear una carpeta compartida.



Para obtener más información sobre la creación y gestión de recursos compartidos SMB en un sistema de archivos Amazon FSX, consulte "Creación de recursos compartidos de SMB".

1. Una vez que se ha establecido la conectividad, el recurso compartido de SMB se puede conectar y utilizar para los datos de las aplicaciones. Para ello, copie la ruta de uso compartido y utilice la opción Map Network Drive para montar el volumen en el equipo virtual que se ejecuta en VMware Cloud en el centro de datos definido por software de AWS.



Conecte un FSX para la LUN de ONTAP de NetApp a un host mediante iSCSI

Conecte un FSX para la LUN de ONTAP de NetApp 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 para ONTAP de NetApp, siga la documentación encontrada "aquí".

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

En este documento, se muestra la conexión del LUN iSCSI a un host Windows:

Aprovisionar un LUN en FSX para ONTAP de NetApp:

1. Acceda a la CLI de ONTAP de NetApp mediante el puerto de gestión de FSX para el sistema de archivos ONTAP.
2. Cree las LUN con el tamaño necesario tal y como se indica en la salida de ajuste de tamaño.

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

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

1. Cree los iGroups necesarios para controlar qué hosts tienen acceso a una LUN específica.

```
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 las 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
```

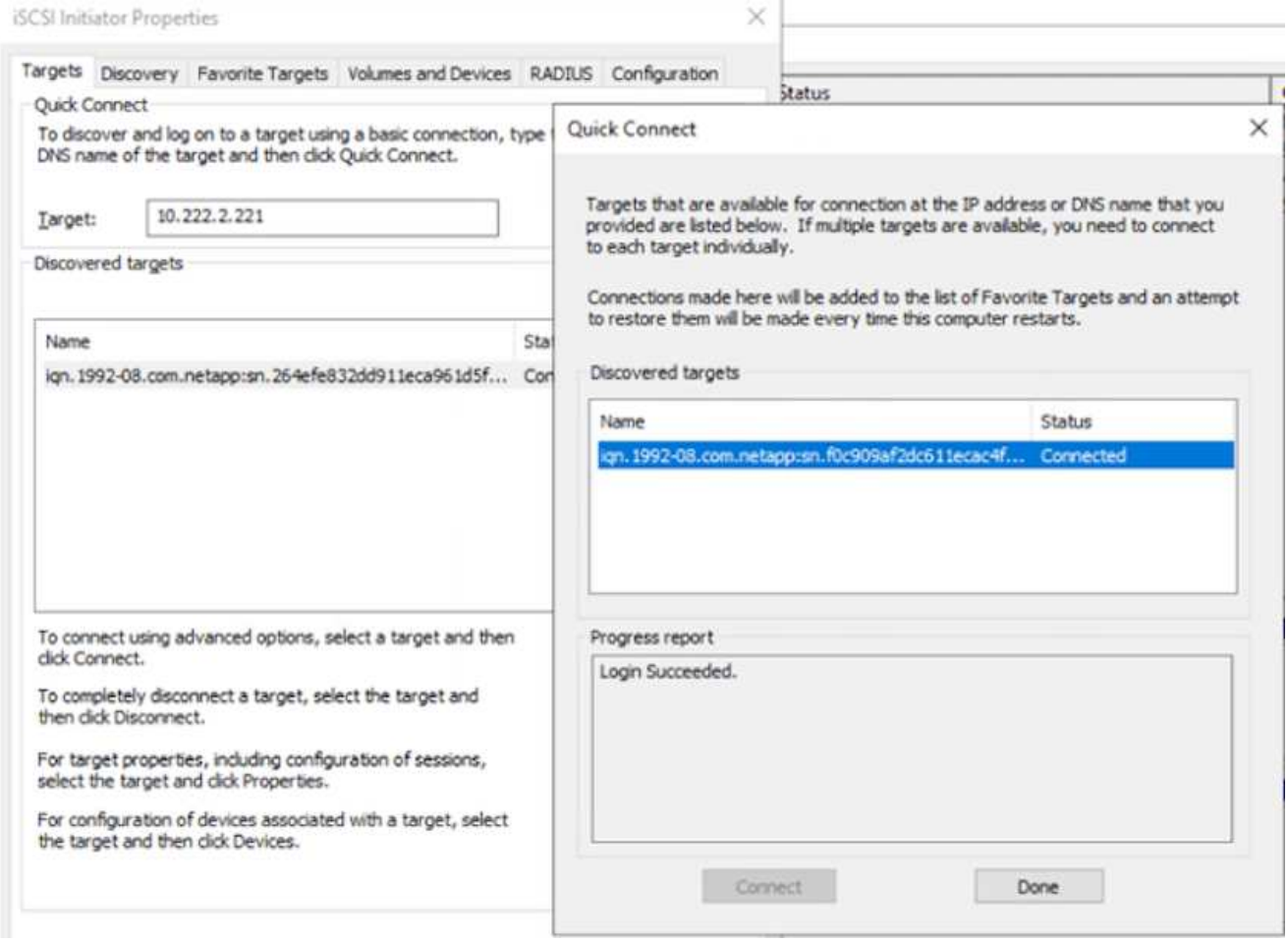
Se mostraron dos entradas.

1. Conectar la LUN recién aprovisionada a una máquina virtual Windows:

Para conectar el nuevo LUN tor un host de Windows que reside en el cloud de VMware en el centro de datos definido por software de AWS, complete los siguientes pasos:

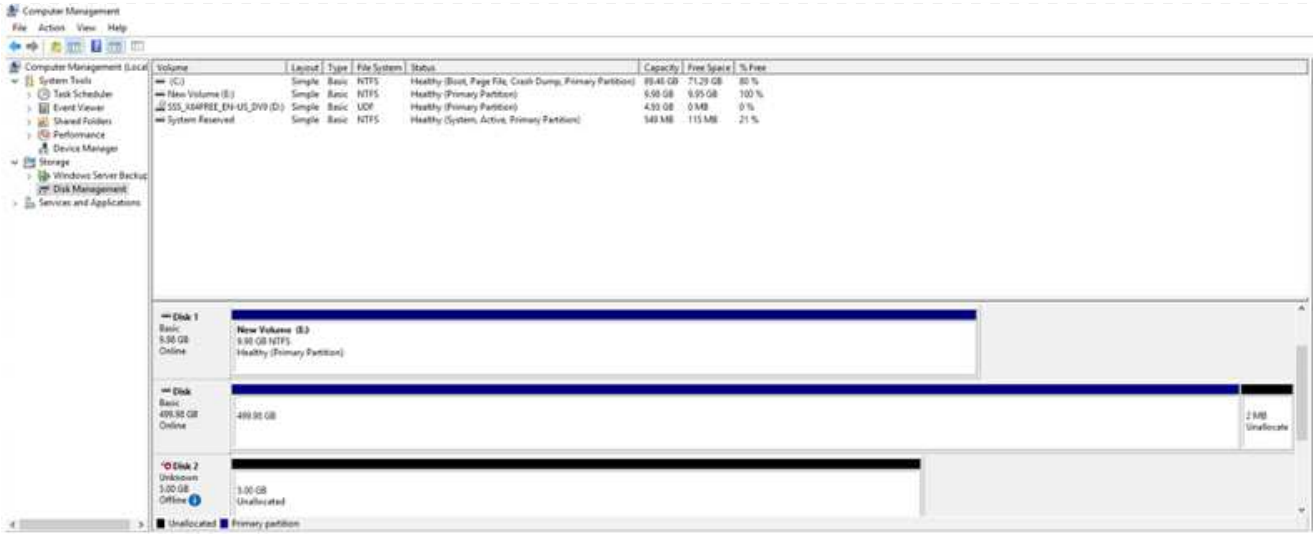
1. RDP a la máquina virtual de Windows alojada en VMware Cloud en el SDDC de AWS.
2. Vaya a Administrador de servidores > Panel > Herramientas > iniciador iSCSI para abrir el cuadro de diálogo Propiedades del iniciador iSCSI.
3. En la pestaña Discovery, haga clic en Discover Portal o Add Portal y, a continuación, introduzca la dirección IP del puerto de destino iSCSI.
4. En la pestaña Destinos, seleccione el objetivo detectado y haga clic en Iniciar sesión o conectar.
5. Seleccione Activar acceso múltiple y, a continuación, seleccione “Restaurar automáticamente esta conexión 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 con cada nodo del clúster. El DSM nativo selecciona las mejores rutas que se van a utilizar.



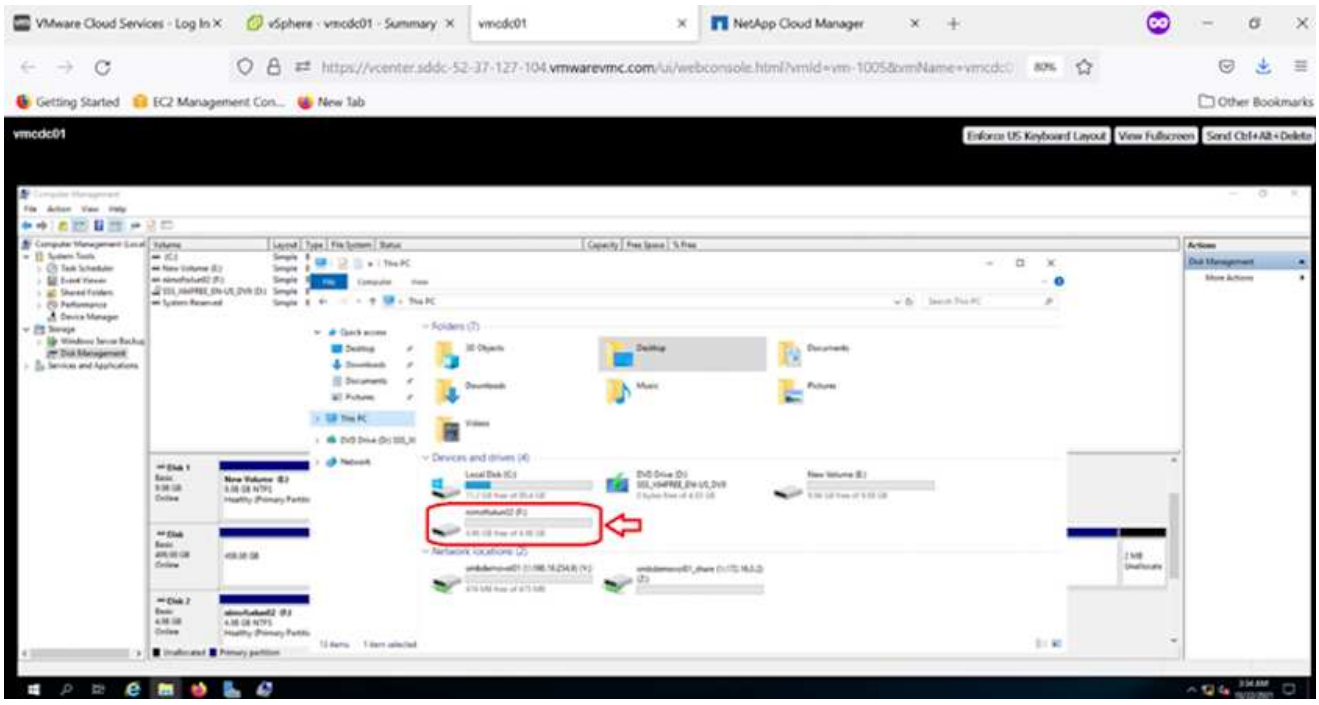
Los LUN de la máquina virtual de almacenamiento (SVM) aparecen como discos en el host Windows. El host no detecta automáticamente los nuevos discos que se añaden. Active una detección repetida manual para detectar los discos realizando los pasos siguientes:

1. Abra la utilidad 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 > discos de reexploración.



Cuando el host Windows accede por primera vez a una nueva LUN, no tiene sistema de archivos o partición. Inicialice la LUN y, de manera opcional, formatee la LUN con un sistema de archivos realizando los pasos siguientes:

1. Inicie Administración de discos de Windows.
2. Haga clic con el botón derecho en el LUN y seleccione el disco o el tipo de partición necesarios.
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 el cloud líder del sector que se basa en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Se trata de una versión de ONTAP definida por software que consume almacenamiento nativo del cloud, lo

que le permite tener el mismo software de almacenamiento en el cloud y en las instalaciones, lo que reduce la necesidad de volver a formar al personal INFORMÁTICO en todos los métodos nuevos para gestionar sus datos.

CVO ofrece a los clientes la capacidad de mover datos del perímetro, al centro de datos, al cloud y al backup sin problemas, de tal modo que su cloud híbrido se aúna, todo ello gestionado con una consola de gestión de panel único, Cloud Manager de NetApp.

Por su diseño, CVO ofrece un rendimiento extremo y capacidades de gestión de datos avanzadas para responder incluso a sus aplicaciones más exigentes en el cloud

Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado

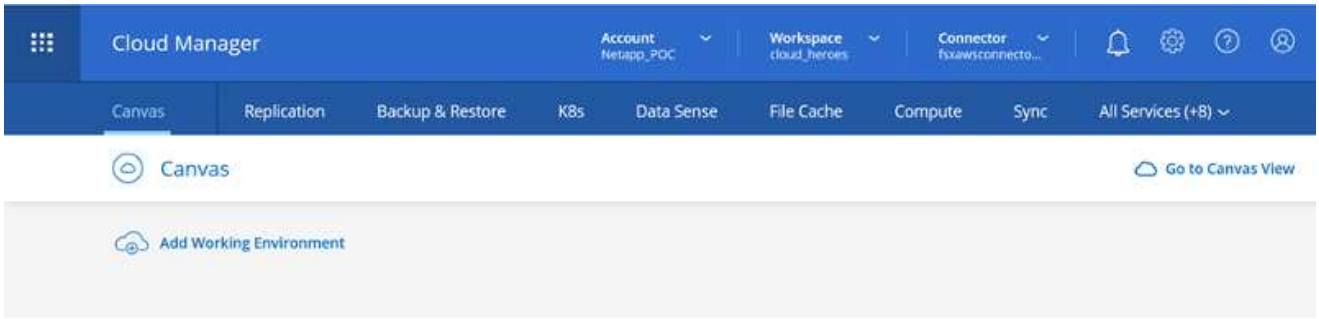
Implemente una nueva instancia de Cloud Volumes ONTAP en AWS (hágalo usted mismo)

Los recursos compartidos y las LUN de Cloud Volumes ONTAP se pueden montar a partir de máquinas virtuales que se crean en VMware Cloud en un entorno SDDC de AWS. Los volúmenes también se pueden montar en clientes Windows nativos de VM de AWS, y se puede acceder A LUN en clientes Linux o Windows como dispositivos de bloque cuando se monta a través de iSCSI, porque Cloud Volumes ONTAP admite los protocolos iSCSI, SMB y NFS. Los volúmenes de Cloud Volumes ONTAP se pueden configurar en unos pocos pasos sencillos.

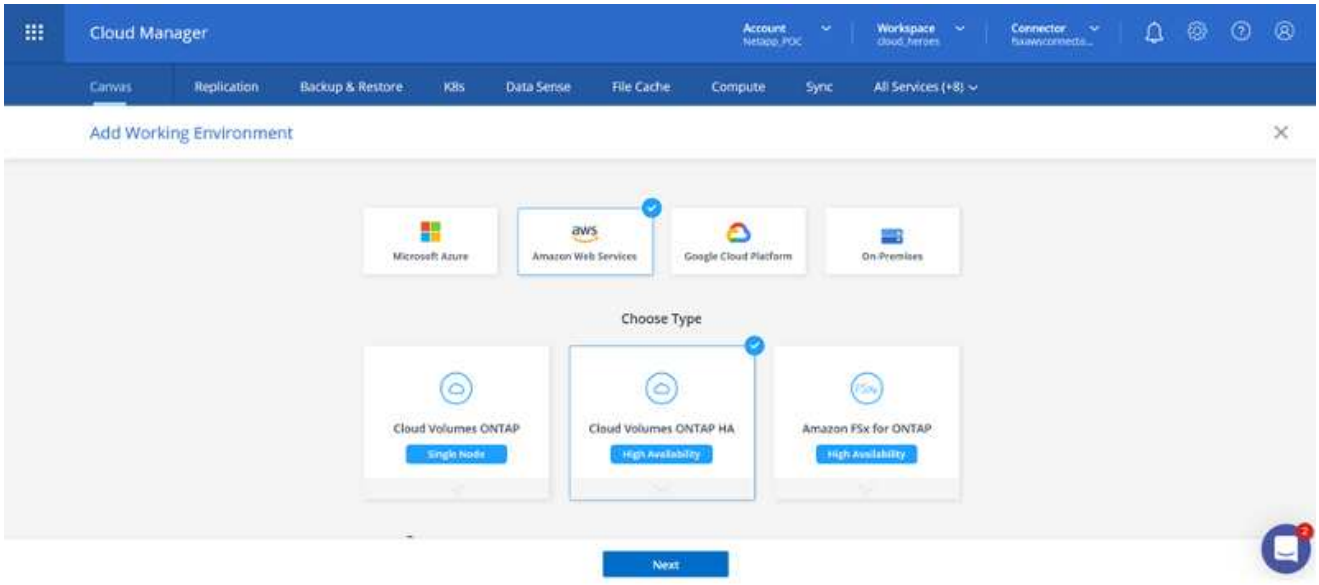
Para replicar volúmenes de un entorno local al cloud por motivos de recuperación ante desastres o migración, establezca la conectividad de red a AWS mediante una VPN de sitio a sitio o DirectConnect. La replicación de datos de las instalaciones a Cloud Volumes ONTAP no se encuentra fuera del alcance de este documento. Para replicar datos entre sistemas Cloud Volumes ONTAP y locales, consulte "Configurar la replicación de datos entre sistemas".

Utilice la "Configuración de Cloud Volumes ONTAP" Para ajustar el tamaño de las instancias de Cloud Volumes ONTAP de forma precisa. Además, supervise el rendimiento local para utilizarlo como entradas en el dimensionador de Cloud Volumes ONTAP.

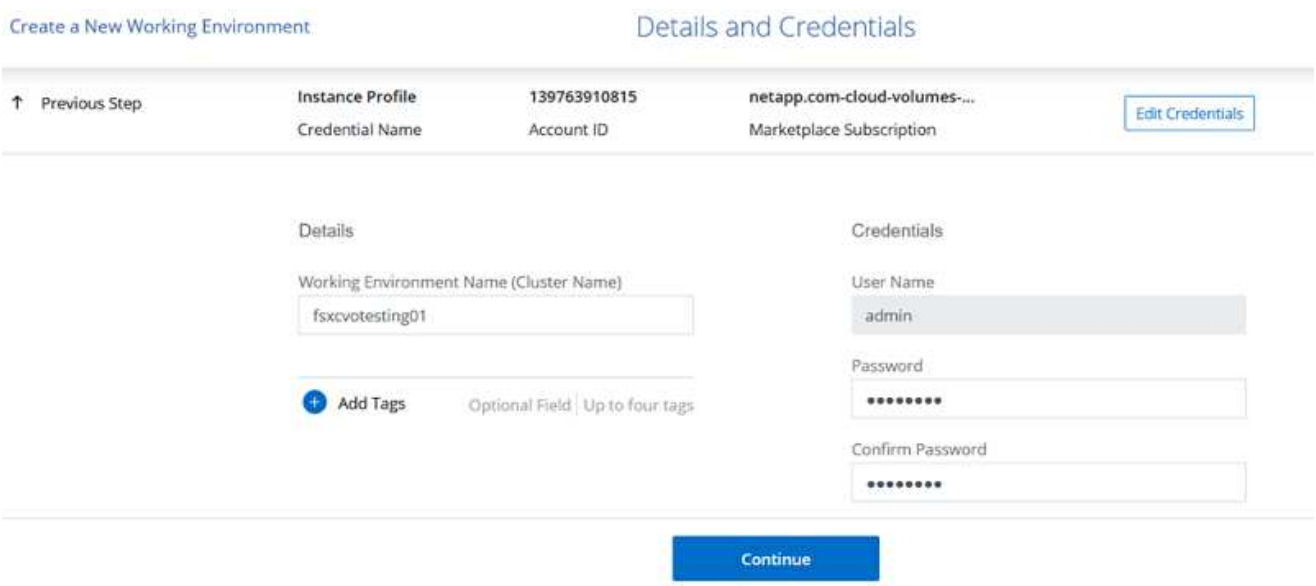
1. Inicie sesión en NetApp Cloud Central; aparecerá la pantalla Fabric View. Localice la pestaña Cloud Volumes ONTAP y seleccione Go to Cloud Manager. Una vez que haya iniciado sesión, aparecerá la pantalla Canvas.



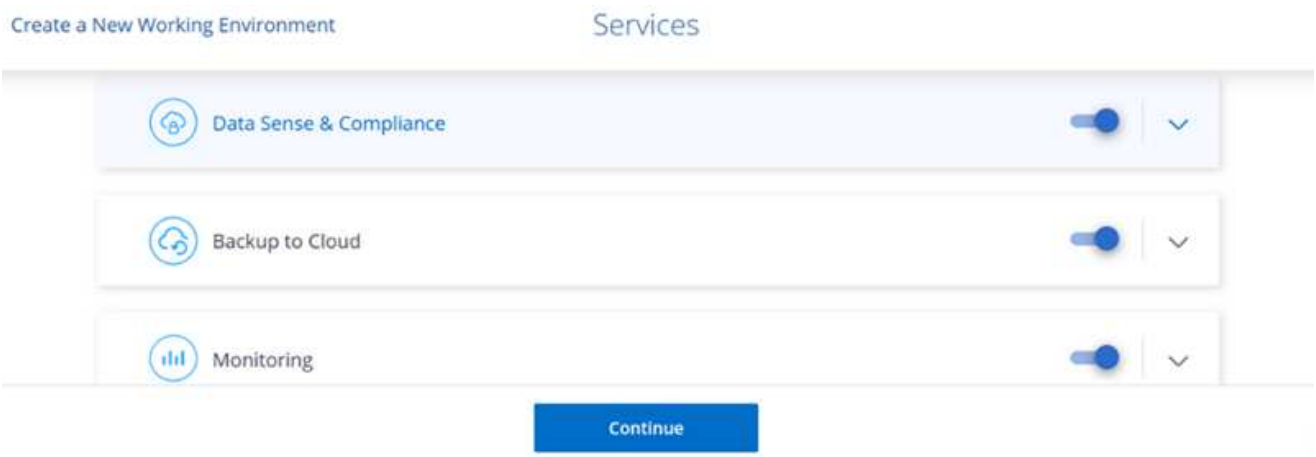
1. En la página de inicio de Cloud Manager, haga clic en Add a Working Environment y, a continuación, seleccione AWS como cloud y el tipo de configuración del sistema.



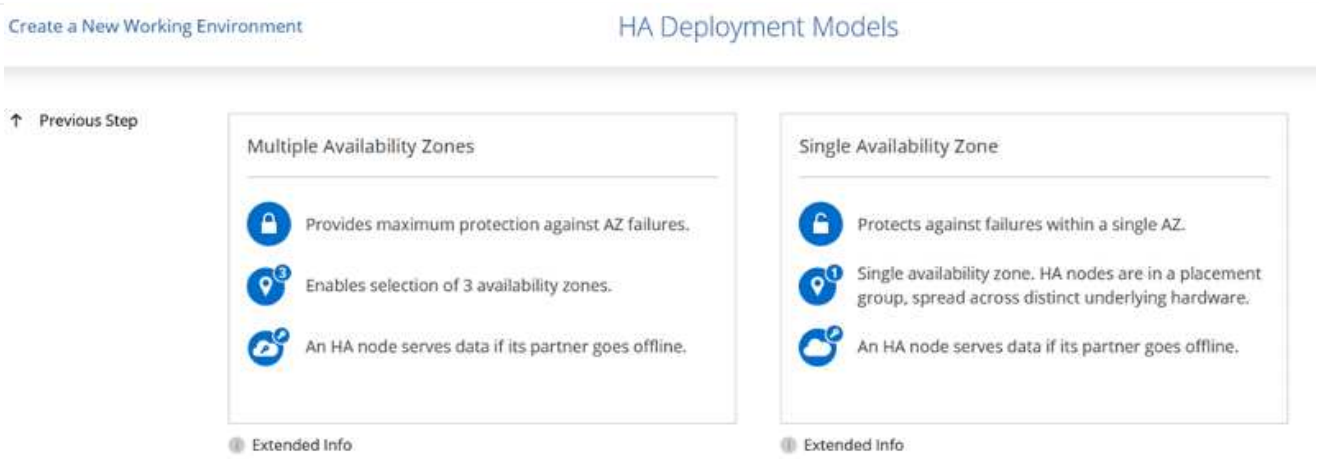
1. Proporcione los detalles del entorno que se va a crear, incluidos el nombre del entorno y las credenciales de administración. Haga clic en Continue.



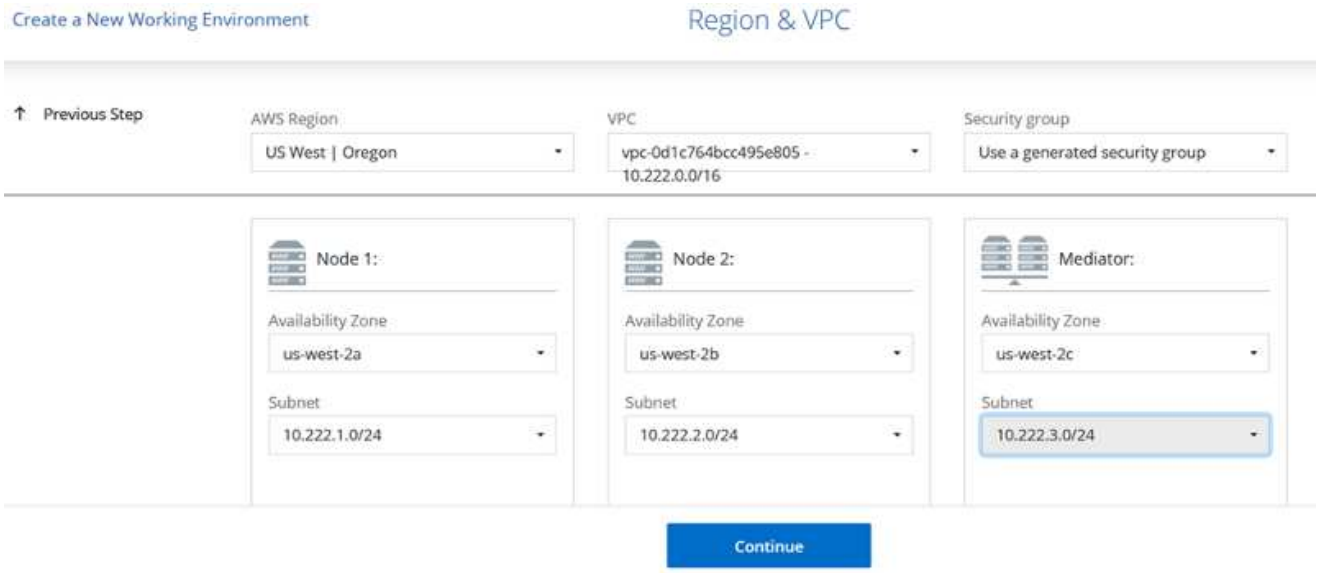
1. Selecciona los servicios complementarios para la implementación de Cloud Volumes ONTAP, que incluyen la clasificación de BlueXP, el backup y la recuperación de datos de BlueXP, y Cloud Insights. Haga clic en Continue.



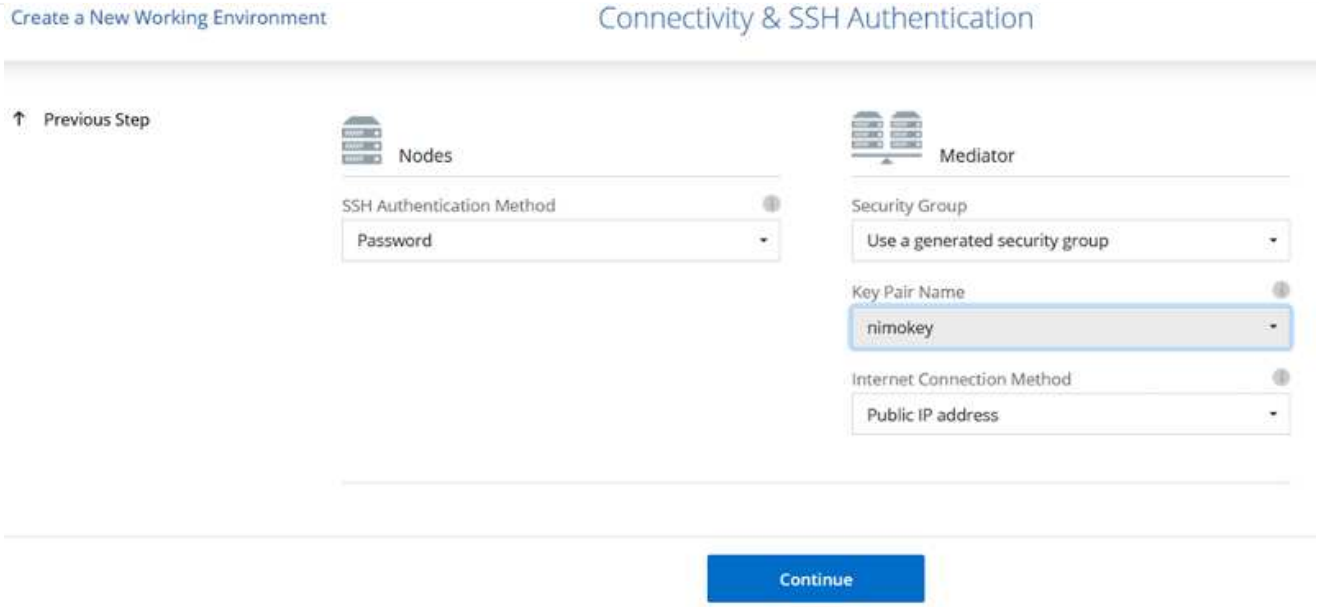
1. En la página ha Deployment Models, elija la configuración de varias zonas de disponibilidad.



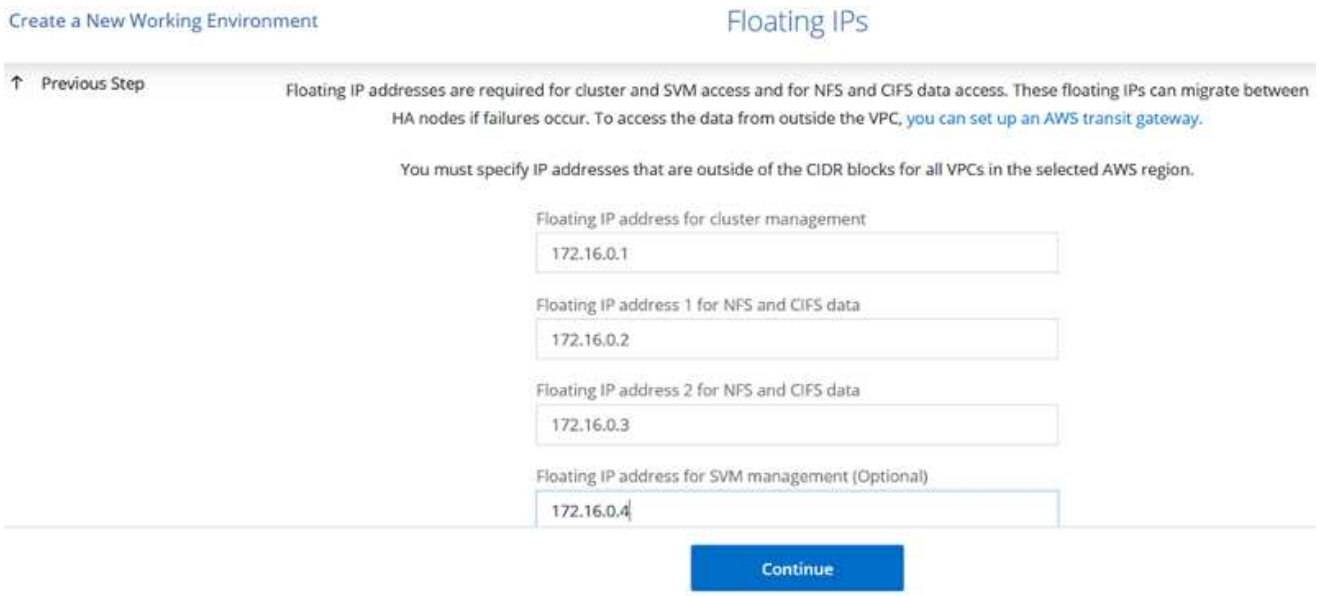
1. En la página Region & VPC, introduzca la información de red y, a continuación, haga clic en Continue.



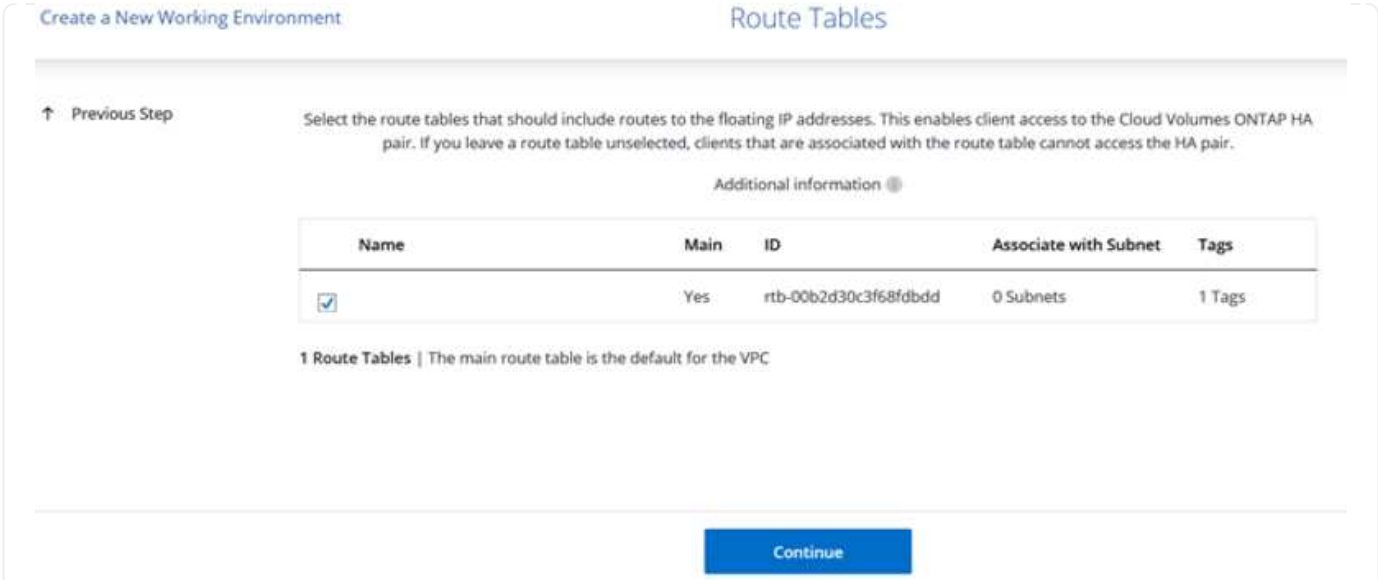
1. En la página conectividad y autenticación SSH, elija los métodos de conexión para el par de alta disponibilidad y el mediador.



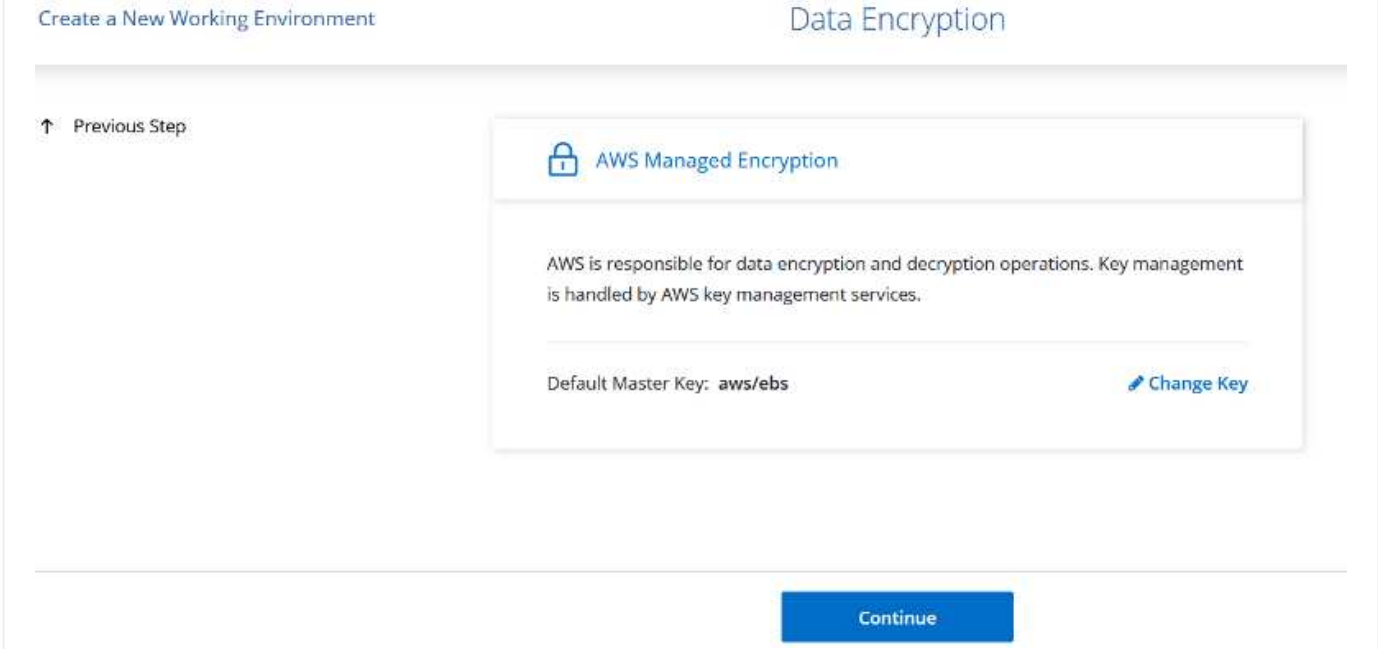
1. Especifique las direcciones IP flotantes y, a continuación, haga clic en continuar.



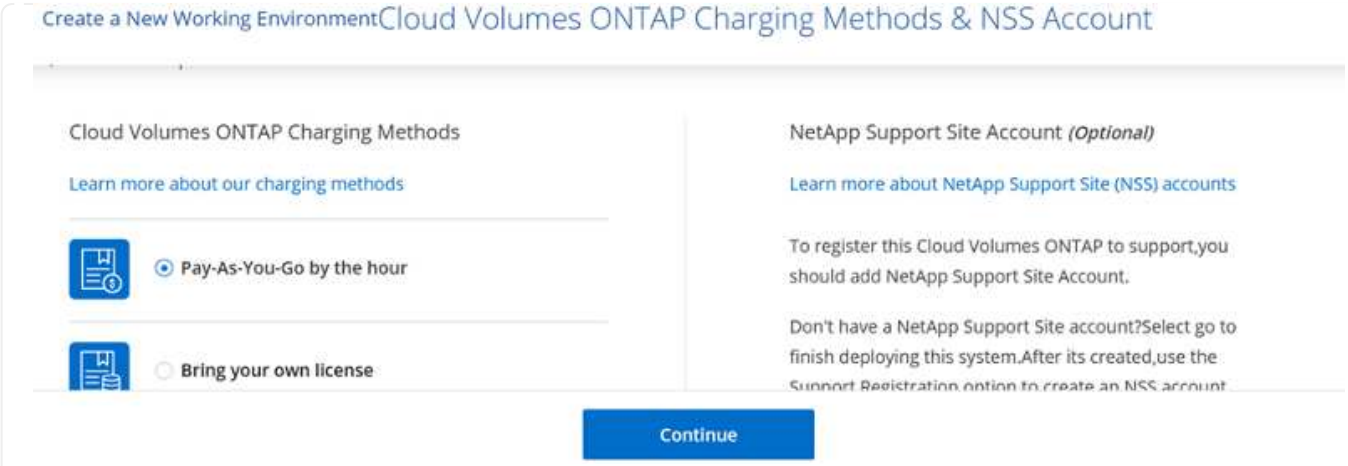
1. Seleccione las tablas de rutas adecuadas para incluir rutas a las direcciones IP flotantes y, a continuación, haga clic en continuar.



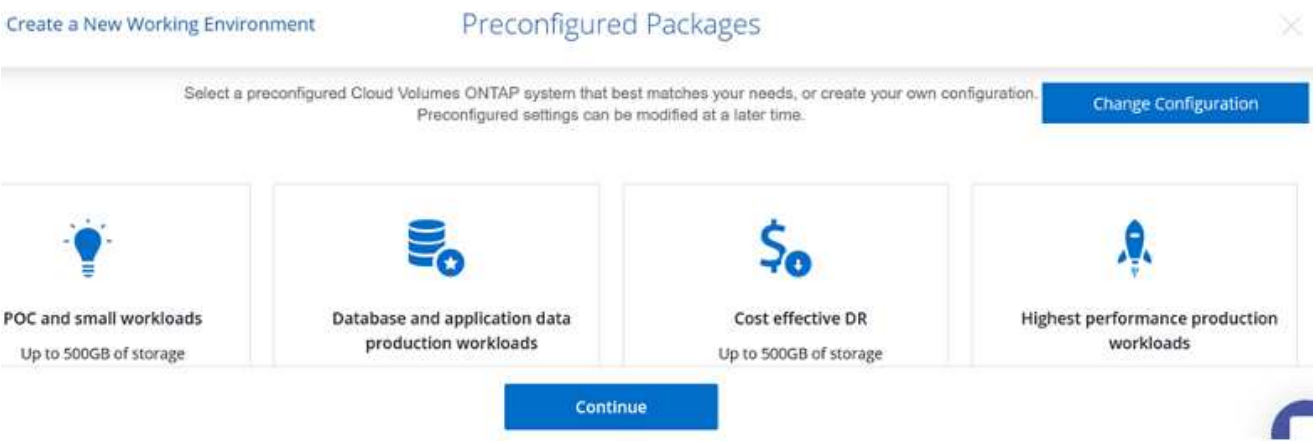
1. En la página Data Encryption, elija el cifrado gestionado por AWS.



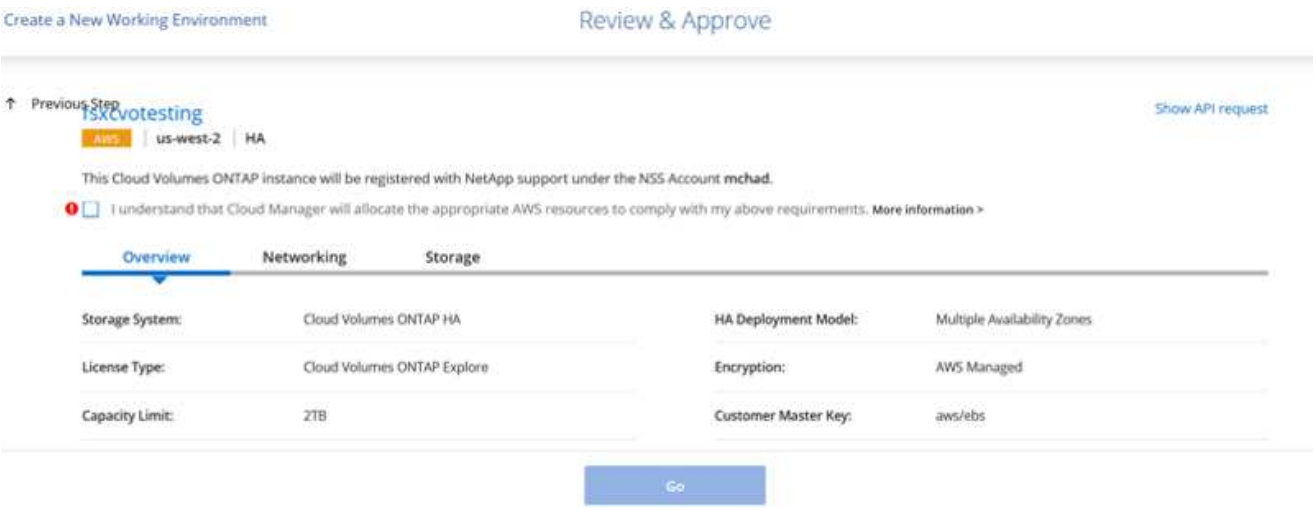
1. Seleccione la opción de licencia: Pago por uso o BYOL para usar una licencia existente. En este ejemplo, se utiliza la opción de pago por uso.



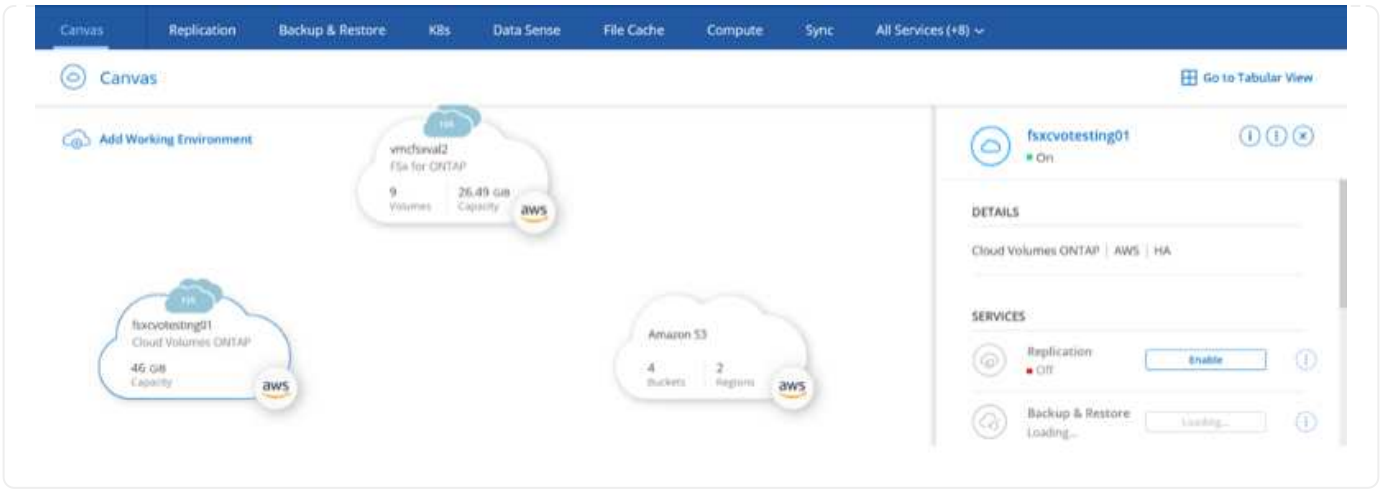
1. Seleccione entre varios paquetes preconfigurados disponibles en función del tipo de carga de trabajo que se va a poner en marcha en equipos virtuales que se ejecuten en el cloud de VMware en AWS SDDC.



1. En la página Review & Approve, revise y confirme las selecciones.para crear la instancia de Cloud Volumes ONTAP, haga clic en Go.

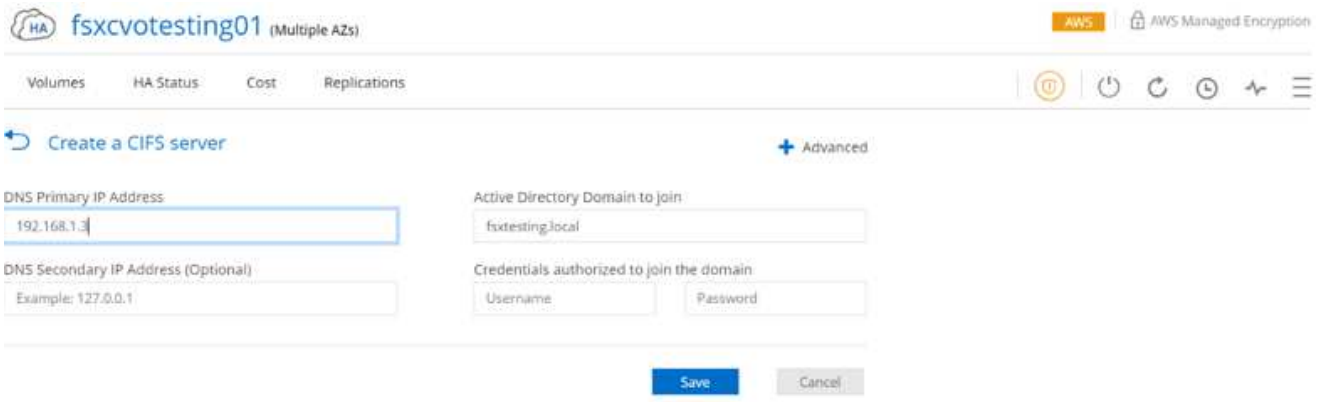


1. Una vez que se ha aprovisionado Cloud Volumes ONTAP, se muestra en los entornos de trabajo de la página lienzo.

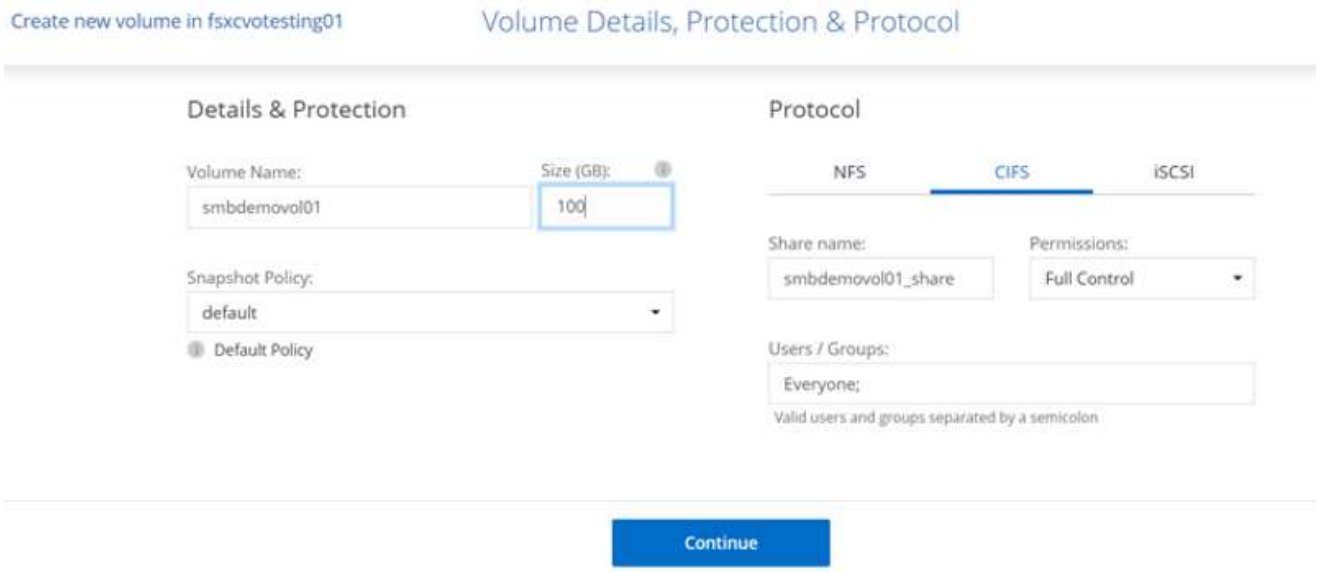

Canvas
Replication
Backup & Restore
K8s
Data Sense
File Cache
Compute
Sync
All Services (+8)
Canvas
Go to Tabular View
Add Working Environment
vmcfsaval2
FSx for ONTAP
9
Volumes
26.49 GiB
Capacity
fsxcvotesting01
Cloud Volumes ONTAP
46 GiB
Capacity
Amazon S3
4
Buckets
2
Regions
fsxcvotesting01
On
DETAILS
Cloud Volumes ONTAP | AWS | HA
SERVICES
Replication
Off
Enable
Backup & Restore
Loading...

Configuraciones adicionales para volúmenes SMB

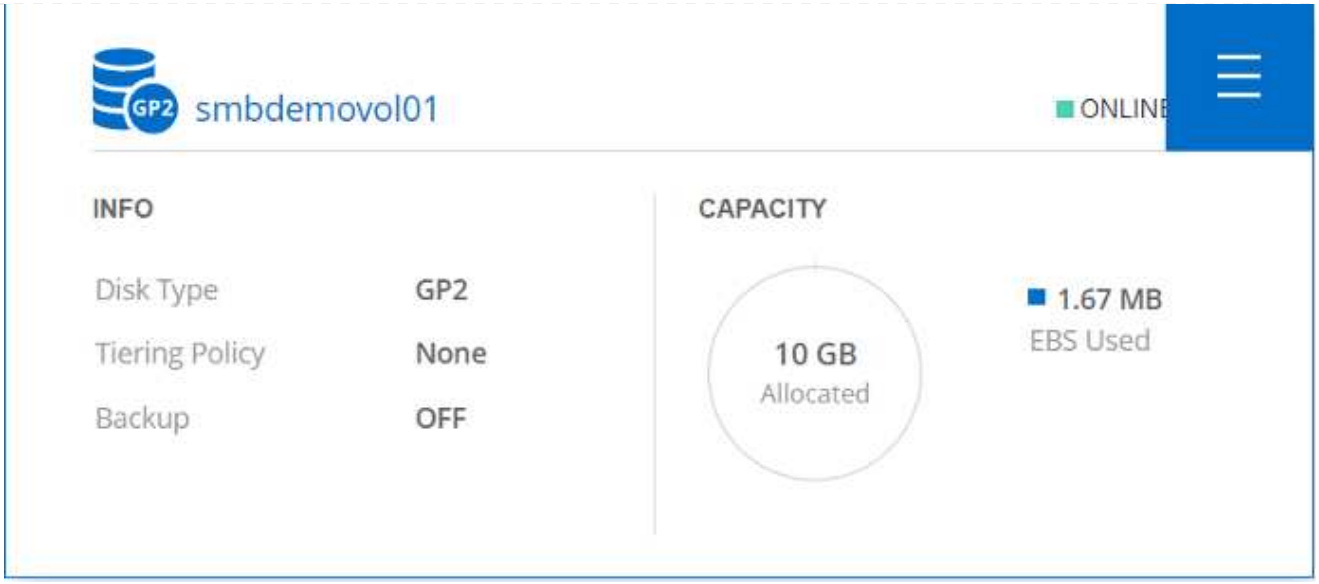
1. Una vez listo el entorno de trabajo, asegúrese de que el servidor CIFS esté configurado con los parámetros de configuración DNS y Active Directory adecuados. Este paso es necesario para poder crear el volumen de SMB.



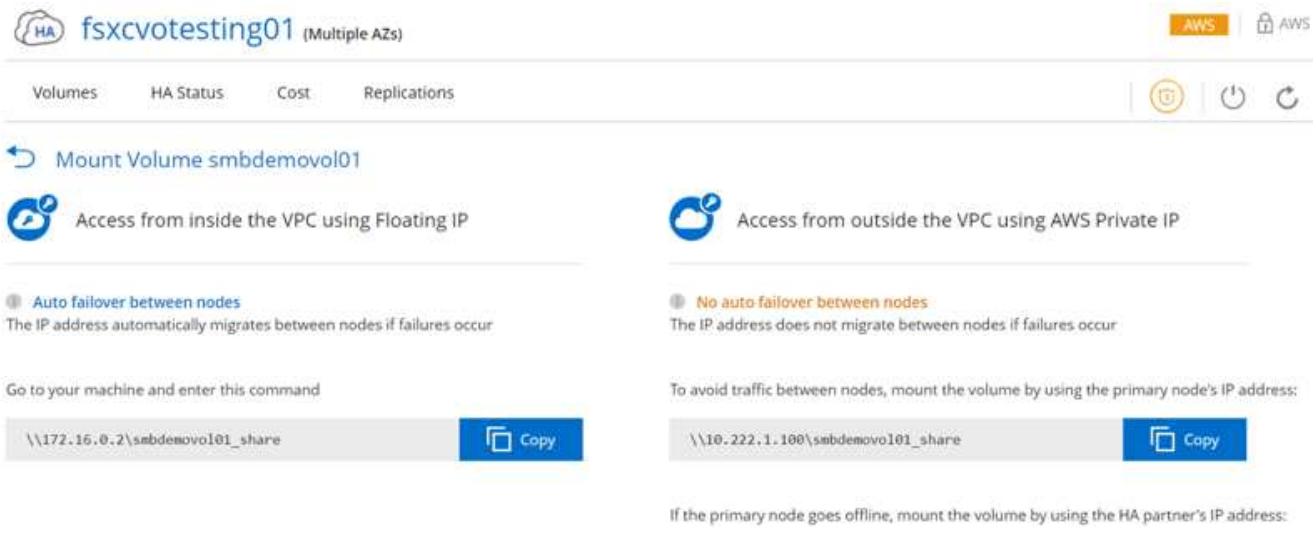
1. Seleccione la instancia de CVO para crear el volumen y haga clic en la opción Create Volume. Elija el tamaño adecuado y el gestor de cloud elija el agregado que lo contiene o utilice un mecanismo de asignación avanzado para colocarlo en un agregado concreto. En esta demostración, se ha seleccionado SMB como protocolo.

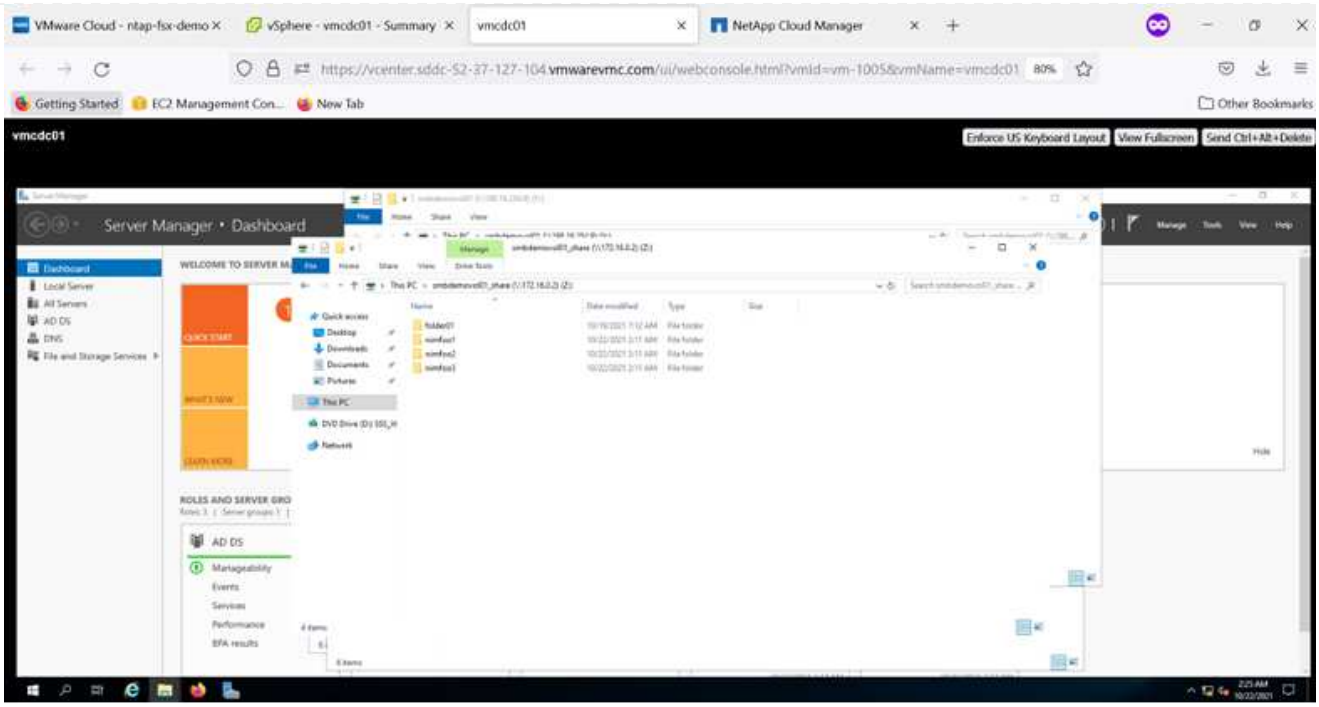


1. Una vez que el volumen se ha aprovisionado, está disponible en el panel Volumes. Debido a que se aprovisiona un recurso compartido de CIFS, debe otorgar a sus usuarios o grupos permiso a los archivos y carpetas y comprobar que esos usuarios pueden acceder al recurso compartido y crear un archivo.



1. Una vez creado el volumen, utilice el comando de montaje para conectarse al recurso compartido desde la máquina virtual que se ejecuta en VMware Cloud en hosts SDDC de AWS.
2. Copie la siguiente ruta y utilice la opción Map Network Drive para montar el volumen en el equipo virtual que se ejecuta en VMware Cloud en el centro de datos definido por software de AWS.

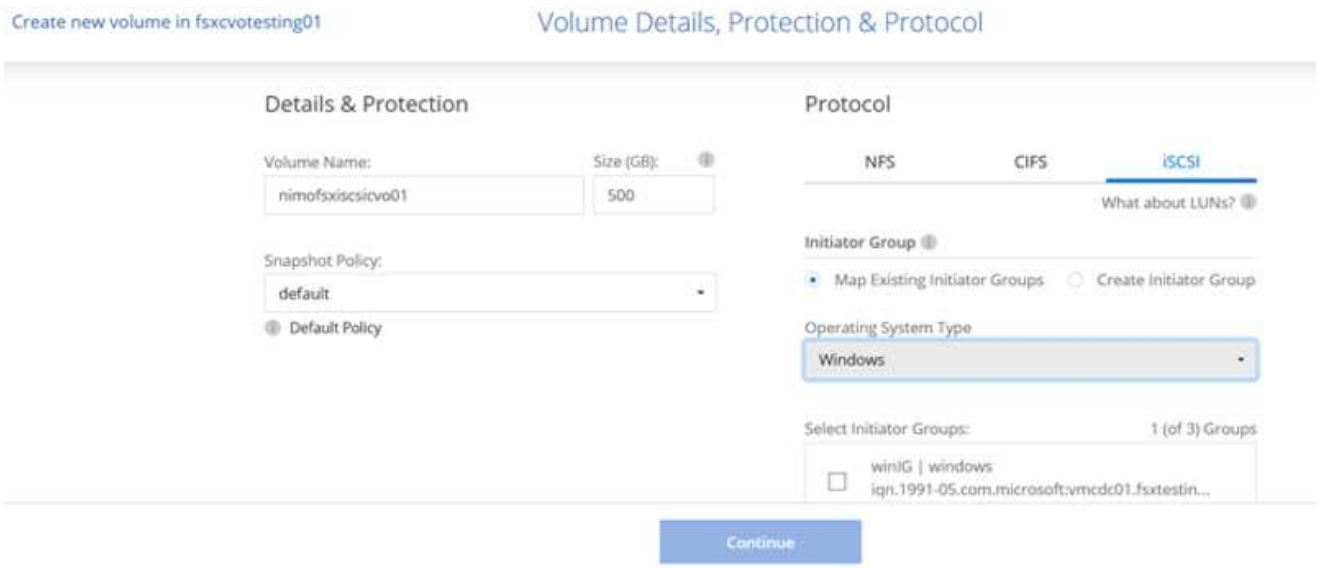


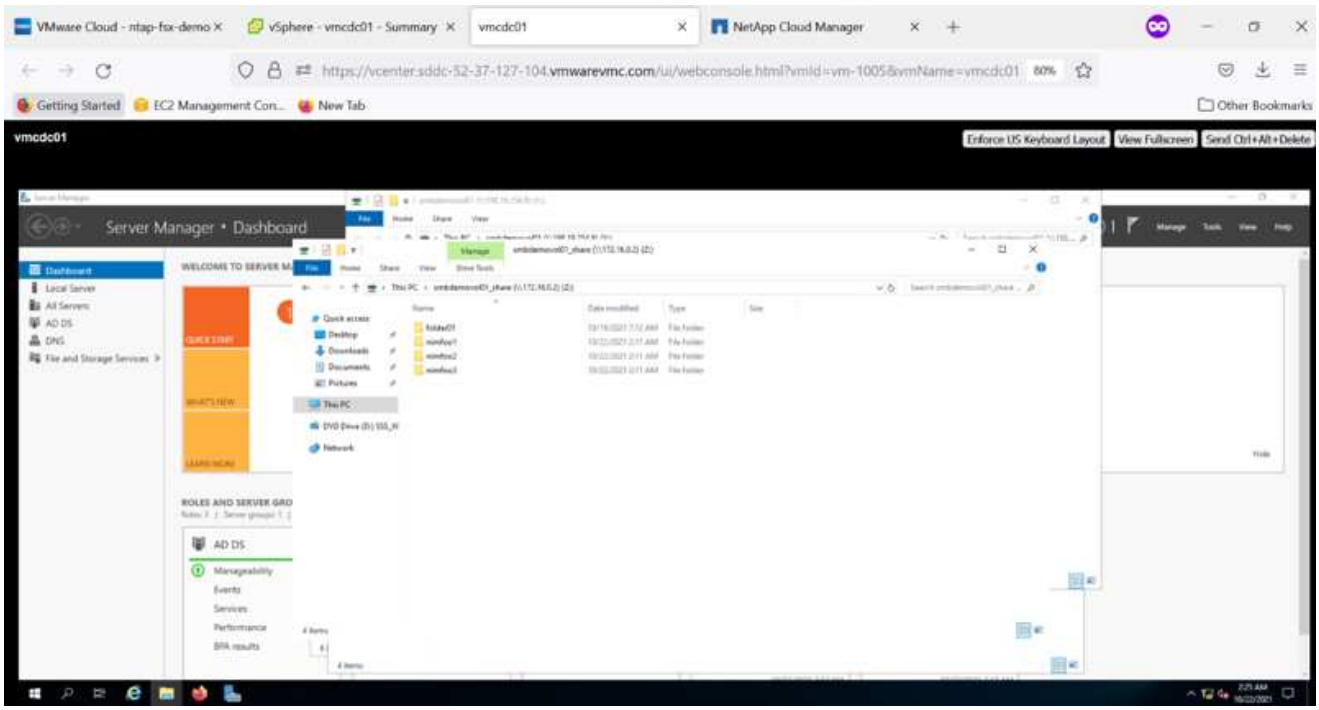

VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Dashboard
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER GROUPS
AD DS
Manageability
Events
Services
Performance
BPA results
This PC
Network
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_X
Manage
Tools
View
Help

Conectar el LUN a un host

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

1. En la página lienzo de Cloud Manager, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP para crear y gestionar volúmenes.
2. Haga clic en Add Volume > New Volume, seleccione iSCSI y haga clic en Create Initiator Group. Haga clic en Continue.





1. Una vez que se haya aprovisionado el volumen, seleccione el volumen y, a continuación, haga clic en IQN de destino. Para copiar el nombre completo de iSCSI (IQN), haga clic en Copy. Configurar una conexión iSCSI desde el host al LUN.

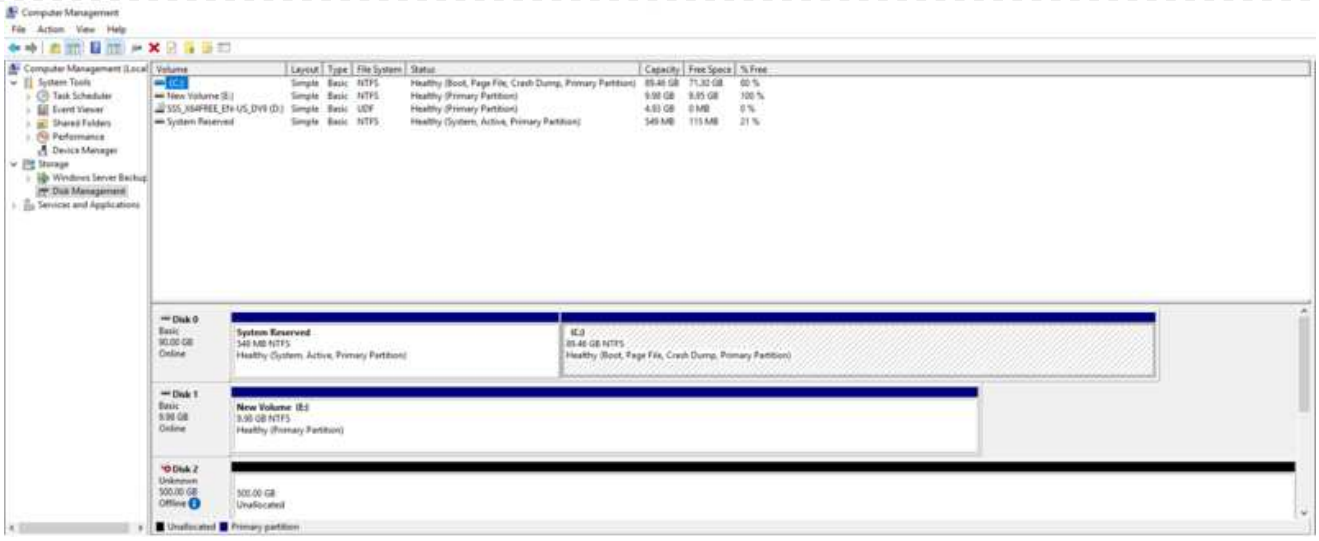
Para realizar lo mismo con el host que reside en VMware Cloud en SDDC de AWS, complete los pasos siguientes:

1. RDP a la máquina virtual alojada en el cloud de VMware en AWS.
2. Abra el cuadro de diálogo Propiedades del iniciador iSCSI: Administrador del servidor > Panel > Herramientas > Iniciador iSCSI.
3. En la pestaña Discovery, haga clic en Discover Portal o Add Portal y, a continuación, introduzca la dirección IP del puerto de destino iSCSI.
4. En la pestaña Destinos, seleccione el objetivo detectado y haga clic en Iniciar sesión o conectar.
5. Seleccione Activar acceso múltiple y, a continuación, seleccione Restaurar automáticamente esta conexión 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 con cada nodo del clúster. El DSM nativo selecciona las mejores rutas que se van a utilizar.

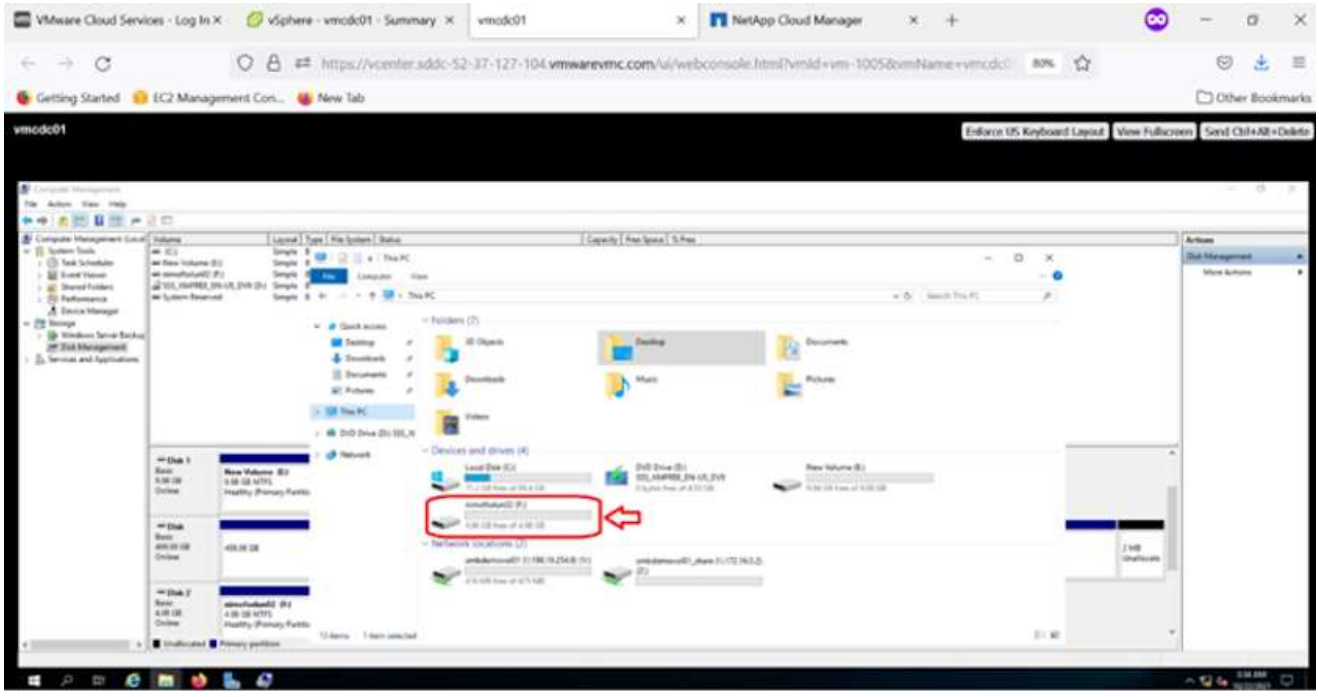
Los LUN de la SVM se muestran como discos al host Windows. El host no detecta automáticamente los nuevos discos que se añaden. Active una detección repetida manual para detectar los discos realizando los pasos siguientes:

1. Abra la utilidad 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 > discos de reexploración.



Cuando el host Windows accede por primera vez a una nueva LUN, no tiene sistema de archivos o partición. Inicialice la LUN y, de manera opcional, formatee la LUN con un sistema de archivos realizando los pasos siguientes:

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



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

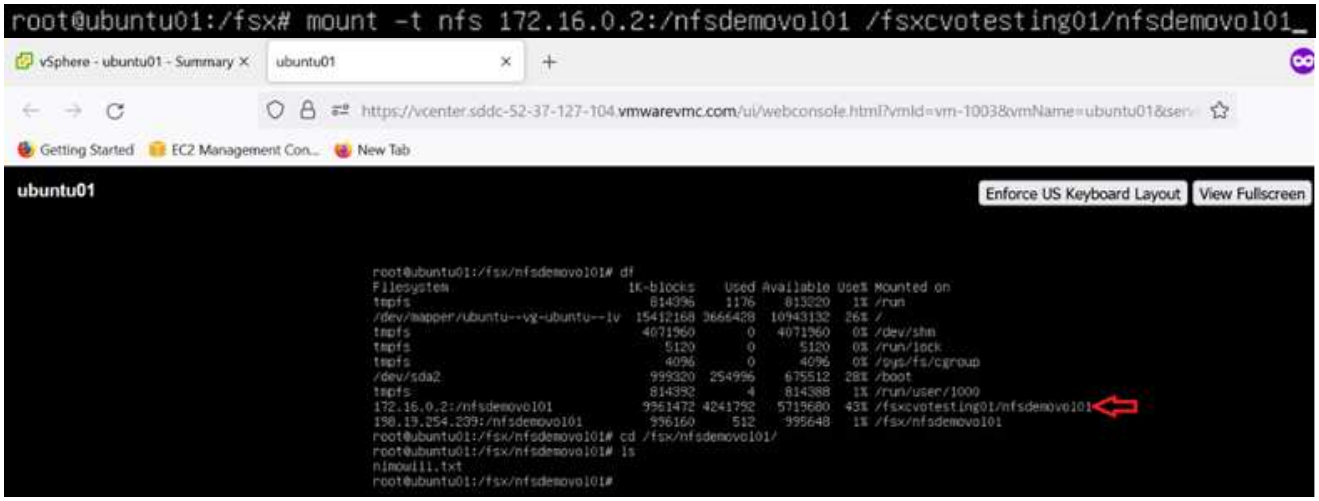
Montar el volumen NFS de Cloud Volumes ONTAP en el cliente Linux

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

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

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. Monte el volumen NFS de Amazon FSX para ONTAP de NetApp en el
directorio creado en el paso anterior.
```

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



Descripción general de las soluciones de almacenes de datos de ANF

Todas las organizaciones exitosas se encuentran en el camino de la transformación y la modernización. Como parte de este proceso, las empresas suelen utilizar sus inversiones existentes en VMware a la vez que aprovechan las ventajas de la nube y estudian cómo se pueden implementar procesos de migración, ráfaga, extensión y recuperación tras desastres de la manera más fluida posible. Los clientes que migran a la nube deben evaluar los problemas de elasticidad y ráfaga, salida del centro de datos, consolidación del centro de datos, escenarios de fin de vida, fusiones, adquisiciones, etc. El enfoque adoptado por cada organización puede variar en función de sus prioridades de negocio respectivas. A la hora de elegir las operaciones basadas en cloud, elegir un modelo de bajo coste con el rendimiento adecuado y un impedimento mínimo es uno de los objetivos cruciales. Además de elegir la plataforma adecuada, es especialmente

importante coordinar el almacenamiento y el flujo de trabajo para liberar el poder de la puesta en marcha del cloud y la elasticidad.

Casos de uso

Aunque la solución Azure VMware ofrece funcionalidades híbridas únicas a un cliente, las opciones de almacenamiento nativo limitadas han restringido su utilidad para las organizaciones con cargas de trabajo con un gran volumen de almacenamiento. Debido a que el almacenamiento está directamente ligado a los hosts, la única forma de escalar el almacenamiento es añadir más hosts, lo cual puede aumentar los costes entre un 35 % y un 40 % o más para cargas de trabajo con un uso intensivo del almacenamiento. Estas cargas de trabajo necesitan almacenamiento adicional, no una potencia adicional, pero esto implica pagar por hosts adicionales.

Consideremos el siguiente escenario: Un cliente requiere seis hosts para la potencia (vCPU/vmem), pero también tienen un requisito fundamental para el almacenamiento. Tras su evaluación, necesitan 12 hosts para satisfacer los requisitos de almacenamiento. Esto aumenta el TCO general porque deben comprar toda la capacidad adicional cuando todo lo que realmente necesitan es más almacenamiento. Esto es aplicable en cualquier caso de uso, incluidos la migración, la recuperación ante desastres, bursting, prueba/desarrollo, y así sucesivamente.

Otro caso de uso común para la solución VMware de Azure es la recuperación ante desastres (DR). La mayoría de las organizaciones no cuentan con una estrategia de recuperación ante desastres infalible o puede haber dificultades para justificar la ejecución de un centro de datos fantasma justo para la recuperación ante desastres. Los administradores podrían explorar opciones de recuperación ante desastres sin necesidad de espacio con un clúster sin piloto o un clúster bajo demanda. Entonces podrían escalar el almacenamiento sin añadir hosts adicionales, lo que podría ser una opción atractiva.

De este modo, en resumen, los casos de uso se pueden clasificar de dos formas:

- Escalar la capacidad de almacenamiento con almacenes de datos ANF
- Uso de almacenes de datos ANF como objetivo de recuperación ante desastres para un flujo de trabajo de recuperación optimizado en coste desde las instalaciones o en 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 vista previa pública) Junto con las mejores funcionalidades de recuperación ante desastres y protección de datos de su clase en una solución Azure VMware, que le permite descargar la capacidad de almacenamiento del almacenamiento VSAN.

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

Opciones de VMware Cloud en Azure

Solución Azure VMware

La solución VMware para Azure (AVS) es un servicio de cloud híbrido que proporciona centros de datos VMware completamente funcionales en un cloud público de Microsoft Azure. AVS es una solución de primera parte totalmente gestionada y compatible con Microsoft y verificada por VMware que utiliza infraestructura de Azure. Por lo tanto, los clientes obtienen VMware ESXi para virtualización informática, VSAN para almacenamiento hiperconvergente y NSX para redes y seguridad, todo ello al tiempo que aprovechan la presencia global de Microsoft Azure, instalaciones de centros de datos líderes en su clase y la proximidad al ecosistema enriquecido de servicios y soluciones nativos de Azure. Una combinación de un SDDC de la solución para Azure VMware y Azure NetApp Files proporciona el mejor rendimiento con una latencia de red

mínima.

Independientemente del cloud utilizado, cuando se pone en marcha un SDDC de VMware, el clúster inicial incluye los siguientes componentes:

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

Conclusión

Tanto si su objetivo es adoptar un enfoque de todo el cloud como del cloud híbrido, Azure NetApp Files ofrece excelentes opciones para poner en marcha y gestionar las cargas de trabajo de las aplicaciones junto con servicios de archivos, a la vez que reduce el TCO permitiendo que los requisitos de datos se reduzcan a la capa de la aplicación. Independientemente del caso práctico, elija la solución VMware de Azure junto con Azure NetApp Files para comprender rápidamente las ventajas del cloud, una infraestructura consistente y operaciones en las instalaciones y varios clouds, portabilidad bidireccional de cargas de trabajo, y capacidad y rendimiento de nivel empresarial. Se trata del mismo proceso y procedimientos que ya conoce para conectar el almacenamiento. Recuerde que solo la posición de los datos ha cambiado con un nuevo nombre; las herramientas y los procesos siguen siendo los mismos y Azure NetApp Files ayuda a optimizar la implementación general.

Puntos

Los puntos clave de este documento son:

- Ahora puede usar Azure NetApp Files como almacén de datos en AVS SDDC.
- Aumentar los tiempos de respuesta de las aplicaciones y ofrecer un mayor nivel de disponibilidad para proporcionar acceso a los datos de cargas de trabajo donde y cuando sea necesario.
- Simplifique la complejidad general del almacenamiento VSAN con funciones de cambio de tamaño sencillas e instantáneas.
- Rendimiento garantizado para cargas de trabajo críticas mediante una nueva formulación dinámica.
- Si el cloud de la solución para VMware Azure es el destino, Azure NetApp Files es la solución de almacenamiento adecuada para la puesta en marcha optimizada.

Dónde encontrar información adicional

Si quiere más información sobre la información descrita en este documento, consulte los siguientes enlaces a sitios web:

- Documentación de la solución VMware de Azure

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

- Documentación de Azure NetApp Files

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

- Conectar almacenes de datos Azure NetApp Files a hosts de soluciones VMware Azure (avance)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-

hosts?tabs=azure-portal/

Opciones de almacenamiento conectado a invitado de NetApp para Azure

Azure admite almacenamiento de NetApp conectado como invitado con el servicio Azure NetApp Files (ANF) nativo o con Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure NetApp Files lleva la gestión de datos y el almacenamiento de clase empresarial a Azure para que pueda gestionar sus cargas de trabajo y aplicaciones fácilmente. Migre sus cargas de trabajo al cloud y ejecútelas sin sacrificar el rendimiento.

Azure NetApp Files elimina obstáculos, de forma que puede mover todas sus aplicaciones basadas en archivos al cloud. Por primera vez, no tiene que volver a crear la arquitectura de sus aplicaciones y obtiene almacenamiento persistente para sus aplicaciones sin complejidad.

Dado que el servicio se ofrece mediante Microsoft Azure Portal, los usuarios disfrutan de un servicio totalmente gestionado como parte de su contrato empresarial de Microsoft. El soporte líder, gestionado por Microsoft, le ofrece tranquilidad completa. Esta solución única le permite agregar de forma rápida y fácil cargas de trabajo multiprotocolo. Puede compilar e implementar aplicaciones basadas en archivos de Windows y Linux, incluso para entornos heredados.

Azure NetApp Files (ANF) como almacenamiento conectado como invitado

Configuración de Azure NetApp Files con la solución VMware para Azure (AVS)

Los recursos compartidos de Azure NetApp Files se pueden montar a partir de máquinas virtuales que se crean en el entorno SDDC de la solución Azure VMware. Los volúmenes también pueden montarse en el cliente Linux y asignarse en el cliente Windows, ya que Azure NetApp Files admite los protocolos SMB y NFS. Los volúmenes de Azure NetApp Files se pueden configurar en cinco sencillos pasos.

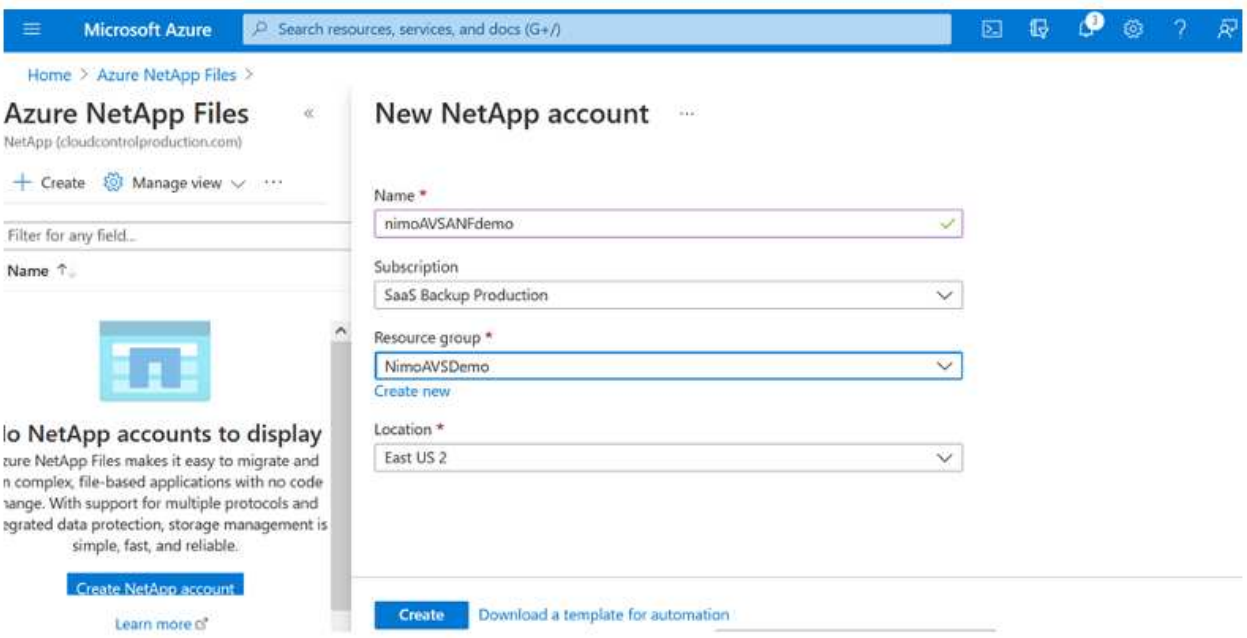
Azure NetApp Files y Azure VMware Solution deben estar en la misma región de Azure.

Cree y monte volúmenes de Azure NetApp Files

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

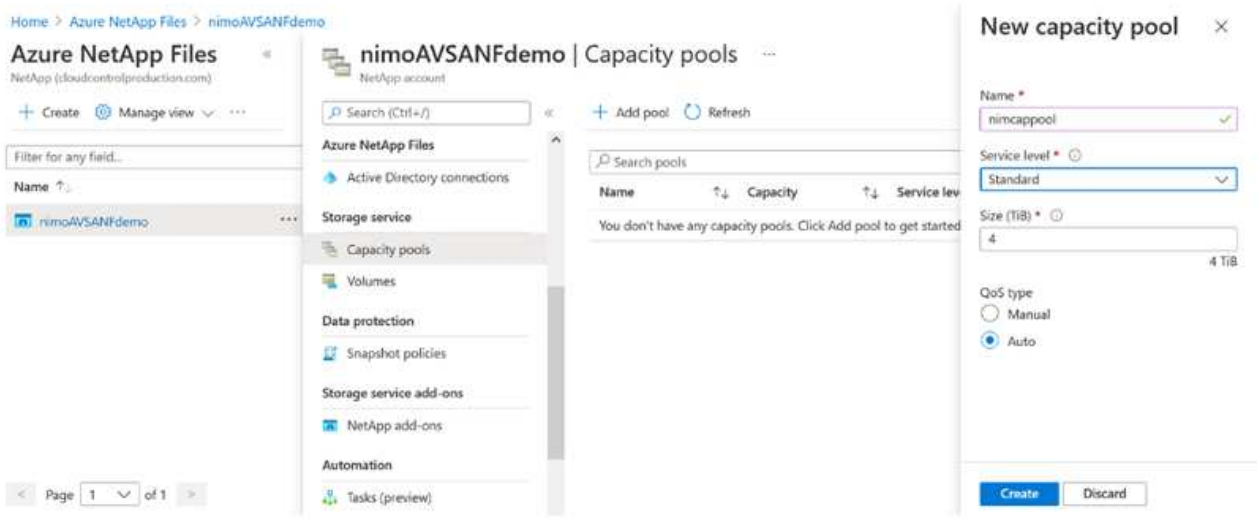
1. Inicie sesión en el portal de Azure y acceda a Azure NetApp Files. Verifique el acceso al servicio Azure NetApp Files y registre el proveedor de recursos Azure NetApp Files utilizando el comando *az provider register --namespace Microsoft.NetApp –wait*. Una vez completado el registro, cree una cuenta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

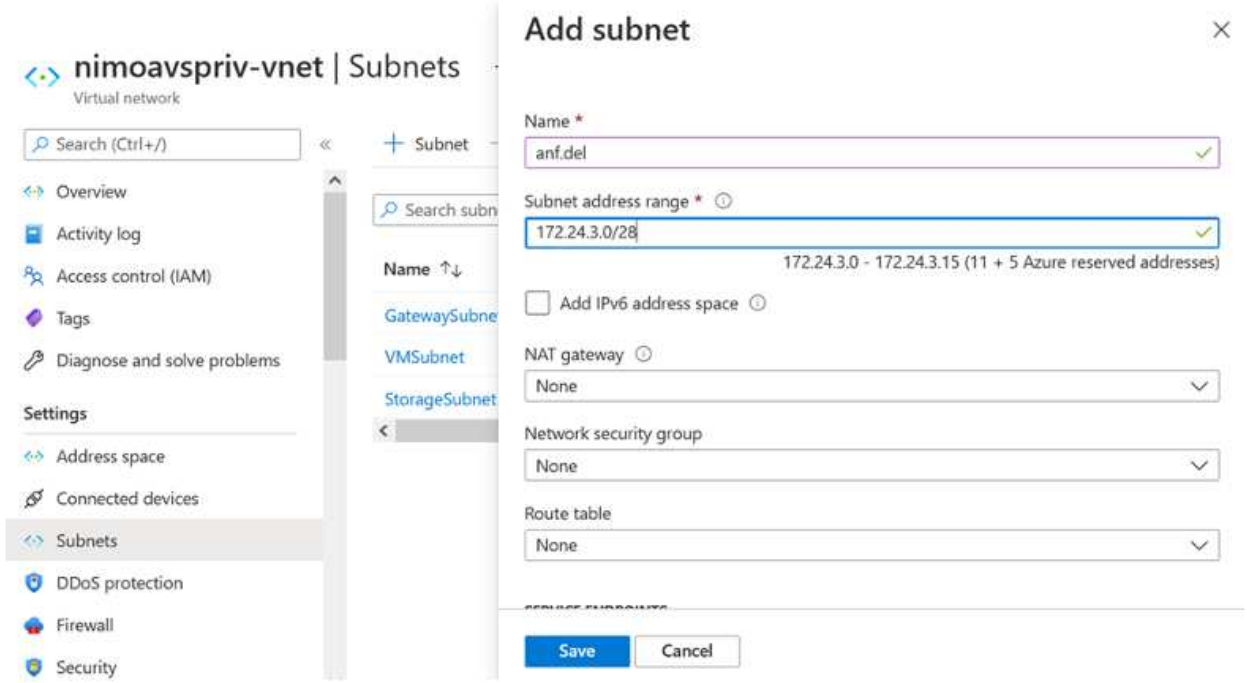


2. Una vez creada la cuenta de NetApp, configure los pools de capacidad con el tamaño y el nivel de servicio requeridos.

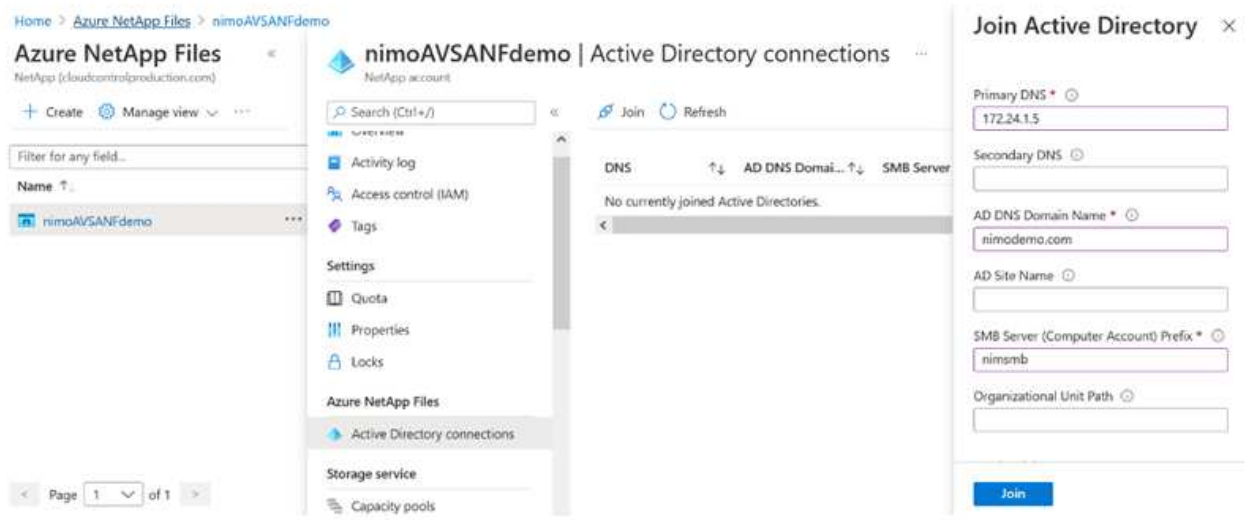
   Para obtener más información, consulte "Configure un pool de capacidad".



3. Configure la subred delegada para Azure NetApp Files y especifique esta subred mientras crea los volúmenes. Para obtener información detallada sobre los pasos para crear una subred delegada, consulte "Delegar una subred en Azure NetApp Files".

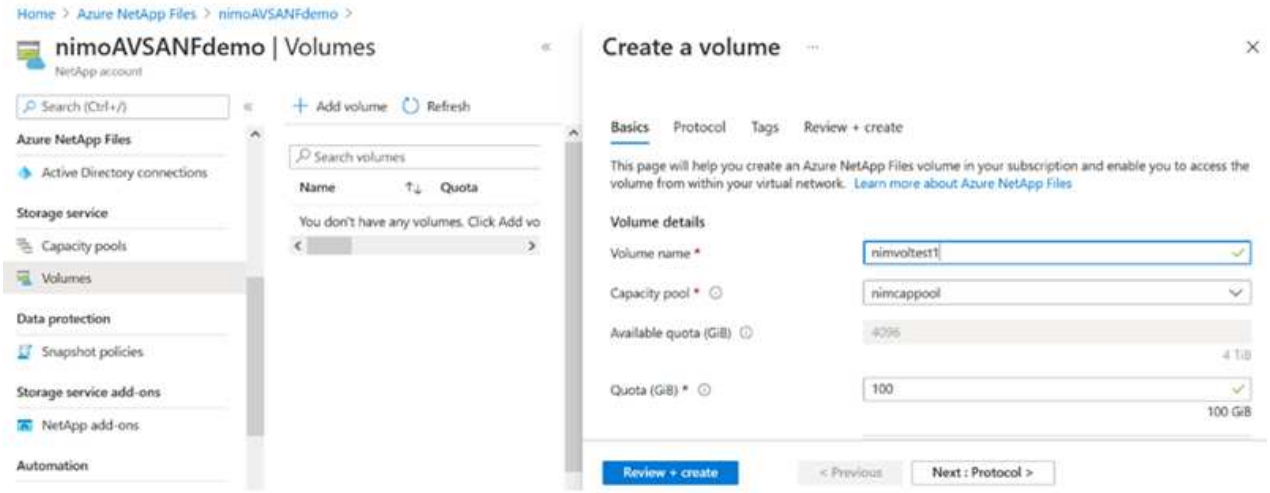


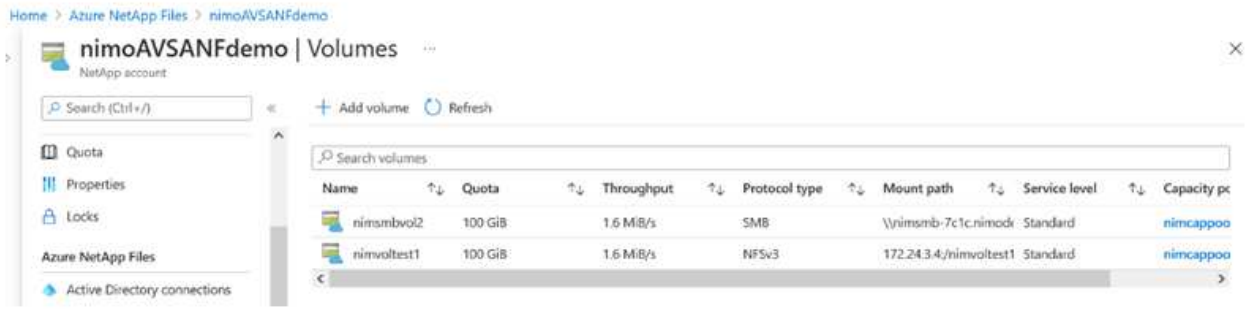
4. Añada un volumen SMB utilizando el blade volúmenes bajo el blade de pools de capacidad. Asegúrese de que el conector de Active Directory esté configurado antes de crear el volumen de SMB.



5. Haga clic en Review + Create para crear el volumen del SMB.

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

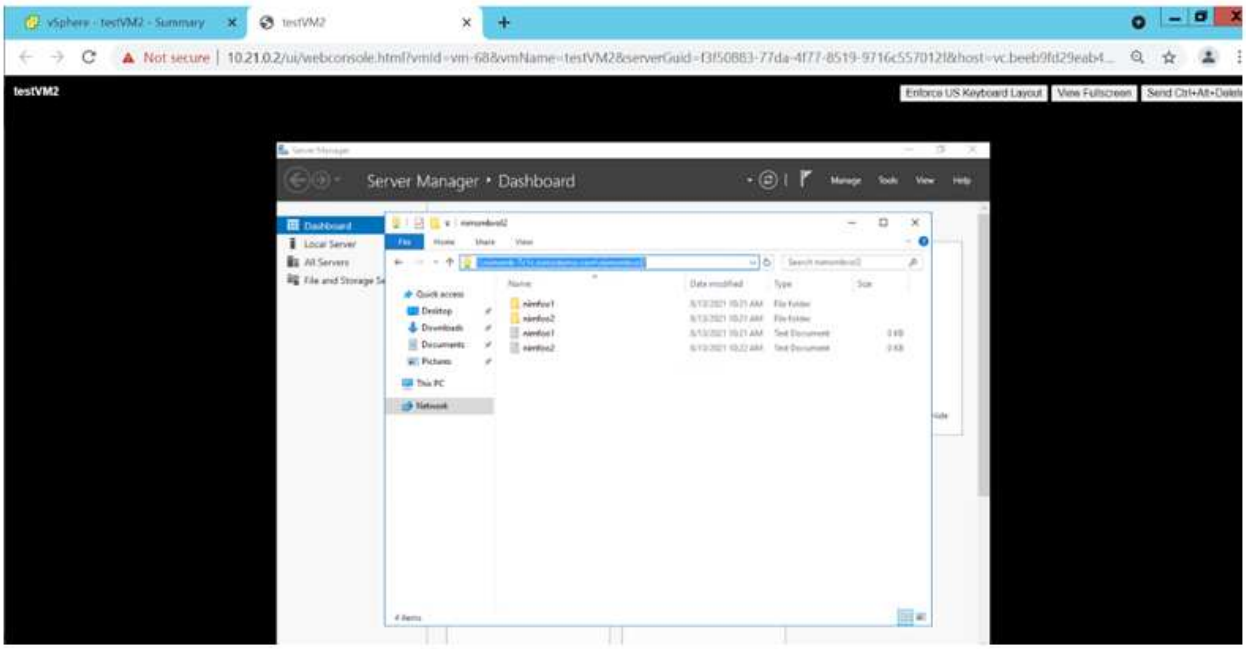


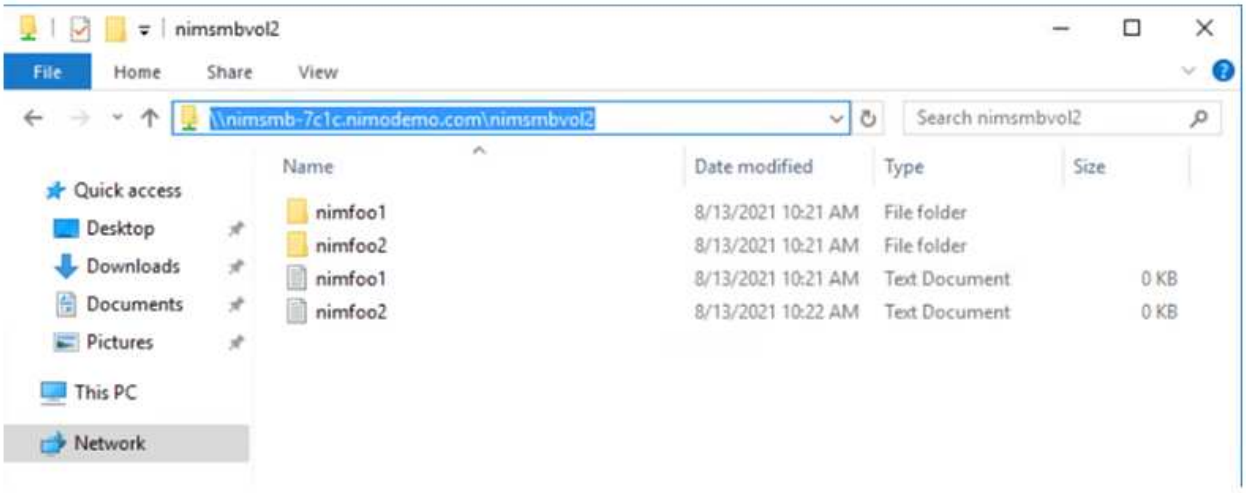


Para obtener más información acerca del rendimiento de Azure NetApp Files Volume por tamaño o cuota, consulte "Consideraciones de rendimiento para Azure NetApp Files".

6. Una vez que se ha establecido la conectividad, el volumen se puede montar y utilizar para los datos de la aplicación.

   Para ello, en el portal de Azure, haga clic en el blade de volúmenes y, a continuación, seleccione el volumen que desea montar y acceder a las instrucciones de montaje. Copie la ruta y utilice la opción Map Network Drive para montar el volumen en el equipo virtual que se ejecuta en el centro definido por software de la solución VMware de Azure.





7. Para montar volúmenes NFS en equipos virtuales Linux que se ejecutan en un SDDC de la solución Azure VMware, utilice este mismo proceso. Usar la funcionalidad de un nuevo estado de los volúmenes o un nivel de servicio dinámico para satisfacer las demandas de las cargas de trabajo.

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                  1K-blocks     Used Available Use% Mounted on
udev                          8168112        0   8168112   0% /dev
tmpfs                         1639548     1488   1638060   1% /run
/dev/sda5                    50824704  7902752  40310496  17% /
tmpfs                         8197728        0   8197728   0% /dev/shm
tmpfs                            5120        0      5120   0% /run/lock
tmpfs                         8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                      56832    56832         0 100% /snap/core18/2128
/dev/loop2                      66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                     224256   224256         0 100% /snap/gnome-3-34-180
4/72
/dev/loop3                      52224    52224         0 100% /snap/snap-store/547
/dev/loop4                      33152    33152         0 100% /snap/snapd/12704
/dev/sda1                      523248        4    523244   1% /boot/efi
tmpfs                         1639544       52   1639492   1% /run/user/1000
/dev/sr0                        54738    54738         0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

Para obtener más información, consulte "Cambie 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 el cloud líder del sector que se basa en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Se trata de una versión de ONTAP definida por software que consume almacenamiento nativo del cloud, lo que le permite tener el mismo software de almacenamiento en el cloud y en las instalaciones, lo que reduce la

necesidad de volver a formar al personal INFORMÁTICO en todos los métodos nuevos para gestionar sus datos.

CVO ofrece a los clientes la capacidad de mover datos del perímetro, al centro de datos, al cloud y al backup sin problemas, de tal modo que su cloud híbrido se aúna, todo ello gestionado con una consola de gestión de panel único, Cloud Manager de NetApp.

Por su diseño, CVO ofrece un rendimiento extremo y capacidades de gestión de datos avanzadas para responder incluso a sus aplicaciones más exigentes en el cloud

Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado

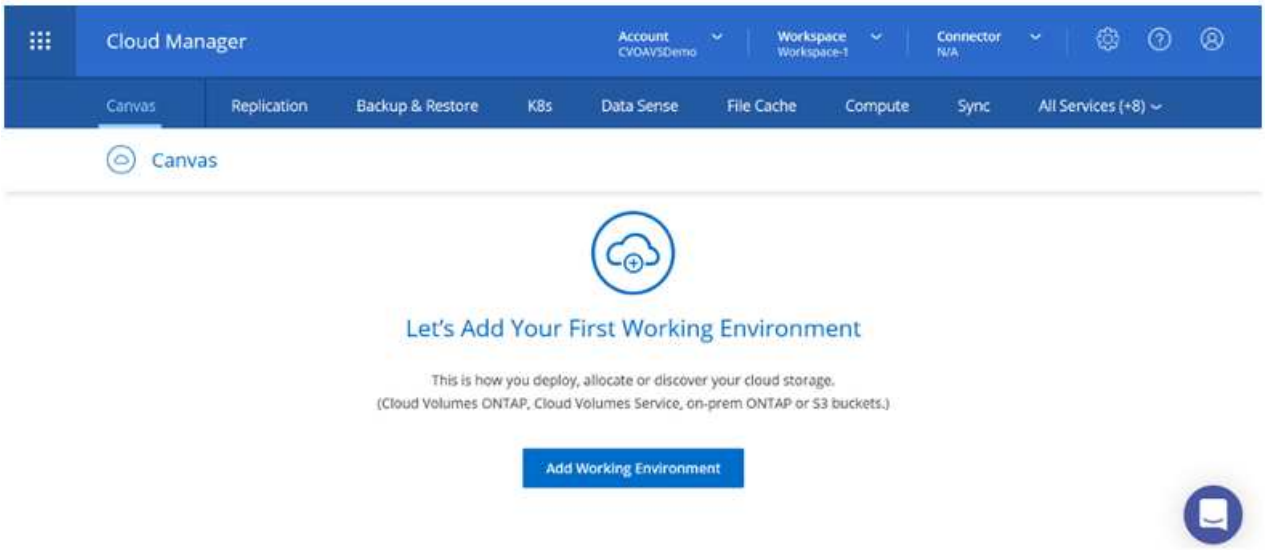
Implemente el nuevo Cloud Volumes ONTAP en Azure

Los recursos compartidos y los LUN de Cloud Volumes ONTAP se pueden montar a partir de máquinas virtuales creadas en el entorno SDDC de la solución para Azure VMware. Los volúmenes también pueden montarse en el cliente Linux y en el cliente Windows, ya que Cloud Volumes ONTAP admite los protocolos iSCSI, SMB y NFS. Los volúmenes de Cloud Volumes ONTAP se pueden configurar en unos pocos pasos sencillos.

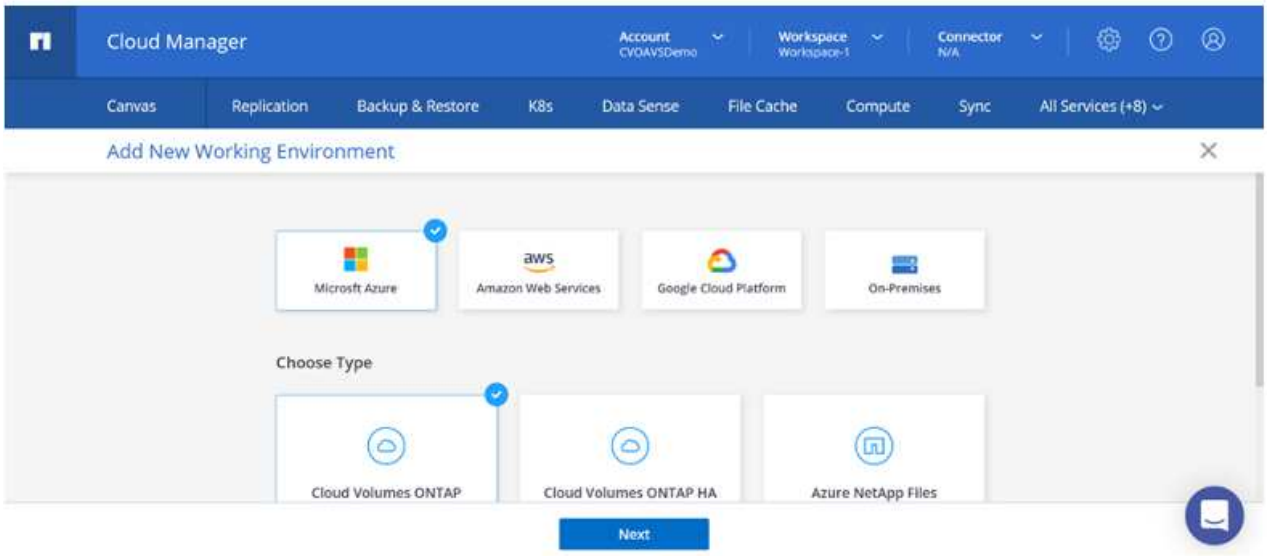
Para replicar volúmenes de un entorno local al cloud por motivos de recuperación ante desastres o migración, establezca la conectividad de red a Azure, ya sea mediante una VPN sitio a sitio o ExpressRoute. La replicación de datos de las instalaciones a Cloud Volumes ONTAP no se encuentra fuera del alcance de este documento. Para replicar datos entre sistemas Cloud Volumes ONTAP y locales, consulte "Configurar la replicación de datos entre sistemas".

Uso "Configuración de Cloud Volumes ONTAP" Para ajustar el tamaño de las instancias de Cloud Volumes ONTAP de forma precisa. Supervise también el rendimiento local para utilizarlo como entradas en el dimensionador Cloud Volumes ONTAP.

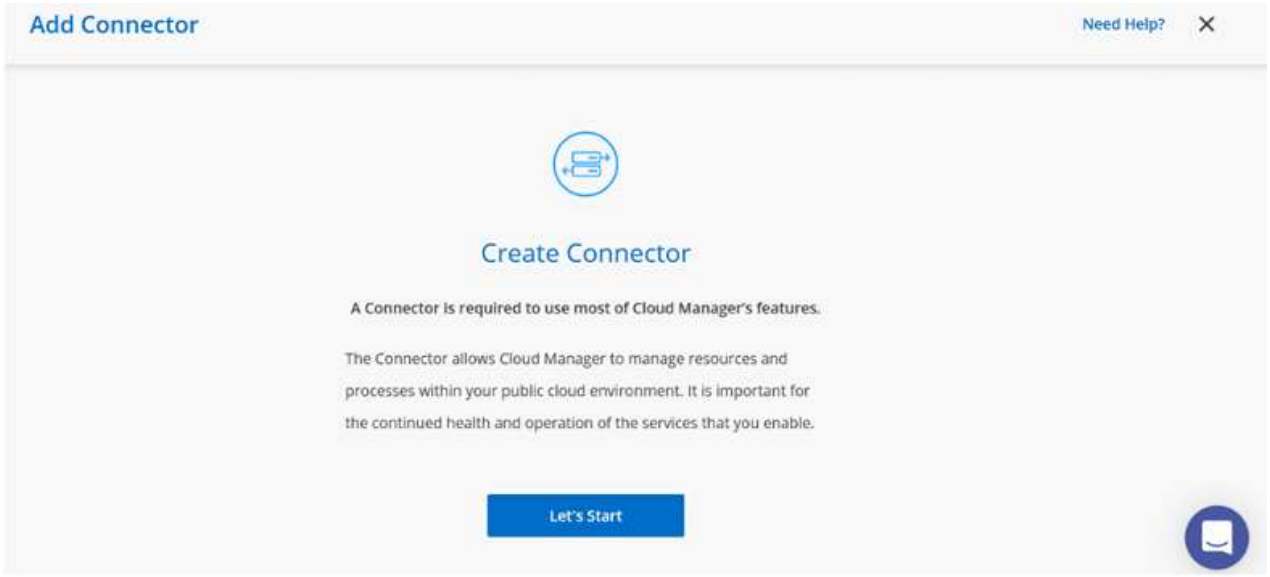
1. Inicie sesión en NetApp Cloud Central: Se mostrará la pantalla Fabric View. Localice la pestaña Cloud Volumes ONTAP y seleccione Go to Cloud Manager. Una vez que haya iniciado sesión, aparecerá la pantalla Canvas.



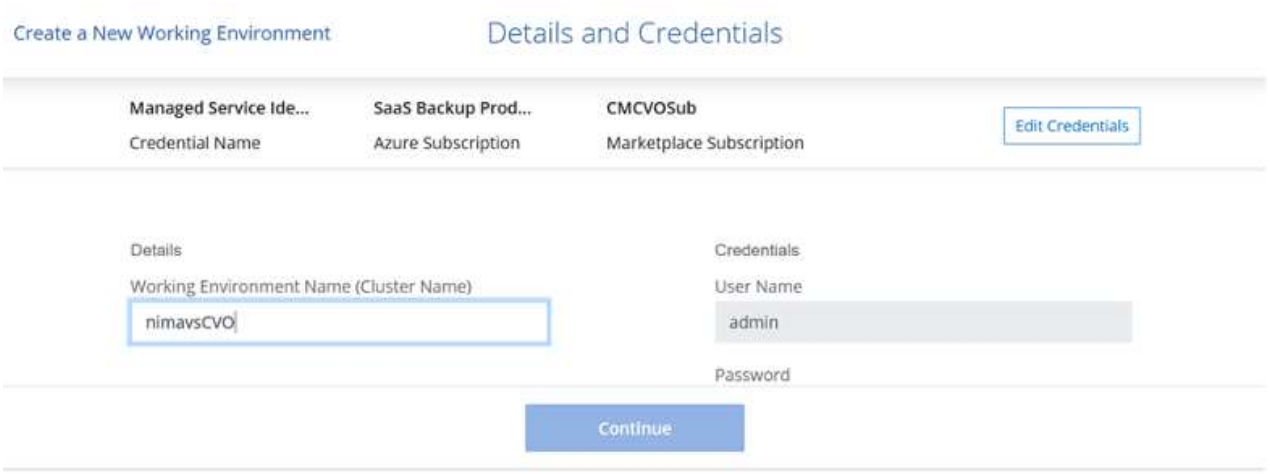
2. En la página de inicio de Cloud Manager, haga clic en Add a Working Environment y, a continuación, seleccione Microsoft Azure como cloud y el tipo de configuración del sistema.



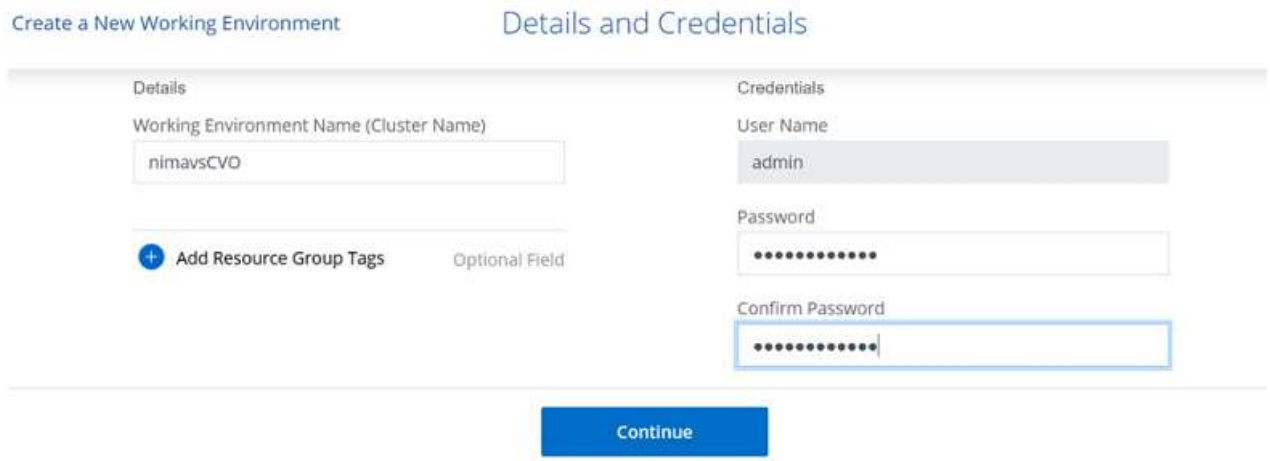
3. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que implemente un conector.



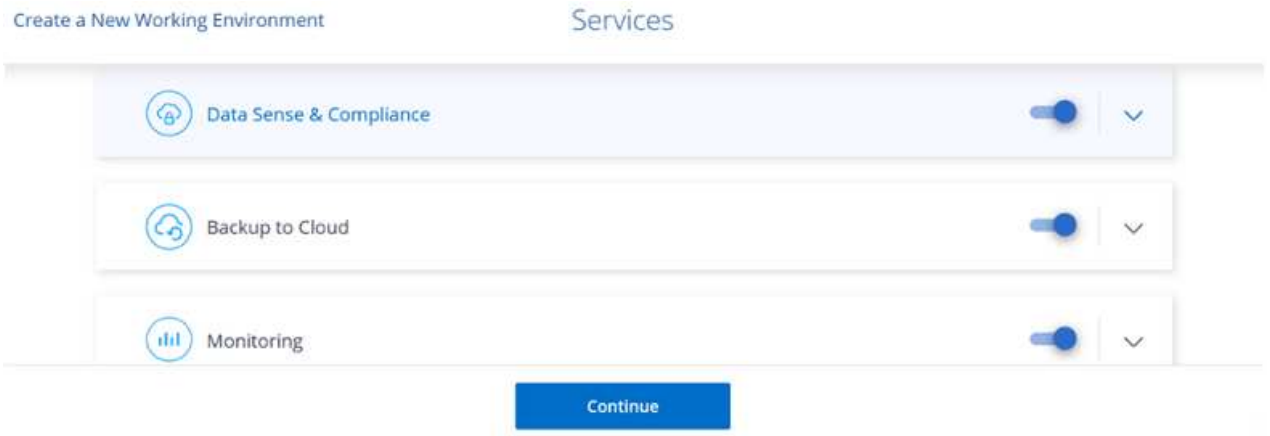
4. Una vez creado el conector, actualice los campos Detalles y credenciales.



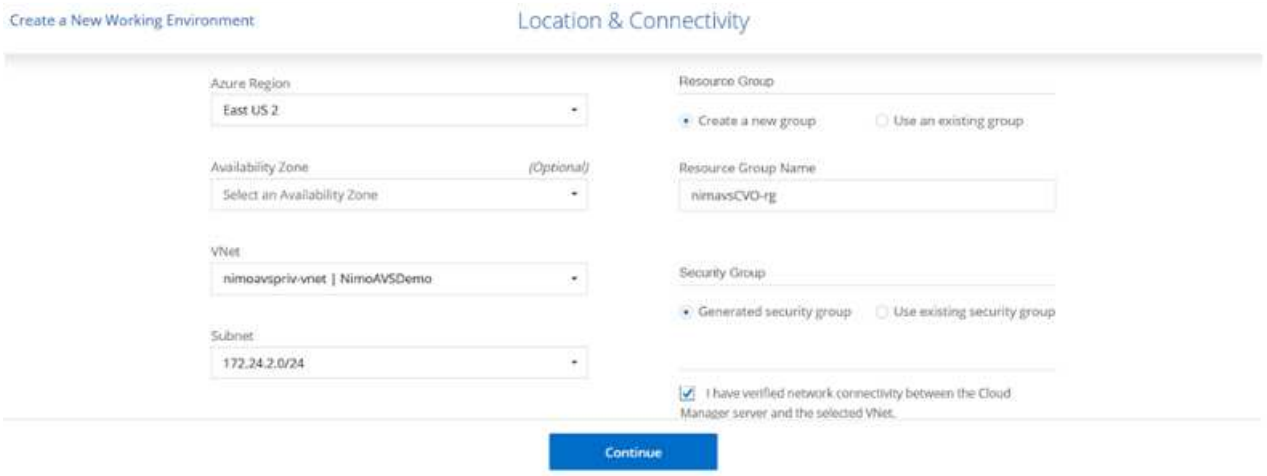
5. Proporcione los detalles del entorno que se va a crear, incluidos el nombre del entorno y las credenciales de administración. Añada etiquetas de grupo de recursos para el entorno de Azure como un parámetro opcional. Una vez que haya terminado, haga clic en continuar.



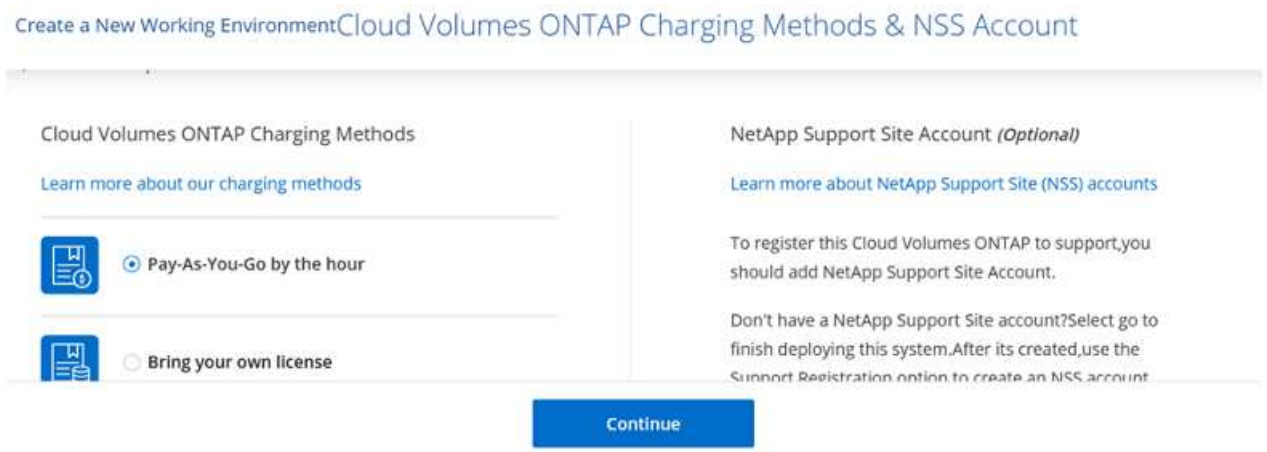
6. Selecciona los servicios complementarios para la implementación de Cloud Volumes ONTAP, que incluyen la clasificación de BlueXP, el backup y la recuperación de datos de BlueXP, y Cloud Insights. Seleccione los servicios y haga clic en Continue.



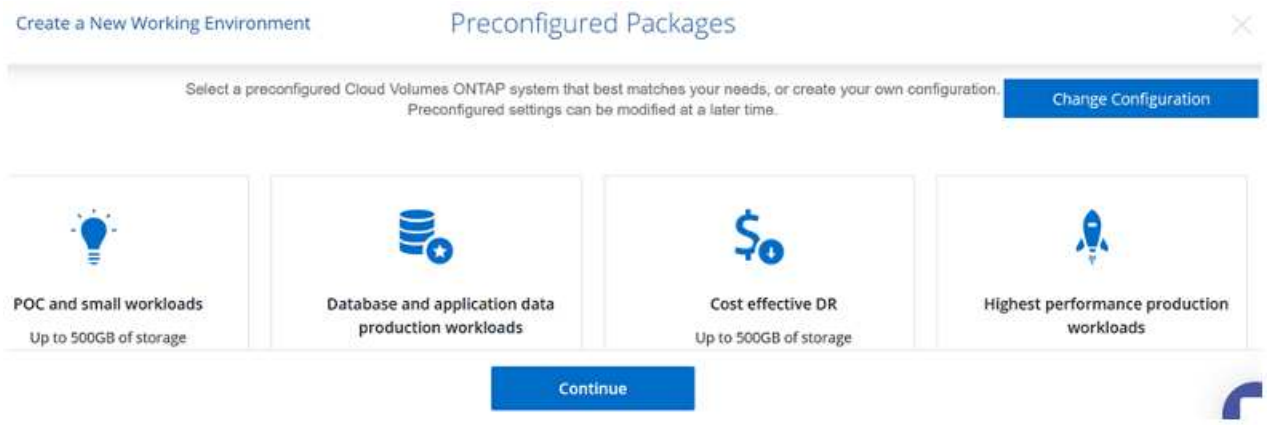
7. Configure la ubicación y la conectividad de Azure. Seleccione la región de Azure, el grupo de recursos, vnet y la subred que desee utilizar.



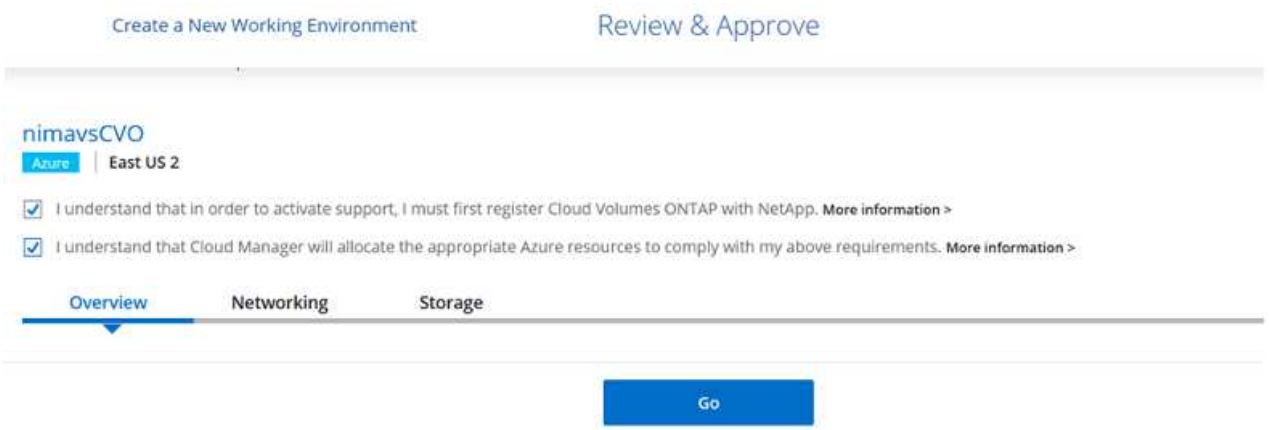
8. Seleccione la opción de licencia: Pago por uso o BYOL para usar la licencia existente. En este ejemplo, se utiliza la opción de pago por uso.



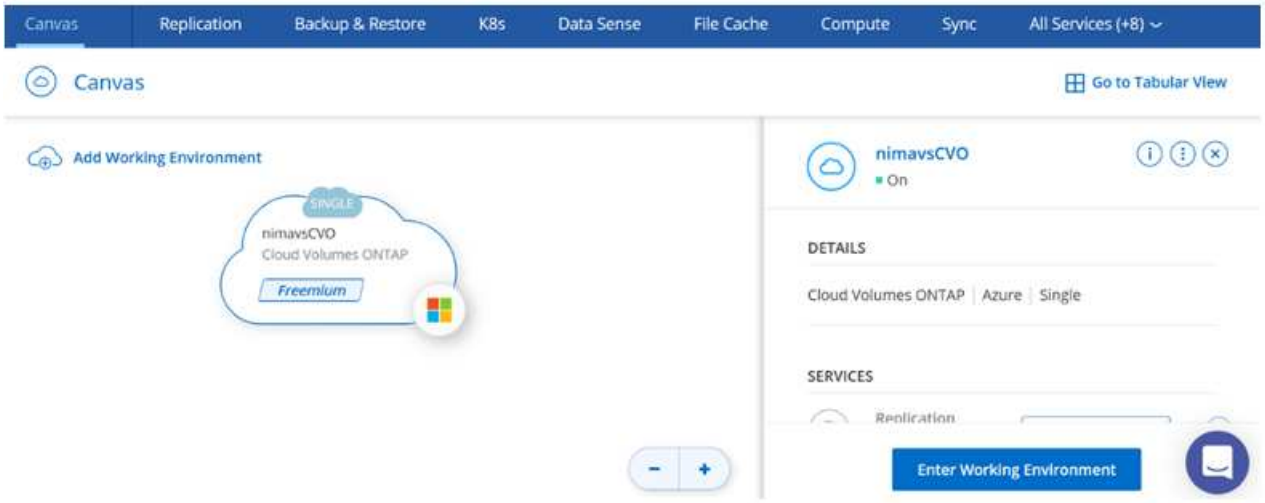
9. Seleccione entre varios paquetes preconfigurados disponibles para los distintos tipos de cargas de trabajo.



10. Acepte los dos acuerdos sobre la activación del soporte y la asignación de recursos de Azure.para crear la instancia de Cloud Volumes ONTAP, haga clic en Go.

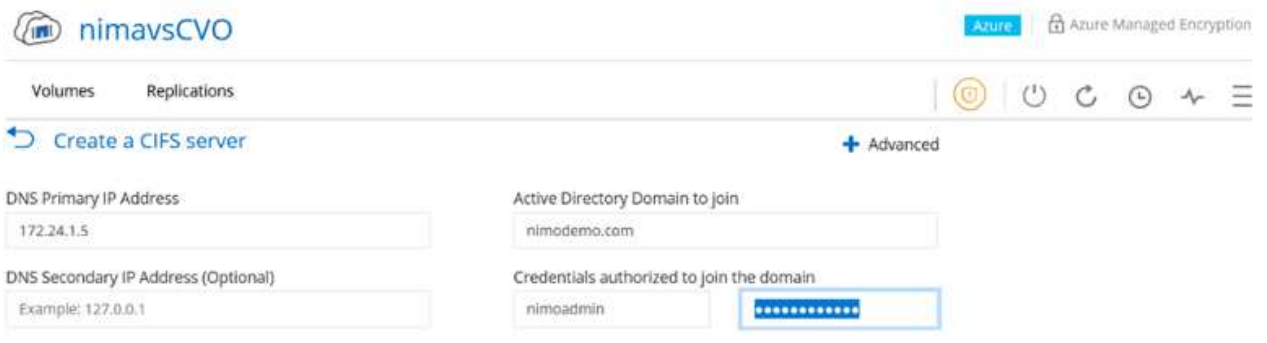


11. Una vez que se ha aprovisionado Cloud Volumes ONTAP, se muestra en los entornos de trabajo de la página lienzo.

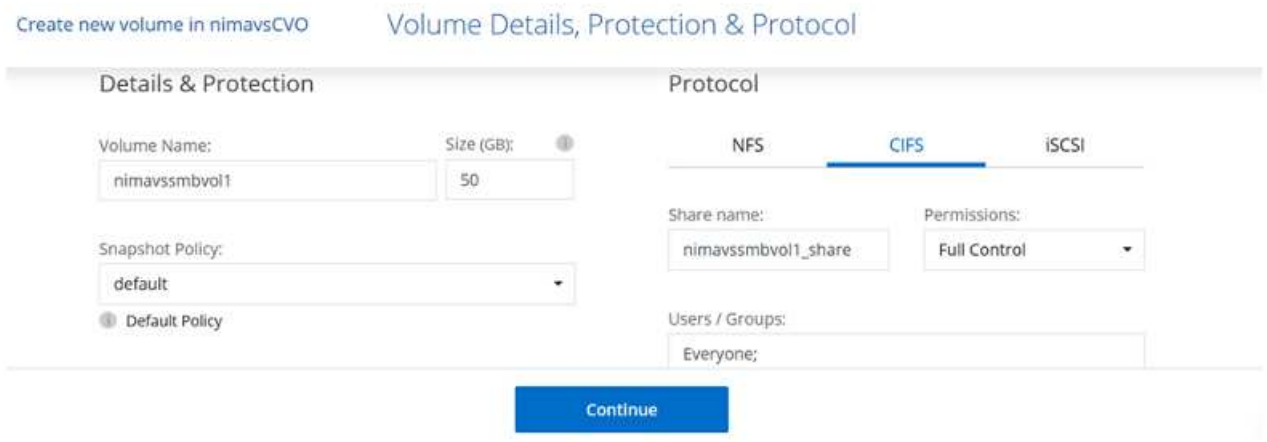


Configuraciones adicionales para volúmenes SMB

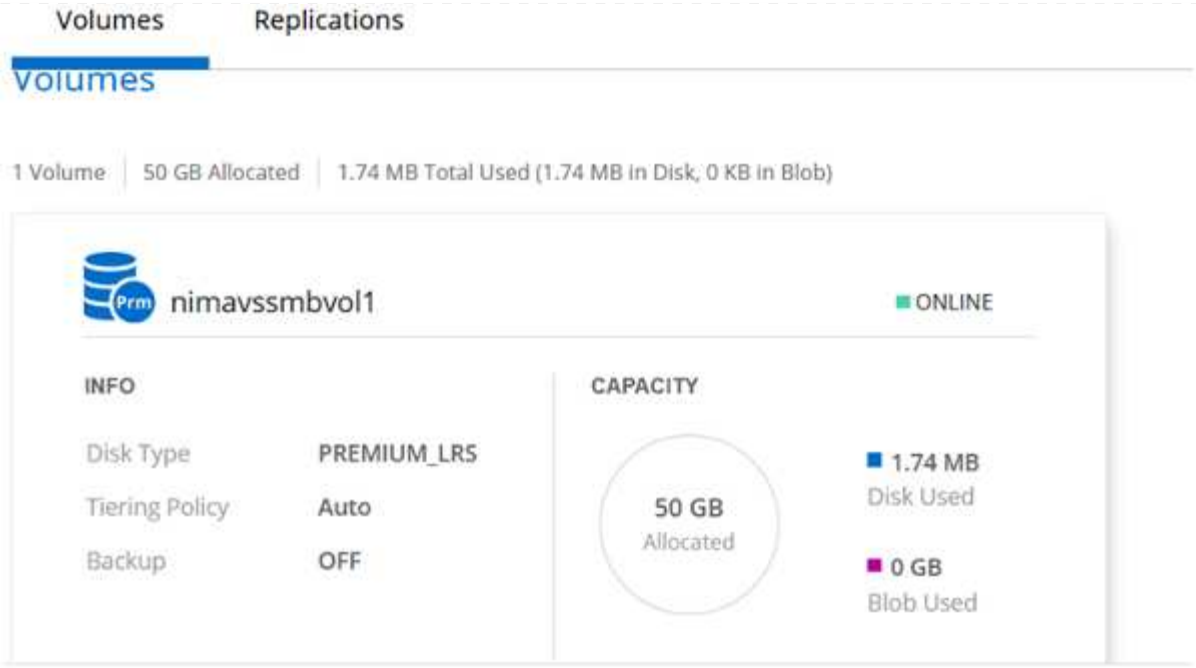
1. Una vez listo el entorno de trabajo, asegúrese de que el servidor CIFS esté configurado con los parámetros de configuración DNS y Active Directory adecuados. Este paso es necesario para poder crear el volumen de SMB.



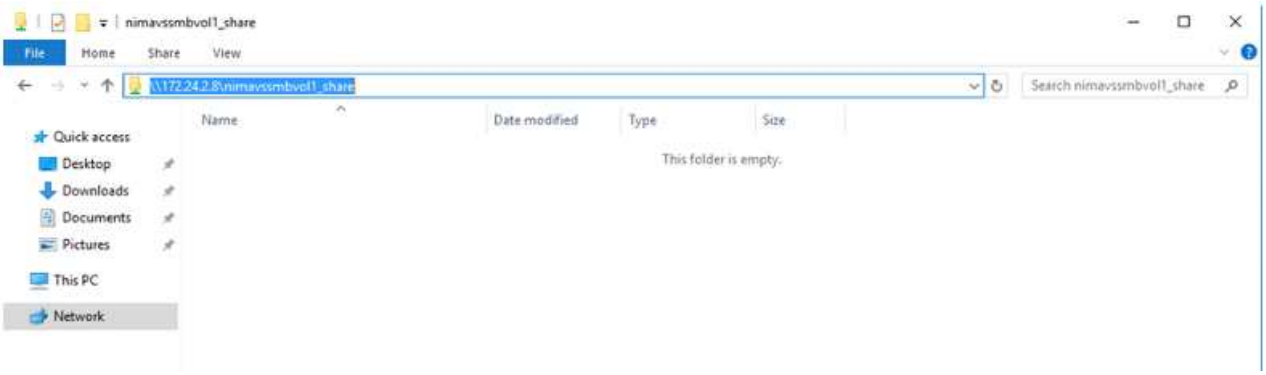
2. La creación del volumen SMB es un proceso sencillo. Seleccione la instancia de CVO para crear el volumen y haga clic en la opción Create Volume. Elija el tamaño adecuado y el gestor de cloud elija el agregado que lo contiene o utilice un mecanismo de asignación avanzado para colocarlo en un agregado concreto. En esta demostración, se ha seleccionado SMB como protocolo.



3. Una vez que el volumen se ha aprovisionado, estará disponible en el panel Volumes. Dado que se aprovisiona un recurso compartido de CIFS, conceda a los usuarios o grupos permiso a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo. Este paso no es necesario si el volumen se replica desde un entorno en las instalaciones, ya que los permisos de archivos y carpetas se conservan como parte de la replicación de SnapMirror.



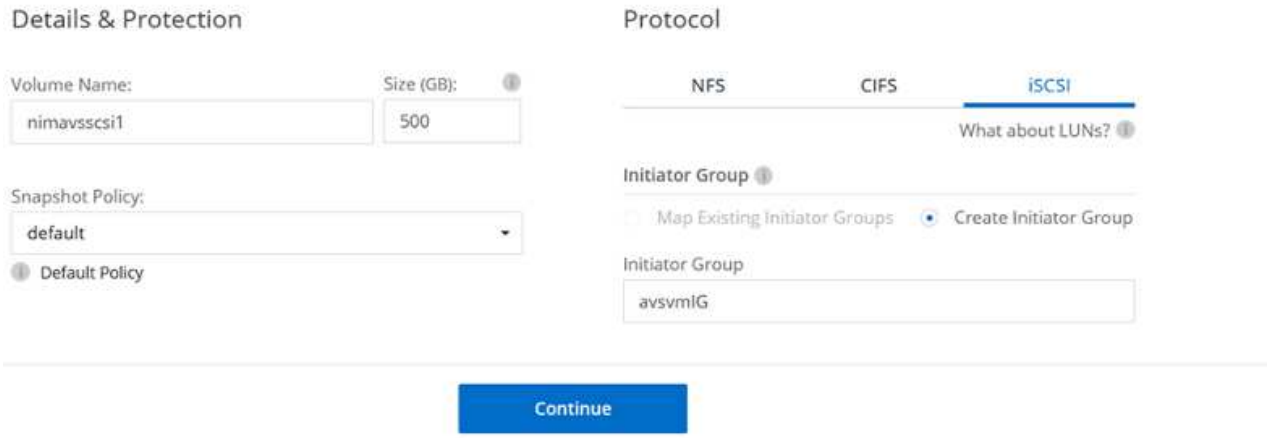
4. Una vez creado el volumen, utilice el comando Mount para conectarse al recurso compartido desde la máquina virtual que se ejecuta en los hosts SDDC de Azure VMware Solution.
5. Copie la siguiente ruta y utilice la opción Map Network Drive para montar el volumen en el equipo virtual que se ejecuta en el centro de datos definido por software de la solución VMware de Azure.



Conectar el LUN a un host

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

1. En la página lienzo, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP para crear y gestionar volúmenes.
2. Haga clic en Add Volume > New Volume, seleccione iSCSI y haga clic en Create Initiator Group. Haga clic en Continue.



3. Una vez que se haya aprovisionado el volumen, seleccione el volumen y, a continuación, haga clic en IQN de destino. Para copiar el nombre completo de iSCSI (IQN), haga clic en Copy. Configurar una conexión iSCSI desde el host al LUN.

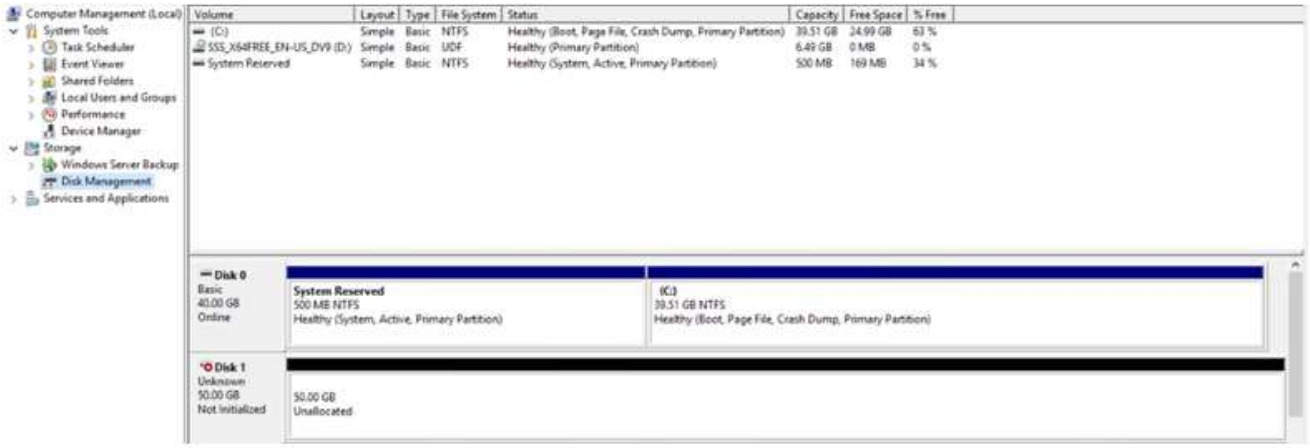
   Para lograr lo mismo con el host que reside en el centro de datos definido por software de la solución VMware de Azure:

   a. RDP a la máquina virtual alojada en el SDDC de la solución Azure VMware.
   b. Abra el cuadro de diálogo Propiedades del iniciador iSCSI: Administrador del servidor > Panel > Herramientas > Iniciador iSCSI.
   c. En la pestaña Discovery, haga clic en Discover Portal o Add Portal y, a continuación, introduzca la dirección IP del puerto de destino iSCSI.
   d. En la pestaña Destinos, seleccione el objetivo detectado y haga clic en Iniciar sesión o conectar.
   e. Seleccione Activar multivía y, a continuación, seleccione Restaurar automáticamente esta conexión cuando se inicie el equipo o Agregar esta conexión a la lista de destinos favoritos. Haga clic en Avanzado.

      Nota: el host Windows debe tener una conexión iSCSI con cada nodo del clúster. El DSM nativo selecciona las mejores rutas que se van a utilizar.

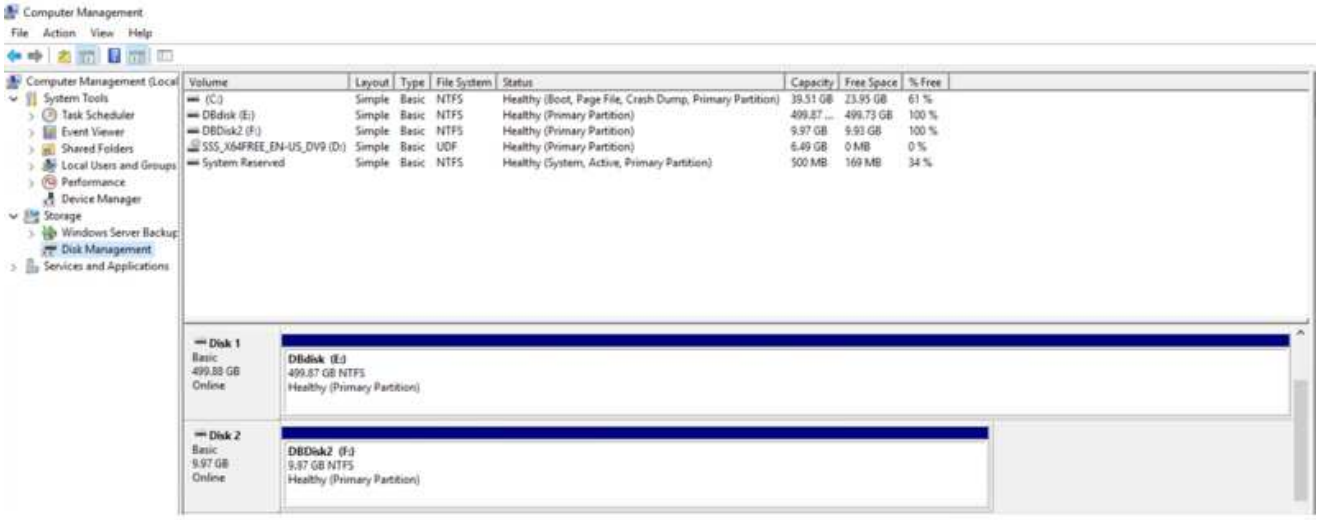
Las LUN de una máquina virtual de almacenamiento (SVM) aparecen como discos en el host Windows. El host no detecta automáticamente los nuevos discos que se añaden. Active una detección repetida manual para detectar los discos realizando los pasos siguientes:

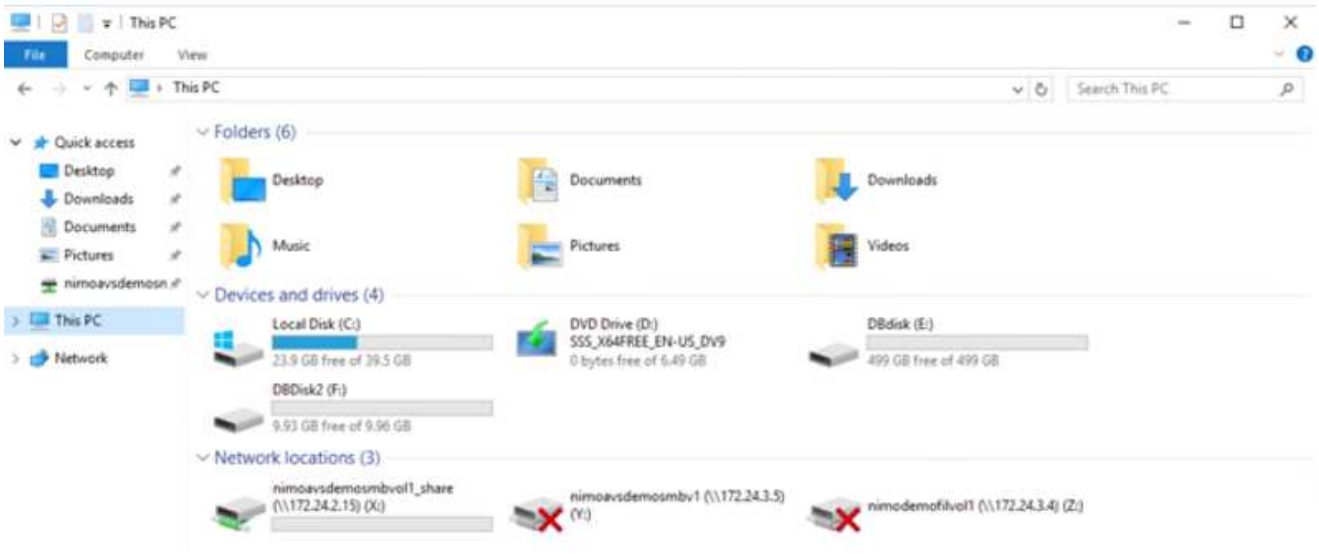
1. Abra la utilidad Administración de equipos de Windows: Inicio > Herramientas administrativas > Administración de equipos.
2. Expanda el nodo almacenamiento en el árbol de navegación.
3. Haga clic en Administración de discos.
4. Haga clic en Acción > discos de reexploración.



Cuando el host Windows accede por primera vez a una nueva LUN, no tiene sistema de archivos o partición. Inicialice la LUN y, de manera opcional, formatee la LUN con un sistema de archivos realizando los pasos siguientes:

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



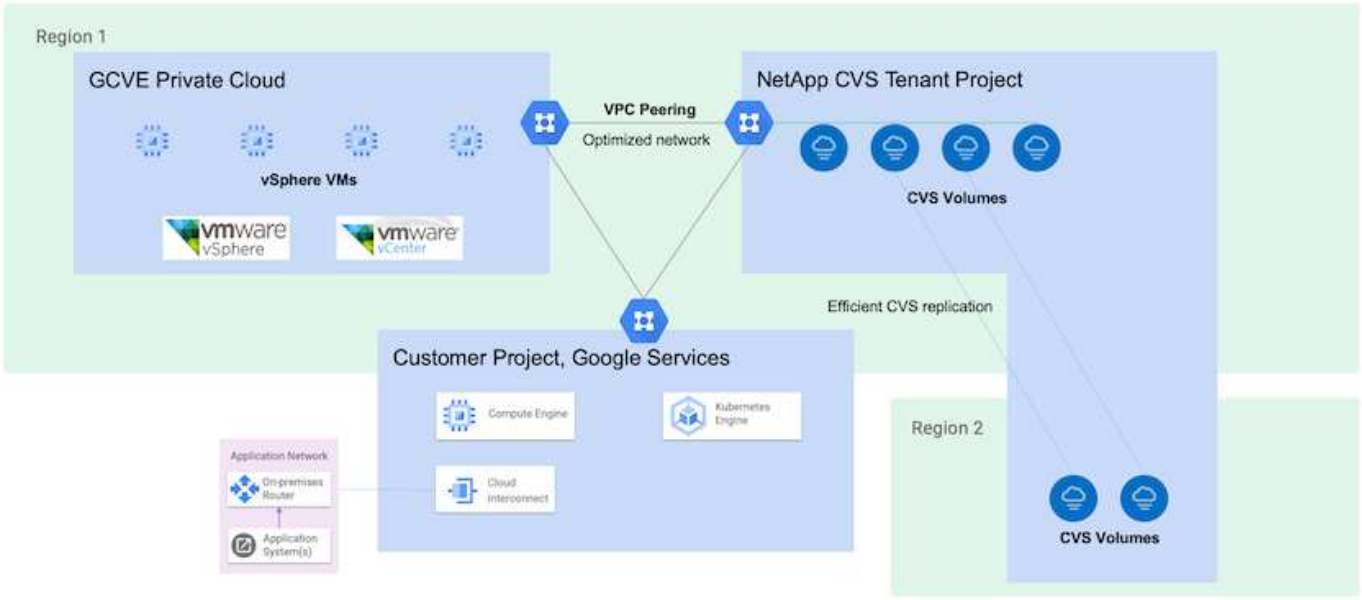


Almacén de datos NFS complementario de Google Cloud VMware Engine con Cloud Volume Service de NetApp

Descripción general

Autores: Suresh Thoppay, NetApp

Los clientes que requieren capacidad de almacenamiento adicional en su entorno de Google Cloud VMware Engine (GCVE) pueden utilizar el servicio Cloud Volume de NetApp para montarlo como almacén de datos NFS complementario.
Almacenar datos en el servicio Cloud Volume de NetApp permite a los clientes replicar entre regiones para protegerlos de la radiodifusión.



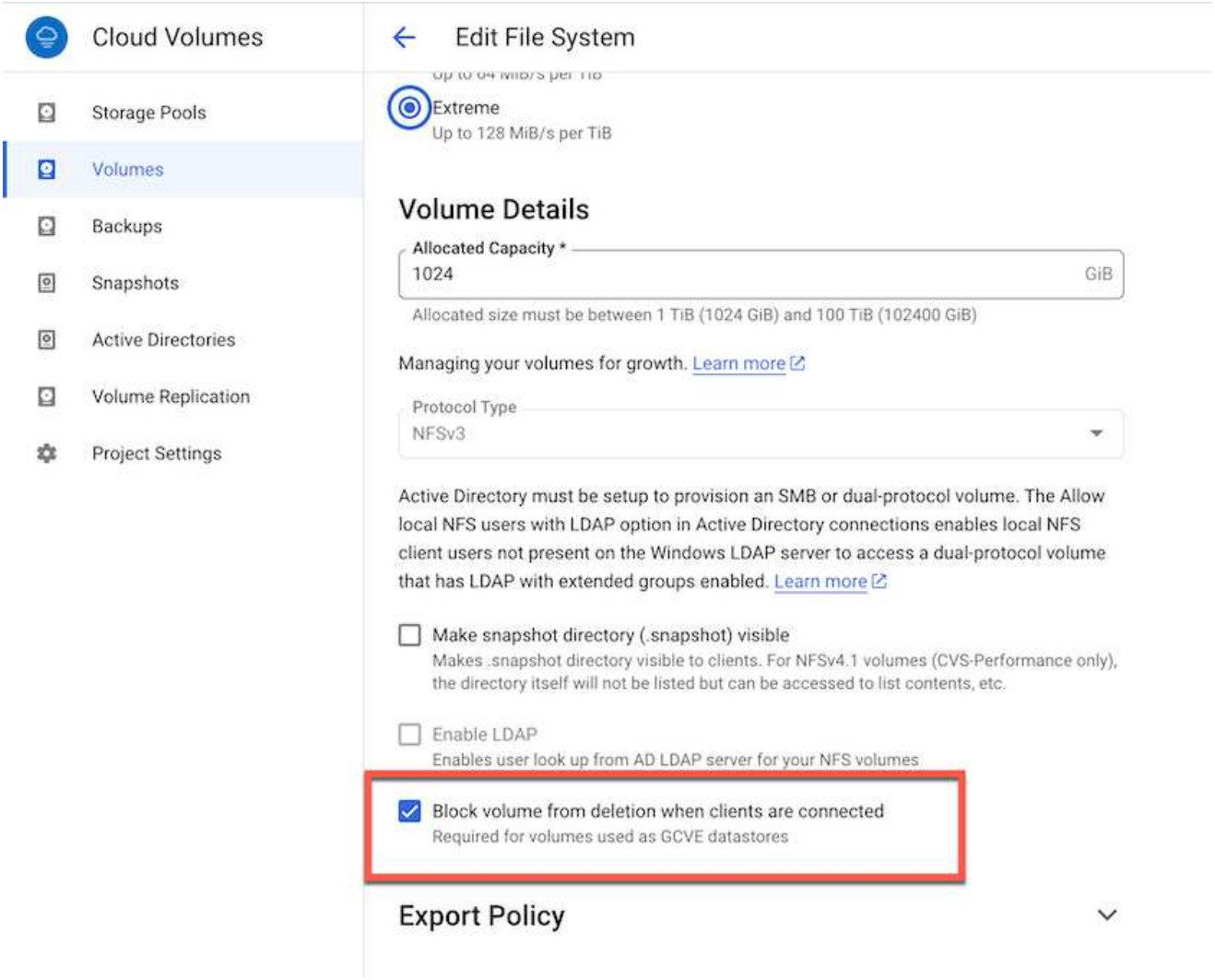
Pasos de implementación para montar el almacén de datos NFS desde CVS de NetApp en GCVE

Aprovisionar volumen de CVS-Performance

El volumen de servicio de volúmenes de cloud de NetApp se puede aprovisionar
"Uso de la consola de Google Cloud"
"Mediante la API o el portal de NetApp BlueXP"

Marque ese volumen CVS como no eliminable

Para evitar la eliminación accidental del volumen mientras la máquina virtual se está ejecutando, asegúrese de que el volumen esté marcado como no eliminable, como se muestra en la siguiente captura de pantalla.



Para obtener más información, consulte "Creando volumen NFS" documentación.

Asegúrese de que existe una conexión privada en GCVE para el VPC de inquilino de NetApp CVS.

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

Montar el almacén de datos de NFS

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

> Dado que Google gestiona los hosts de vSphere, no tiene acceso para instalar NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB).
> Si necesita soporte para Virtual Volumes (VVol), no dude en comunicárnoslo.
> Si desea utilizar Jumbo Frames, consulte "Tamaños máximos de MTU admitidos en GCP"

Ahorro con Cloud Volume Service de NetApp

Para obtener más información sobre su posible ahorro con Cloud Volume Service de NetApp para sus demandas de almacenamiento en GCVE, visite "Calculadora de ROI de NetApp"

Enlaces de referencia

- "Blog de Google: Cómo usar CVS de NetApp como almacenes de datos para el motor de VMware de Google Cloud"
- "Blog de NetApp: Una forma mejor de migrar tus aplicaciones con gran cantidad de almacenamiento a Google Cloud"

Opciones de almacenamiento de NetApp para GCP

GCP admite almacenamiento NetApp conectado como invitado con Cloud Volumes ONTAP (CVO) o Cloud Volumes Service (CVS).

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, o CVO, es la solución de gestión de datos en el cloud líder del sector que se basa en el software de almacenamiento ONTAP de NetApp, disponible de forma nativa en Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).

Se trata de una versión de ONTAP definida por software que consume almacenamiento nativo del cloud, lo que le permite tener el mismo software de almacenamiento en el cloud y en las instalaciones, lo que reduce la necesidad de volver a formar al personal INFORMÁTICO en todos los métodos nuevos para gestionar sus datos.

CVO ofrece a los clientes la capacidad de mover datos del perímetro, al centro de datos, al cloud y al backup sin problemas, de tal modo que su cloud híbrido se aúna, todo ello gestionado con una consola de gestión de panel único, Cloud Manager de NetApp.

Por su diseño, CVO ofrece un rendimiento extremo y capacidades de gestión de datos avanzadas para responder incluso a sus aplicaciones más exigentes en el cloud

Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado

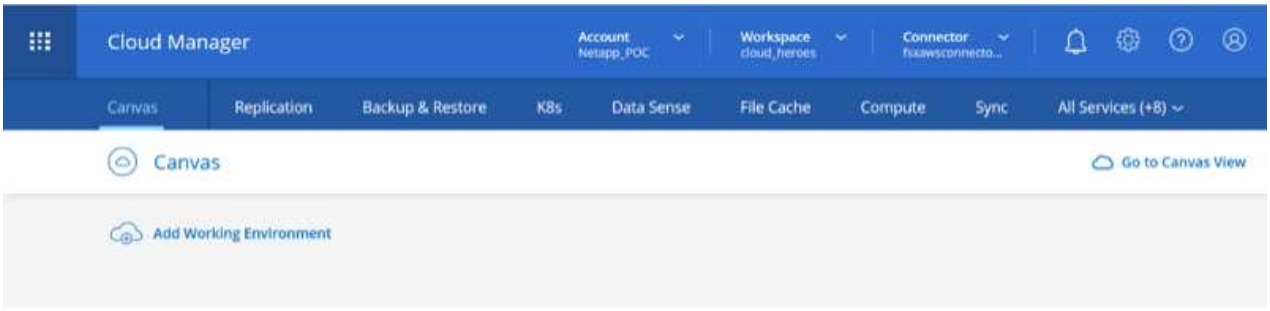
Implemente Cloud Volumes ONTAP en Google Cloud (hágalo usted mismo)

Los recursos compartidos y LUN de Cloud Volumes ONTAP se pueden montar a partir de equipos virtuales creados en el entorno de cloud privado GCVE. Los volúmenes también pueden montarse en el cliente Linux y en el cliente Windows y se puede acceder A LUN y LUN en clientes Linux o Windows como dispositivos de bloque cuando se monta a través de iSCSI, porque Cloud Volumes ONTAP admite los protocolos iSCSI, SMB y NFS. Los volúmenes de Cloud Volumes ONTAP se pueden configurar en unos pocos pasos sencillos.

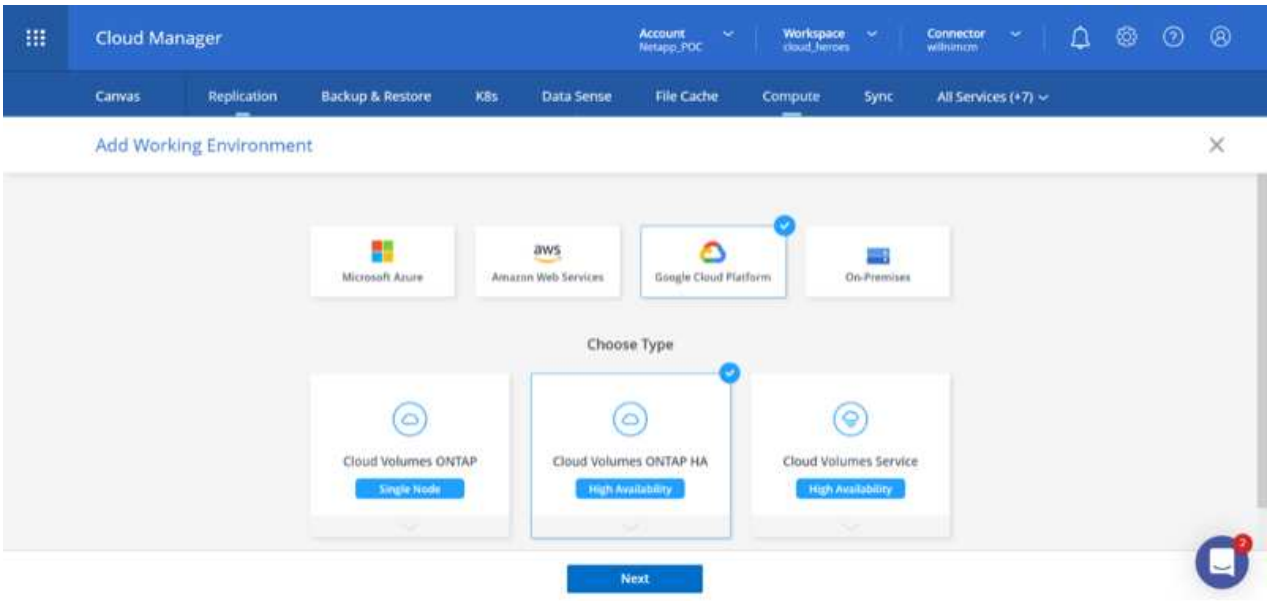
Para replicar volúmenes de un entorno local al cloud por motivos de recuperación ante desastres o migración, establezca la conectividad de red con Google Cloud, ya sea mediante una VPN de sitio a sitio o Cloud Interconnect. La replicación de datos de las instalaciones a Cloud Volumes ONTAP no se encuentra fuera del alcance de este documento. Para replicar datos entre sistemas Cloud Volumes ONTAP y locales, consulte xref:./ehc/"Configurar la replicación de datos entre sistemas".

Uso "Configuración de Cloud Volumes ONTAP" Para ajustar el tamaño de las instancias de Cloud Volumes ONTAP de forma precisa. Supervise también el rendimiento local para utilizarlo como entradas en el dimensionador Cloud Volumes ONTAP.

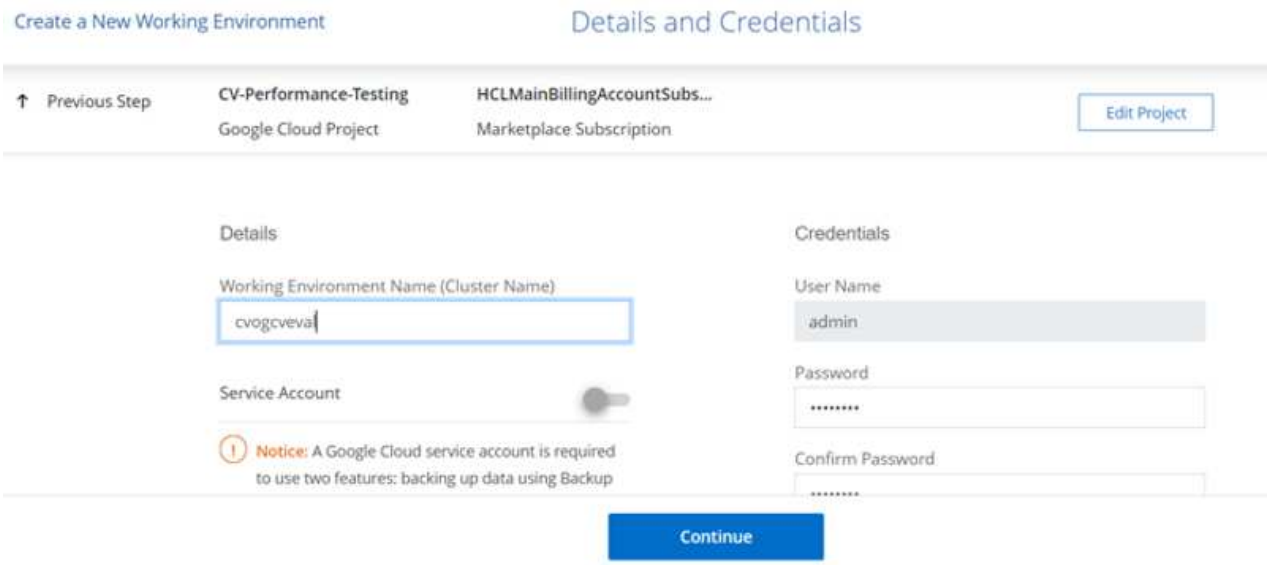
1. Inicie sesión en NetApp Cloud Central: Se mostrará la pantalla Fabric View. Localice la pestaña Cloud Volumes ONTAP y seleccione Go to Cloud Manager. Una vez que haya iniciado sesión, aparecerá la pantalla Canvas.



2. En la ficha lienzo de Cloud Manager, haga clic en Agregar un entorno de trabajo y, a continuación, seleccione Google Cloud Platform como la nube y el tipo de configuración del sistema. A continuación, haga clic en Siguiente.

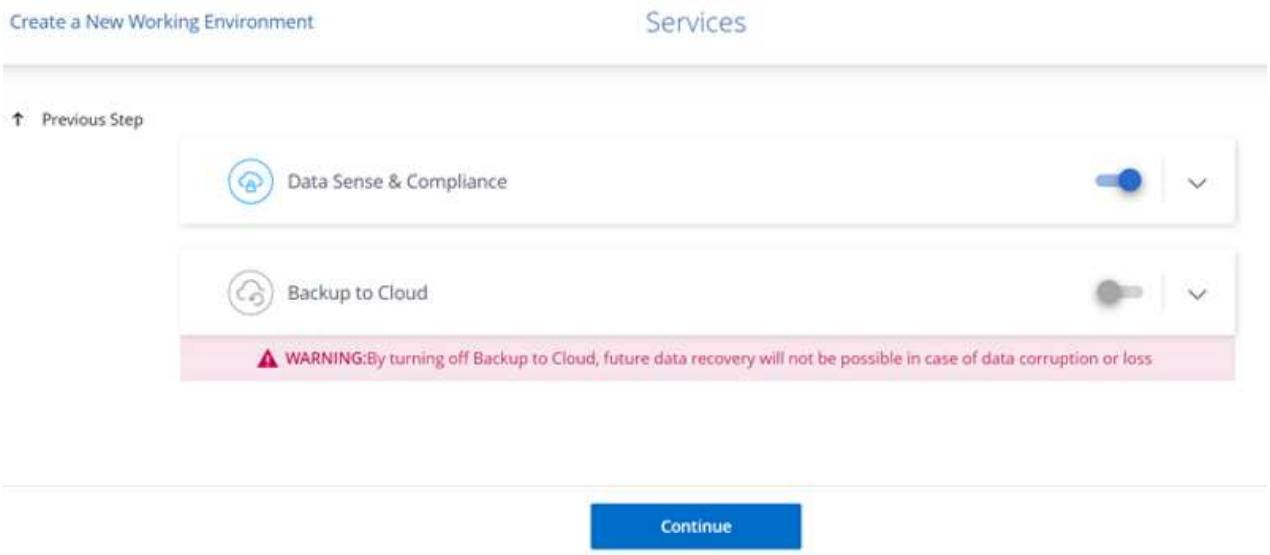


3. Proporcione los detalles del entorno que se va a crear, incluidos el nombre del entorno y las credenciales de administración. Una vez que haya terminado, haga clic en continuar.

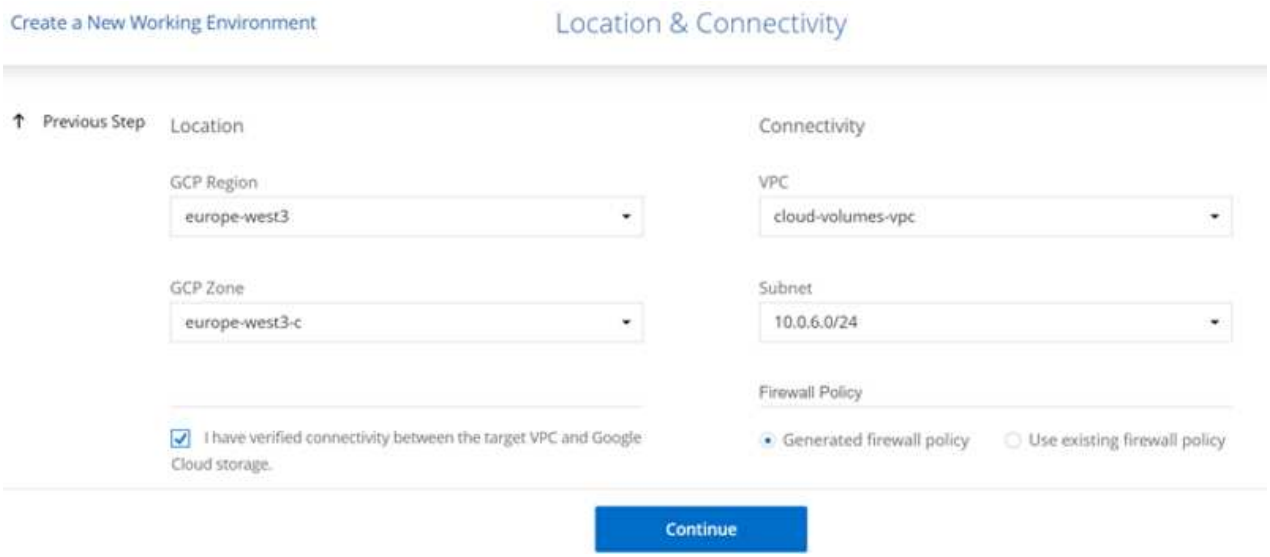


4. Seleccione o anule la selección de los servicios complementarios para la implementación de Cloud Volumes ONTAP, como detección de datos y cumplimiento de normativas o backup en el cloud. A continuación, haga clic en continuar.

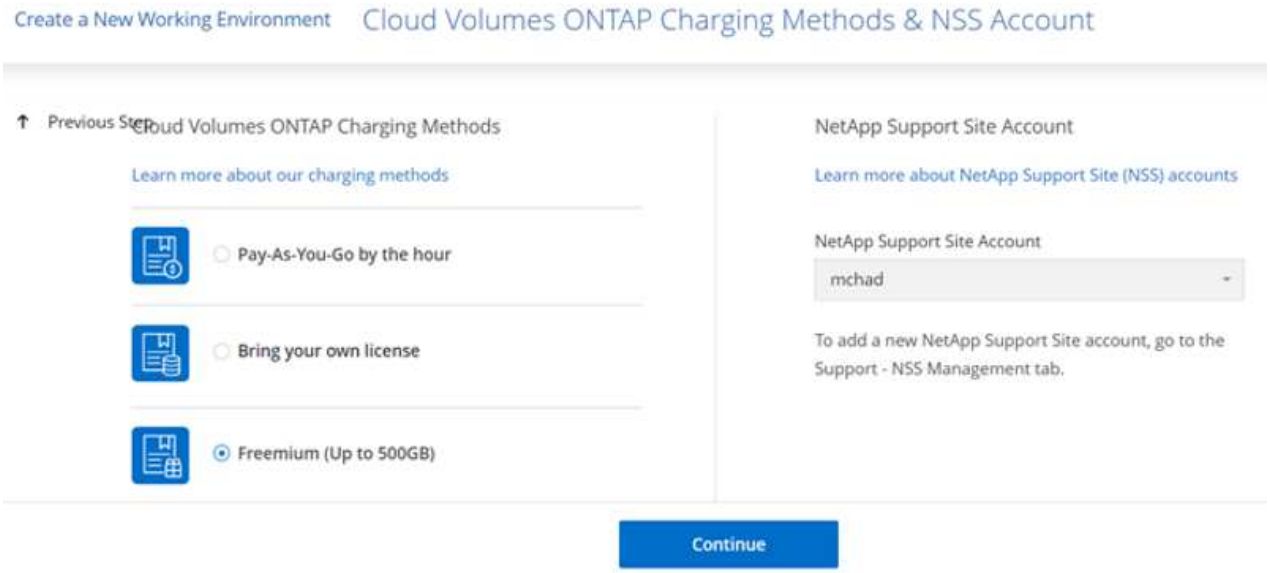
   SUGERENCIA: Se mostrará un mensaje emergente de verificación al desactivar los servicios de complemento. Los servicios complementarios se pueden agregar o eliminar después de la implementación de CVO, considere deseleccionarlos si no son necesarios desde el principio para evitar costes.



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

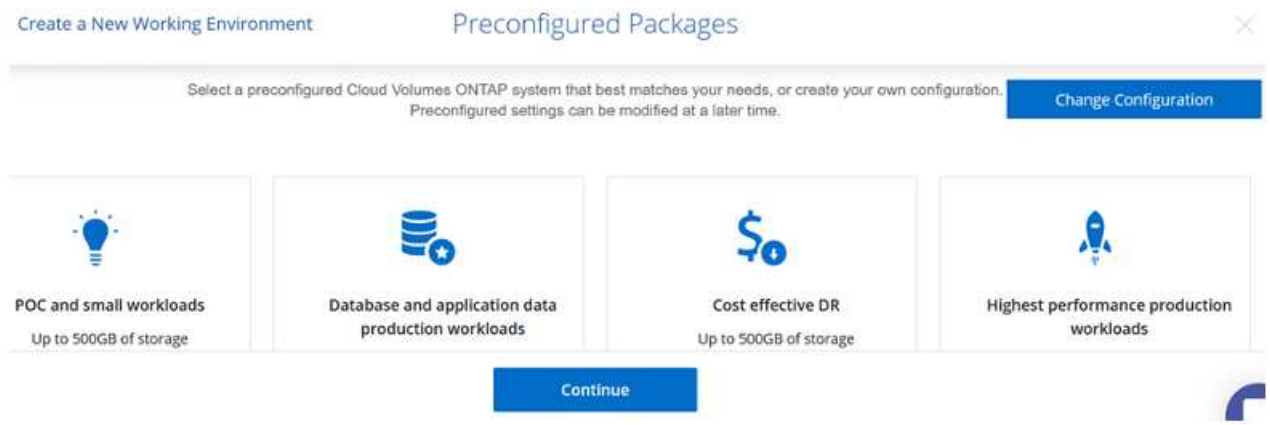


6. Seleccione la opción de licencia: Pago por uso o BYOL para usar la licencia existente. En este ejemplo, se utiliza la opción Freemium. A continuación, haga clic en continuar.

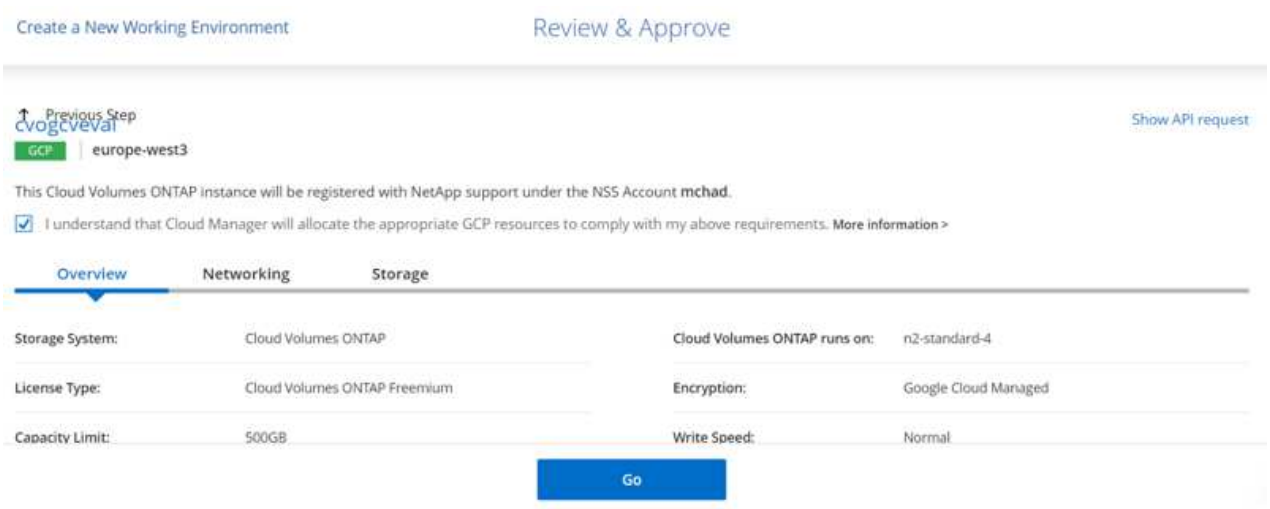


7. Seleccione entre varios paquetes preconfigurados disponibles en función del tipo de carga de trabajo que se pondrá en marcha en máquinas virtuales que se ejecuten en VMware Cloud en AWS SDDC.

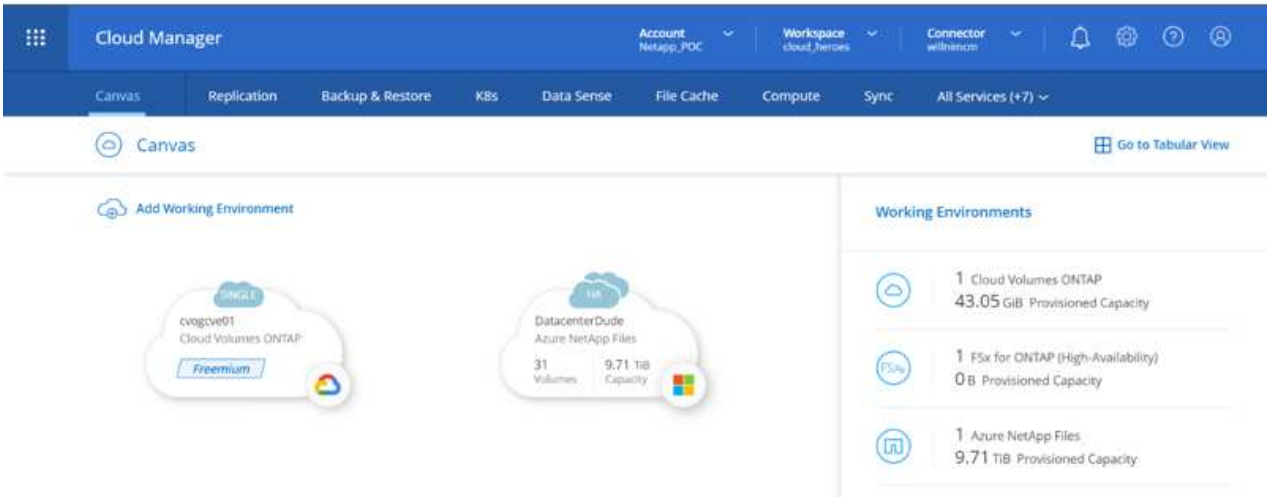
   SUGERENCIA: Coloque el ratón sobre los mosaicos para obtener más información o personalice los componentes de CVO y la versión de ONTAP haciendo clic en Cambiar configuración.



8. En la página Review & Approve, revise y confirme las selecciones.para crear la instancia de Cloud Volumes ONTAP, haga clic en Go.



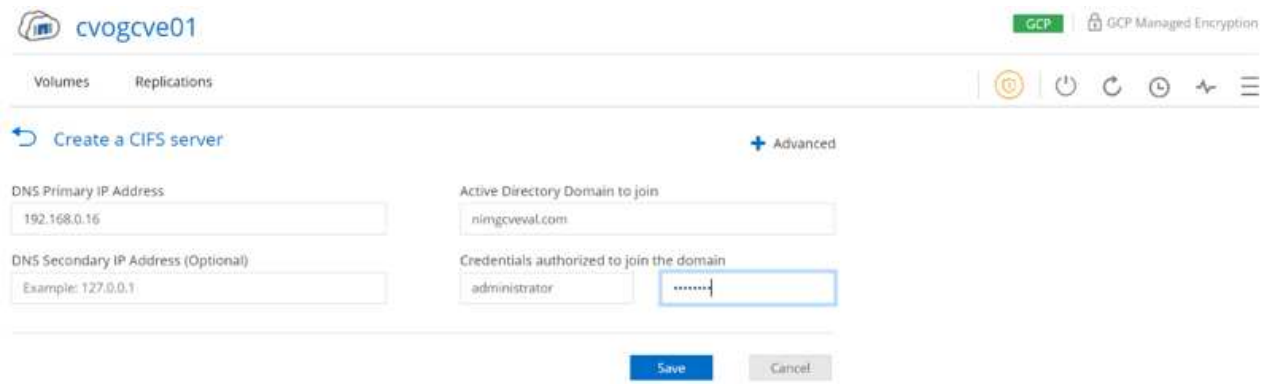
9. Una vez que se ha aprovisionado Cloud Volumes ONTAP, se muestra en los entornos de trabajo de la página lienzo.



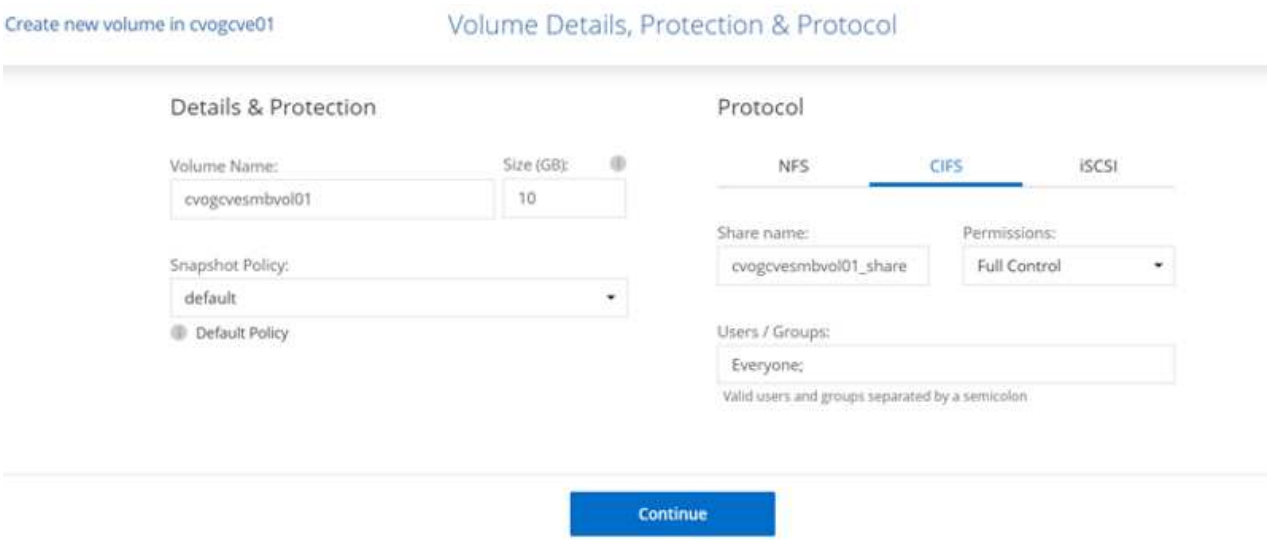
Configuraciones adicionales para volúmenes SMB

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

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



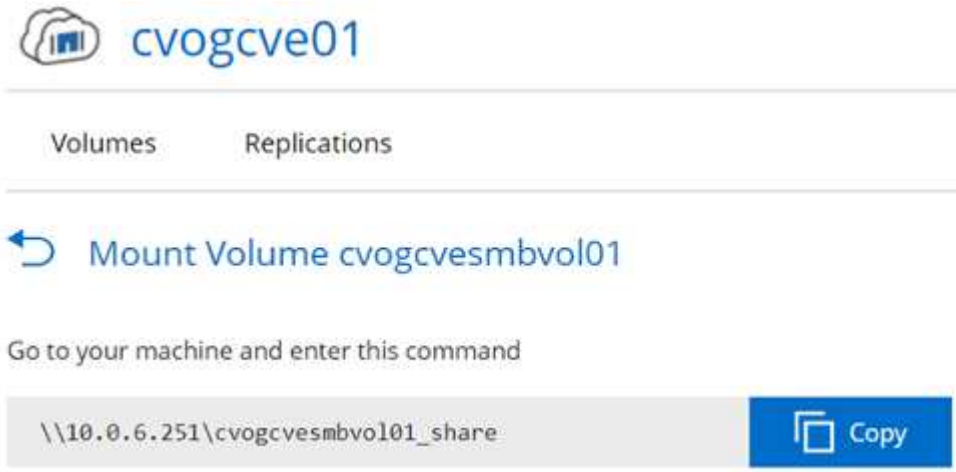
2. La creación del volumen SMB es un proceso sencillo. En lienzo, haga doble clic en el entorno de trabajo Cloud Volumes ONTAP para crear y gestionar volúmenes y haga clic en la opción Crear volumen. Elija el tamaño adecuado y el gestor de cloud elija el agregado que lo contiene o utilice un mecanismo de asignación avanzado para colocarlo en un agregado concreto. Para esta demostración, se selecciona CIFS/SMB como protocolo.



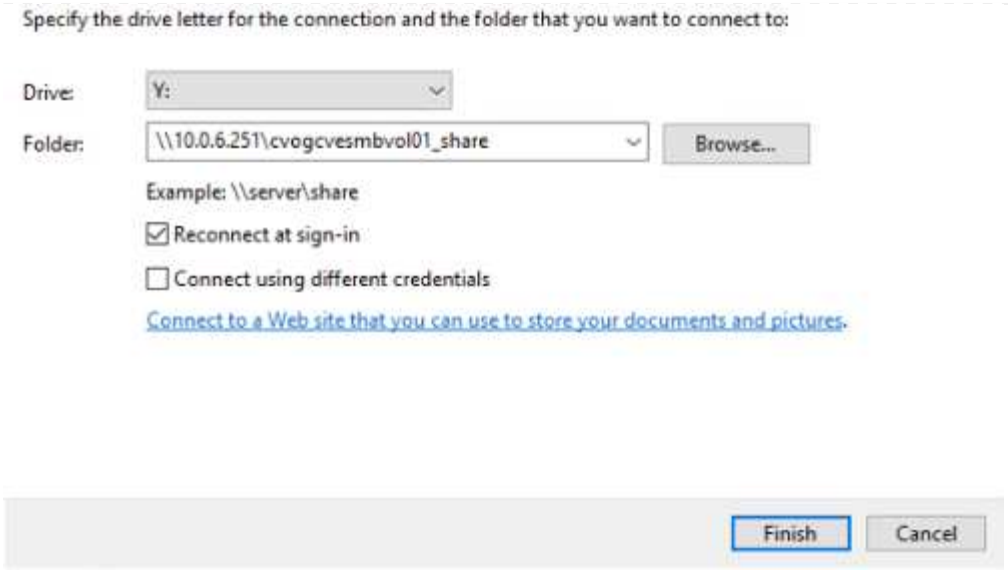
3. Una vez que el volumen se ha aprovisionado, estará disponible en el panel Volumes. Dado que se aprovisiona un recurso compartido de CIFS, conceda a los usuarios o grupos permiso a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo. Este paso no es necesario si el volumen se replica desde un entorno en las instalaciones, ya que 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 mostrar sus opciones.

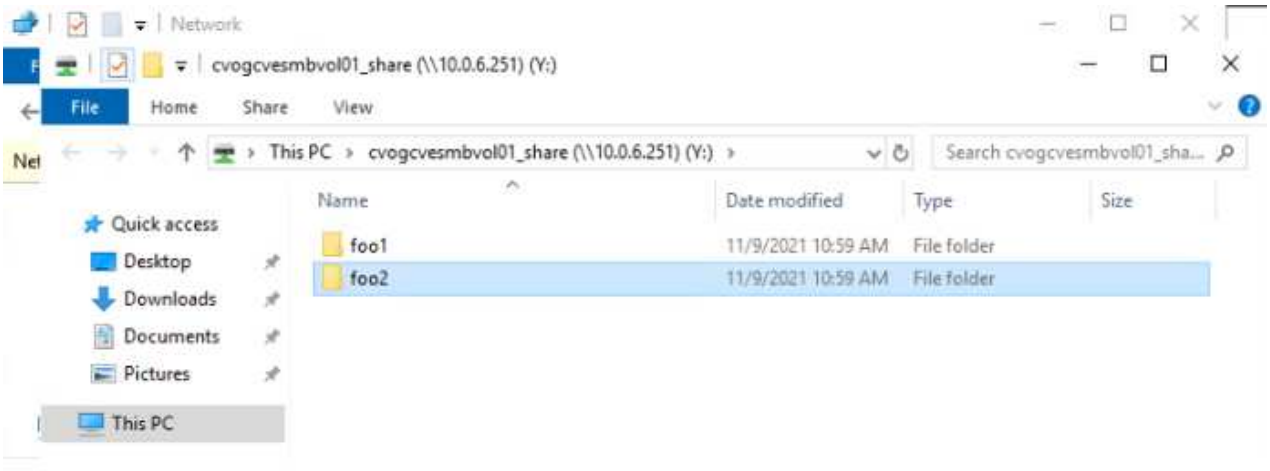
4. Una vez creado el volumen, utilice el comando de montaje para mostrar las instrucciones de conexión de volúmenes y, a continuación, conéctese al recurso compartido desde las máquinas virtuales en Google Cloud VMware Engine.



5. Copie la siguiente ruta y utilice la opción Map Network Drive para montar el volumen en la máquina virtual que se ejecuta en el motor de VMware de Google Cloud.



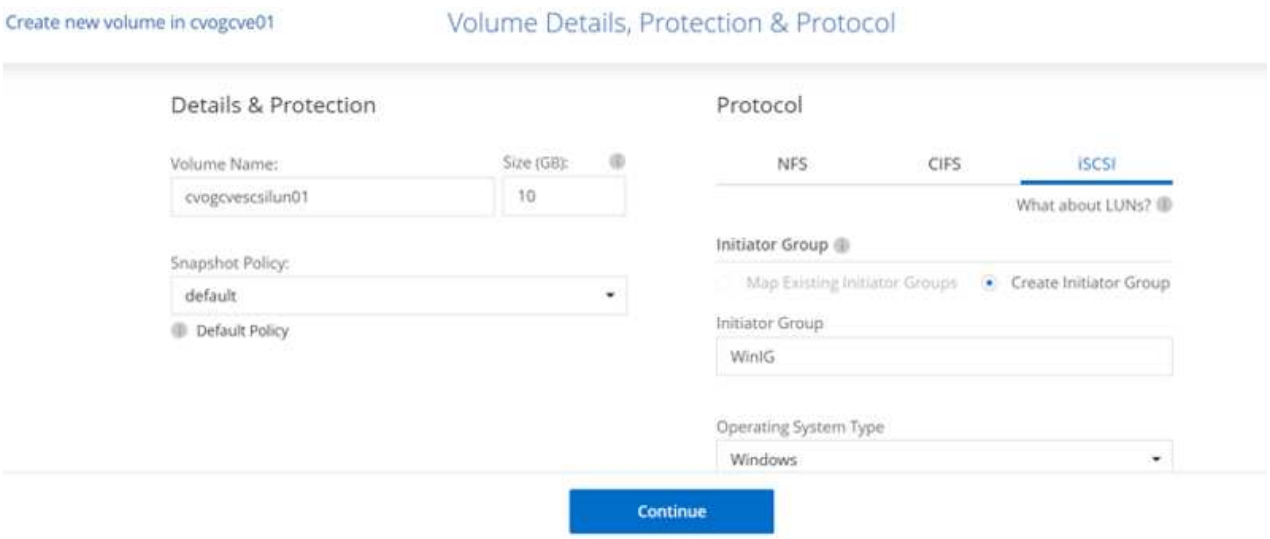
Una vez asignado, se puede acceder fácilmente y los permisos NTFS se pueden establecer en consecuencia.

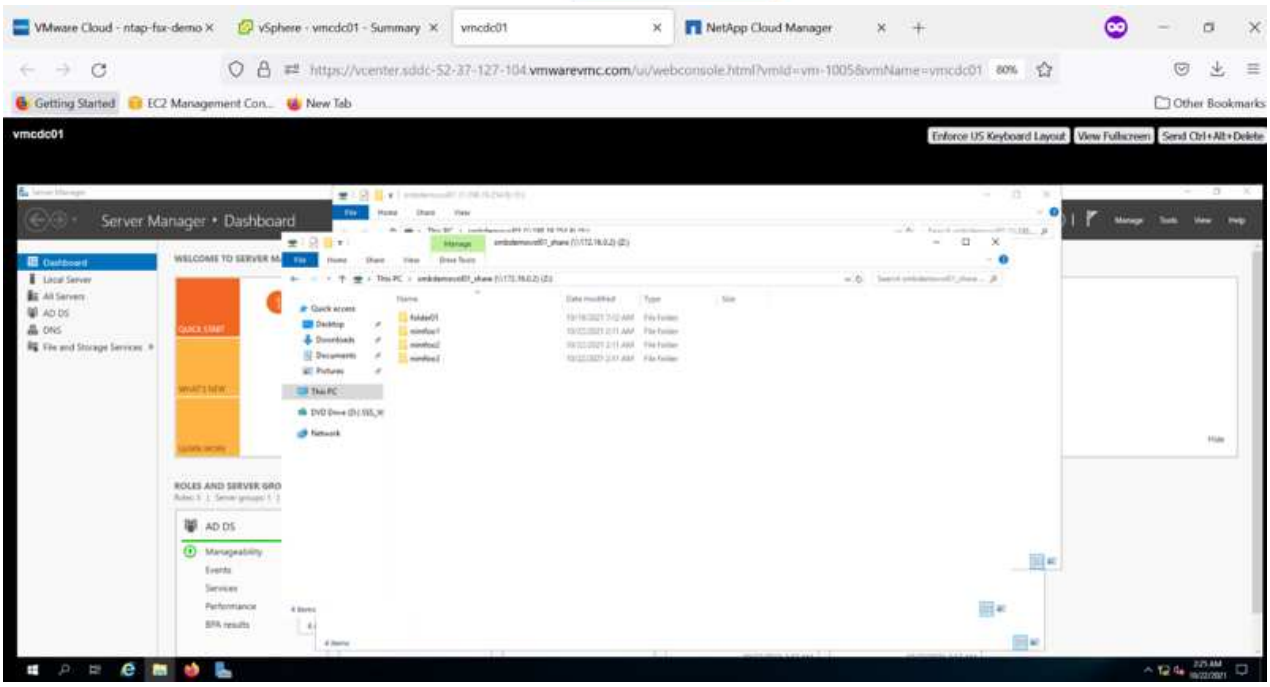


Conectar el LUN en Cloud Volumes ONTAP a un host

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

1. En la página lienzo, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP para crear y gestionar volúmenes.
2. Haga clic en Add Volume > New Volume, seleccione iSCSI y haga clic en Create Initiator Group. Haga clic en Continue.





3. Una vez que se ha aprovisionado el volumen, seleccione el menú volumen (º) y, a continuación, haga clic en Target IQN. Para copiar el nombre completo de iSCSI (IQN), haga clic en Copy. Configurar una conexión iSCSI desde el host al LUN.

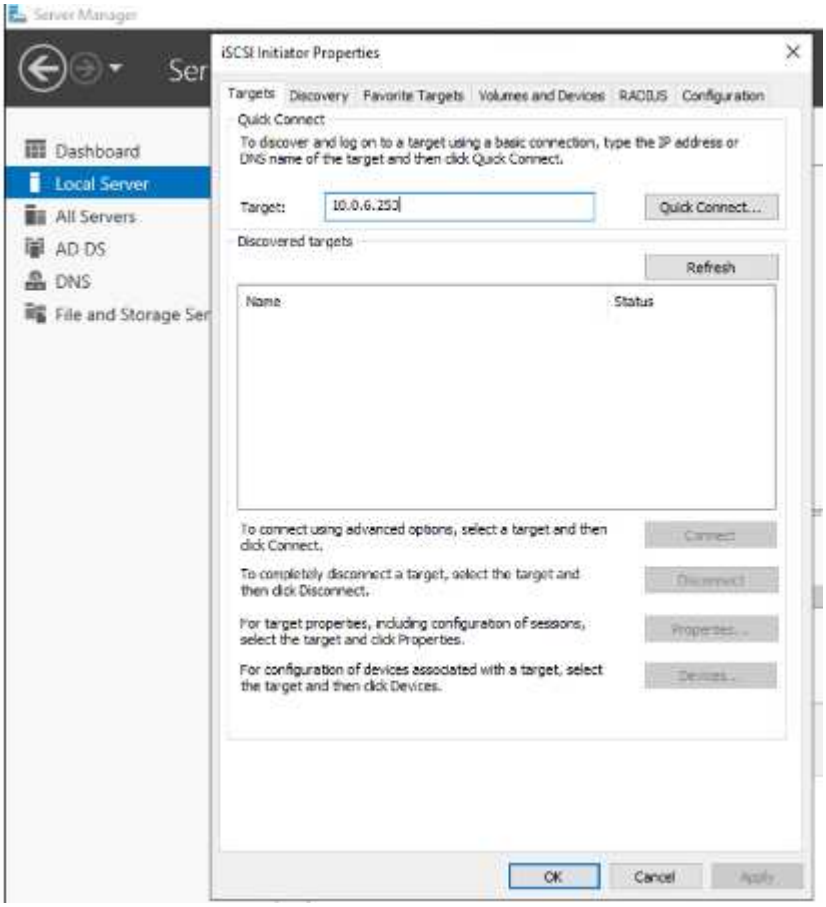
Para lograr lo mismo para el host que reside en Google Cloud VMware Engine:

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 >

Herramientas > Iniciador iSCSI.

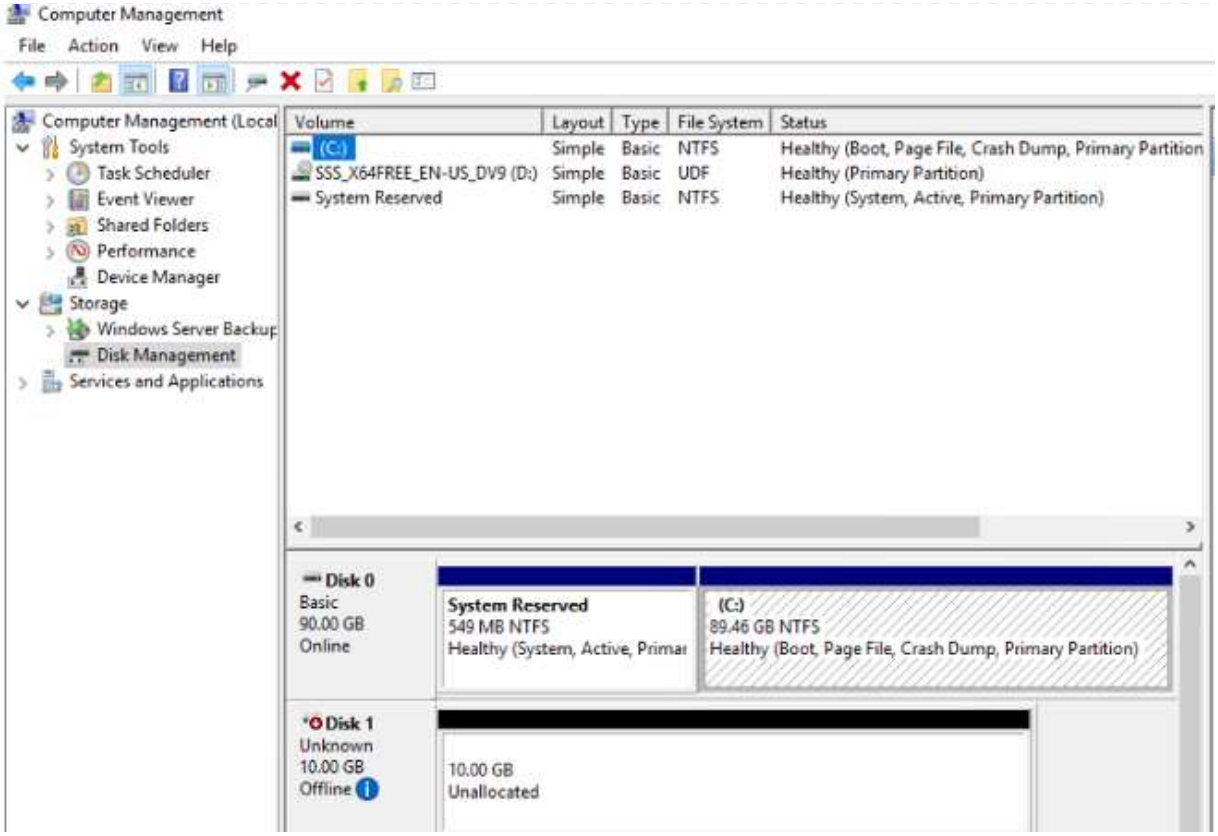
3. En la pestaña Discovery, haga clic en Discover Portal o Add Portal y, a continuación, introduzca la dirección IP del puerto de destino iSCSI.
4. En la pestaña Destinos, seleccione el objetivo detectado y haga clic en Iniciar sesión o conectar.
5. Seleccione Activar multivía y, a continuación, seleccione Restaurar automáticamente esta conexión 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 con cada nodo del clúster. El DSM nativo selecciona las mejores rutas que se van a utilizar.



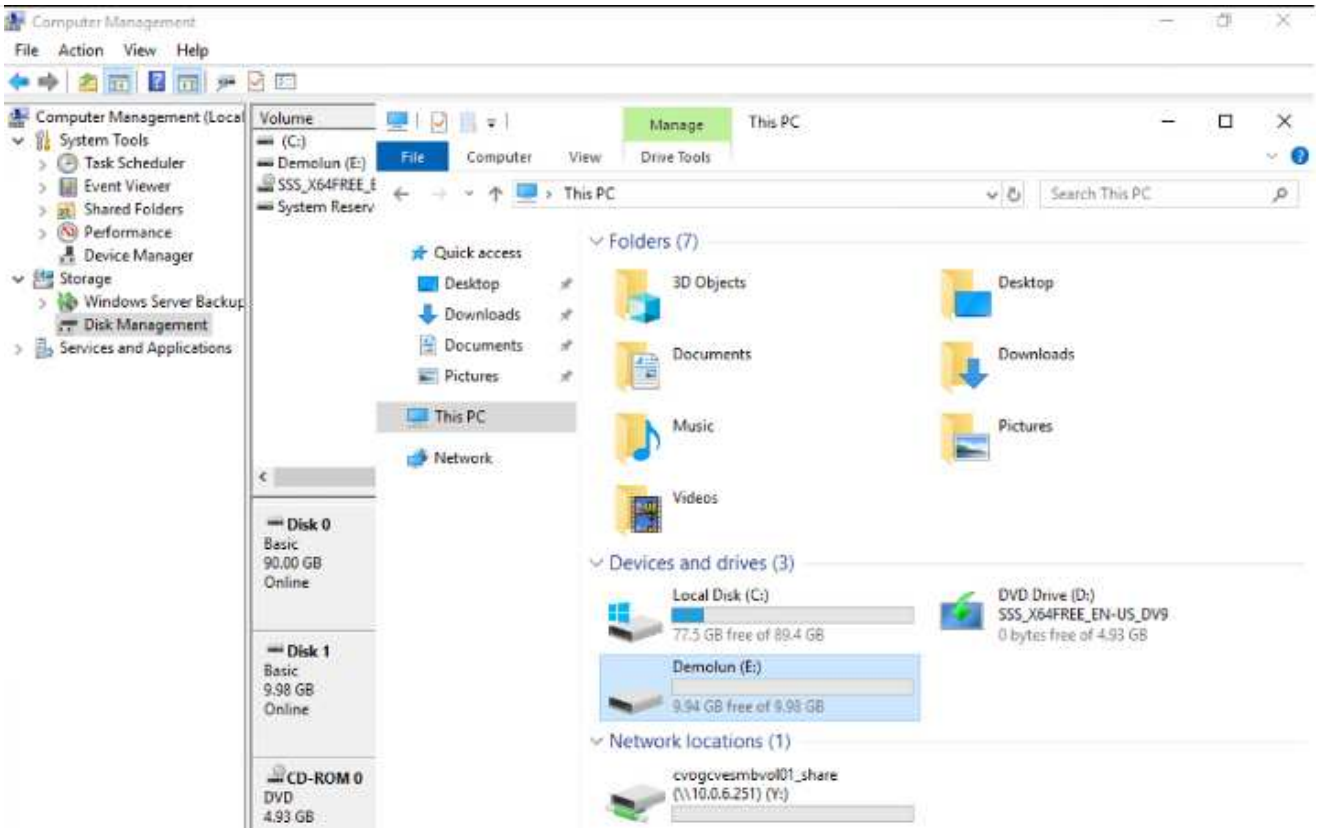
Las LUN de una máquina virtual de almacenamiento (SVM) aparecen como discos en el host Windows. El host no detecta automáticamente los nuevos discos que se añaden. Active una detección repetida manual para detectar los discos realizando los pasos siguientes:

a. Abra la utilidad 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 > discos de reexploración.



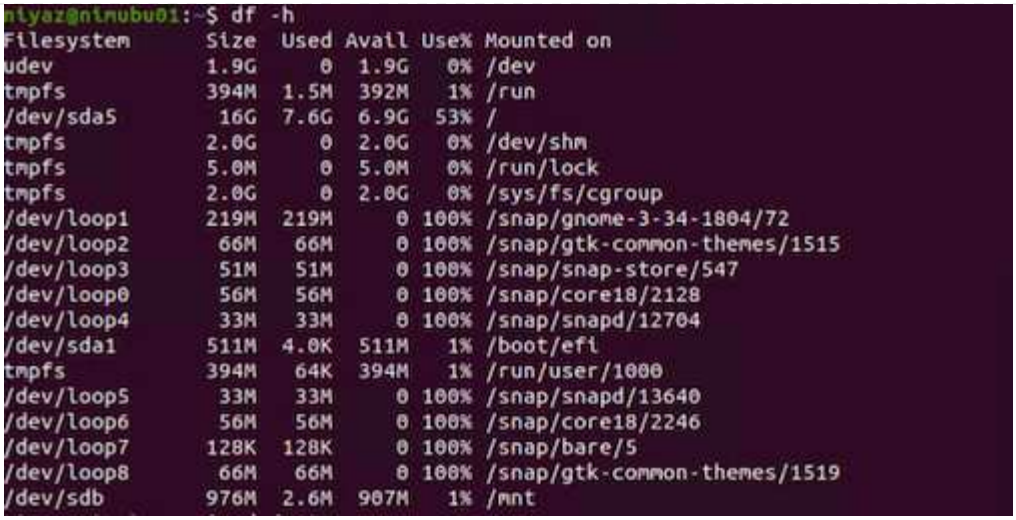
Cuando el host Windows accede por primera vez a una nueva LUN, no tiene sistema de archivos o partición. Inicialice la LUN y, de manera opcional, formatee la LUN con un sistema de archivos realizando los pasos siguientes:

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



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

```
niyaz@nimubu01:~$ 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
```

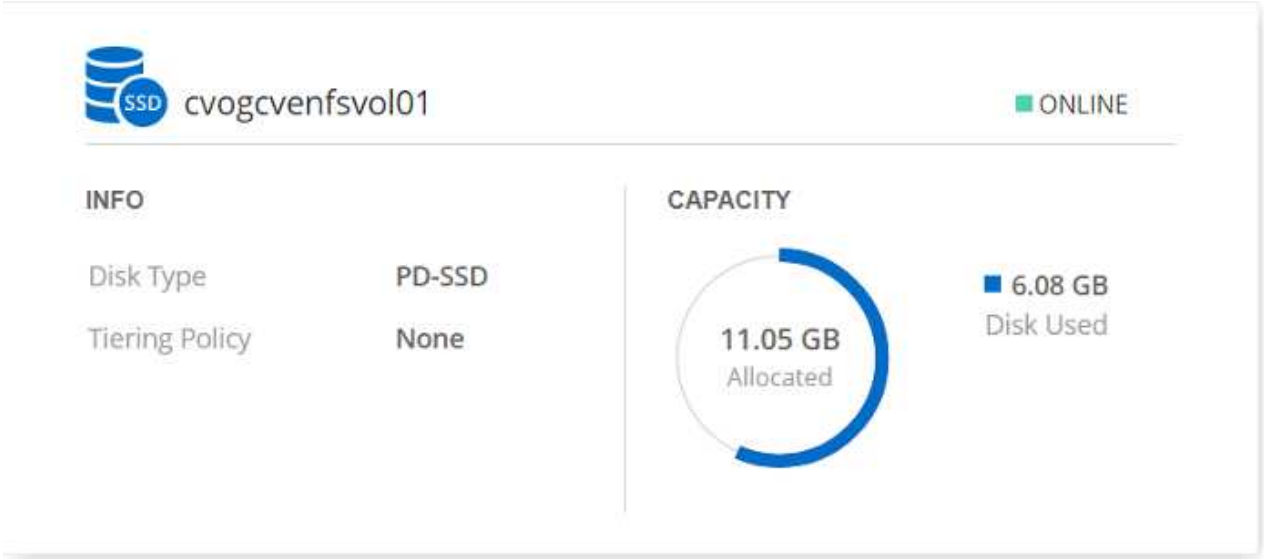

niyaz@ninubu01:~$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 1.9G 0 1.9G 0% /dev
tmpfs 394M 1.5M 392M 1% /run
/dev/sda5 16G 7.6G 6.9G 53% /
tmpfs 2.0G 0 2.0G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/loop1 219M 219M 0 100% /snap/gnome-3-34-1804/72
/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 el volumen NFS de Cloud Volumes ONTAP en el cliente Linux

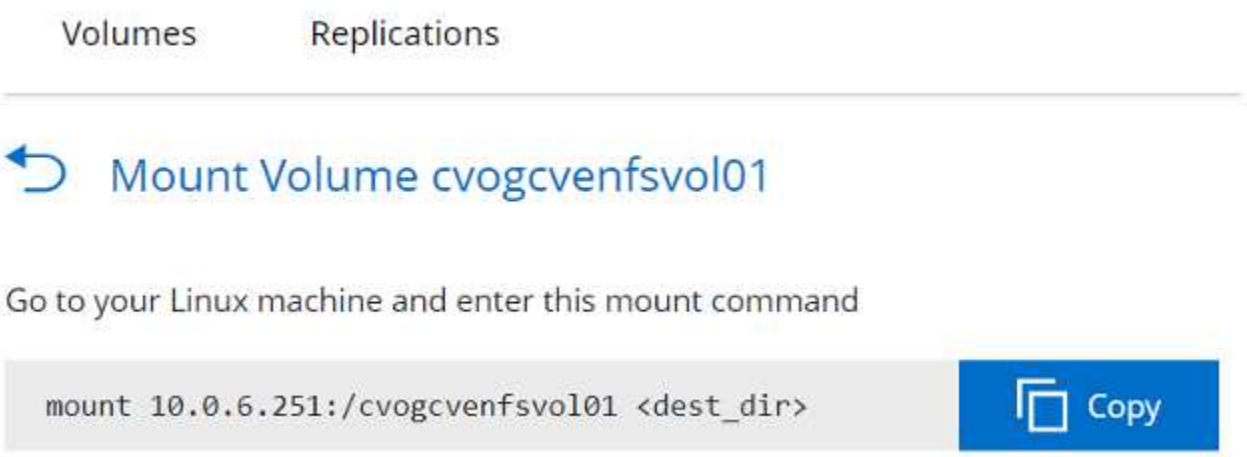
Para montar el sistema de archivos Cloud Volumes ONTAP (DIY) desde máquinas virtuales en Google Cloud VMware Engine, siga los siguientes pasos:

Aprovisione el volumen siguiendo los pasos que se indican a continuación

1. En la pestaña Volumes, haga clic en Create New Volume.
2. En la página Create New Volume, seleccione un tipo de volumen:



3. En la ficha volúmenes, coloque el cursor del ratón sobre el volumen, seleccione el icono de menú (º) y, a continuación, haga clic en Mount Command.



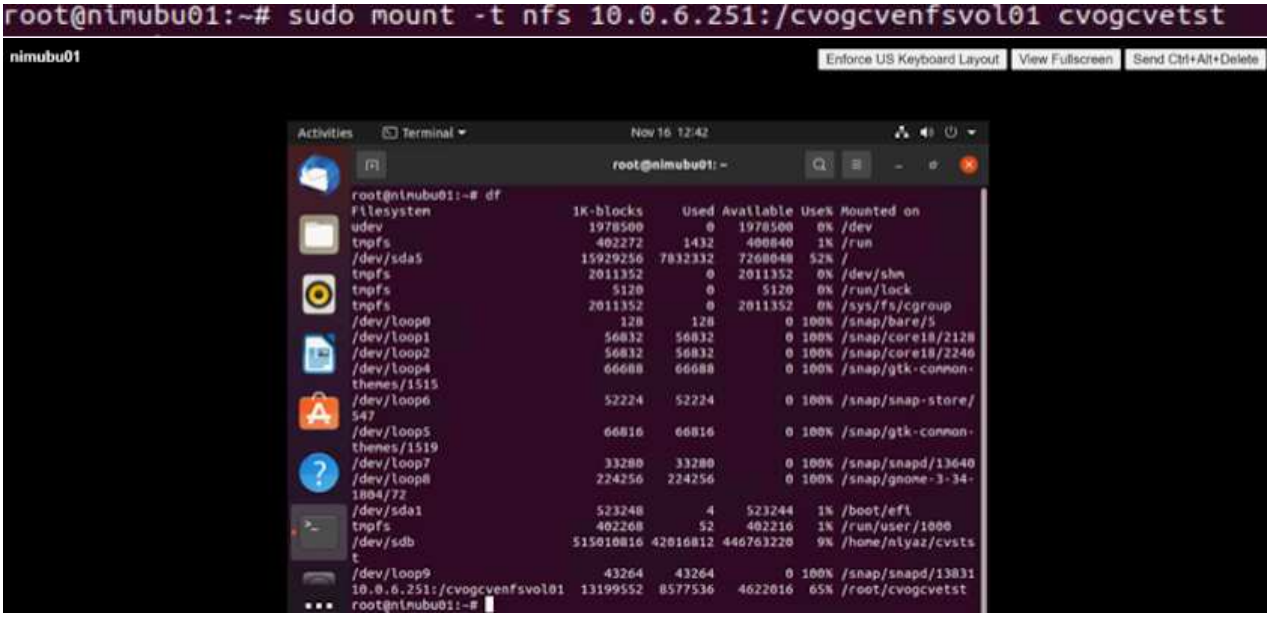
4. Haga clic en Copiar.
5. Conéctese a la instancia de Linux designada.
6. Abra un terminal en la instancia mediante el shell seguro (SSH) e inicie sesión con las credenciales adecuadas.
7. Cree un directorio para el punto de montaje del volumen con el comando siguiente.

```
$ sudo mkdir /cvogcvetst
```

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

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

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



Cloud Volumes Service (CVS)

Cloud Volumes Services (CVS) es una cartera completa de servicios de datos que ofrece soluciones avanzadas de cloud. Cloud Volumes Services admite varios protocolos de acceso a archivos para los principales proveedores de cloud (compatibilidad con NFS y SMB).

Otras ventajas y funciones incluyen: Protección de datos y restauración con Snapshot; funciones especiales para replicar, sincronizar y migrar destinos de datos en las instalaciones o en el cloud; y alto rendimiento constante en el nivel de un sistema de almacenamiento flash dedicado.

Cloud Volumes Service (CVS) como almacenamiento conectado como invitado

Configuración de Cloud Volumes Service con el motor de VMware

Los recursos compartidos de Cloud Volumes Service se pueden montar a partir de máquinas virtuales que se crean en el entorno de motor de VMware. Los volúmenes también pueden montarse en el cliente Linux y asignarse en el cliente Windows, ya que Cloud Volumes Service admite los protocolos SMB y NFS. Los volúmenes de Cloud Volumes Service se pueden configurar en pasos sencillos.

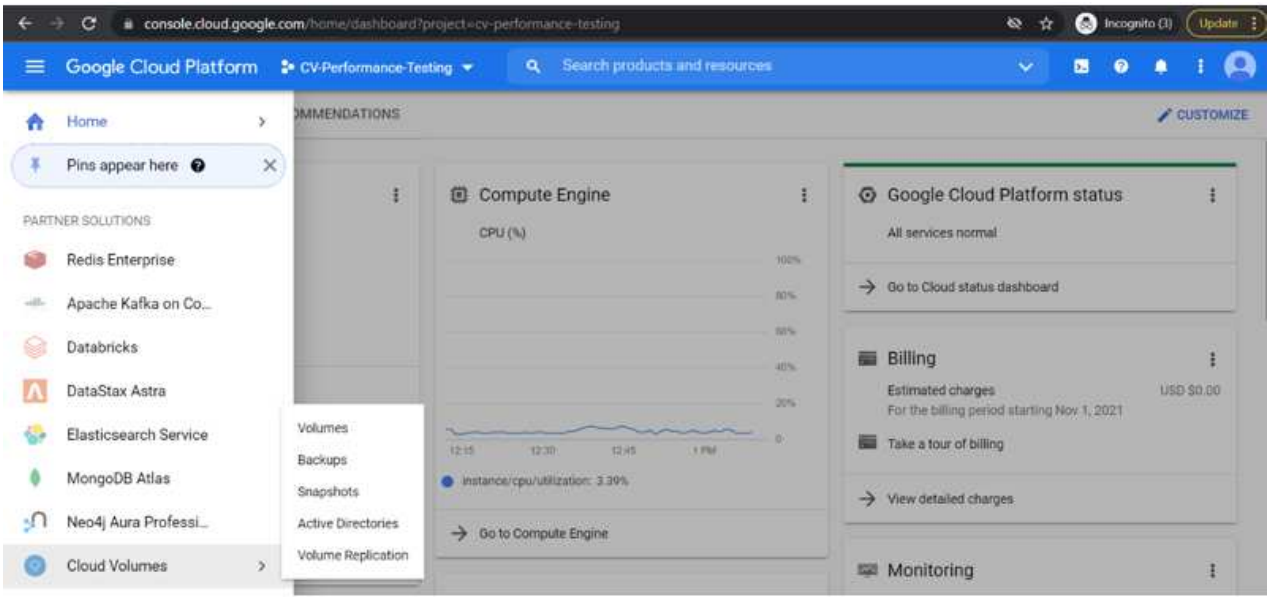
Cloud Volume Service y el cloud privado Google Cloud VMware Engine deben encontrarse en la misma región.

Para comprar, habilitar y configurar Cloud Volumes Service de NetApp para Google Cloud desde Google Cloud Marketplace, siga este detallado "guía".

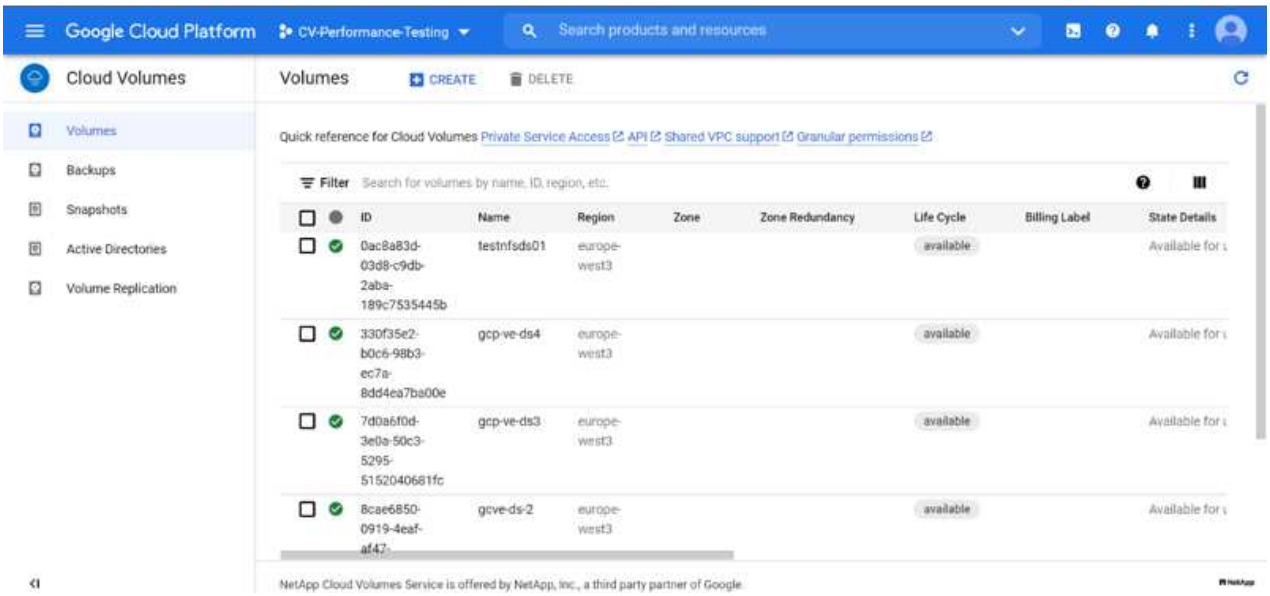
Cree un volumen CVS NFS en el cloud privado de GCVE

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

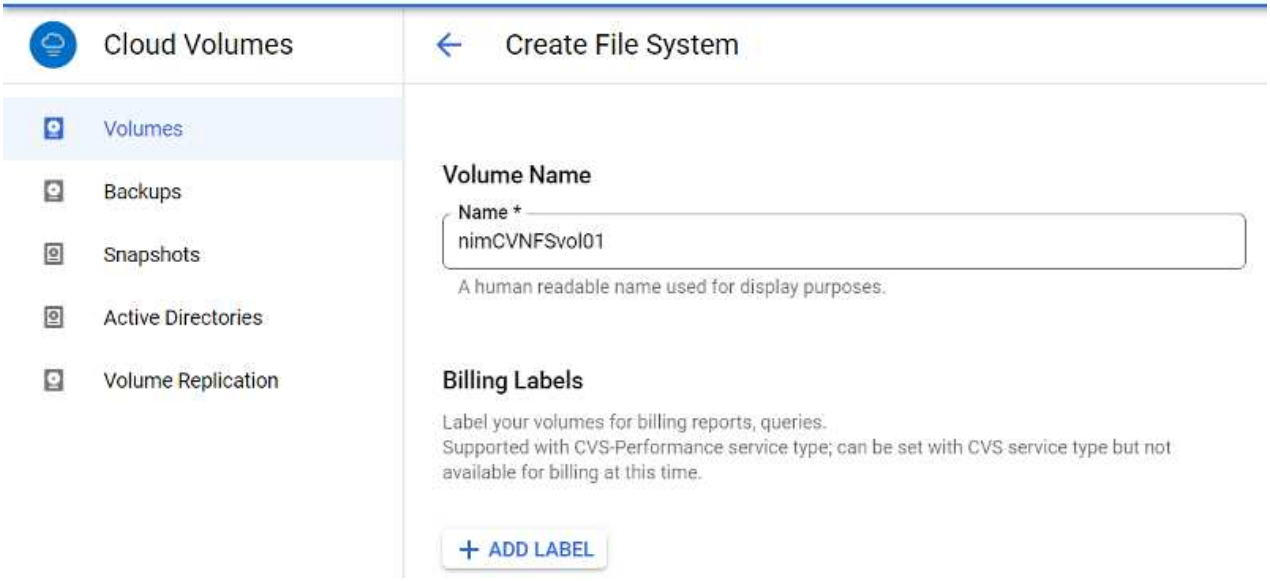
1. Acceda a Cloud Volumes desde Soluciones de partners dentro de la consola cloud de Google.



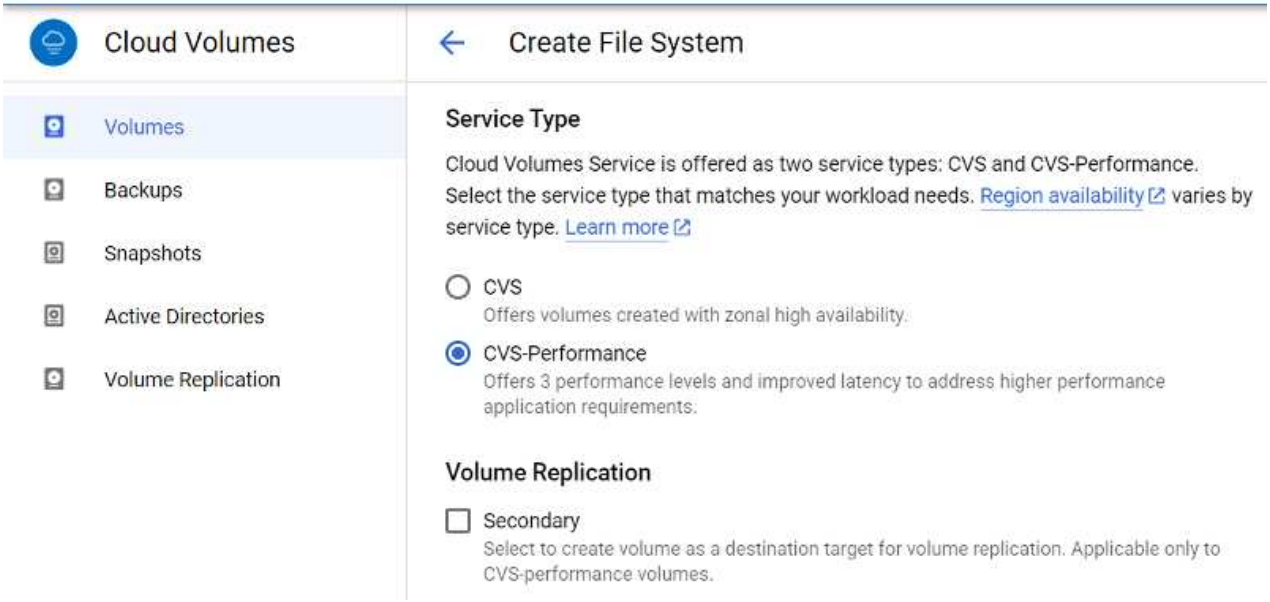
2. En la consola Cloud Volumes, vaya a la página Volumes y haga clic en Create.



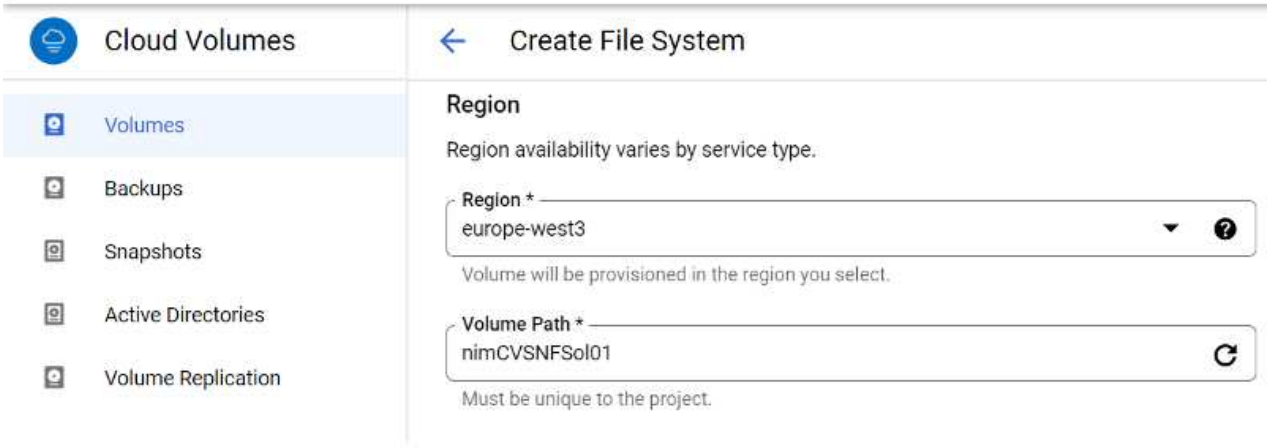
3. En la página Create File System, especifique el nombre del volumen y las etiquetas de facturación según sea necesario para los mecanismos de pago por uso.



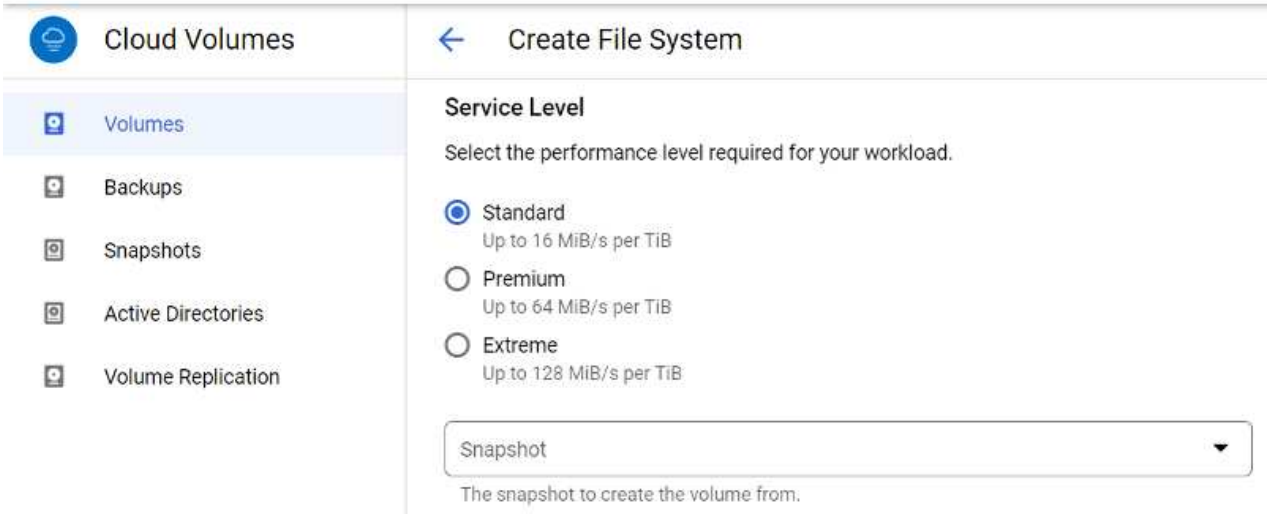
4. Seleccione el servicio adecuado. Para GCVE, seleccione CVS-Performance y el nivel de servicio deseado para la mejora de la latencia y el rendimiento superior en función de los requisitos de la carga de trabajo de la aplicación.



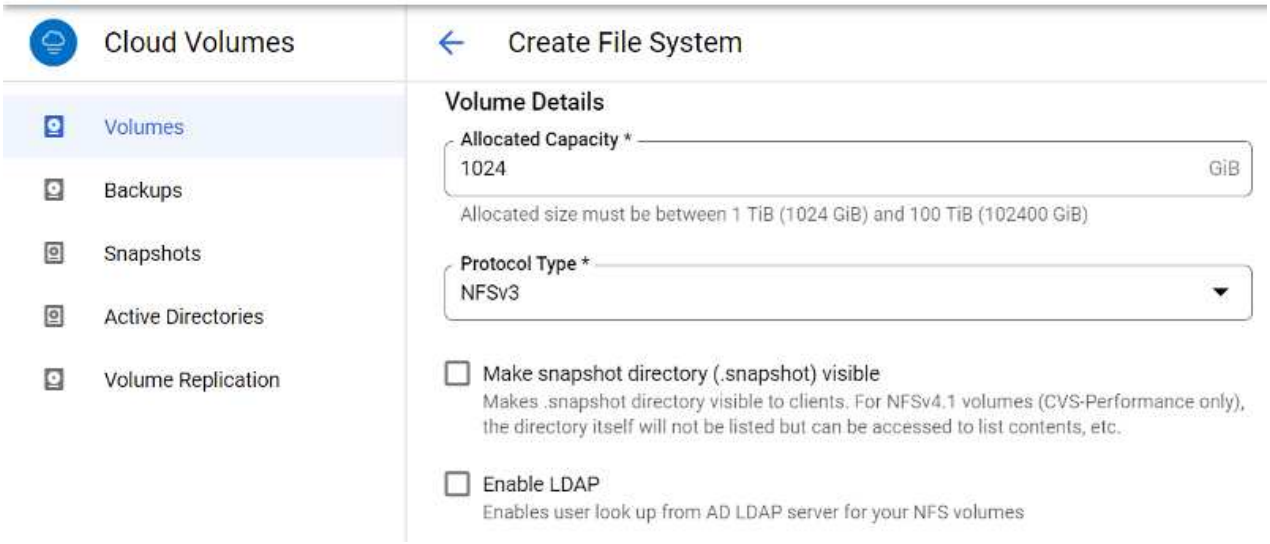
5. Especifique la región de Google Cloud para el volumen y la ruta del volumen (la ruta del volumen debe ser única en todos los volúmenes de cloud del proyecto)



6. Seleccione el nivel de rendimiento del volumen.

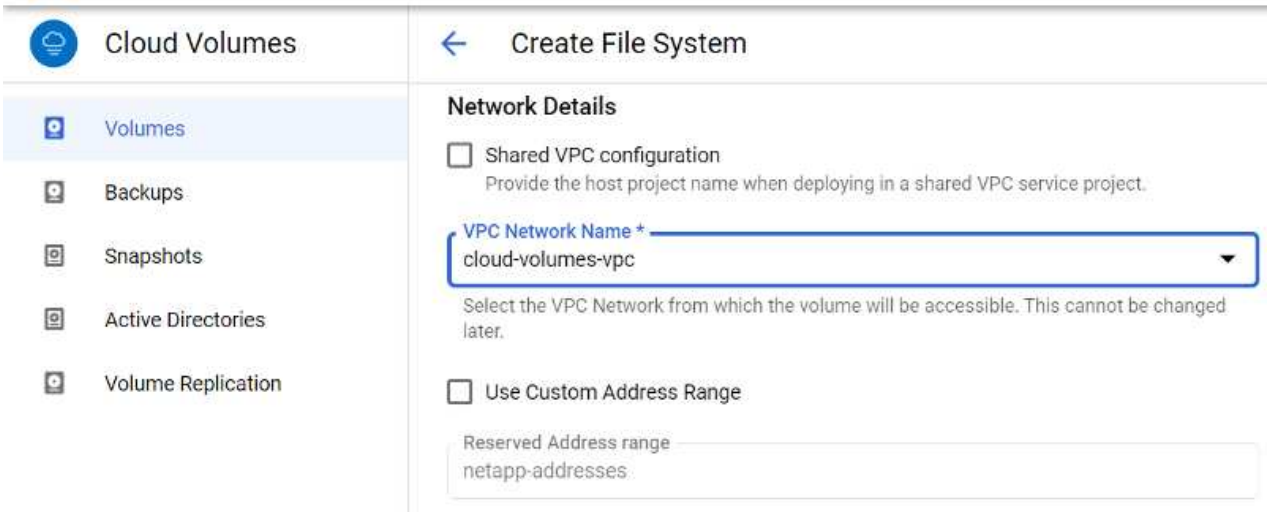


7. Especifique el tamaño del volumen y el tipo de protocolo. En esta prueba, se utiliza NFSv3.



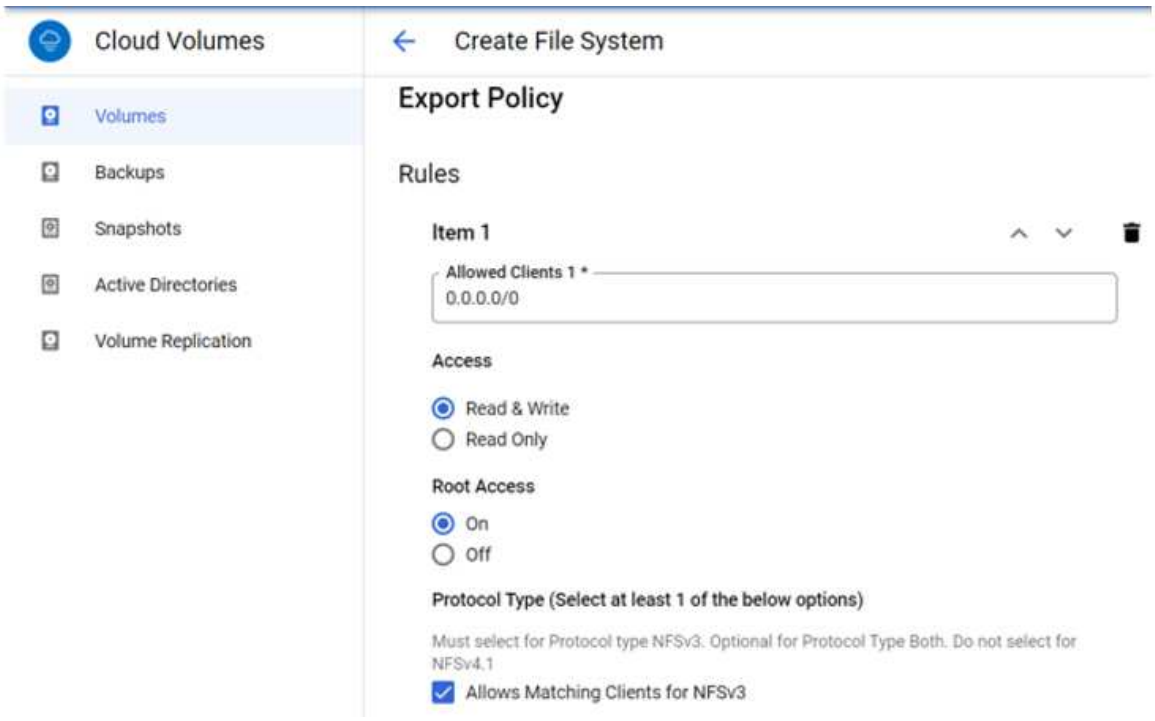
8. En este paso, seleccione la red VPC desde la que se podrá acceder al volumen. Compruebe que la agrupación de VPC esté en su lugar.

SUGERENCIA: Si VPC peering no se ha hecho, aparecerá un botón emergente que le guiará a través de los comandos peering. Abra una sesión de Cloud Shell y ejecute los comandos adecuados para conectar el VPC con el productor de Cloud Volumes Service. Si decide previamente preparar la agrupación en VPC, consulte estas instrucciones.



9. Gestione las reglas de política de exportación agregando las reglas adecuadas y seleccione la casilla de verificación para la versión 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.

Montar exportaciones de NFS a máquinas virtuales que se ejecutan en el motor de VMware

Antes de preparar el montaje del volumen NFS, asegúrese de que el estado de la conexión entre iguales de la conexión privada aparezca como activo. Una vez el estado es activo, utilice el comando Mount.

Para montar un volumen NFS, haga lo siguiente:

1. En Cloud Console, vaya a Cloud Volumes > Volumes.
2. Vaya a la página Volumes
3. Haga clic en el volumen NFS para el que desea montar las exportaciones NFS.
4. Desplácese a la derecha, en Mostrar más, haga clic en Mount Instructions.

Para realizar el proceso de montaje desde el SO invitado del equipo virtual de VMware, siga estos pasos:

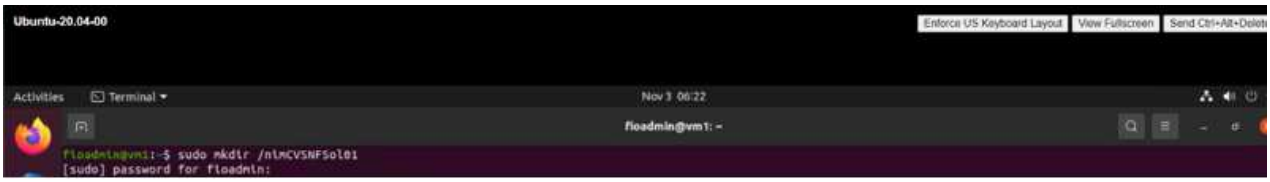
1. Use SSH Client y SSH en la máquina virtual.
2. Instale el cliente nfs en la instancia.
   a. En la instancia de Red Hat Enterprise Linux o SuSE Linux:

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

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

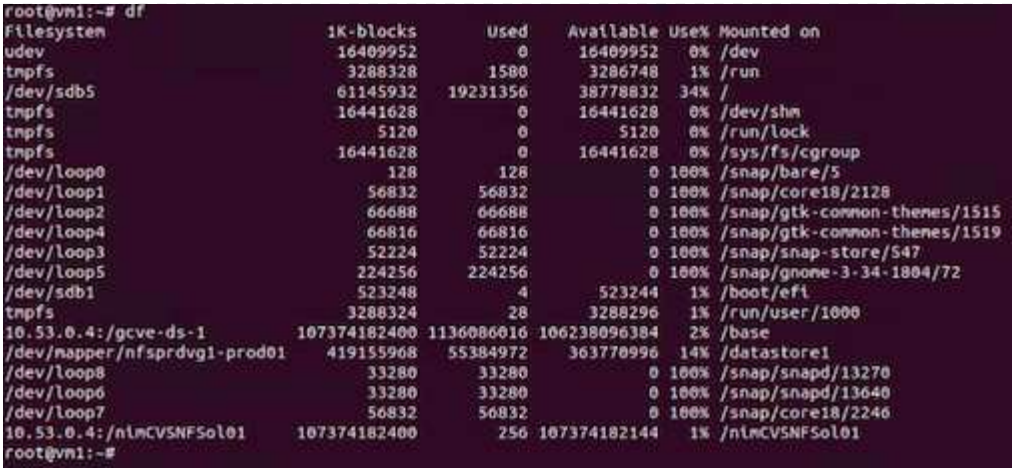
3. Cree un nuevo directorio en la instancia, como "/nimCVSNFSol01":

```
sudo mkdir /nimCVSNFSol01
```



4. Monte el volumen con el comando correspondiente. A continuación se muestra el comando de ejemplo del laboratorio:

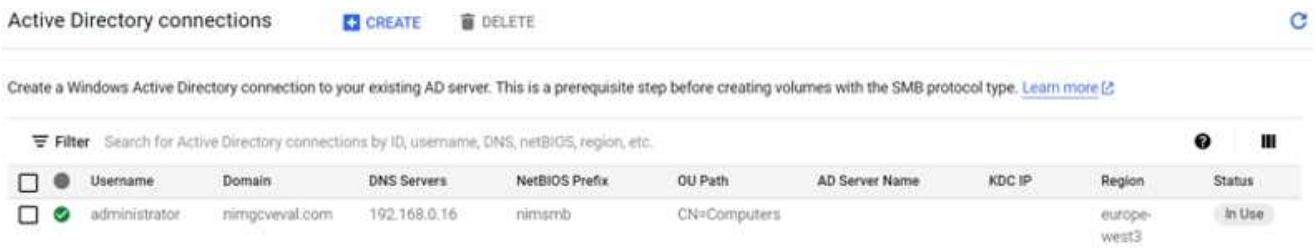
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     38778832  34% /
tmpfs                           16441628           0     16441628   0% /dev/shm
tmpfs                               5120           0         5120   0% /run/lock
tmpfs                           16441628           0     16441628   0% /sys/fs/cgroup
/dev/loop0                            128         128            0 100% /snap/bare/5
/dev/loop1                          56832       56832            0 100% /snap/core18/2128
/dev/loop2                          66688       66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                          66816       66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                          52224       52224            0 100% /snap/snap-store/547
/dev/loop5                         224256      224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                          523248           4       523244   1% /boot/efi
tmpfs                             3288324          28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1          107374182400  1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01     419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nlmCVSNFSol01      107374182400         256 107374182144   1% /nlmCVSNFSol01
root@vm1:~#
```

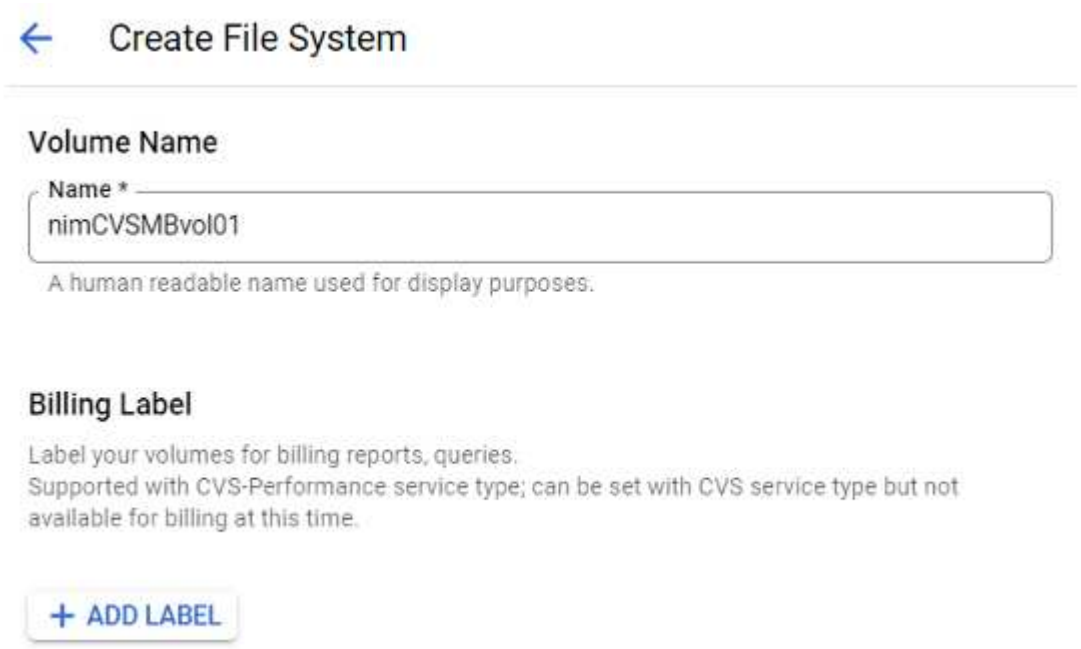
Crear y montar SMB comparte con máquinas virtuales que se ejecutan en VMware Engine

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

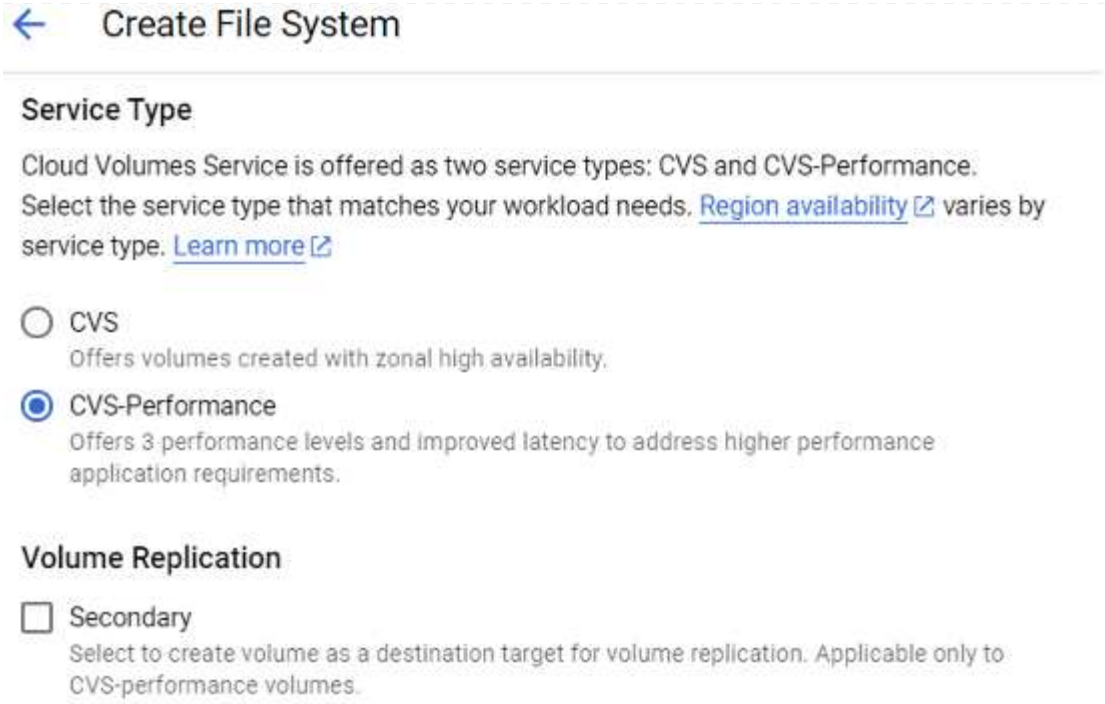


Una vez que la conexión AD esté en su lugar, cree el volumen con el nivel de servicio deseado. Los pasos son similares a crear un volumen NFS, excepto seleccionar el protocolo adecuado.

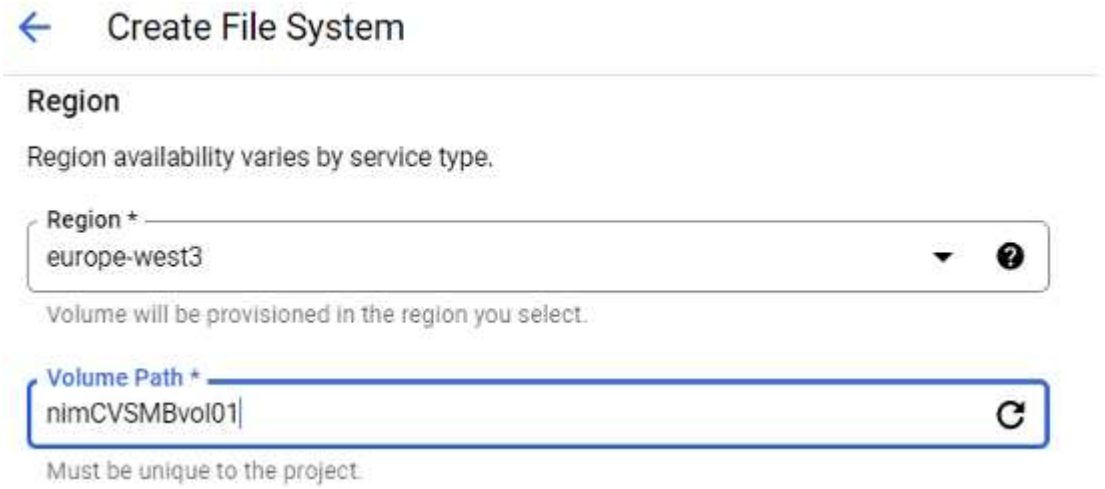
1. En la consola Cloud Volumes, vaya a la página Volumes y haga clic en Create.
2. En la página Create File System, especifique el nombre del volumen y las etiquetas de facturación según sea necesario para los mecanismos de pago por uso.



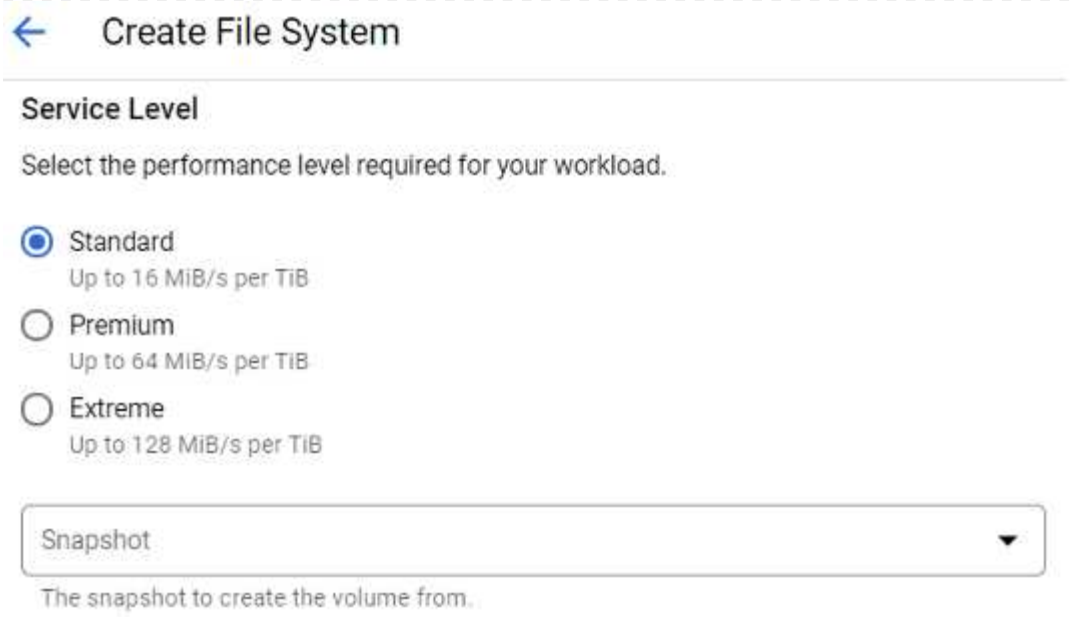
3. Seleccione el servicio adecuado. Para GCVE, seleccione CVS-Performance y el nivel de servicio deseado para la mejora de la latencia y el rendimiento superior en función de los requisitos de la carga de trabajo.



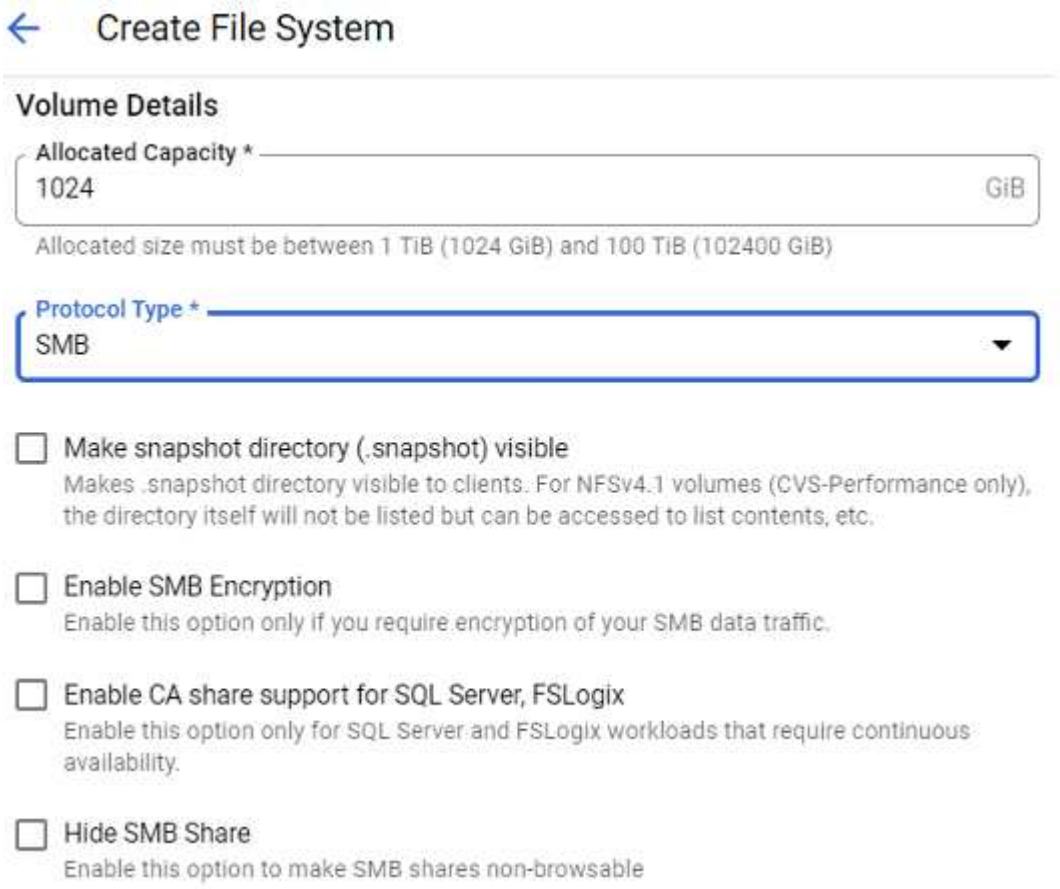
4. Especifique la región de Google Cloud para el volumen y la ruta del volumen (la ruta del volumen debe ser única en todos los volúmenes de cloud del proyecto)



5. Seleccione el nivel de rendimiento del volumen.



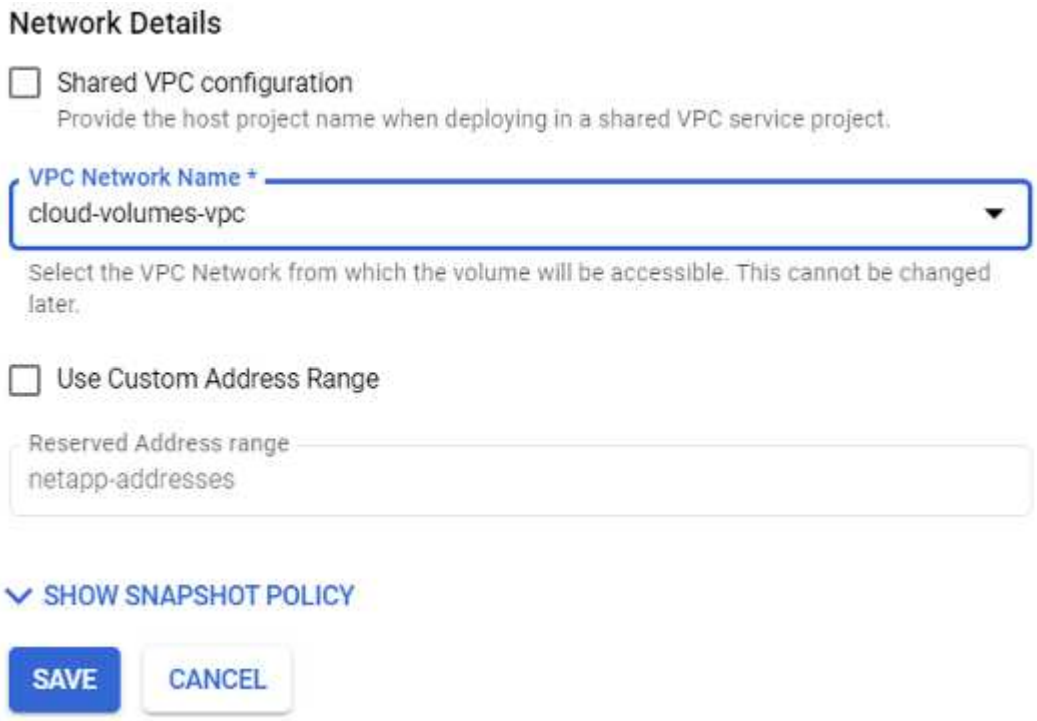
6. Especifique el tamaño del volumen y el tipo de protocolo. En esta prueba, se utiliza SMB.



7. En este paso, seleccione la red VPC desde la que se podrá acceder al volumen. Compruebe que la agrupación de VPC esté en su lugar.

   SUGERENCIA: Si VPC peering no se ha hecho, aparecerá un botón emergente que le guiará a través de los comandos peering. Abra una sesión de Cloud Shell y ejecute los comandos adecuados para conectar el VPC con el productor de Cloud Volumes Service. Si decide previamente preparar la

agrupación VPC, consulte las mismas "instrucciones".



8. Haga clic en Guardar para crear el volumen.

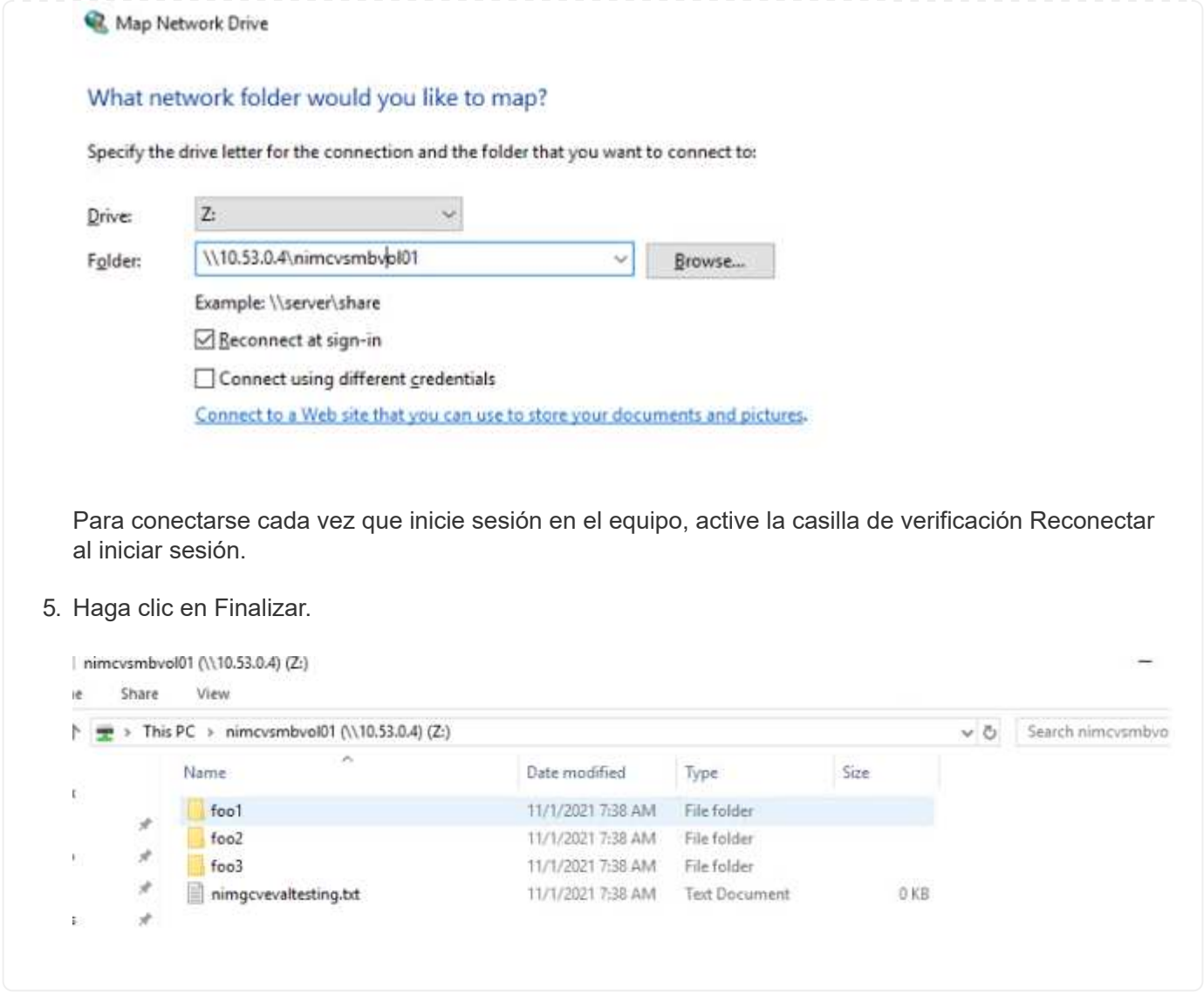
Para montar el volumen SMB, haga lo siguiente:

1. En Cloud Console, vaya a Cloud Volumes > Volumes.
2. Vaya a la página Volumes
3. Haga clic en el volumen de SMB para el que desea asignar un recurso compartido de SMB.
4. Desplácese a la derecha, en Mostrar más, haga clic en Mount Instructions.

Para realizar el proceso de montaje desde el SO invitado Windows del equipo virtual VMware, siga los pasos que se indican a continuación:

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

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



Para conectarse cada vez que inicie sesión en el equipo, active la casilla de verificación Reconectar al iniciar sesión.

5. Haga clic en Finalizar.

Disponibilidad de región para almacenes de datos NFS suplementarios en AWS, Azure y GCP

Obtenga más información sobre la compatibilidad de región global para almacenes de datos NFS complementarios en AWS, Azure y Google Cloud Platform (GCP).

Disponibilidad de regiones de AWS

Amazon define la disponibilidad de almacenes de datos NFS complementarios en AWS/VMC. Primero, debe determinar si tanto VMC como FSxN están disponibles en una región específica. A continuación, debe determinar si el almacén de datos NFS complementario FSxN es compatible en esa región.

- Compruebe la disponibilidad del VMC "aquí".
- La guía de precios de Amazon ofrece información sobre dónde está disponible FSxN (FSX ONTAP). Usted puede encontrar esa información "aquí".
- La disponibilidad del almacén de datos NFS complementario FSxN para VMC estará disponible próximamente.

Aunque aún se dispone de información, el siguiente gráfico identifica el soporte actual de VMC, FSxN y FSxN como almacén de datos NFS complementario.

América

Región de AWS	Disponibilidad VMC	Disponibilidad de ONTAP FSX	Disponibilidad del almacén de datos NFS
Este DE EE. UU. (Virginia del Norte)	Sí	Sí	Sí
Este DE EE. UU. (Ohio)	Sí	Sí	Sí
Oeste DE EE. UU. (Norte de California)	Sí	No	No
Oeste DE EE. UU. (Oregón)	Sí	Sí	Sí
GovCloud (oeste de EE. UU.)	Sí	Sí	Sí
Canadá (Central)	Sí	Sí	Sí
Sudamérica (São Paulo)	Sí	Sí	Sí

Última actualización el: 2 de junio de 2022.

EMEA

Región de AWS	Disponibilidad VMC	Disponibilidad de ONTAP FSX	Disponibilidad del almacén de datos NFS
Europa (Irlanda)	Sí	Sí	Sí
Europa (Londres)	Sí	Sí	Sí
Europa (Frankfurt)	Sí	Sí	Sí
Europa (París)	Sí	Sí	Sí
Europa (Milán)	Sí	Sí	Sí
Europa (Estocolmo)	Sí	Sí	Sí

Última actualización el: 2 de junio de 2022.

Asia-Pacífico

Región de AWS	Disponibilidad VMC	Disponibilidad de ONTAP FSX	Disponibilidad del almacén de datos NFS
APAC (Sidney)	Sí	Sí	Sí
APAC (Tokio)	Sí	Sí	Sí
APAC (Osaka)	Sí	No	No
APAC (Singapur)	Sí	Sí	Sí
APAC (Seúl)	Sí	Sí	Sí
APAC (Bombay)	Sí	Sí	Sí
APAC (Yakarta)	No	No	No

APAC (Hong Kong)	Sí	Sí	Sí

Última actualización el: 28 de septiembre de 2022.

Disponibilidad de regiones de Azure

La disponibilidad de almacenes de datos NFS complementarios en Azure/AVS es definida por Microsoft. En primer lugar, es necesario determinar si tanto el AVS como el ANF están disponibles en una región específica. A continuación, debe determinar si el almacén de datos NFS suplementario ANF es compatible con esa región.

- Compruebe la disponibilidad de AVS y ANF "aquí".
- Compruebe la disponibilidad del almacén de datos NFS complementario ANF "aquí".

Disponibilidad de región de GCP

La disponibilidad de la región de GCP se publicará cuando GCP entre en una disponibilidad pública.

Resumen y conclusión: Por qué elegir el multicloud híbrido de NetApp con VMware

NetApp Cloud Volumes junto con las soluciones de VMware para los principales proveedores a hiperescala ofrecen un gran potencial para las organizaciones que desean aprovechar el cloud híbrido. El resto de esta sección proporciona los casos de uso que muestran la integración de NetApp Cloud Volumes para ofrecer auténticas funcionalidades de multicloud híbrido.

Caso de uso n.o 1: Optimización del almacenamiento

Cuando se realiza un ejercicio de configuración con salida RVtools, siempre es evidente que la escala de la potencia (vCPU/vmem) es paralela al almacenamiento. Muchas veces, las organizaciones se encuentran en una situación en la que el espacio de almacenamiento requiere el tamaño del clúster mucho más allá de lo que se necesita para la potencia.

Al integrar Cloud Volumes de NetApp, las organizaciones pueden desarrollar una solución cloud basada en vSphere con un método de migración simple, sin necesidad de volver a plataformas, sin cambios de IP ni cambios de arquitectura. Asimismo, esta optimización le permite escalar el espacio de almacenamiento a la vez que mantiene el número de hosts al menor tiempo necesario en vSphere, pero sin cambios en la jerarquía de almacenamiento, la seguridad ni los archivos que se han puesto a disposición. Esto permite optimizar la puesta en marcha y reducir el TCO general entre un 35 y un 45 %. Esta integración también le permite ampliar el almacenamiento del almacenamiento de datos templados al rendimiento de producción en segundos.

Caso de uso n.o 2: Migración al cloud

Las organizaciones sufren la presión de migrar aplicaciones desde los centros de datos en las instalaciones al cloud público por varios motivos: Un vencimiento del arrendamiento inminente; una directiva financiera para pasar de gastos de capital a gastos operativos (gastos operativos) o, simplemente, una obligación descendente para trasladarlo todo al cloud.

Cuando la velocidad es crucial, solo es posible utilizar un método de migración optimizado, ya que volver a crear plataformas y refactorizar aplicaciones para adaptarse a la plataforma IaaS en particular del cloud es lenta y cara y, a menudo, lleva meses. Al combinar Cloud Volumes de NetApp con la replicación de SnapMirror con gestión eficiente del ancho de banda para el almacenamiento conectado al «guest» (incluidos

RDM en combinación con las copias Snapshot coherentes con las aplicaciones y HCX, la migración específica del cloud (como Azure Migrate) o productos de terceros para replicar máquinas virtuales), esta transición es incluso más fácil que depender de mecanismos de filtros de I/o que requieren tiempo.

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

Cuando un centro de datos alcanza límites de capacidad debido a los picos de demanda estacionales o simplemente a un crecimiento orgánico constante, cambiar a VMware alojado en cloud junto con Cloud Volumes de NetApp es una solución sencilla. El aprovechamiento de Cloud Volumes de NetApp permite la creación, replicación y expansión del almacenamiento de forma muy sencilla, al proporcionar alta disponibilidad en las zonas de disponibilidad y funcionalidades de escalado dinámico. El aprovechamiento de Cloud Volumes de NetApp ayuda a minimizar la capacidad de clústeres de hosts, ya que permite superar la necesidad de ampliar clústeres.

Caso de uso n.o 4: Recuperación ante desastres en el cloud

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

Mediante el uso de Cloud Volumes de NetApp para almacenamiento conectado al invitado con la replicación de SnapCenter y SnapMirror desde las instalaciones junto con soluciones de virtualización de cloud público, es posible diseñar un mejor método para la recuperación ante desastres que permita la recuperación de réplicas de equipos virtuales en una infraestructura VMware SDDC totalmente coherente junto con herramientas de recuperación específicas para cloud (Por ejemplo, Azure Site Recovery) o herramientas de terceros equivalentes, como Veeam. Este enfoque también le permite realizar simulacros de recuperación ante desastres y recuperar rápidamente desde el ransomware. Esto también permite escalar a producción completa para pruebas o durante un desastre añadiendo hosts bajo demanda.

Caso de uso n.o 5: Modernización de aplicaciones

Una vez que las aplicaciones se encuentran en el cloud público, las organizaciones querrán aprovechar los cientos de potentes servicios de cloud para modernizarlas y ampliarlas. Con el uso de Cloud Volumes de NetApp, la modernización es un proceso sencillo, ya que los datos de aplicaciones no están bloqueados en VSAN y permite la movilidad de datos en una amplia variedad de casos de uso, incluido Kubernetes.

Conclusión

Tanto si su objetivo es llegar a un cloud híbrido como en un cloud all-cloud, NetApp Cloud Volumes ofrece opciones excelentes para poner en marcha y gestionar las cargas de trabajo de las aplicaciones, junto con los servicios de archivos y protocolos de bloques, a la vez que reduce el TCO, pues permite que los requisitos de datos se cumplan sin problemas en la capa de la aplicación.

Sea cual sea el caso de uso, elija su cloud preferido/proveedor a hiperescala junto con Cloud Volumes de NetApp para la realización rápida de las ventajas del cloud, una infraestructura consistente y operaciones en las instalaciones y en varios clouds, la portabilidad bidireccional de las cargas de trabajo, y la capacidad y el rendimiento de nivel empresarial.

Es el mismo proceso y procedimientos que ya conocen y que se utilizan para conectar el almacenamiento. Recuerde que solo la posición de los datos ha cambiado con nuevos nombres; las herramientas y los procesos siguen siendo los mismos y Cloud Volumes de NetApp ayuda a optimizar la puesta en marcha general.

Casos de uso de cloud híbrido de VMware

Casos de uso del multicloud híbrido de NetApp con VMware

Una descripción de los casos de uso que son importantes para la organización TECNOLÓGICA al planificar una puesta en marcha de cloud híbrido o cloud-first.

Casos de uso populares

Sus casos de uso son:

- Recuperación tras desastres,
- Alojar cargas de trabajo durante el mantenimiento del centro de datos; * explosión rápida en la que se necesitan recursos adicionales más allá de lo aprovisionado en el centro de datos local,
- Ampliación de sitios de VMware,
- Migración rápida al cloud,
- Desarrollo/pruebas, y.
- Modernización de aplicaciones aprovechando tecnologías complementarias de cloud.

A lo largo de esta documentación, las referencias de cargas de trabajo del cloud se detaltarán por medio de casos de uso de VMware. Estos casos de uso son:

- Protect (incluye recuperación ante desastres y backup/restauración)
- Migración
- Extender

En el camino hacia la TECNOLOGÍA

La mayoría de las organizaciones se encuentran en un camino hacia la transformación y la modernización. Como parte de este proceso, las empresas intentan aprovechar sus inversiones existentes en VMware al mismo tiempo que aprovechan las ventajas de la nube y exploran las formas de hacer el proceso de migración de la forma más fluida posible. Este enfoque facilita enormemente sus esfuerzos de modernización, ya que los datos ya están en el cloud.

La respuesta más sencilla a este escenario son las ofertas de VMware en cada proveedor a hiperescala. Al igual que Cloud Volumes de NetApp®, VMware proporciona una forma de mover o ampliar los entornos VMware locales a cualquier cloud, lo que le permite conservar activos, habilidades y herramientas existentes en las instalaciones al tiempo que ejecuta cargas de trabajo de forma nativa en el cloud. De este modo se reduce el riesgo, ya que no se producirán interrupciones del servicio ni se necesitarán cambios en la IP, y el equipo DE TECNOLOGÍA podrá utilizar las habilidades y herramientas existentes de la manera en que lo hacen en las instalaciones. Esto puede llevar a migraciones de cloud aceleradas y a una transición mucho más fluida a una arquitectura multicloud híbrida.

Descripción de la importancia de las opciones de almacenamiento de NFS suplementario

Mientras que VMware en cualquier cloud ofrece funcionalidades híbridas únicas a todos los clientes, las opciones de almacenamiento NFS suplementario limitadas han restringido su utilidad para las organizaciones con cargas de trabajo que requieren un gran nivel de almacenamiento. Debido a que el almacenamiento está directamente ligado a los hosts, la única forma de escalar el almacenamiento es añadir más hosts, lo cual puede aumentar los costes entre un 35 y un 40 % o más para cargas de trabajo con un uso intensivo del almacenamiento. Estas cargas de trabajo solo necesitan almacenamiento adicional, no una potencia adicional.

Pero eso significa pagar por los anfitriones adicionales.

Consideremos este caso:

Un cliente solo necesita cinco hosts para CPU y memoria, pero tiene muchas necesidades de almacenamiento y necesita 12 hosts para satisfacer sus requisitos de almacenamiento. Este requisito acaba realmente a la altura del escalado financiero al tener que comprar la potencia adicional cuando solo necesitan aumentar el almacenamiento.

Cuando planifica la adopción y las migraciones de la nube, siempre es importante evaluar el mejor enfoque y tomar el camino más sencillo que reduzca las inversiones totales. El método más habitual y sencillo para la migración de cualquier aplicación es el realojamiento (también conocido como lift and shift), en el que no hay ningún equipo virtual (VM) ni conversión de datos. Al utilizar Cloud Volumes de NetApp con el centro de datos definido por software (SDDC) de VMware, al tiempo que complementa VSAN, proporciona una opción de elevación y cambio sencilla.

Soluciones de NetApp para Amazon VMware Managed Cloud (VMC)

Más información acerca de las soluciones que NetApp aporta a AWS.

VMware define las cargas de trabajo del cloud en una de estas tres categorías:

- Protección (incluida tanto recuperación ante desastres como backup/restauración)
- Migración
- Extender

Consulte las soluciones disponibles en las siguientes secciones.

Proteger

- "Recuperación ante desastres con VMC en AWS (invitado conectado)"
- "Veeam Backup Restaura en VMC con FSx para ONTAP"
- "Recuperación ante desastres (DRO) con FSX para ONTAP y VMC"
- "Usar la replicación de Veeam y FSx para ONTAP para la recuperación ante desastres en VMware Cloud on AWS"

Migración

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

Extender

¡PRÓXIMAMENTE!

Soluciones de NetApp para la solución Azure VMware (AVS)

Obtenga más información acerca de las soluciones que NetApp ofrece a Azure.

VMware define las cargas de trabajo del cloud en una de estas tres categorías:

- Protección (incluida tanto recuperación ante desastres como backup/restauración)
- Migración

- Extender

Consulte 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 de invitado)"
- "Recuperación ante desastres (DRO) con ANF y AVS"
- "Uso de la replicación de Veeam y el almacén de datos de Azure NetApp Files para recuperación ante desastres en la solución de Azure VMware"

Migración

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

Extender

¡PRÓXIMAMENTE!

Soluciones de NetApp para Google Cloud VMware Engine (GCVE)

Más información sobre las soluciones que NetApp ofrece a GCP.

VMware define las cargas de trabajo del cloud en una de estas tres categorías:

- Protección (incluida tanto recuperación ante desastres como backup/restauración)
- Migración
- Extender

Consulte las soluciones disponibles en las siguientes secciones.

Proteger

- "Recuperación ante desastres de aplicaciones con replicación de SnapCenter, Cloud Volumes ONTAP y Veeam"
- "Recuperación ante desastres coherente con las aplicaciones con NetApp SnapCenter y Veeam Replication en NetApp CVS en GCVE"

Migración

- "Migración de cargas de trabajo mediante VMware HCX al almacén de datos NFS de Cloud Volume Service de NetApp"
- "Replicación de máquina virtual mediante Veeam para un almacén de datos NFS del servicio de volúmenes de cloud de NetApp"

Extender

¡PRÓXIMAMENTE!

Funcionalidades de NetApp para VMC de AWS

Obtenga más información acerca de las funcionalidades que NetApp aporta al cloud VMware Cloud (VMC) de AWS: Desde NetApp como dispositivo de almacenamiento conectado como invitado o un almacén de datos NFS complementario a la migración de flujos de trabajo, extensión o repartición al cloud, backup/restauración y recuperación ante desastres.

Para ir a la sección del contenido deseado, seleccione una de las siguientes opciones:

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

Configuración de VMC en AWS

Al igual que en las instalaciones, la planificación de un entorno de virtualización basado en cloud es crucial para tener un entorno preparado para la producción con éxito a la hora de crear equipos virtuales y migración.

En esta sección se describe cómo configurar y gestionar VMware Cloud en AWS SDDC y utilizarlo en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

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

El proceso de configuración puede dividirse en los siguientes pasos:

- Poner en marcha y configurar VMware Cloud para AWS
- Conecte VMware Cloud a FSX ONTAP

Vea el detalles "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 almacenes de datos NFS conectados o como almacenes de datos NFS complementarios, en VMC de AWS.

Visite "Opciones de almacenamiento de NetApp admitidas" si quiere más información.

AWS admite almacenamiento de NetApp con las siguientes configuraciones:

- FSX ONTAP como almacenamiento conectado como invitado
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado
- FSX ONTAP como almacén de datos NFS complementario

Vea el detalles "Opciones de almacenamiento de conexión para invitado para VMC". Vea el detalles "Opciones suplementarias de almacén de datos de NFS para VMC".

Casos de uso de soluciones

Con las soluciones de cloud de NetApp y VMware, la puesta en marcha de muchos casos de uso es sencilla

en su AWS VMC. Los casos de uso se definen para cada una de las áreas cloud definidas por VMware:

- Protect (incluye recuperación ante desastres y backup/restauración)
- Extender
- Migración

"Consulte las soluciones de NetApp para AWS VMC"

Protección de cargas de trabajo en AWS / VMC

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

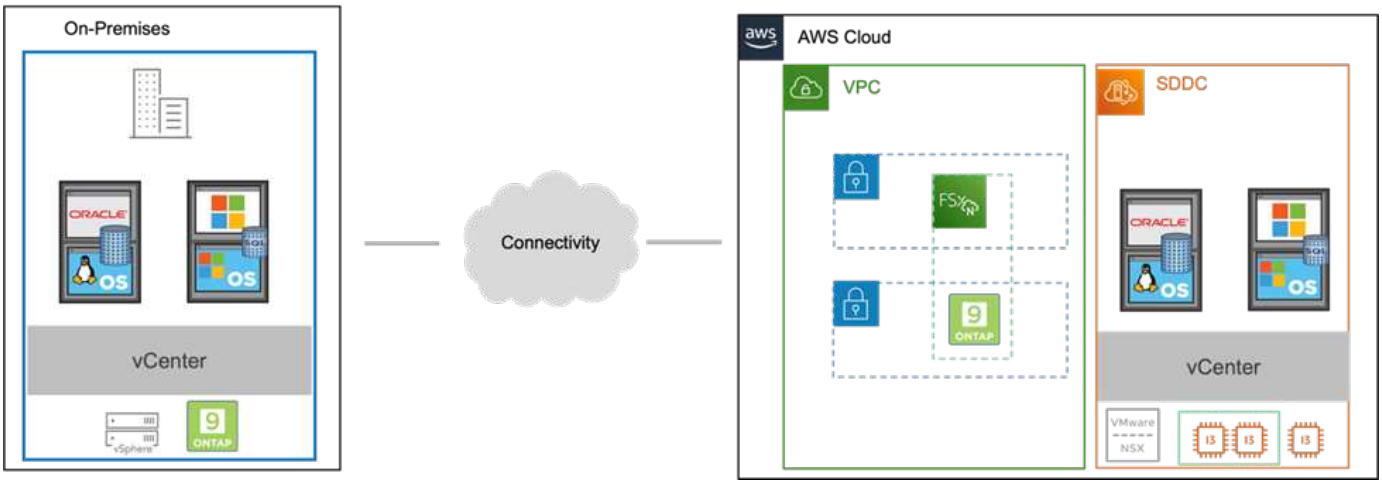
Autores: Chris Reno, Josh Powell y Suresh Toppay - Ingeniería de soluciones de NetApp

Descripción general

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

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

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



Supuestos, requisitos previos y descripción general de los componentes

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

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

Realizar una recuperación ante desastres con SnapCenter

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

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

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

Configurar las relaciones de SnapMirror y los programas de retención

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

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

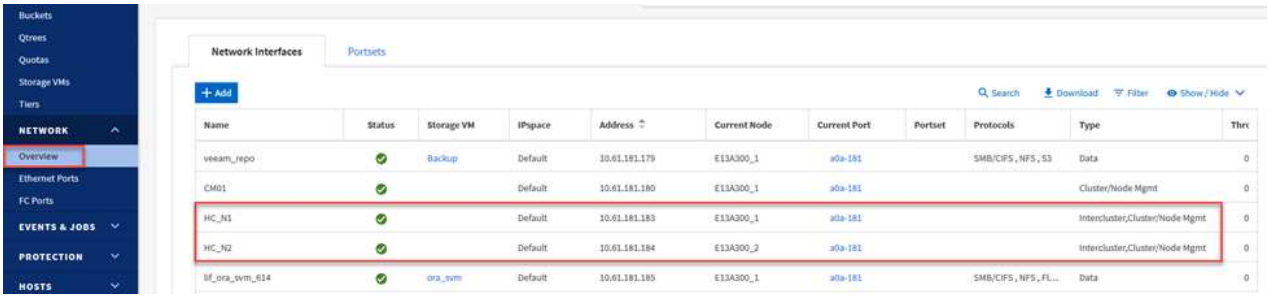
Se requieren los siguientes pasos para configurar las relaciones de SnapMirror entre un sistema ONTAP en las instalaciones y FSX ONTAP:

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

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

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

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



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

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

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

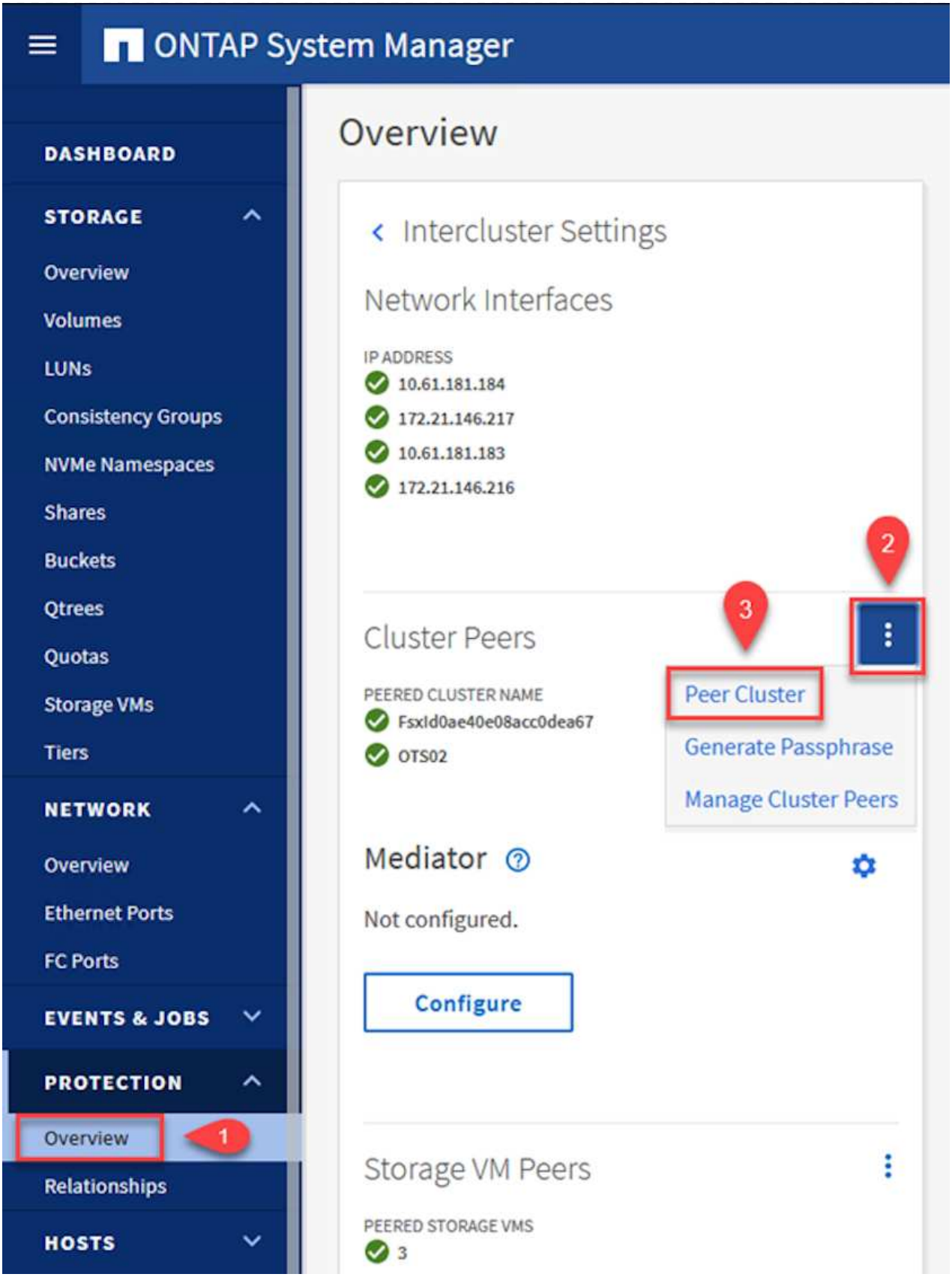
Establecer una relación entre clústeres y FSX y ONTAP

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

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

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

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

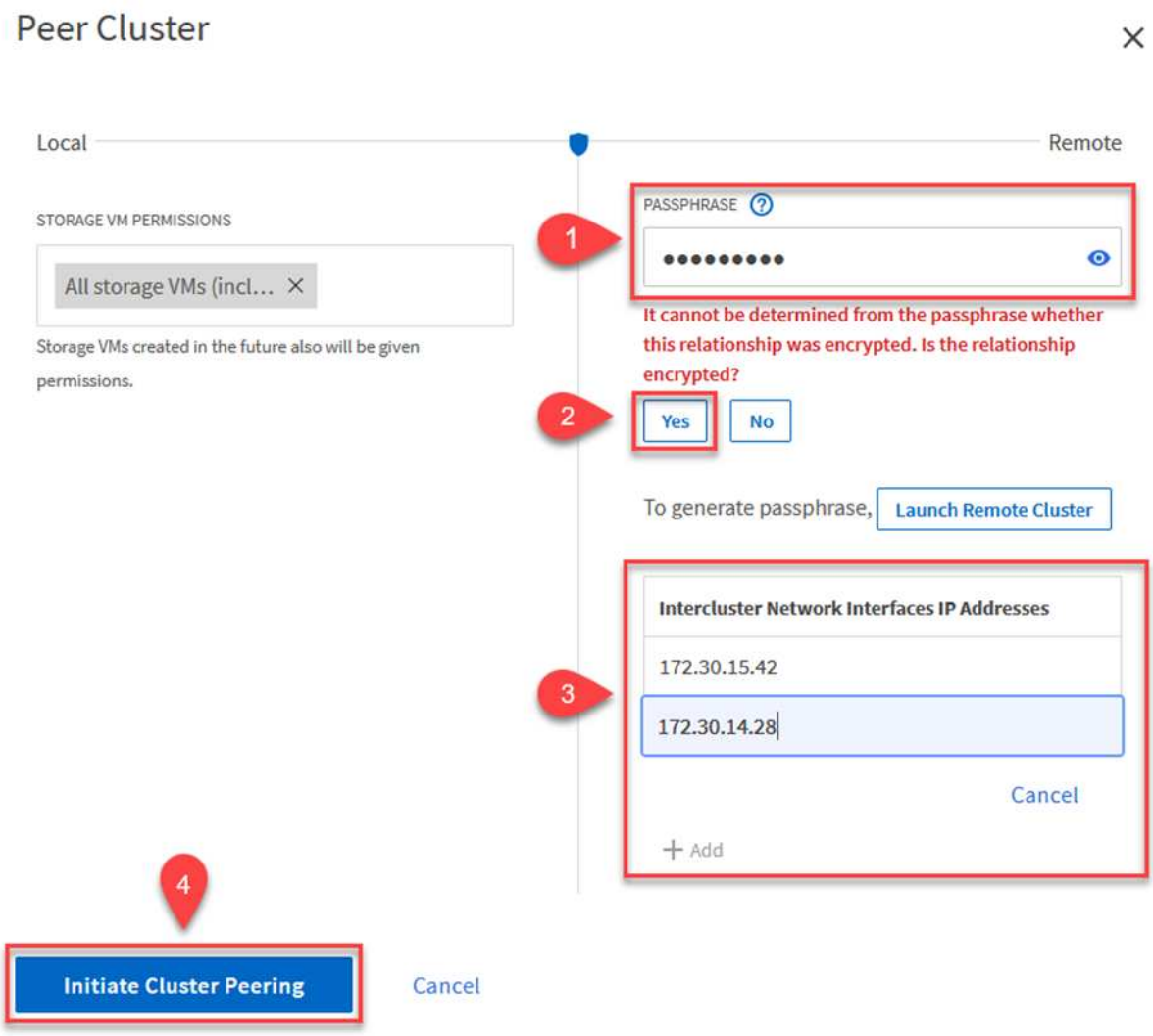


3. En el cuadro de diálogo Peer Cluster, rellene la información que corresponda:
   a. Introduzca la clave de acceso que se utilizó para establecer la relación de clúster entre iguales en el clúster FSX de destino.

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

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

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



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

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

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

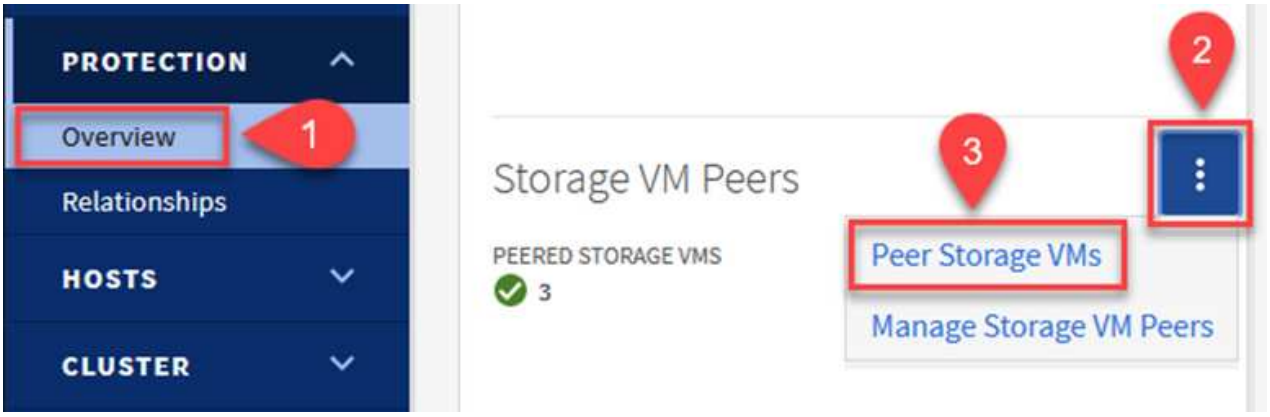
Establecer la relación de paridad de SVM

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

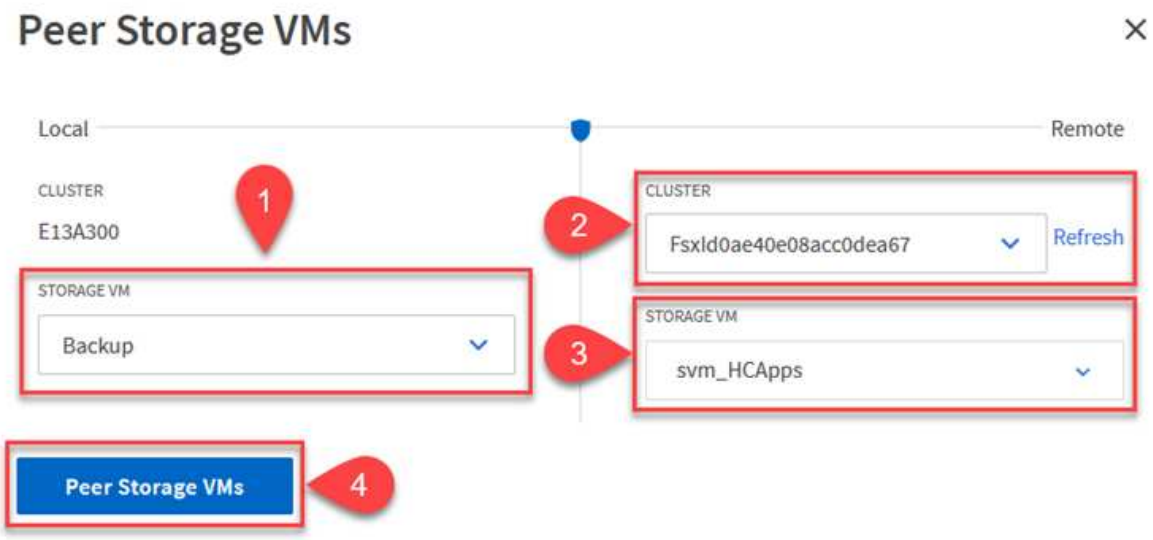
1. En el clúster FSX de origen, use el siguiente comando de la CLI para crear la relación entre iguales de SVM:

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

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



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



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

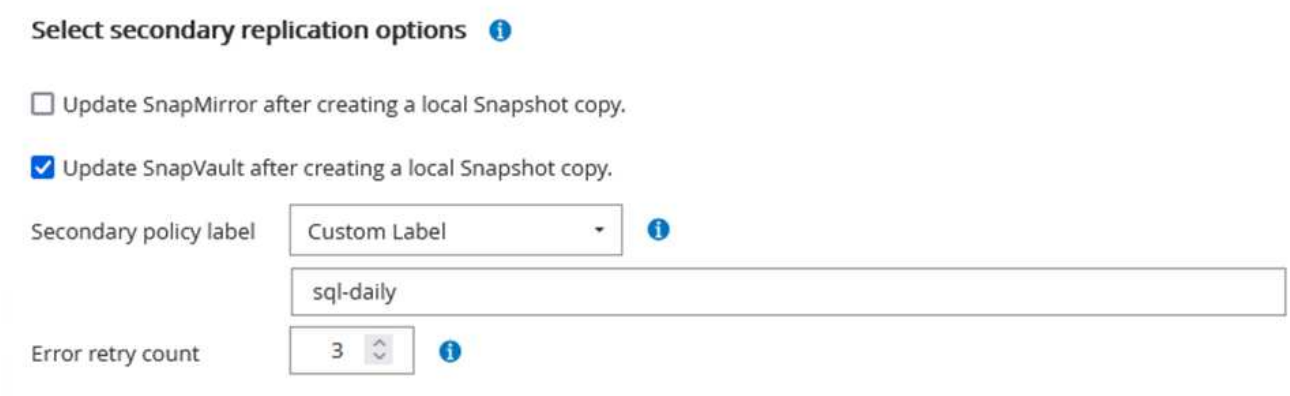
Crear una política de retención de snapshots

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

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

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

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



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

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

1. Cree la política SnapMirror en el clúster FSX.

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

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

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

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

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

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

Crear volúmenes de destino

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

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

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

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

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

Inicializar las relaciones de SnapMirror

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

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

Implemente y configure servidores de Windows SnapCenter localmente.

Ponga en marcha Windows SnapCenter Server en las instalaciones

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

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

El software SnapCenter puede obtenerse en "este enlace".

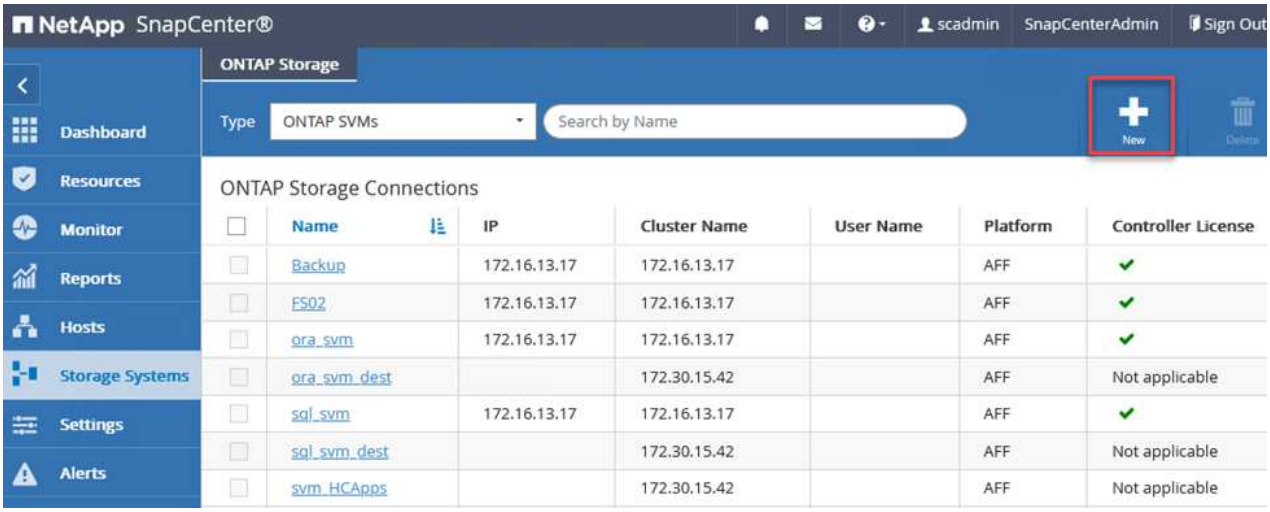
Una vez instalado, puede acceder a la consola SnapCenter desde un explorador Web utilizando *https://Virtual_Cluster_IP_or_FQDN:8146*.

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

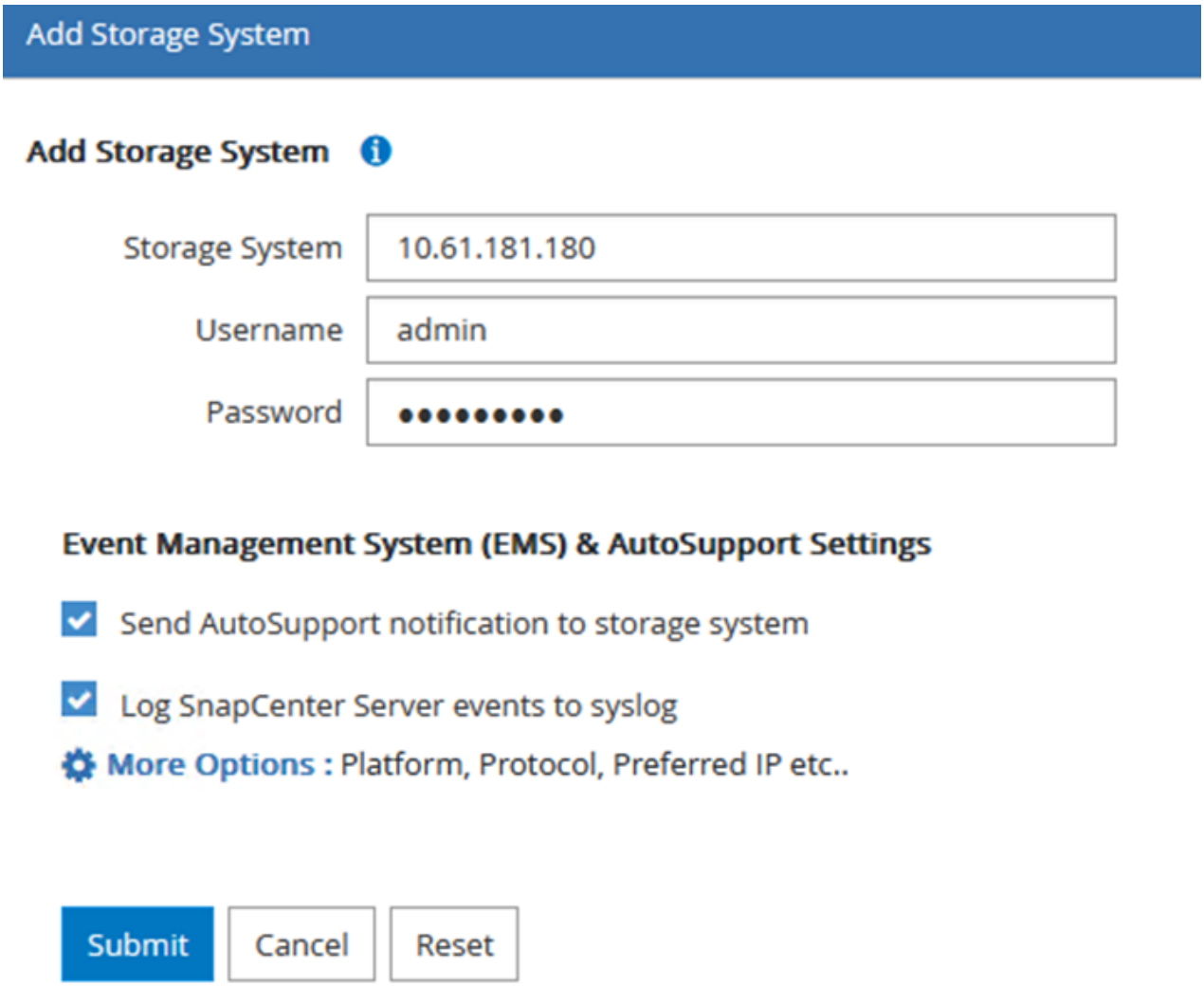
Añada controladoras de almacenamiento a SnapCenter

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

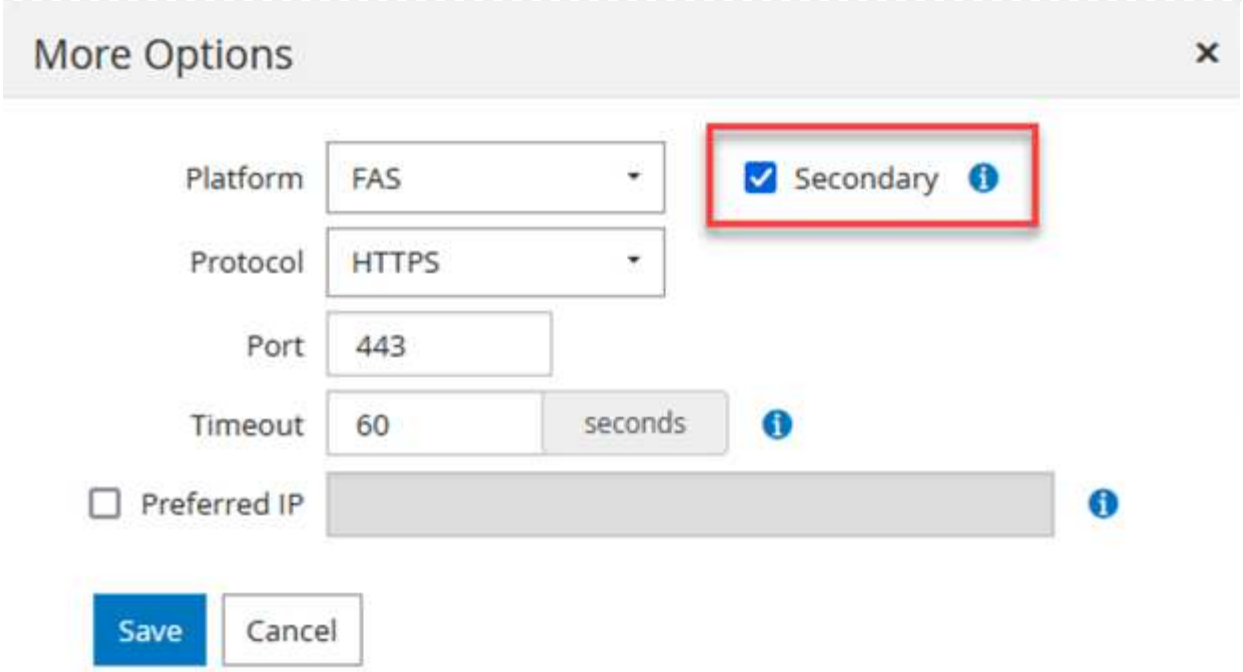
1. En el menú de la izquierda, seleccione Storage Systems y haga clic en New para comenzar el proceso de adición de controladoras de almacenamiento a SnapCenter.



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



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

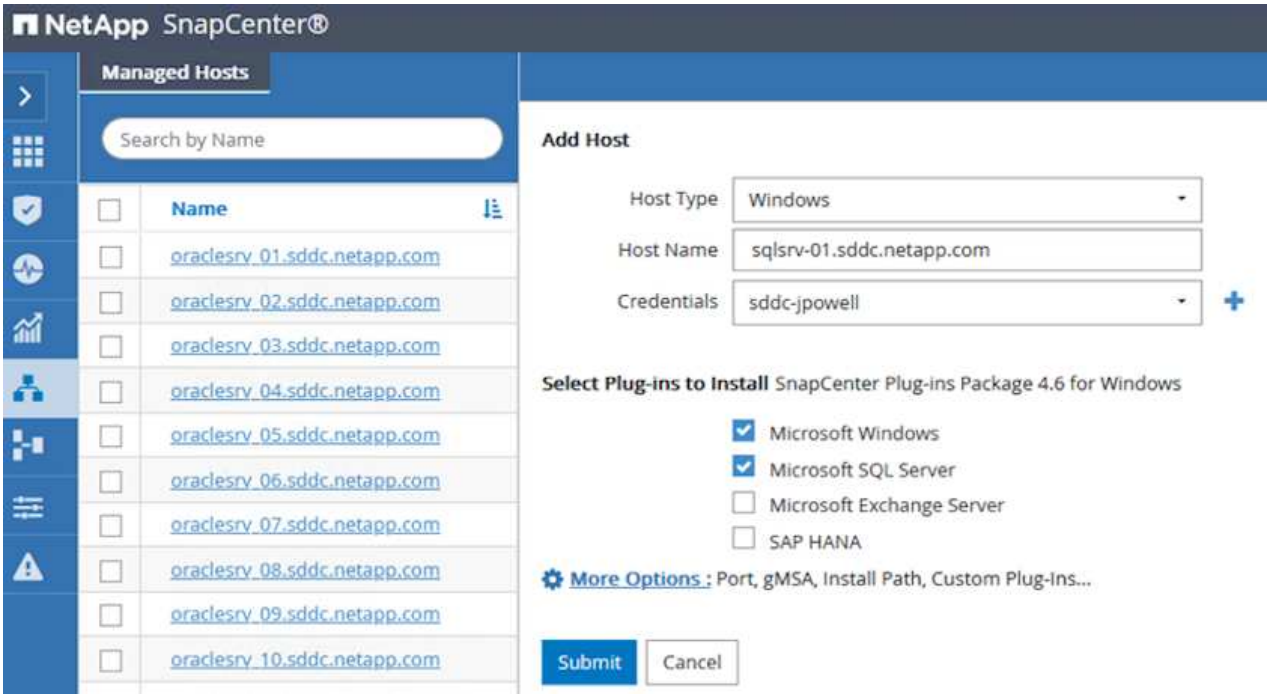


Para obtener más información relacionada con la adición de sistemas de almacenamiento a SnapCenter, consulte la documentación en "este enlace".

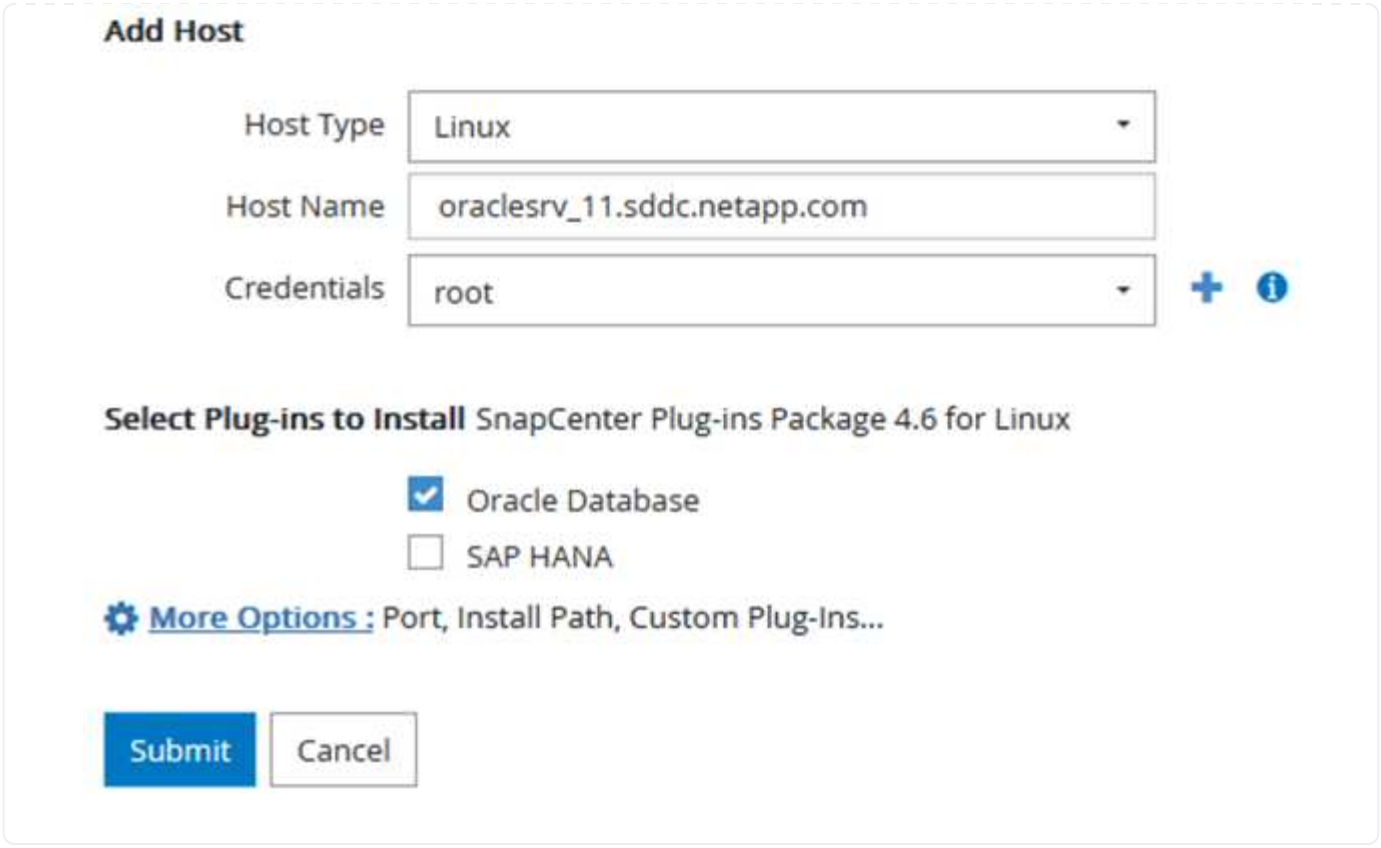
Añada hosts a SnapCenter

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

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



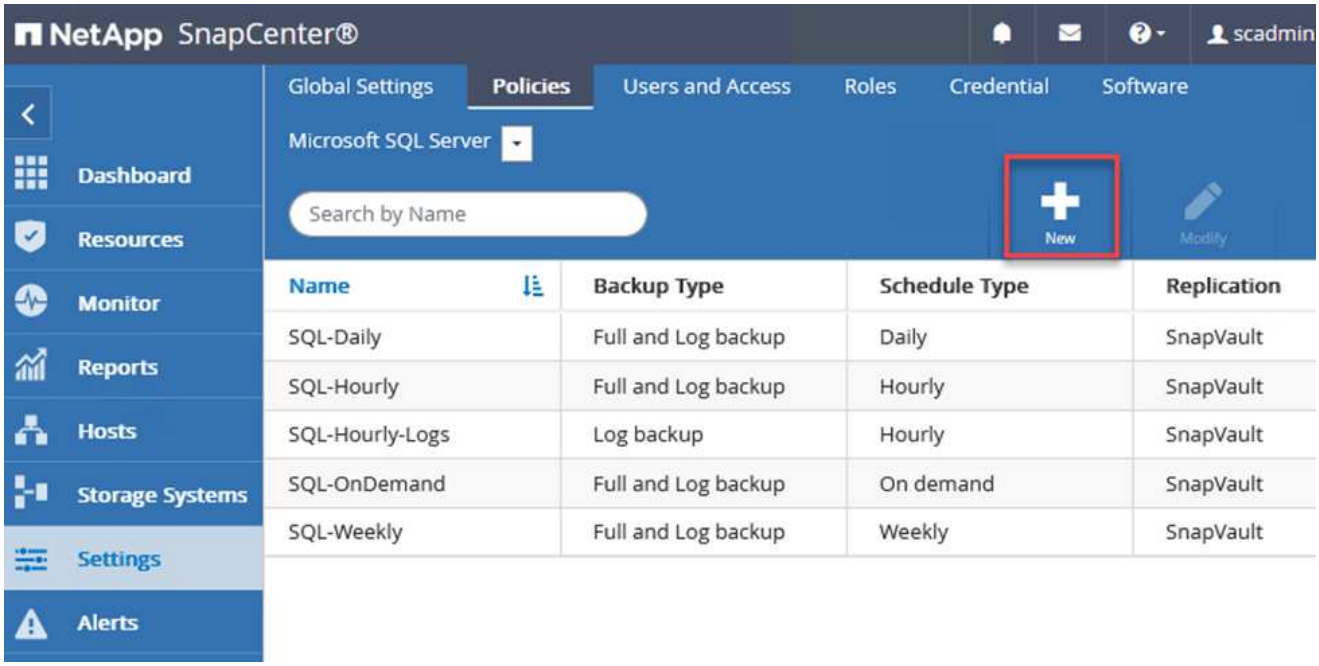
3. Para Oracle, rellene los campos obligatorios en el cuadro de diálogo Add Host y seleccione la casilla de comprobación del plugin de base de datos de Oracle. A continuación, haga clic en Enviar para iniciar el proceso de detección y añadir el host a SnapCenter.


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

Crear políticas de SnapCenter

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

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



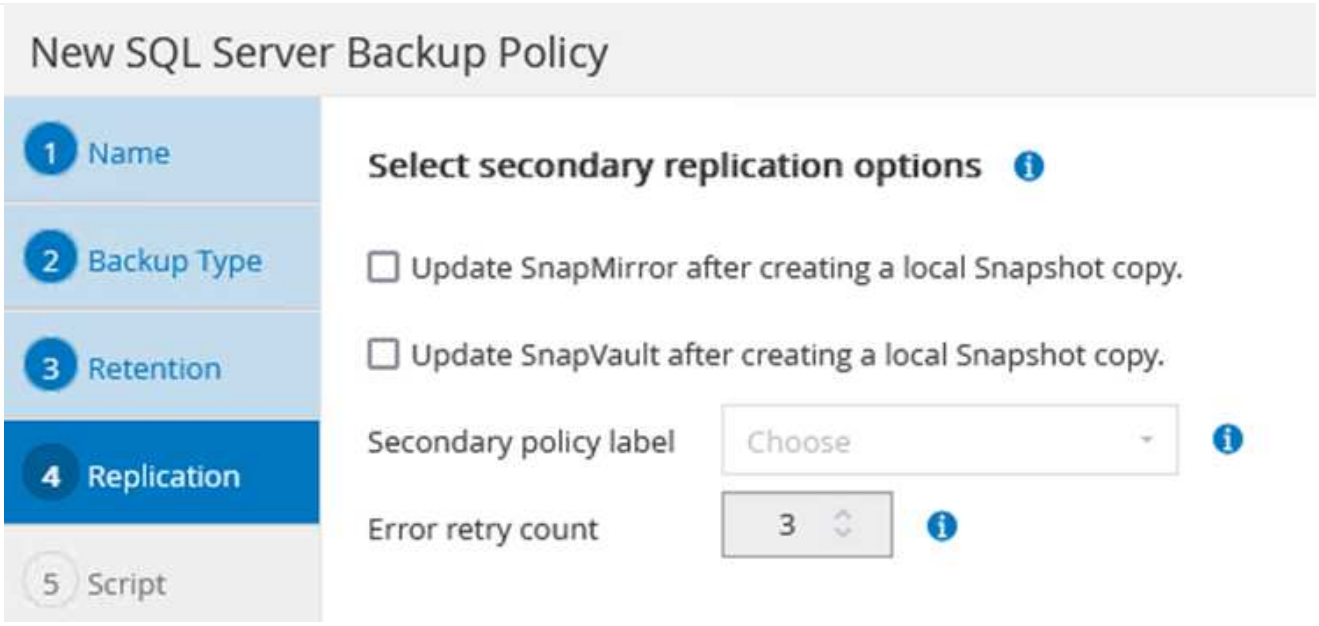
Para obtener información completa sobre la creación de políticas para backups de SQL Server, consulte "Documentación de SnapCenter".

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

Notas:

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

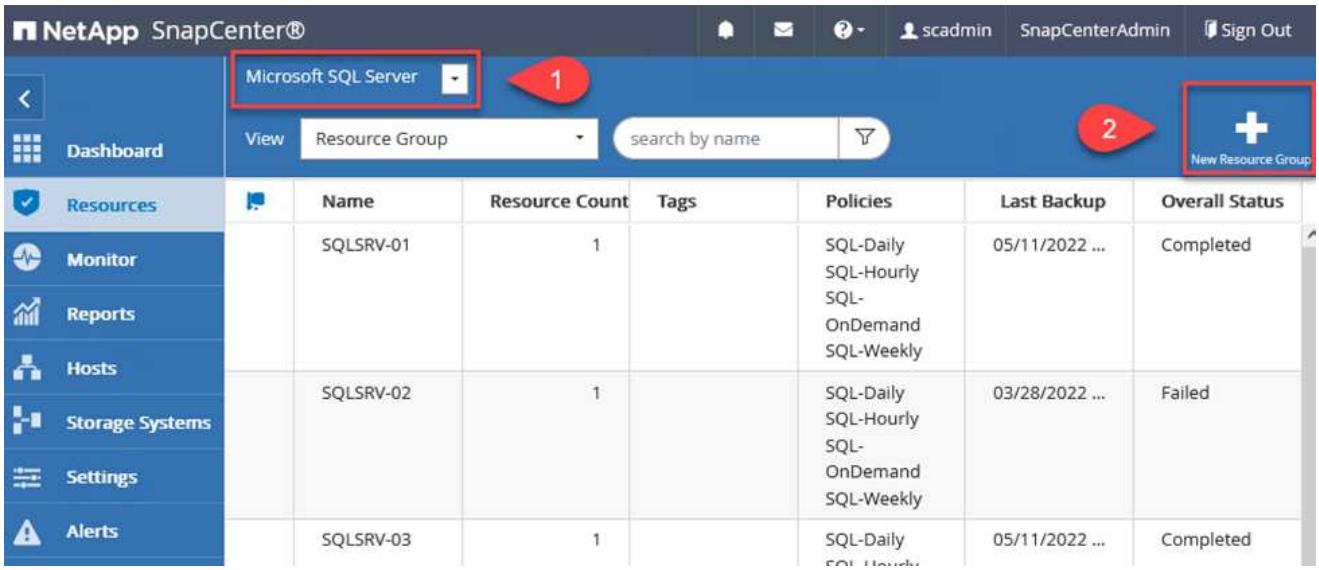
En la siguiente imagen, se muestran las opciones anteriores y su aspecto en el asistente de política de backup.



Crear grupos de recursos de SnapCenter

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

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



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

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

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

Ponga en marcha y configure Veeam Backup Server

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

Configurar el repositorio de backup de escalado horizontal de Veeam

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

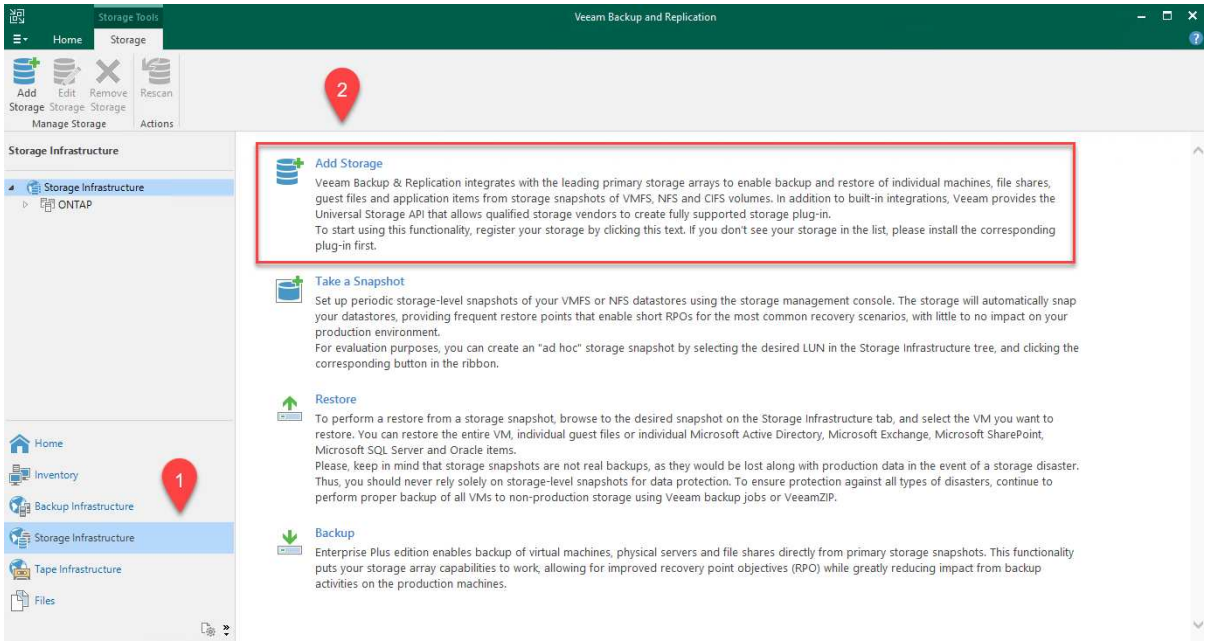
Consulte los siguientes requisitos previos antes de comenzar.

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

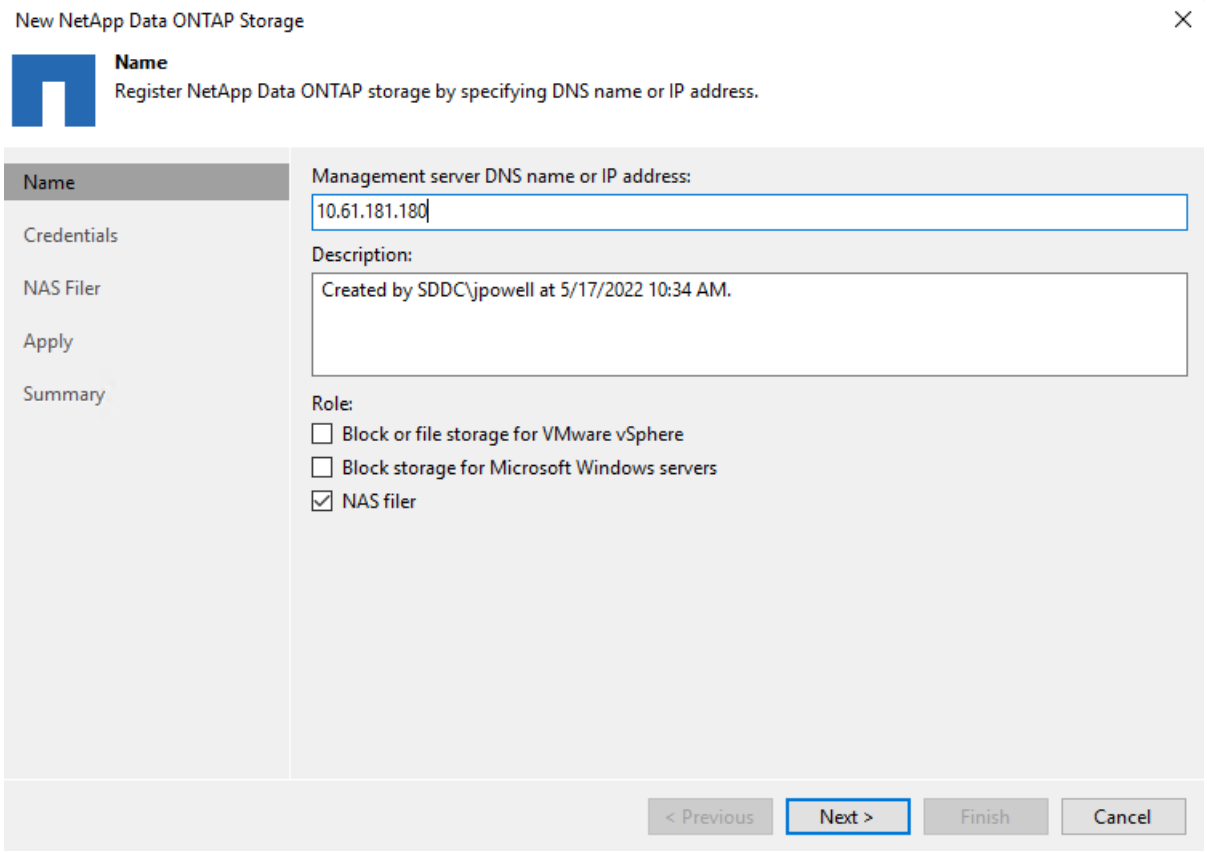
Añada el almacenamiento de ONTAP a Veeam

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

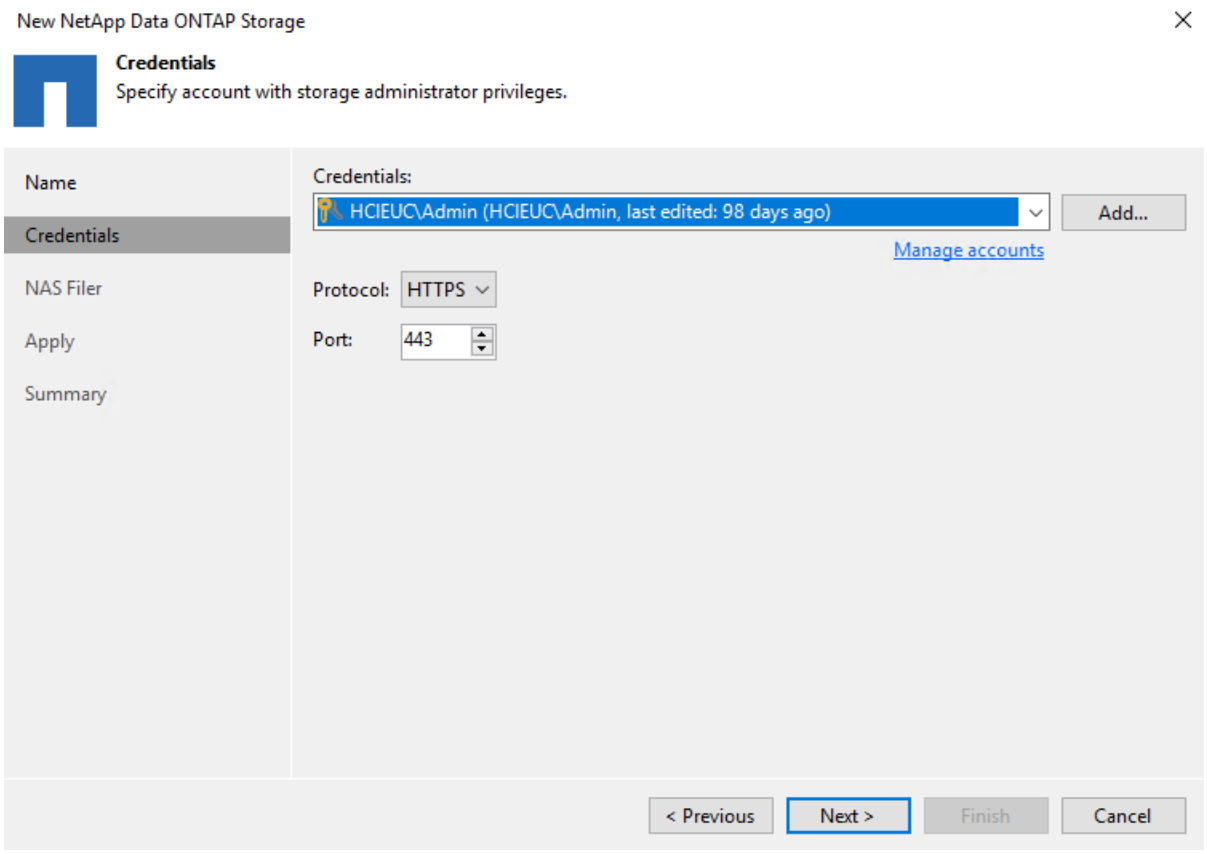
1. Abra la consola de Veeam e inicie sesión. Vaya a Storage Infrastructure y seleccione Add Storage.



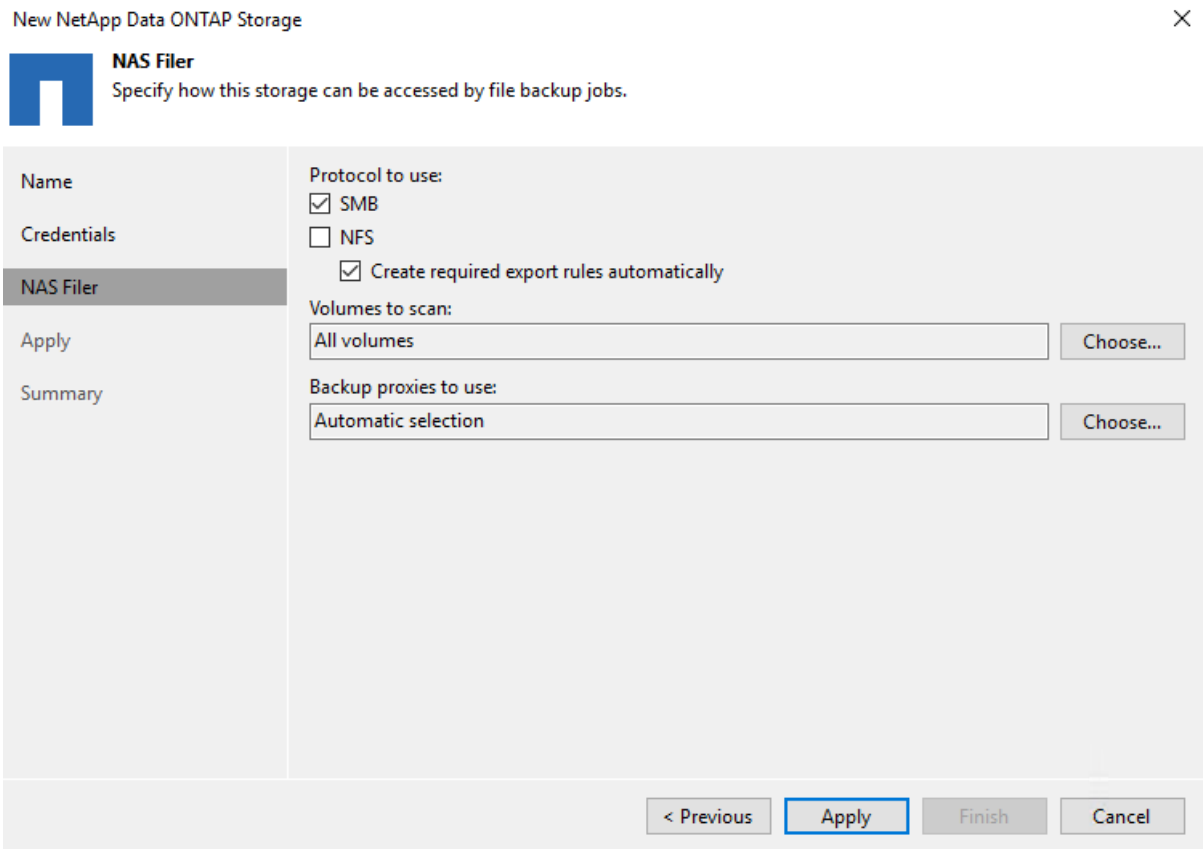
2. En el asistente Add Storage, seleccione NetApp como proveedor de almacenamiento y, a continuación, seleccione Data ONTAP.
3. Introduzca la dirección IP de administración y active la casilla de verificación servidor dedicado a almacenamiento NAS. Haga clic en Siguiente.



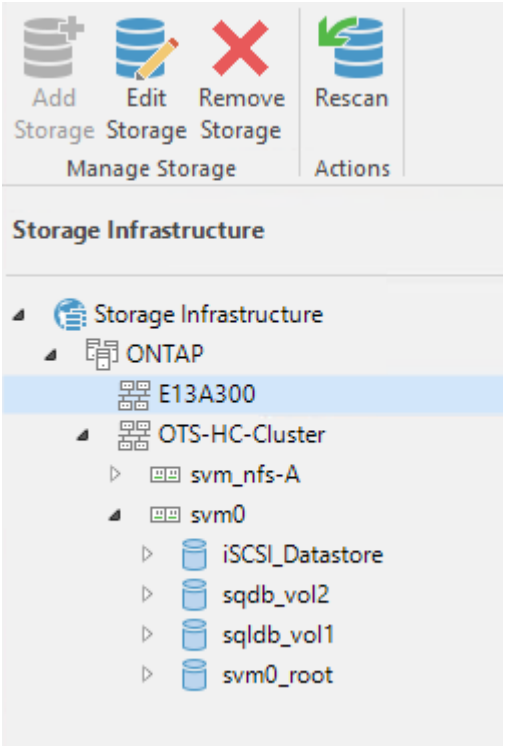
4. Añada sus credenciales para acceder al clúster de ONTAP.



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

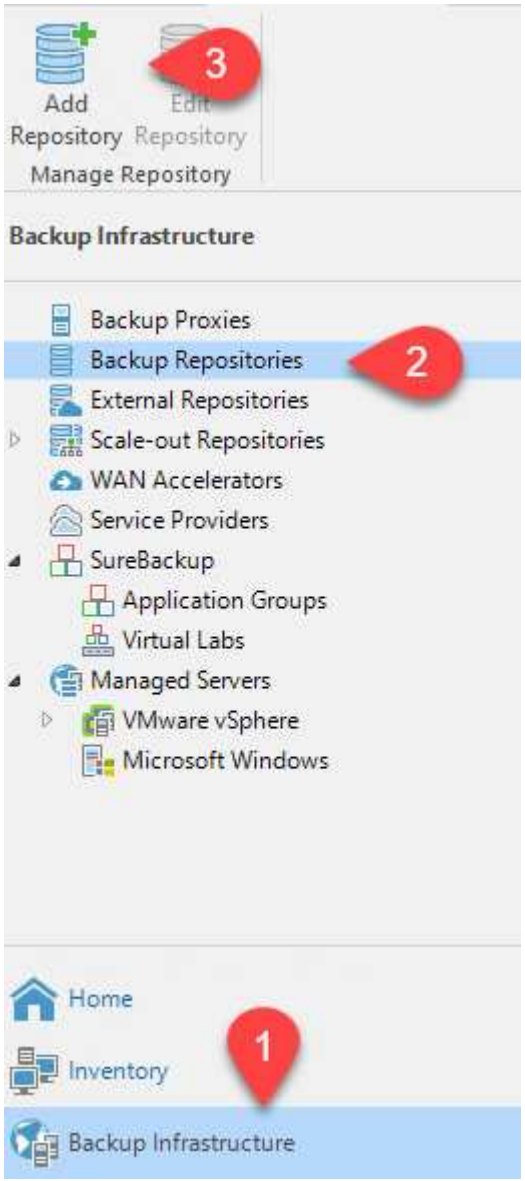


6. Complete las páginas Apply y Summary del asistente y haga clic en Finish para iniciar el proceso de detección de almacenamiento. Una vez finalizada la exploración, se añade el clúster ONTAP junto con los servidores dedicados a almacenamiento NAS como recursos disponibles.

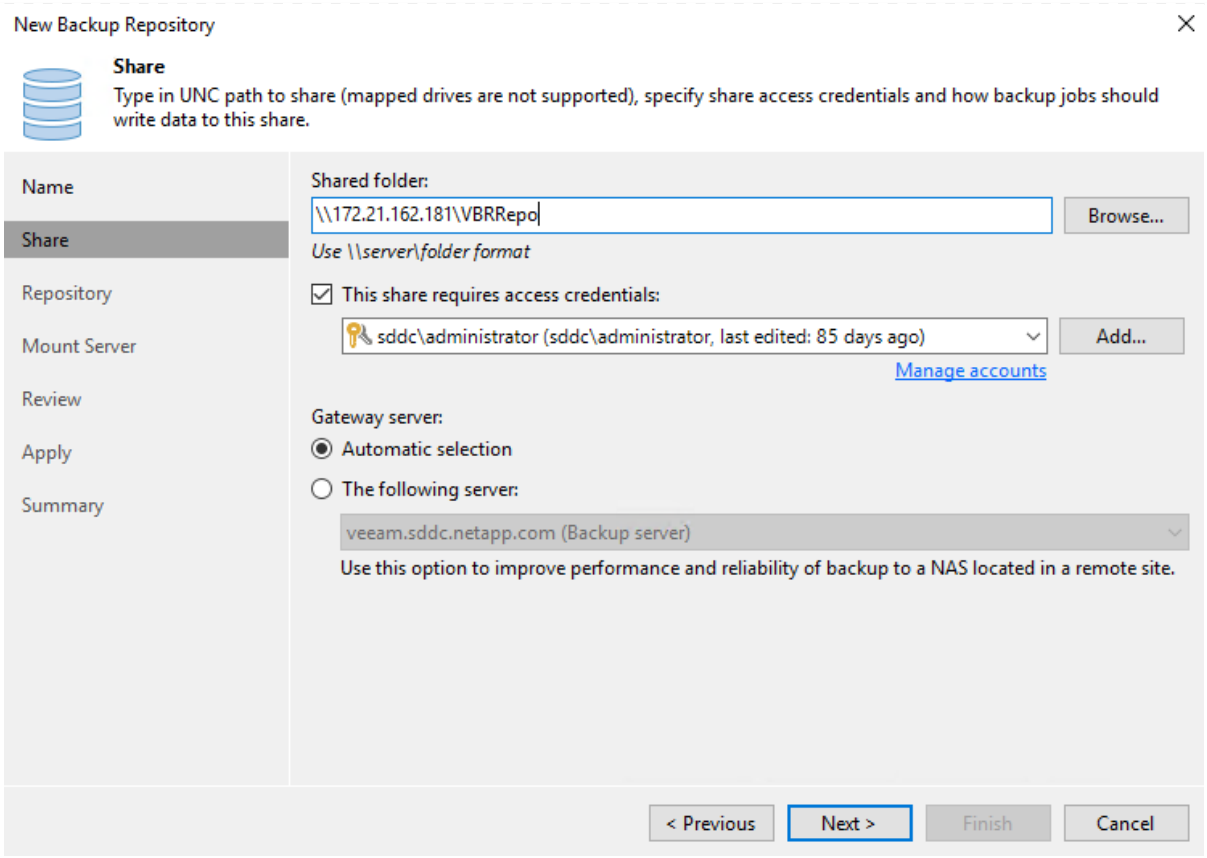


7. Cree un repositorio de backup con los recursos compartidos NAS recién detectados. En Infraestructura de copia de seguridad, seleccione repositorios de copia de seguridad y haga clic

en el elemento de menú Agregar repositorio.



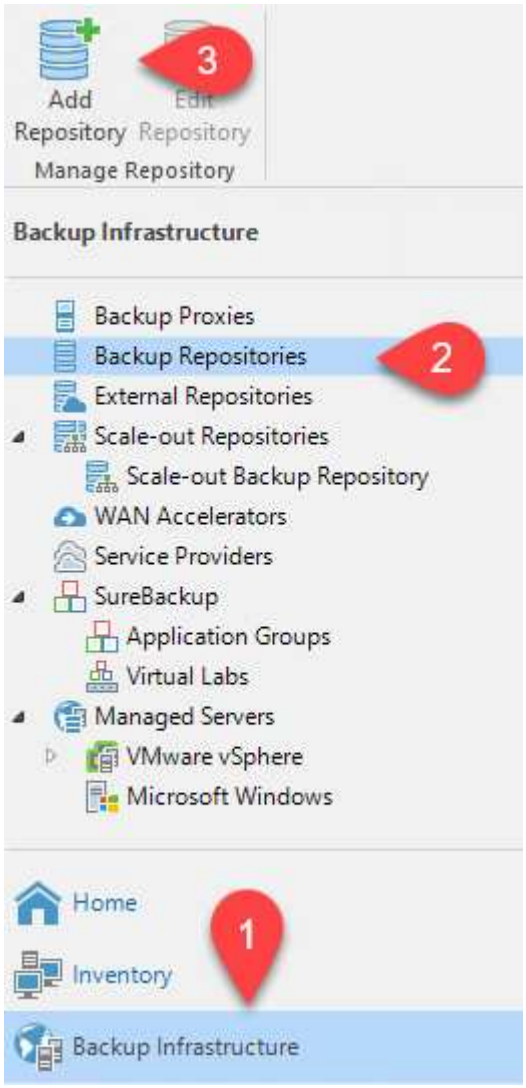
8. Siga todos los pasos del Asistente para crear un repositorio de copia de seguridad nuevo para crear el repositorio. Para obtener información detallada sobre la creación de repositorios de Veeam Backup, consulte "Documentación de Veeam".


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

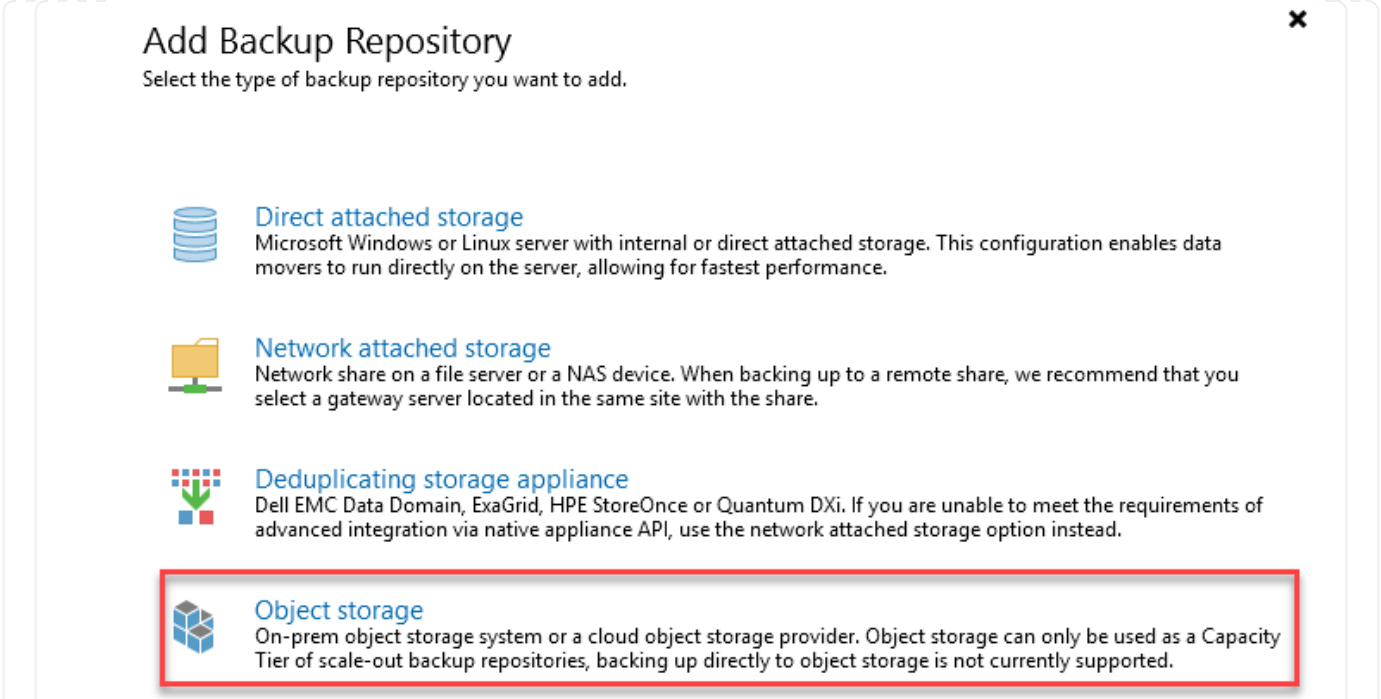
Añada el bloque de Amazon S3 como repositorio de backup

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

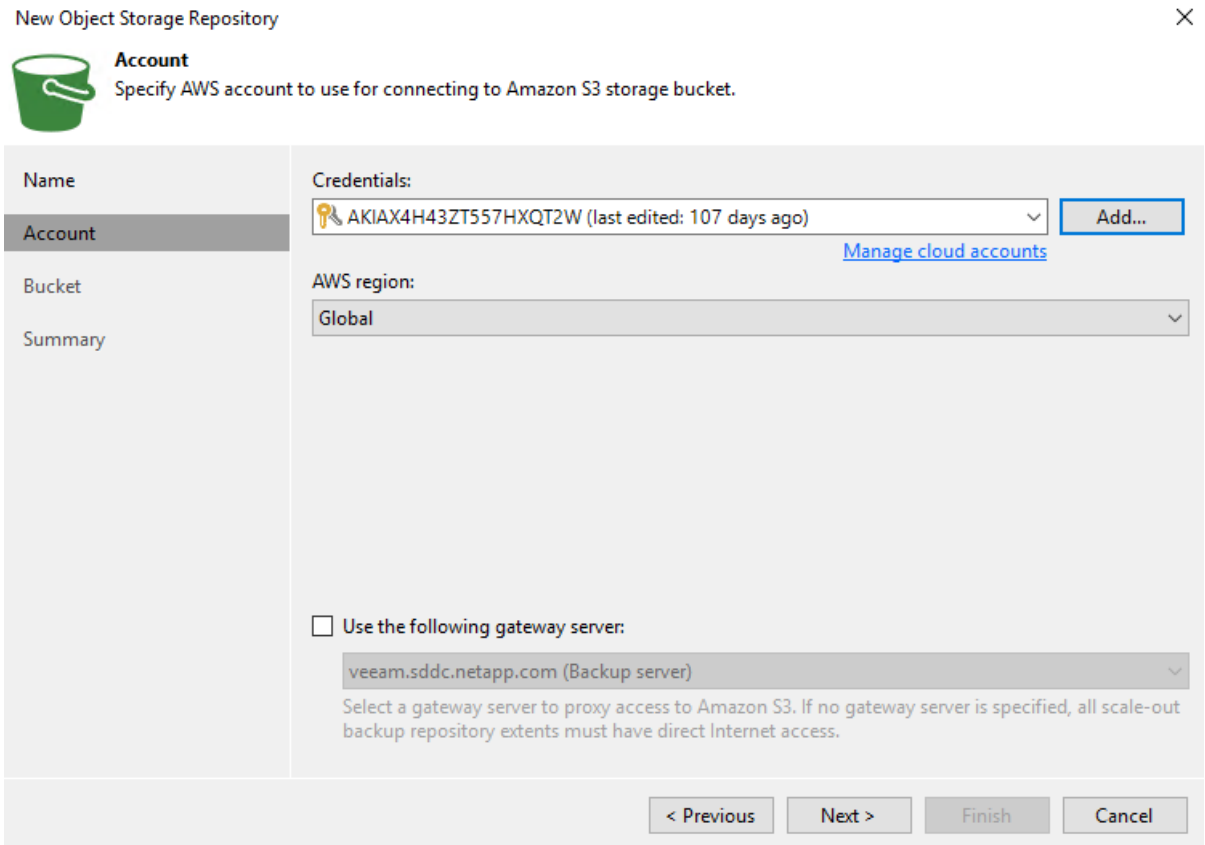
1. Vaya a Backup Infrastructure > repositorios de backup. Haga clic en Add Repository.



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



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

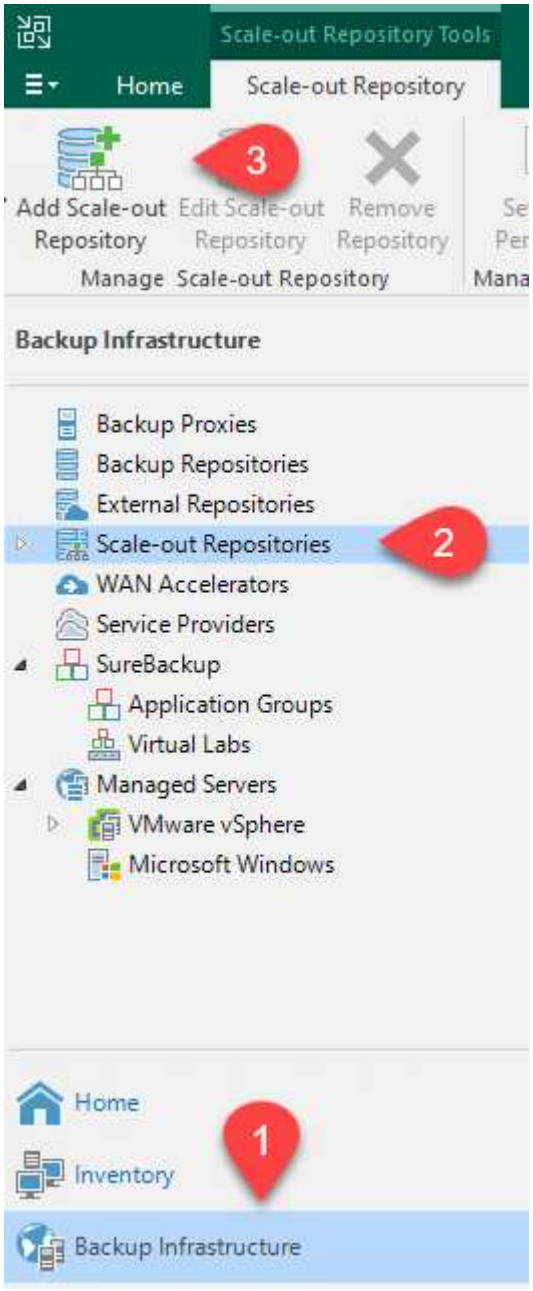


5. Una vez que se haya cargado la configuración de Amazon, seleccione su centro de datos, bloque y carpeta y haga clic en Apply. Por último, haga clic en Finalizar para cerrar el asistente.

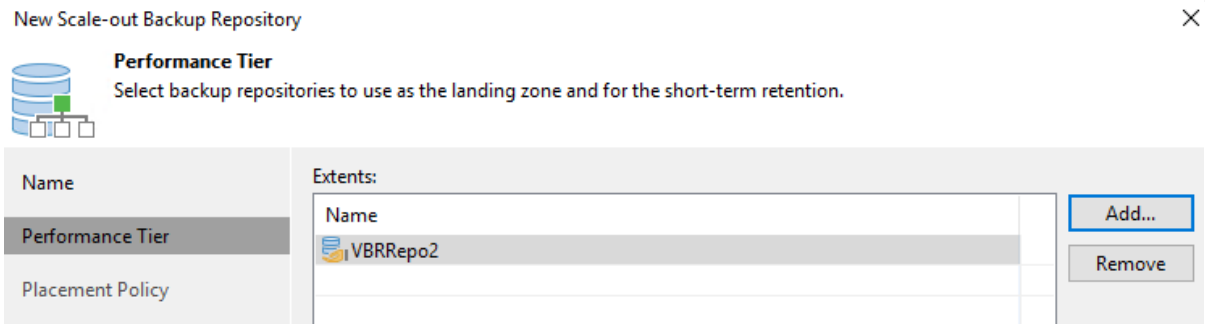
Cree un repositorio de backup de escalado horizontal

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

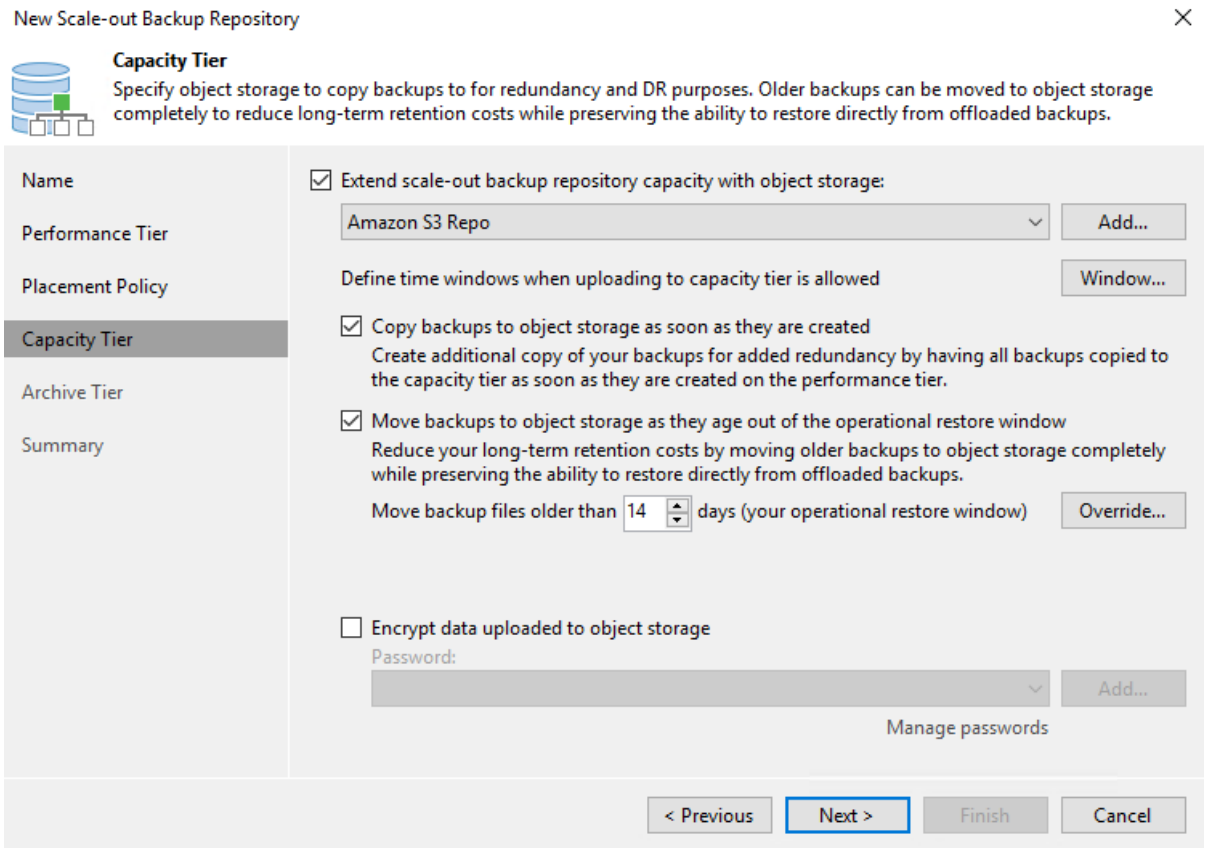
1. En Backup Infrastructure, seleccione repositorios de escalado horizontal y, a continuación, haga clic en el elemento de menú Add Scale-Out Repository.



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



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



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

Crear las tareas del repositorio de backup de escalado horizontal

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

Configuración y herramientas de backup y recuperación de BlueXP

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

Implemente un servidor SnapCenter secundario de Windows

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

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

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

Configurar servidor SnapCenter secundario de Windows

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

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

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

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

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

Configurar el servidor de replicación secundario de Veeam Backup &

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

Para realizar este proceso, deben completarse los siguientes elementos:

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

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

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

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

Requisitos previos de backup de SnapCenter

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

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

Resumen del proceso de backup y restauración de SnapCenter

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

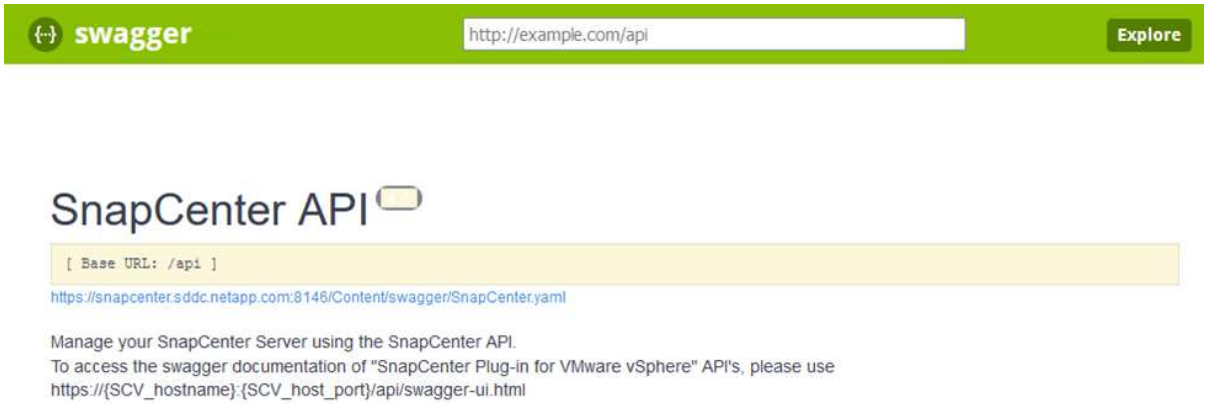
Realice un backup de la base de datos de SnapCenter y la configuración

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

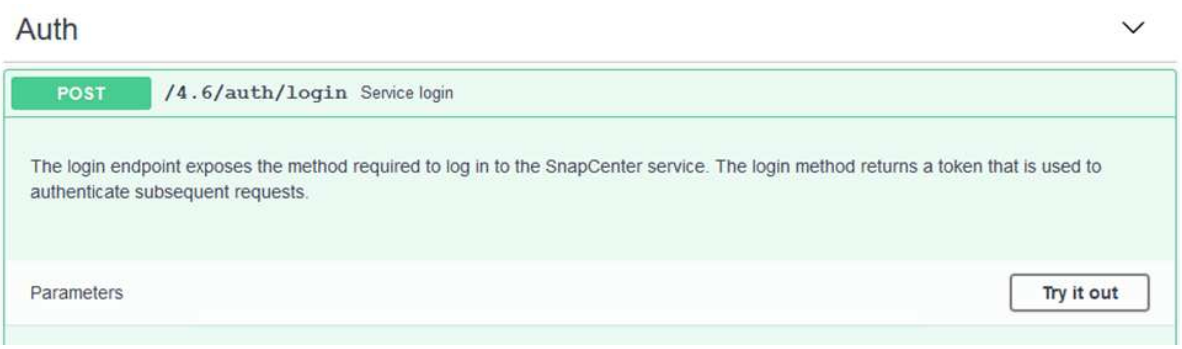
Inicie sesión en Swagger y obtenga el token de autorización

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

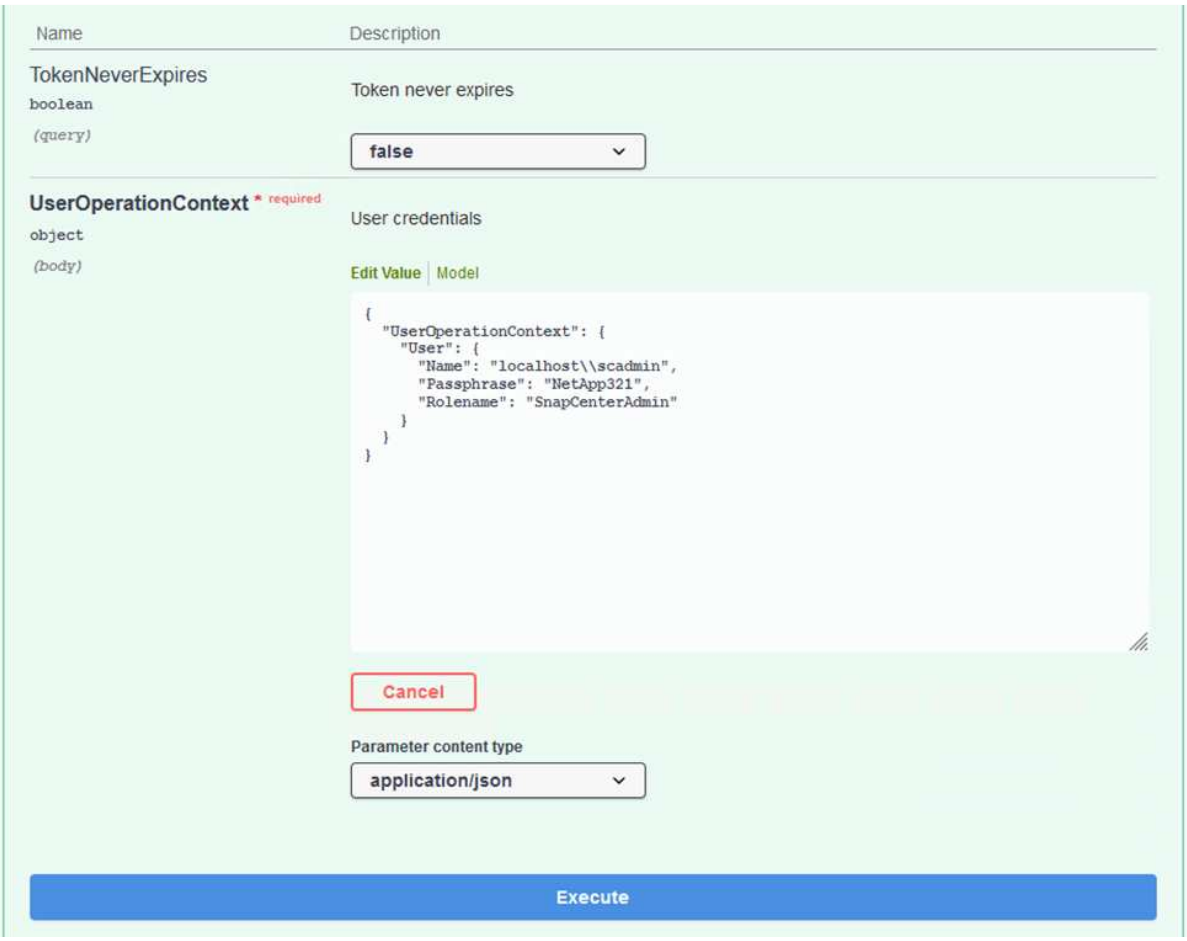
1. Acceda a la página web de API de SnapCenter Swagger en *https://<SnapCenter Server IP>:8146/swagger/*.



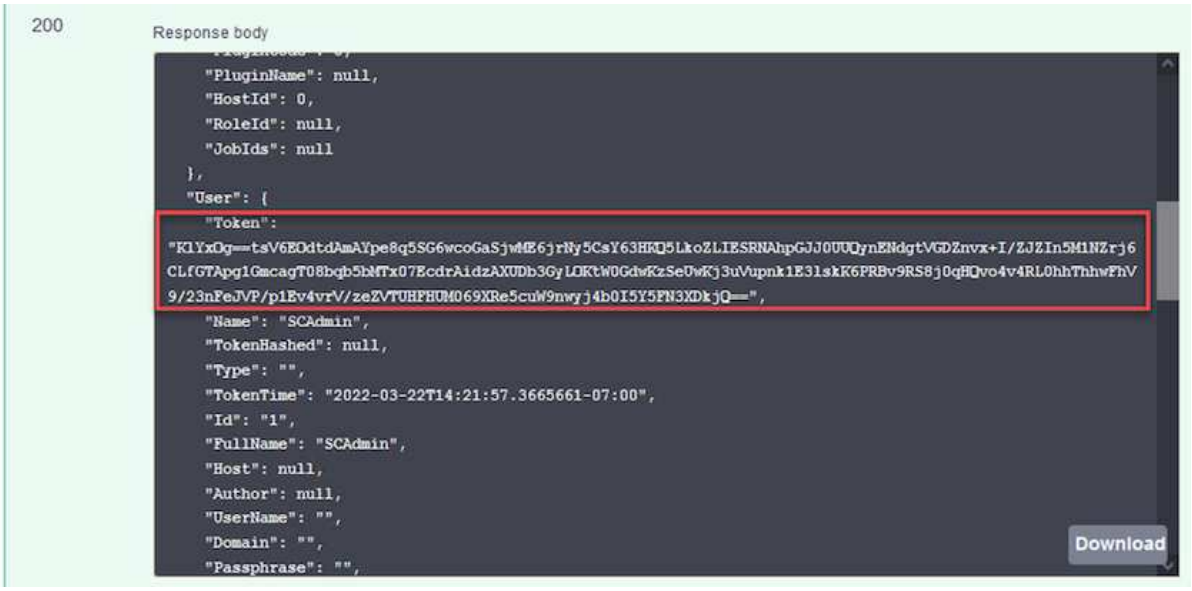
2. Expanda la sección Auth y haga clic en Inténtelo.



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



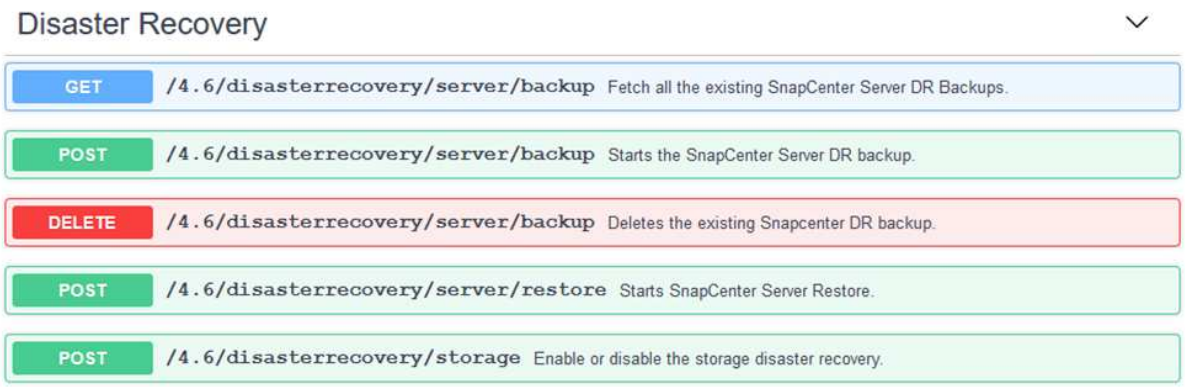
4. En el cuerpo de respuesta que aparece a continuación, puede ver el token. Copie el texto del token para la autenticación al ejecutar el proceso de backup.



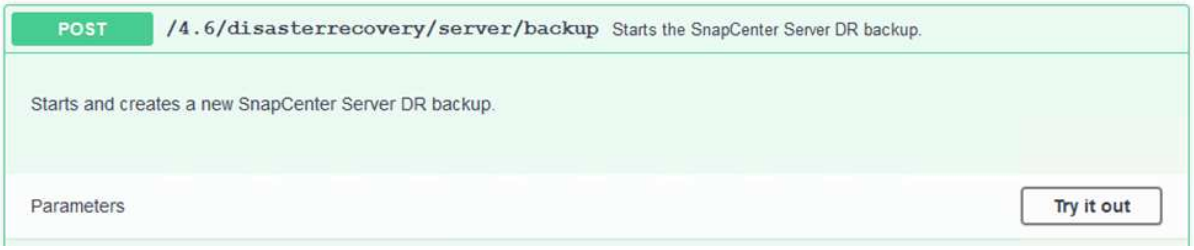
Realizar un backup de base de datos de SnapCenter

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

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

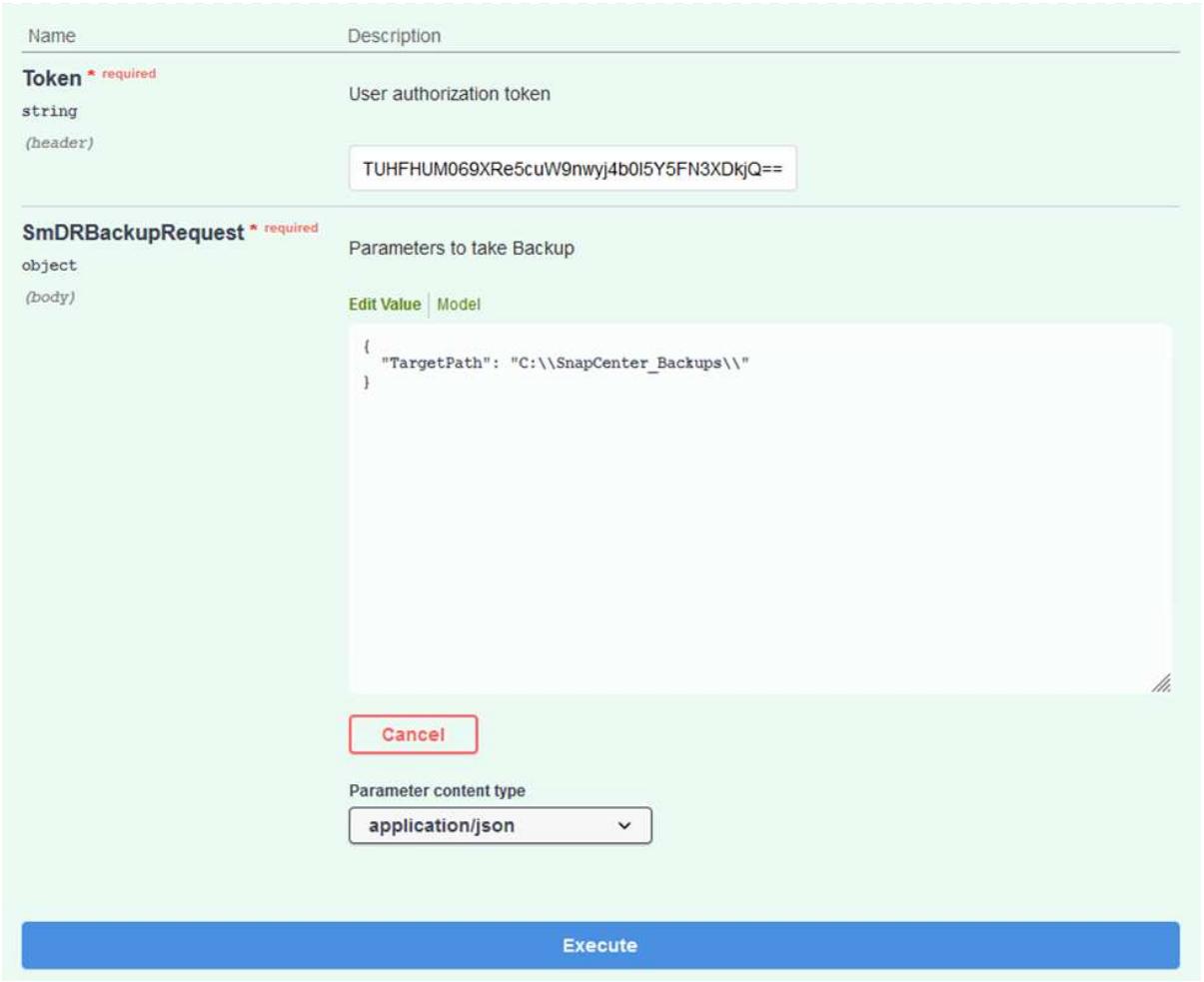


2. Expanda el `/4.6/disasterrecovery/server/backup` Y haga clic en probar.



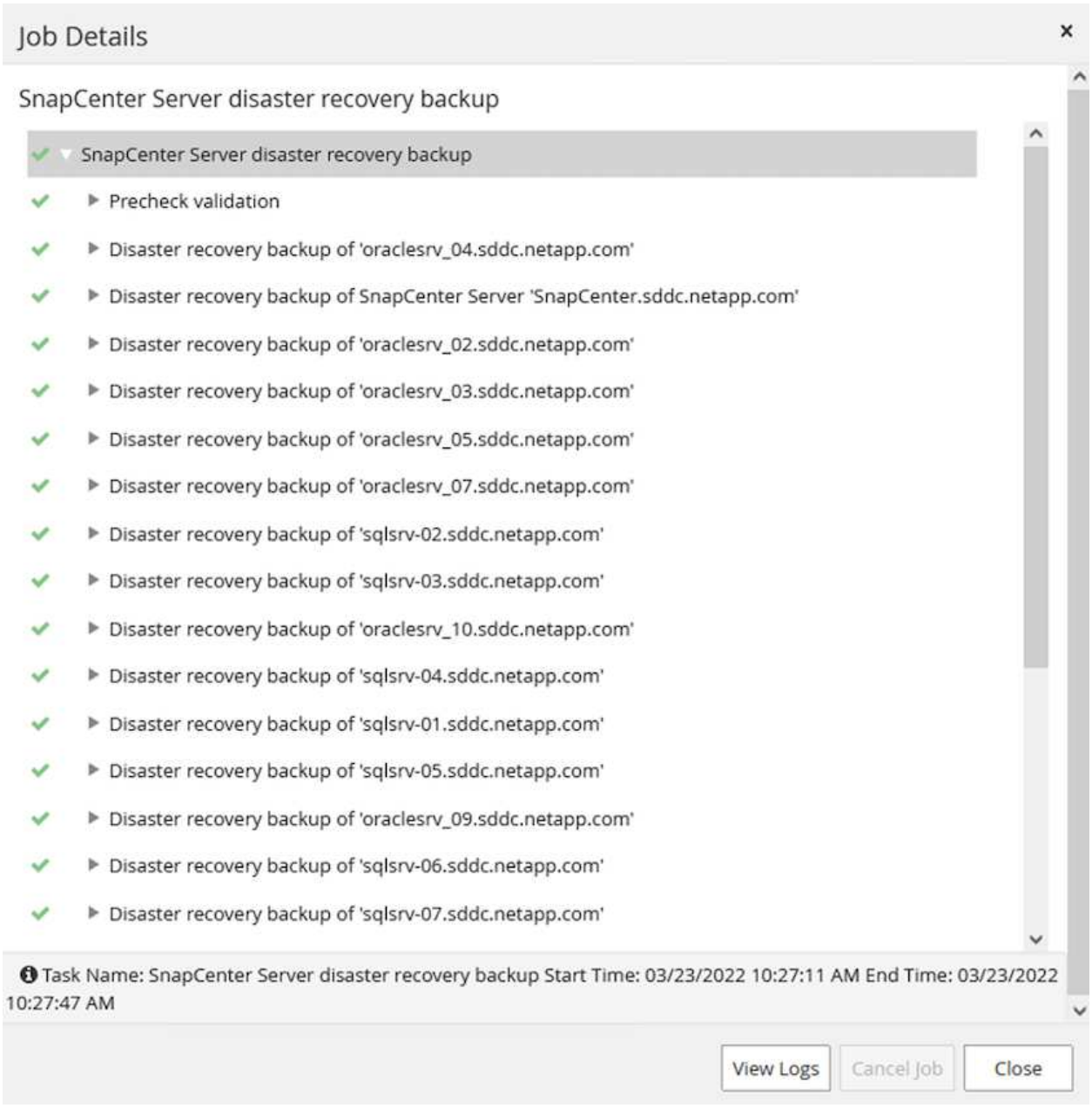
3. En la sección SmDRBackupRequest, añada la ruta de acceso correcta al destino local y seleccione Execute para iniciar el backup de la base de datos y la configuración de SnapCenter.

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


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

Supervise el trabajo de backup desde SnapCenter

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



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

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

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

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

Conmutación al respaldo

Desastre ocurre en el sitio principal

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

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

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

Proceso de restauración de bases de datos de SnapCenter

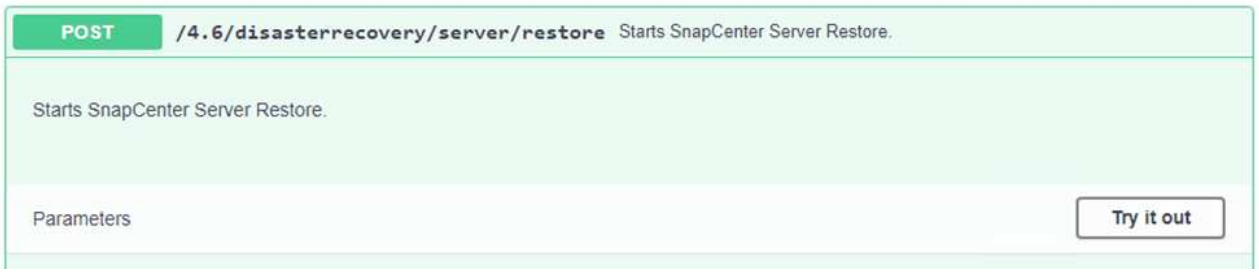
SnapCenter admite escenarios de recuperación ante desastres, ya que permite el backup y la restauración de sus archivos de configuración y base de datos de MySQL. Esto permite a un administrador mantener backups periódicos de la base de datos de SnapCenter en el centro de datos local y restaurar posteriormente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

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

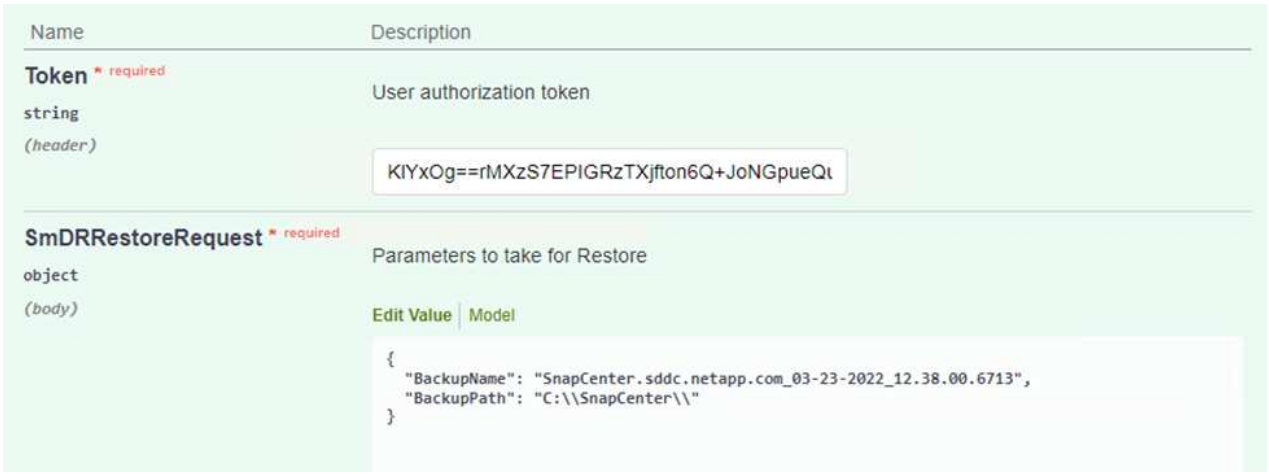
1. Rompa la relación de SnapMirror del clúster FSX y haga que el volumen sea de lectura/escritura.
2. Cree un servidor CIFS (si es necesario) y cree un recurso compartido CIFS que señale la ruta de unión del volumen clonado.
3. Utilice xcopy para copiar los archivos de copia de seguridad en un directorio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

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

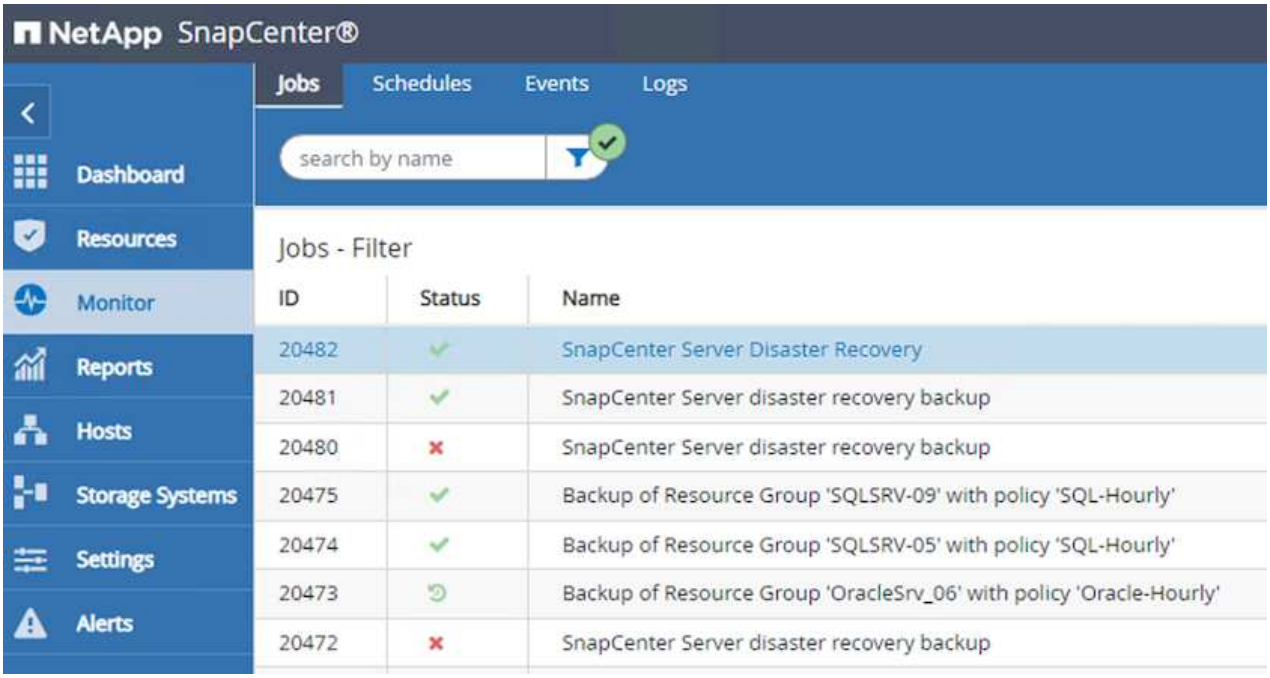
1. Acceda a la página web de API de Swagger para el servidor SnapCenter secundario y siga las instrucciones anteriores para obtener un token de autorización.
2. Desplácese hasta la sección Disaster Recovery de la página Swagger, seleccione `/4.6/disasterrecovery/server/restore`Y haga clic en probar.

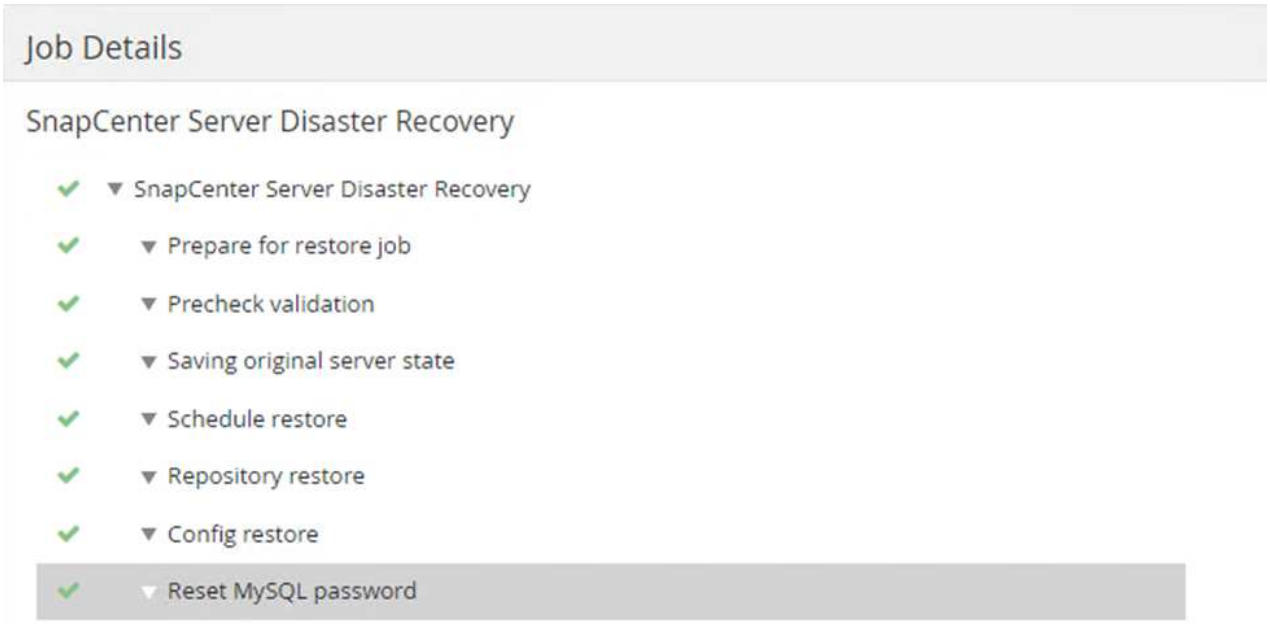


3. Pegue el token de autorización y, en la sección SmDRResterRequest, pegue el nombre del backup y el directorio local del servidor SnapCenter secundario.



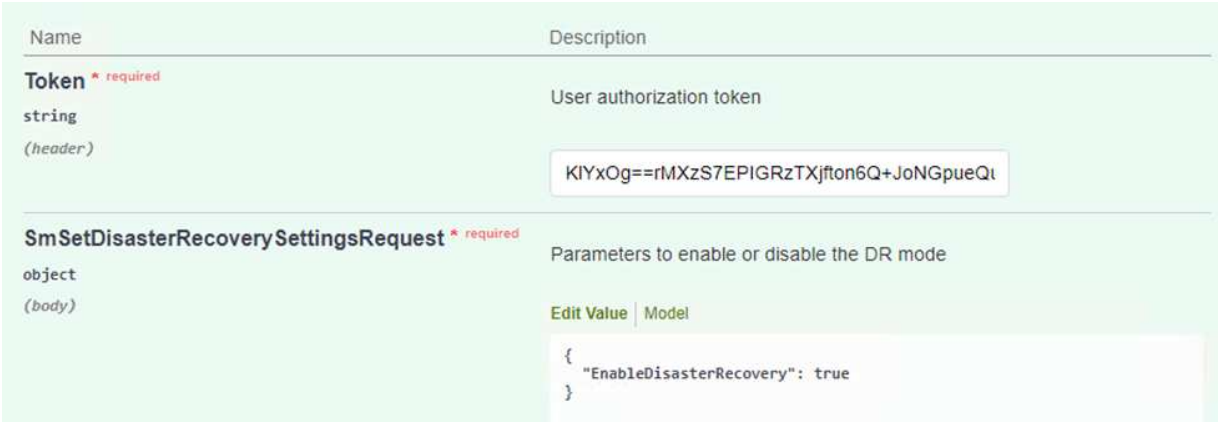
4. Seleccione el botón Ejecutar para iniciar el proceso de restauración.
5. En SnapCenter, desplácese hasta la sección Supervisión para ver el progreso del trabajo de restauración.





6. Para habilitar las restauraciones de SQL Server a partir de almacenamiento secundario, es necesario cambiar la base de datos de SnapCenter al modo de recuperación ante desastres. Esto se realiza como una operación independiente y se inicia en la página web de la API de Swagger.
   a. Desplácese hasta la sección Disaster Recovery y haga clic en `/4.6/disasterrecovery/storage`.
   b. Pegar en el token de autorización de usuario.
   c. En la sección SmSetDisasterRecoverySettingsRequest, cambie `EnableDisasterRecover` para `true`.

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



Consulte los comentarios sobre procedimientos adicionales.

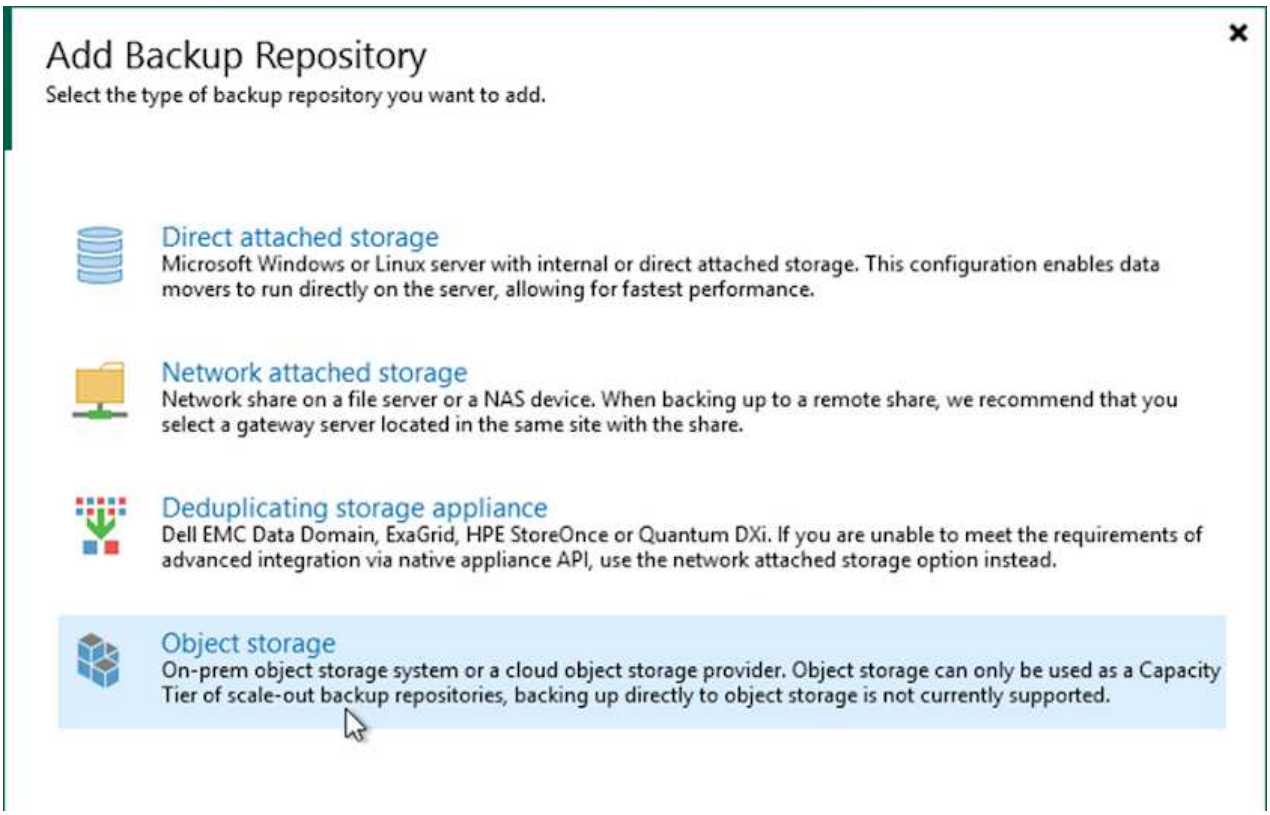
Restaure equipos virtuales de aplicación con la restauración completa de Veeam

Cree un repositorio de backup e importe los backups desde S3

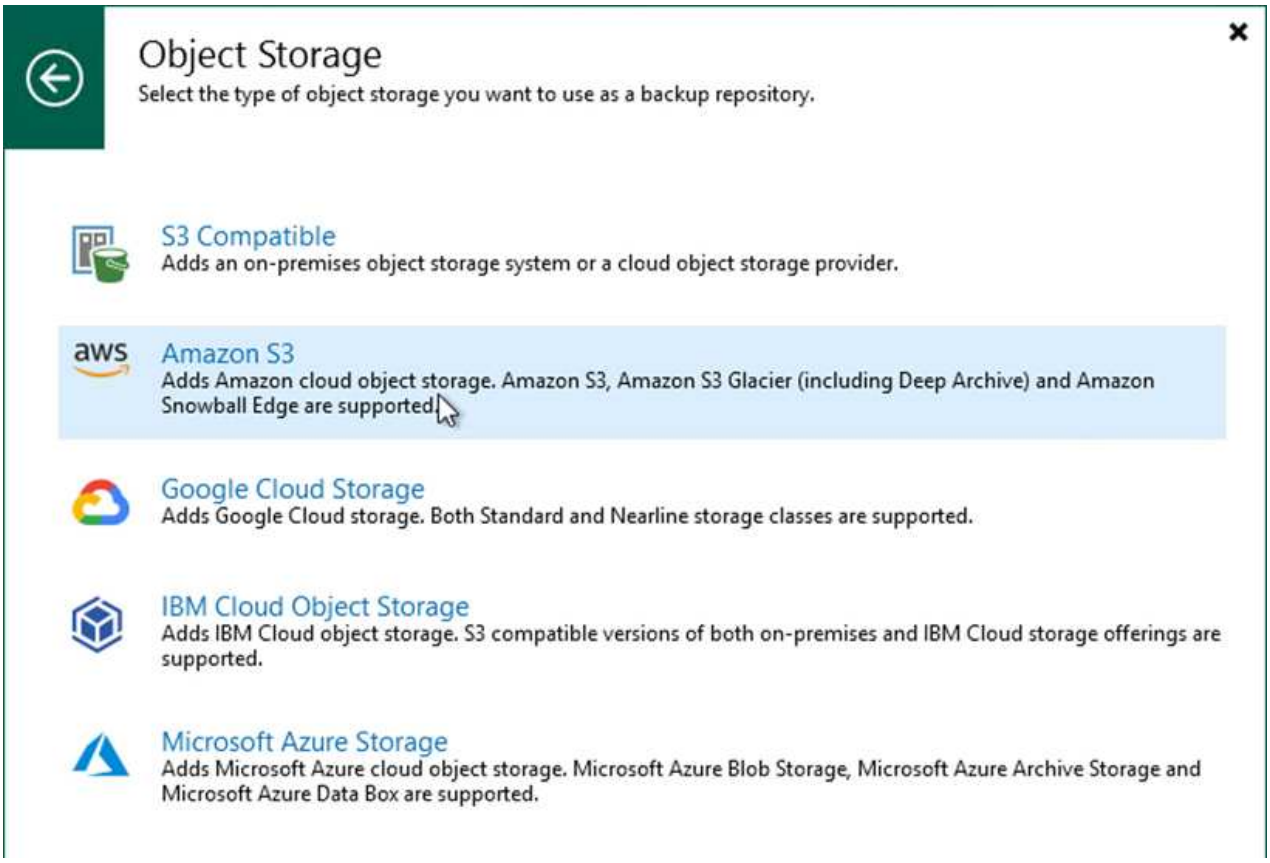
Desde el servidor de Veeam secundario, importe los backups desde el almacenamiento S3 y restaure las máquinas virtuales de SQL Server y Oracle al clúster de VMware Cloud.

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

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

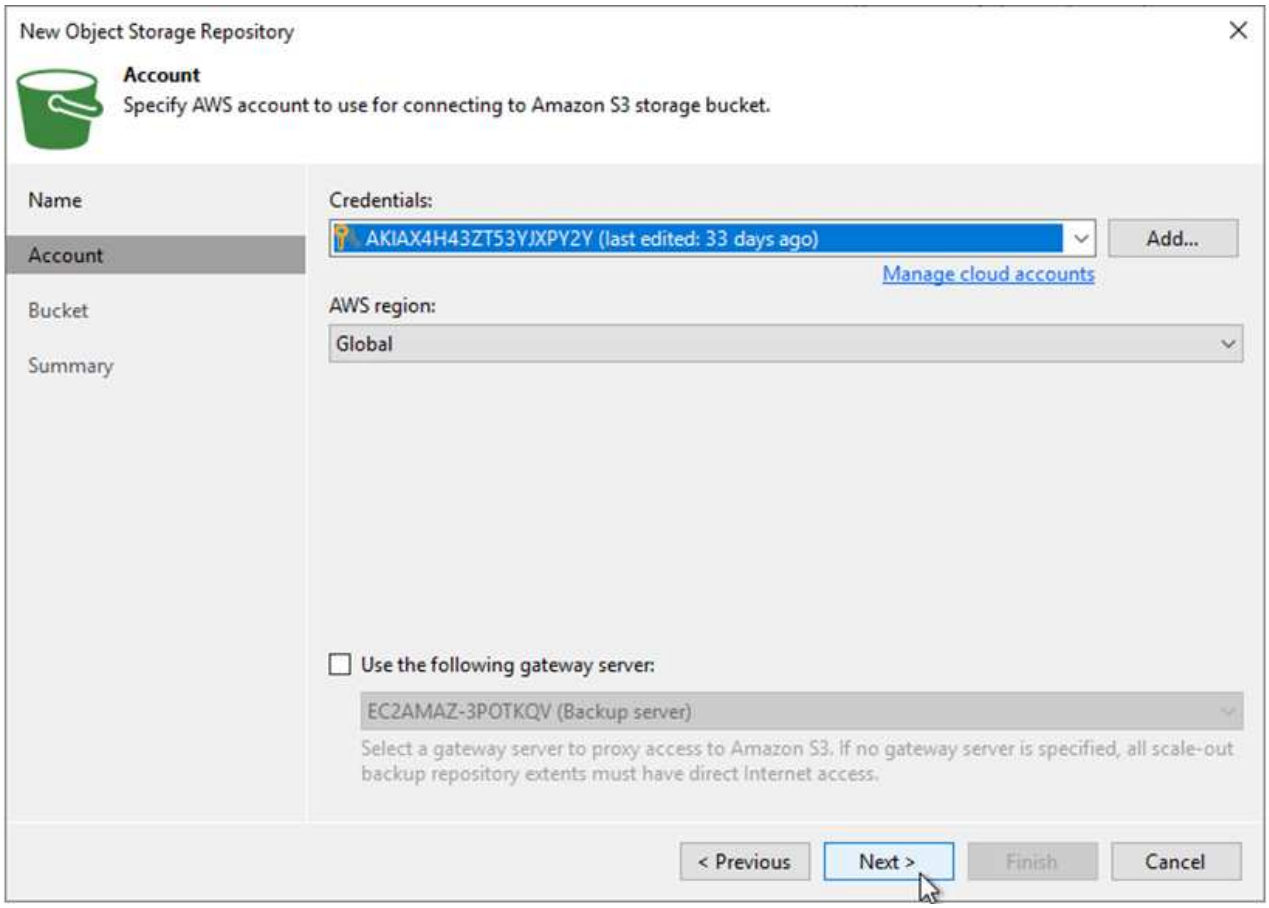


2. Seleccione Amazon S3 como tipo de almacenamiento de objetos.

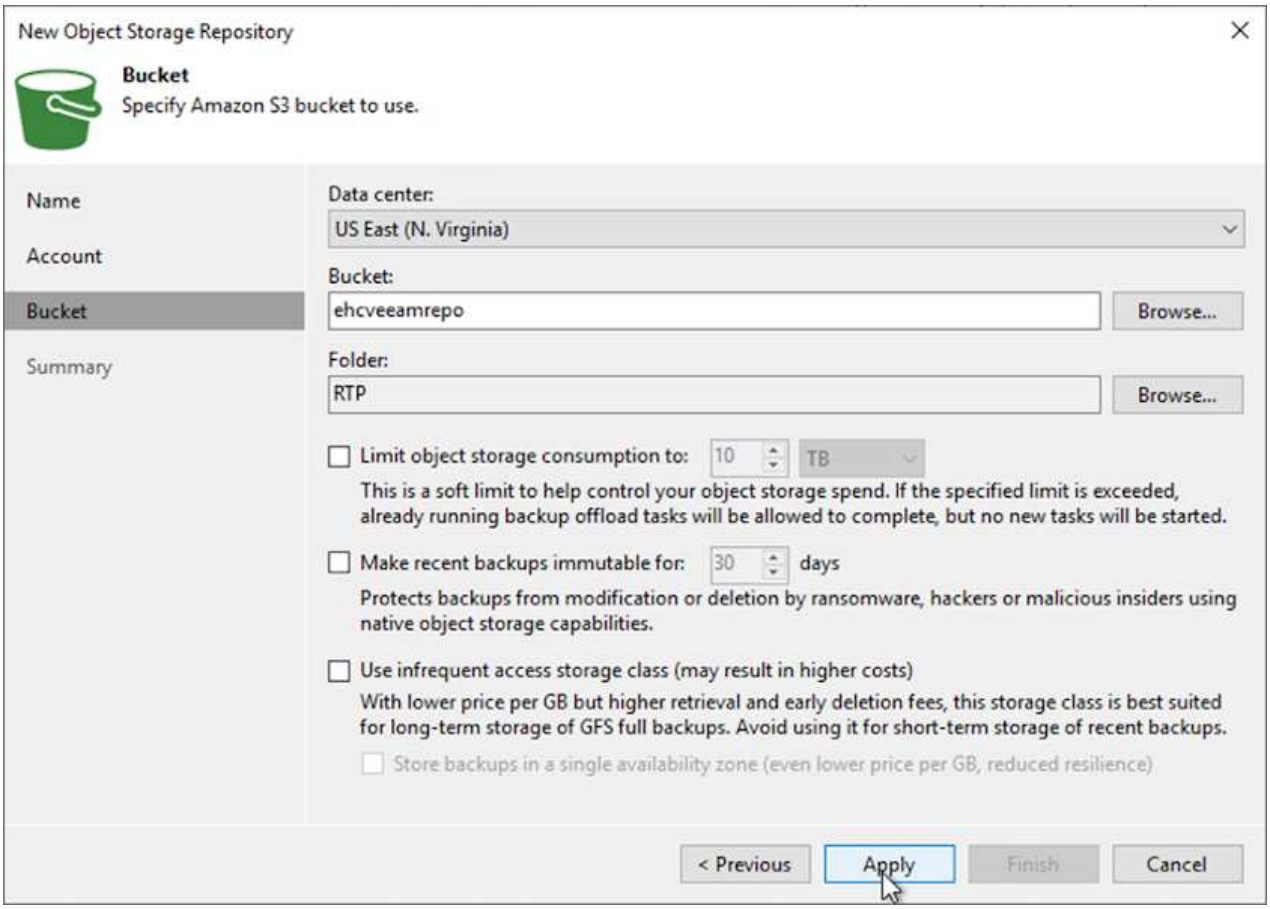


3. En la lista de Amazon Cloud Storage Services, seleccione Amazon S3.

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



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

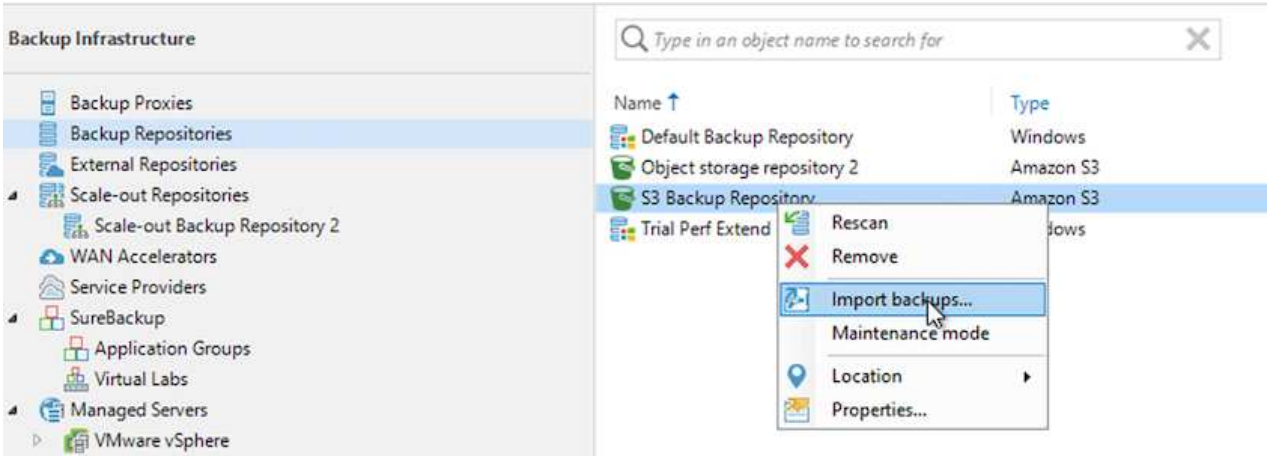


6. Finalmente, seleccione Finalizar para completar el proceso y agregar el repositorio.

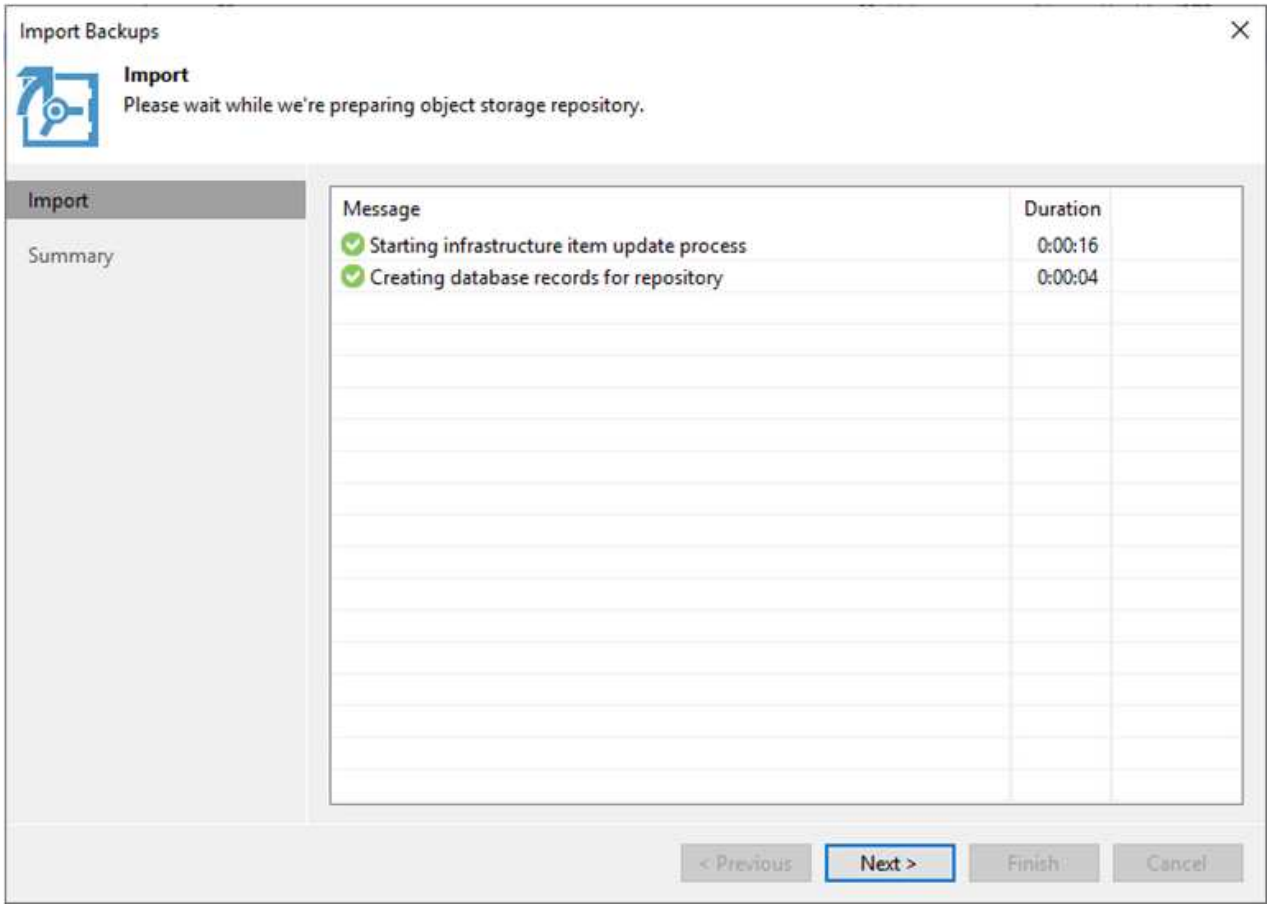
Importe los backups desde el almacenamiento de objetos S3

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

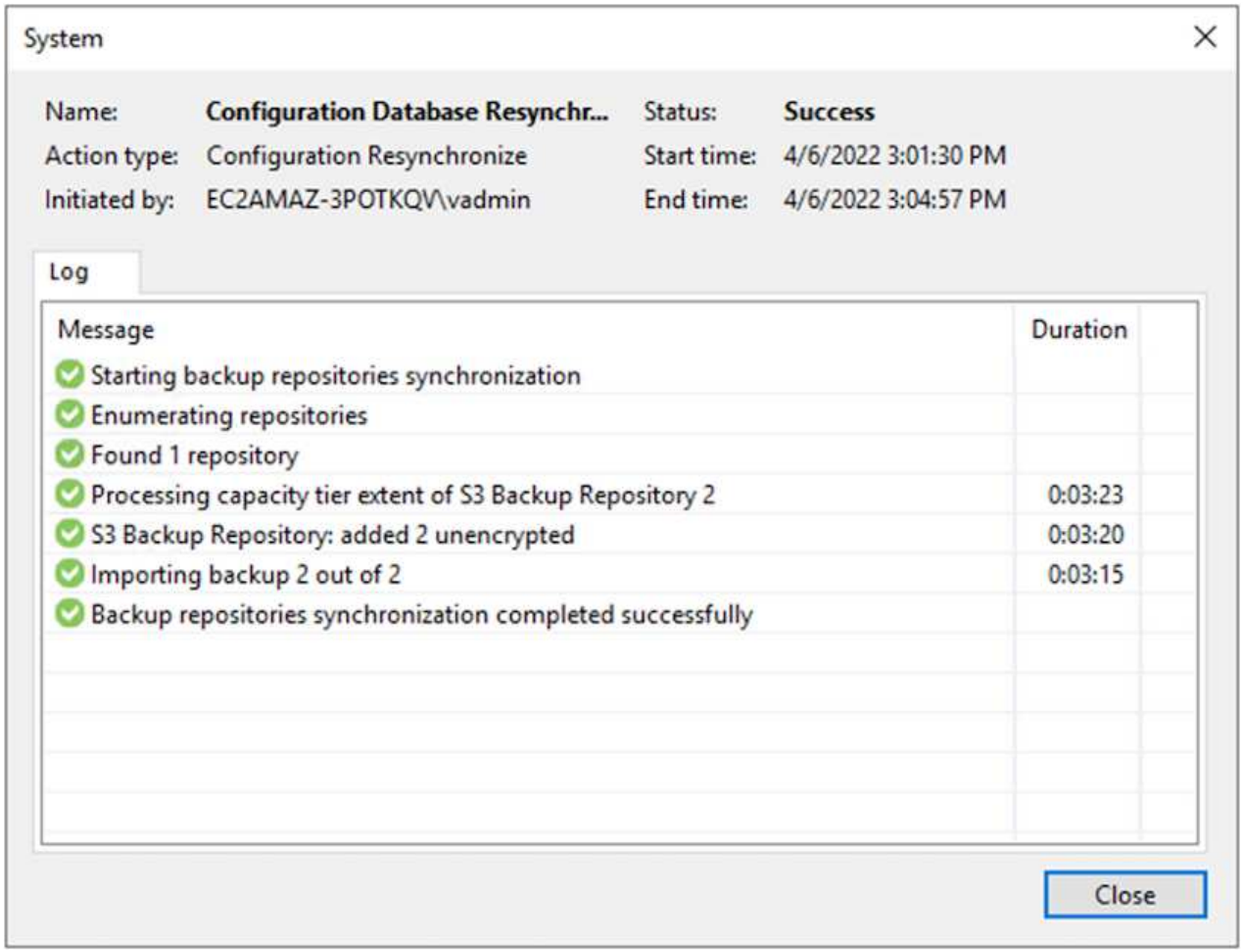
1. En el repositorio de backup de S3, seleccione Import backups para abrir el asistente Import backups.



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



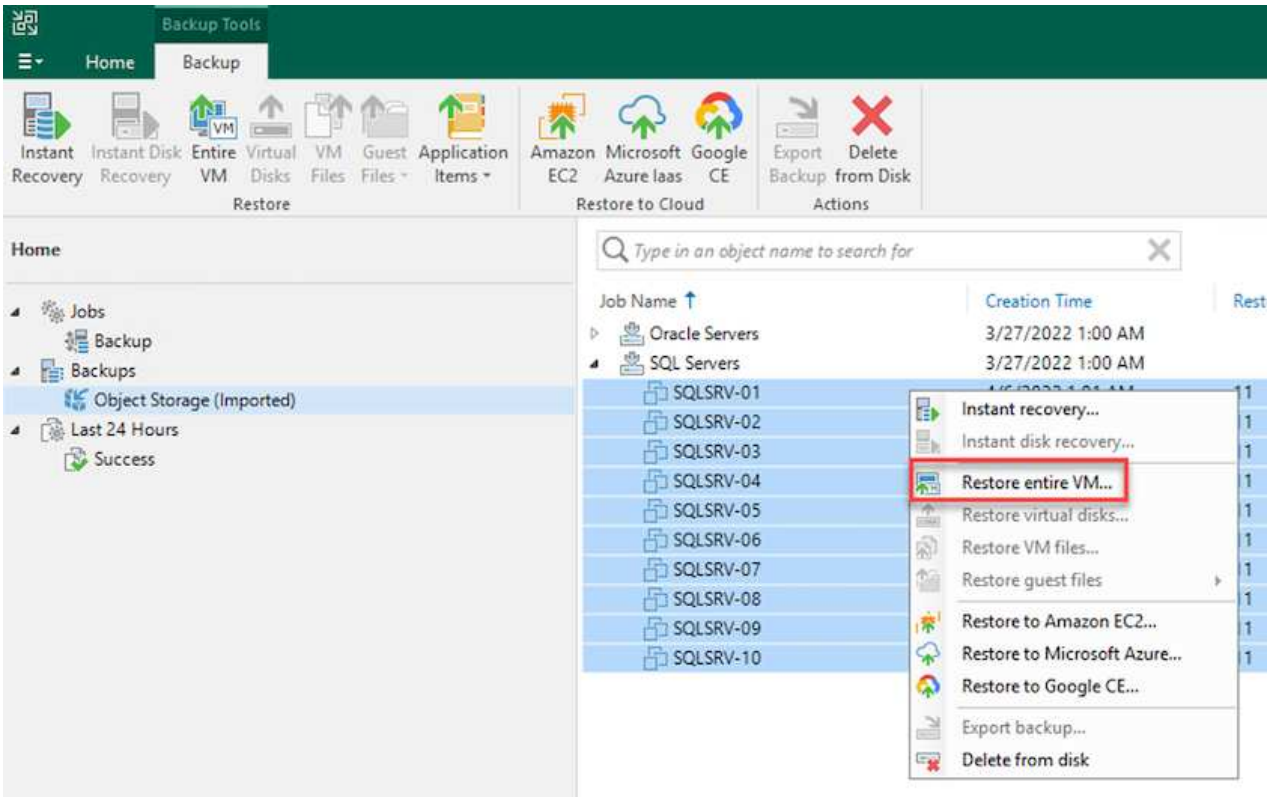
3. Una vez finalizada la importación, puede restaurar máquinas virtuales en el clúster de cloud de VMware.


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

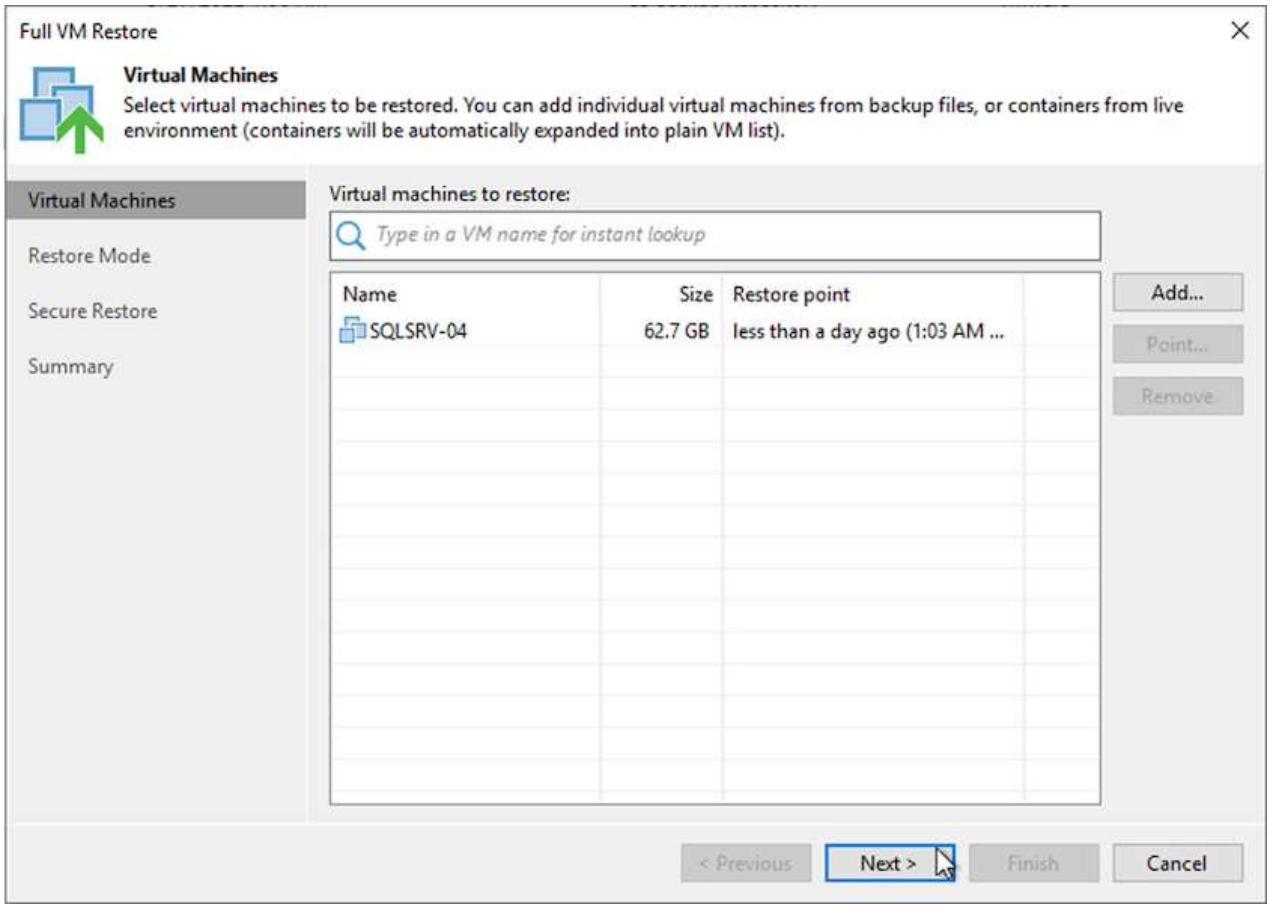
Restaure equipos virtuales de aplicación con la funcionalidad de restauración completa de Veeam en VMware Cloud

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

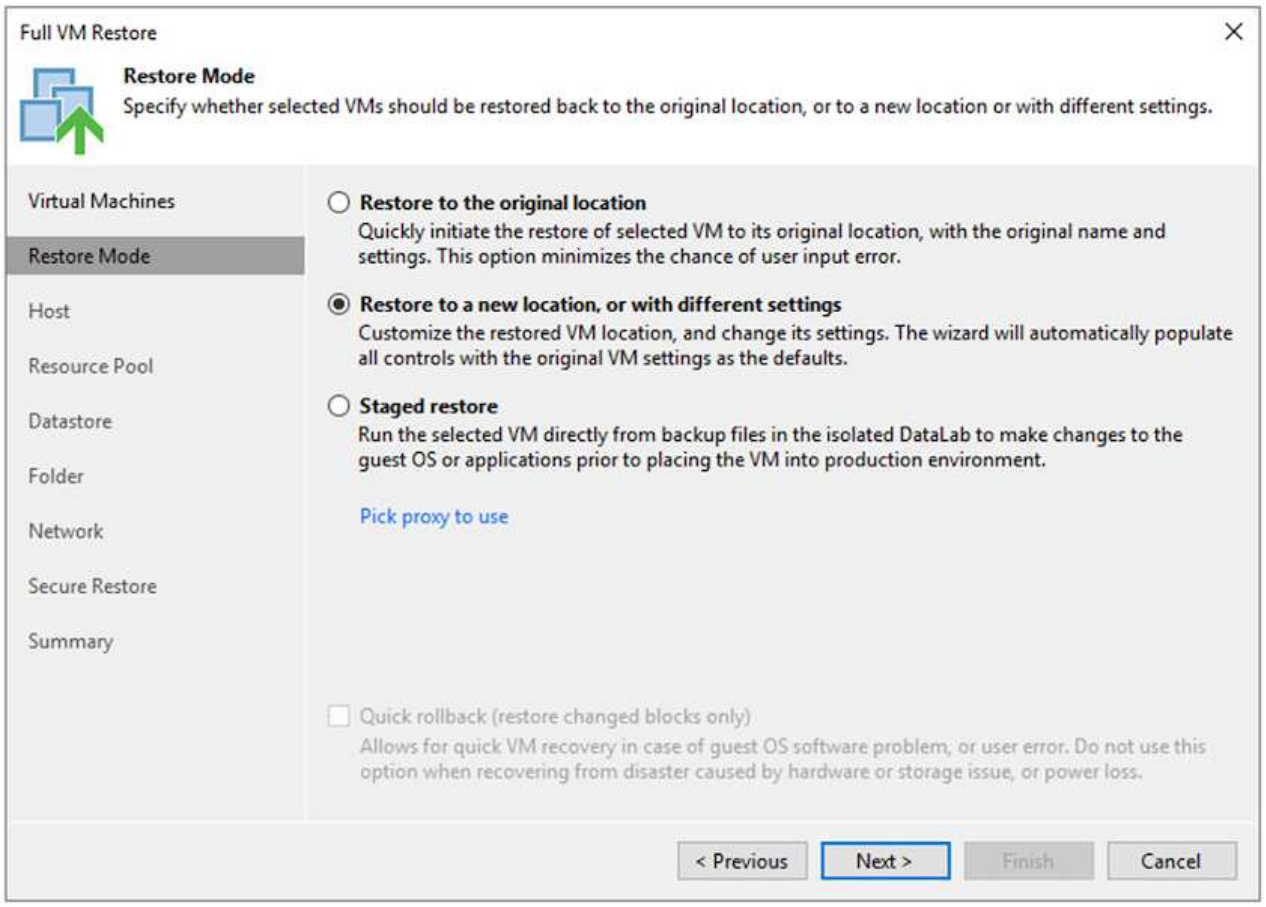
1. En la página Veeam Home, seleccione el almacenamiento de objetos que contiene los backups importados, seleccione las máquinas virtuales que desea restaurar y, a continuación, haga clic con el botón derecho en Restore entire VM.



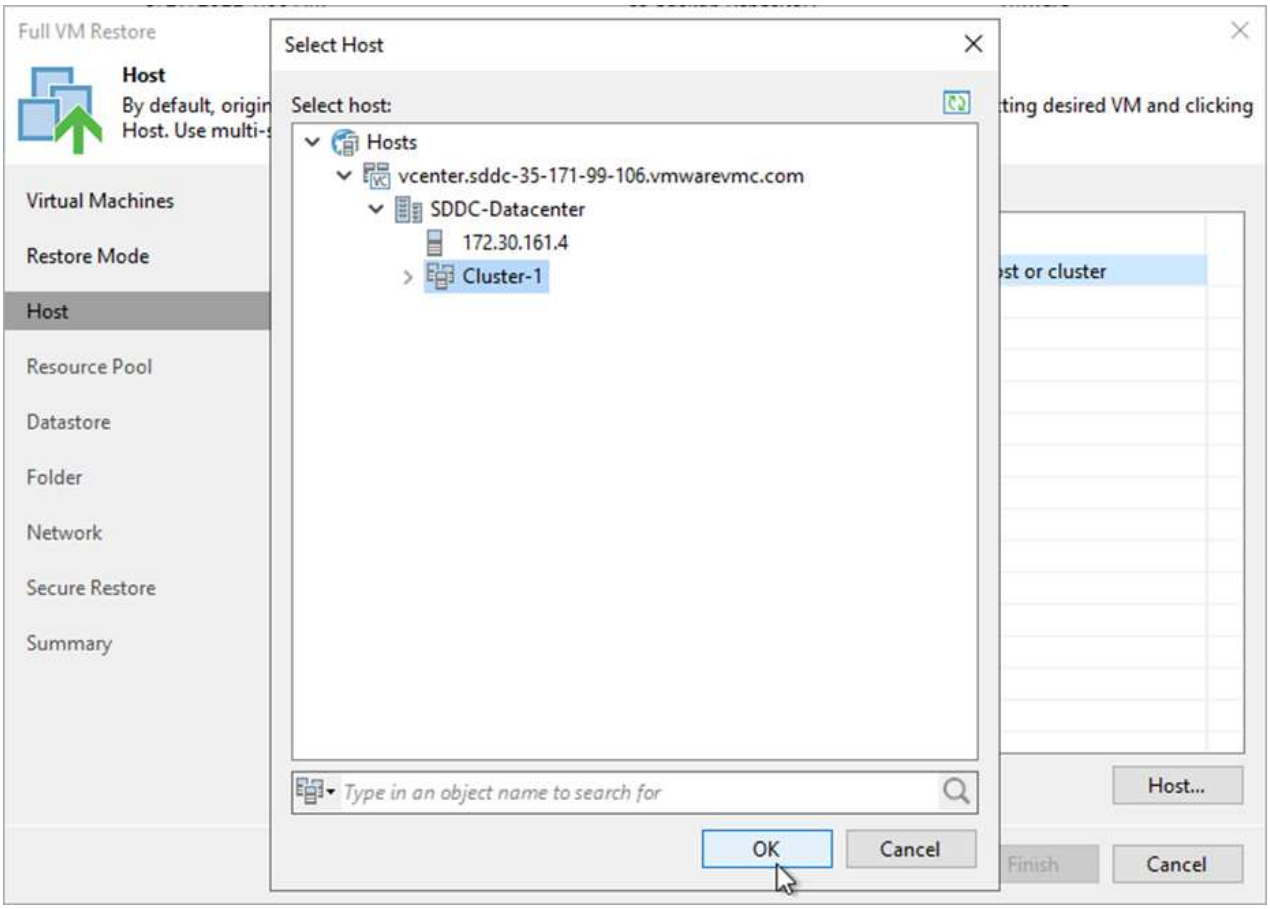
2. En la primera página del asistente Full VM Restore, modifique las máquinas virtuales para realizar el backup si lo desea y seleccione Next.



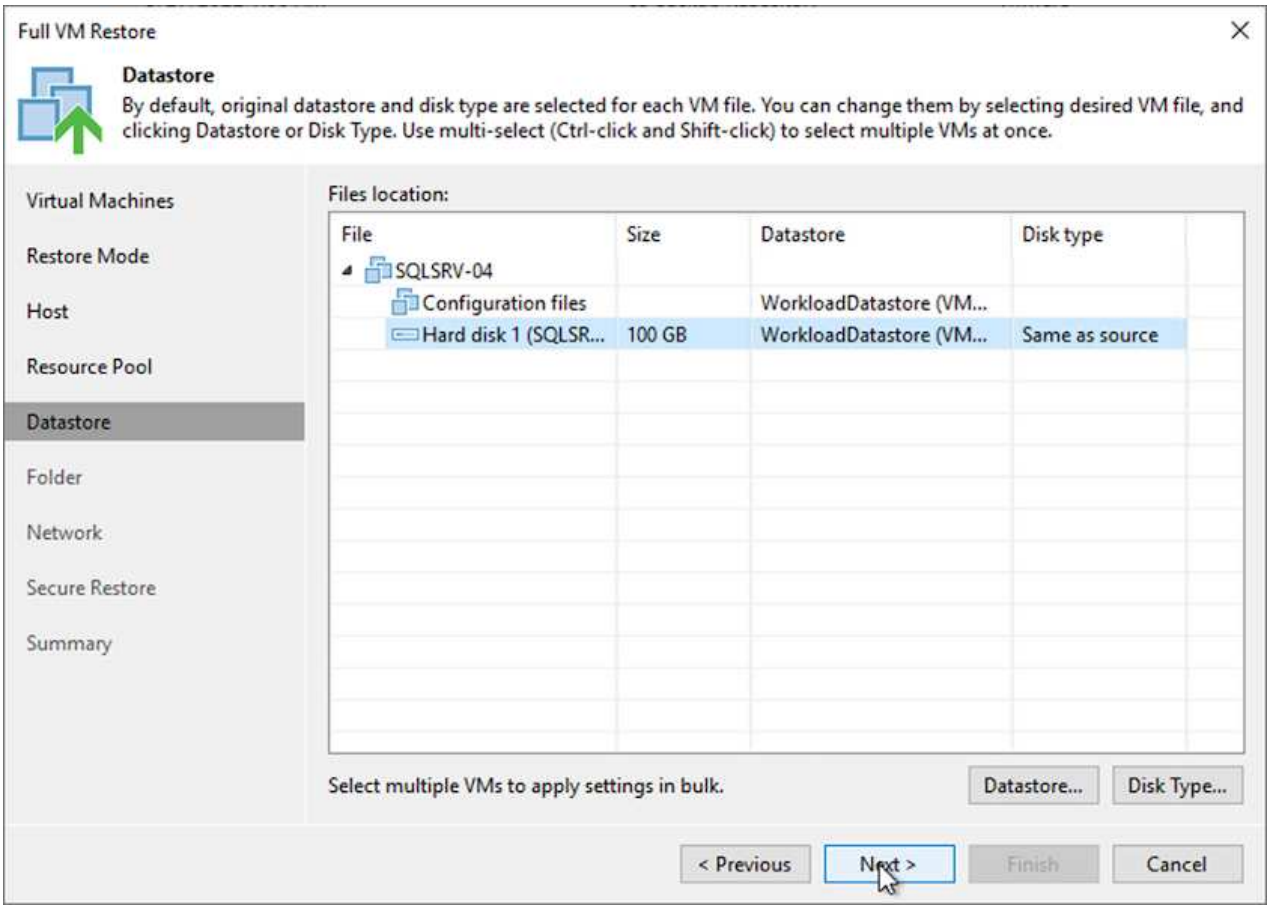
3. En la página Restore Mode, seleccione Restore to a New Location o with Disfruta de una configuración diferente.



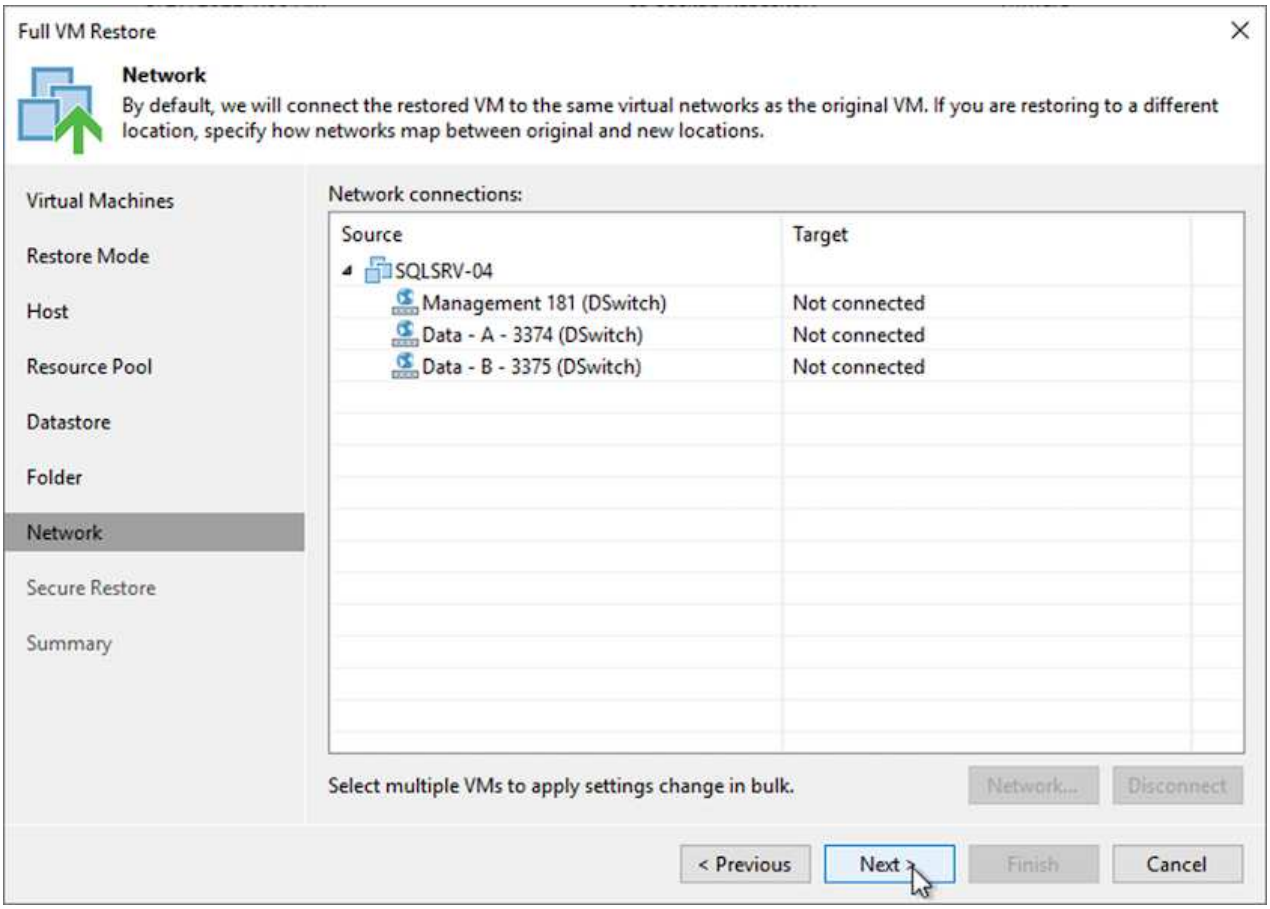
4. En la página host, seleccione el host o el clúster de destino ESXi al que desea restaurar la máquina virtual.

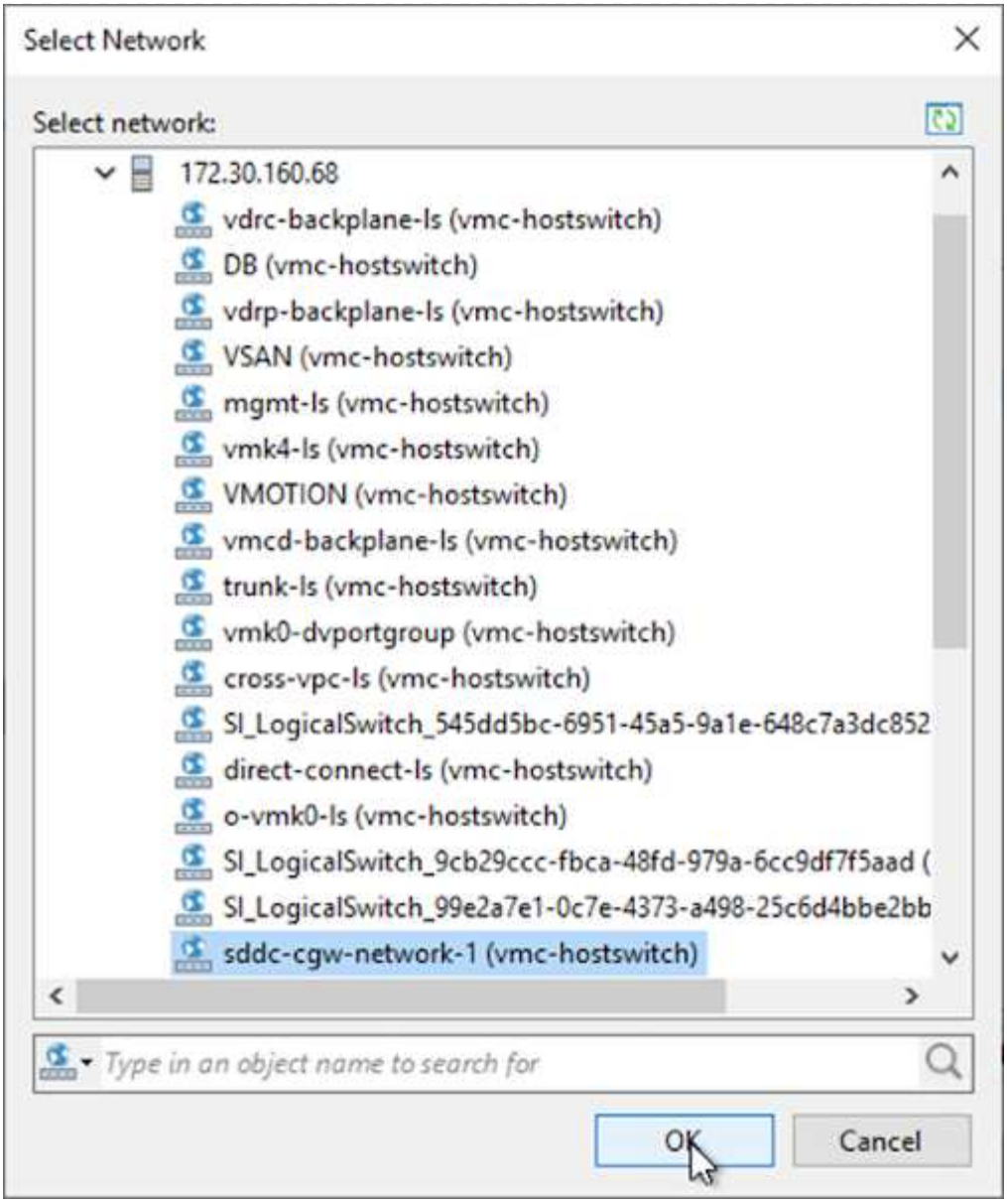


5. En la página datastores, seleccione la ubicación del almacén de datos de destino para los archivos de configuración y el disco duro.



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


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



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

Restauración de datos de aplicaciones de SQL Server

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

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

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

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

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

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

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

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

Configurar almacenamiento FSX para la restauración de SQL Server

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

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

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

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

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

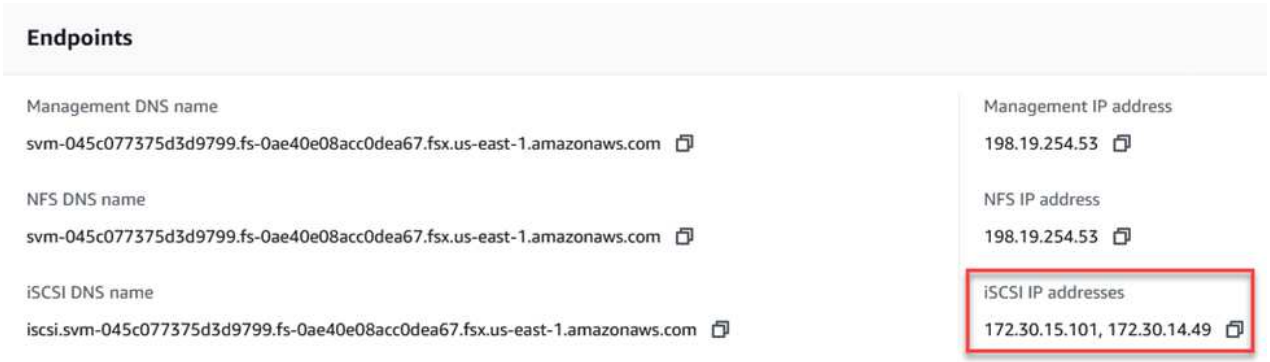
3. Finalmente, asigne las LUN al iGroup que acaba de crear:

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

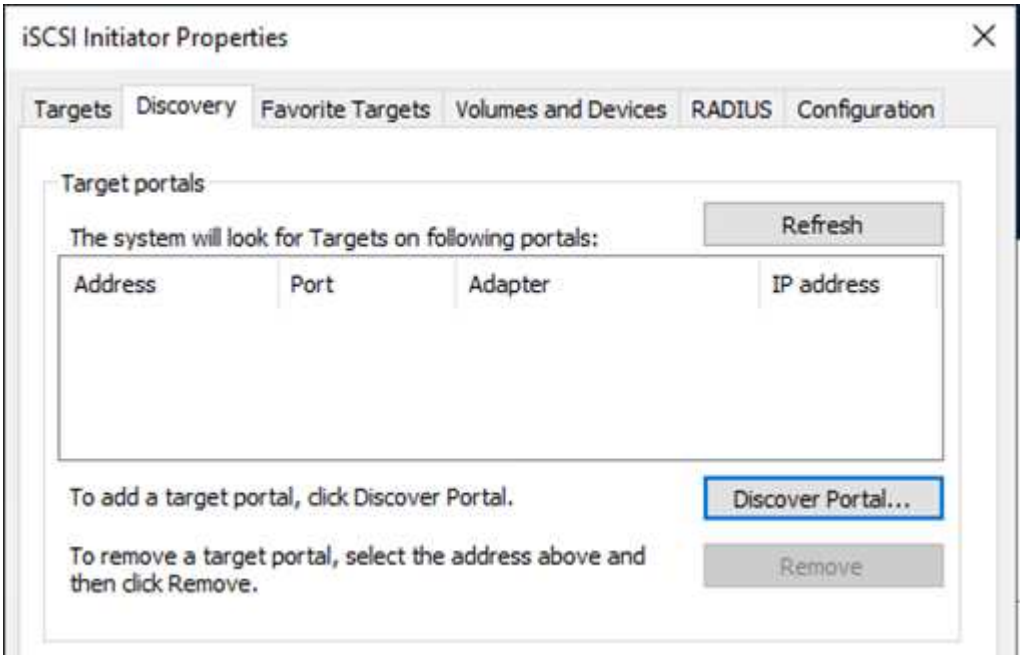
4. Para encontrar el nombre de ruta, ejecute el `lun show` comando.

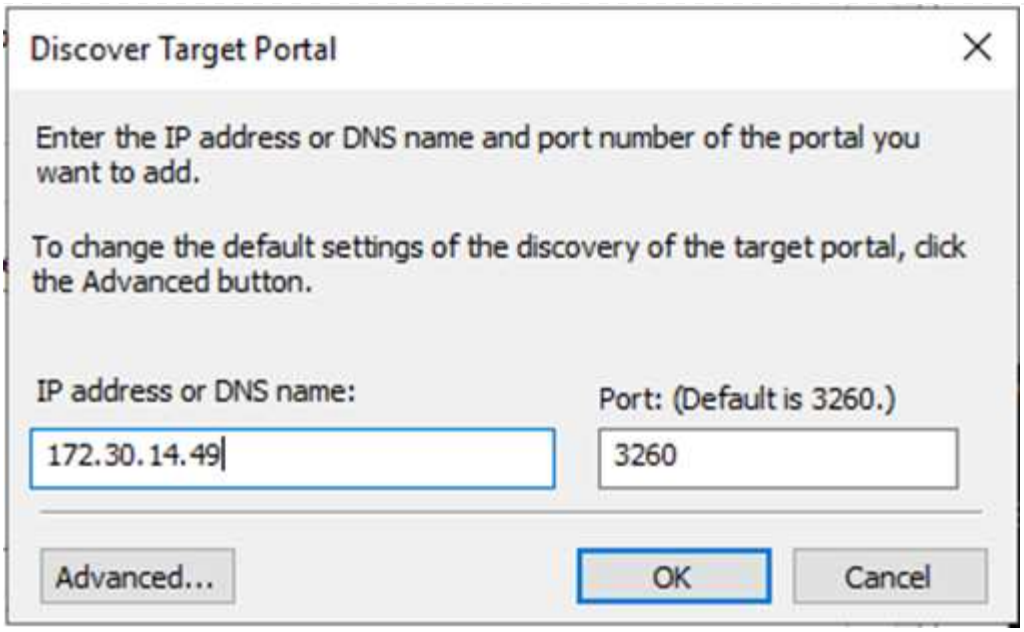
Configure la máquina virtual de Windows para acceder a iSCSI y detectar los sistemas de archivos

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

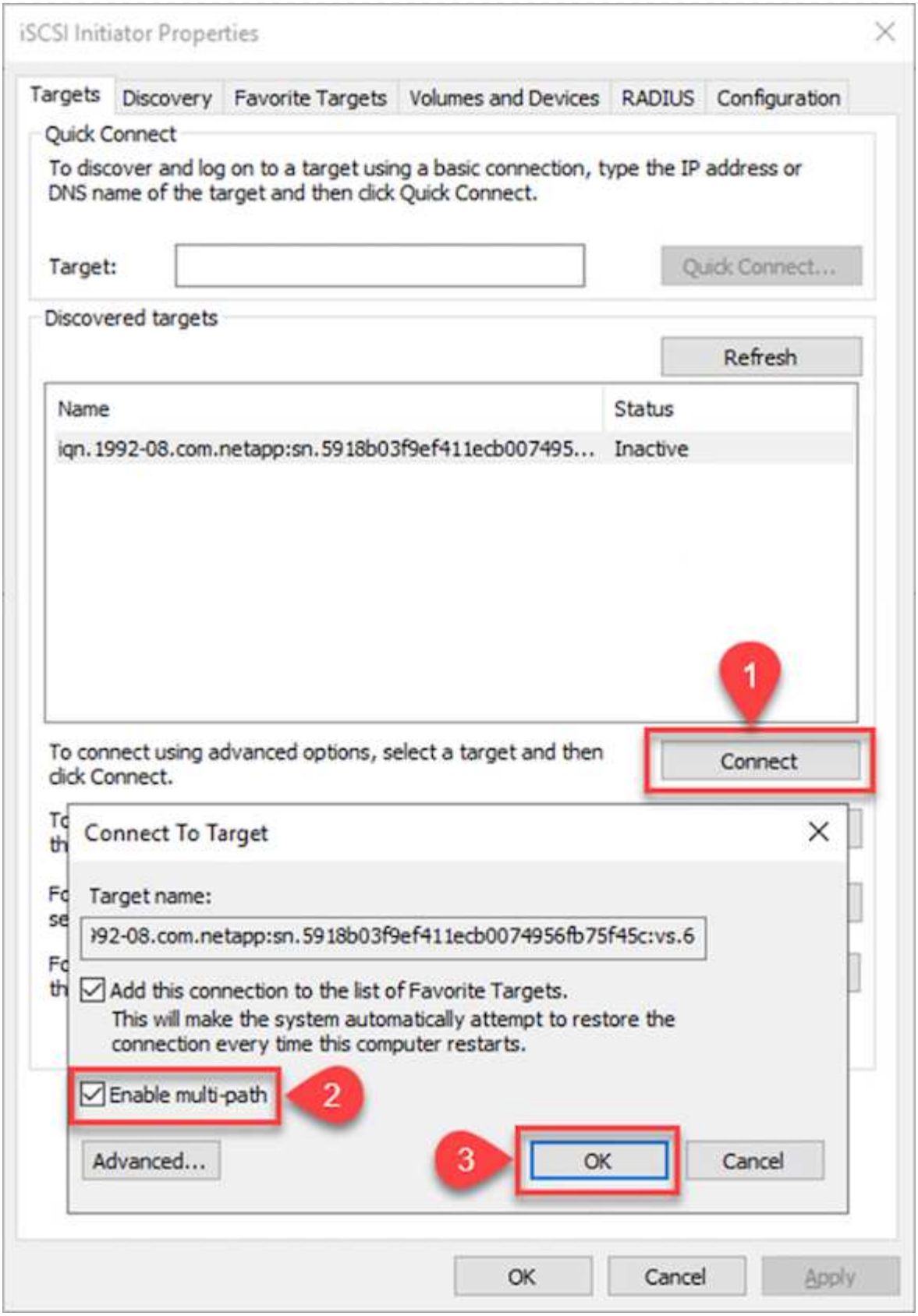


4. En la pestaña Discovery, haga clic en Discover Portal e introduzca las direcciones IP para los destinos iSCSI de FSX.

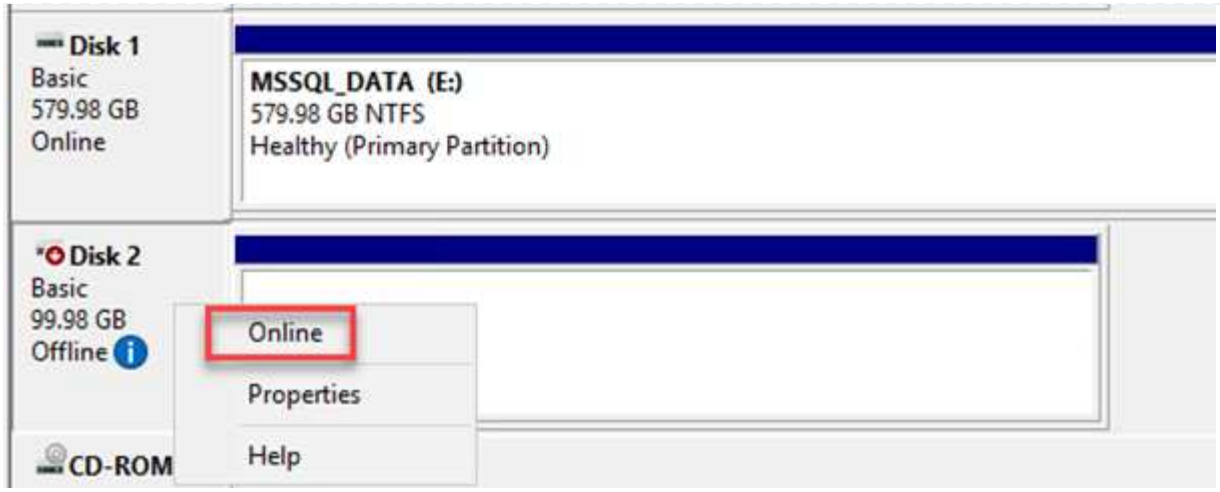




5. En la ficha destino, haga clic en conectar, seleccione Activar Multi-Path si es apropiado para su configuración y, a continuación, haga clic en Aceptar para conectarse al destino.

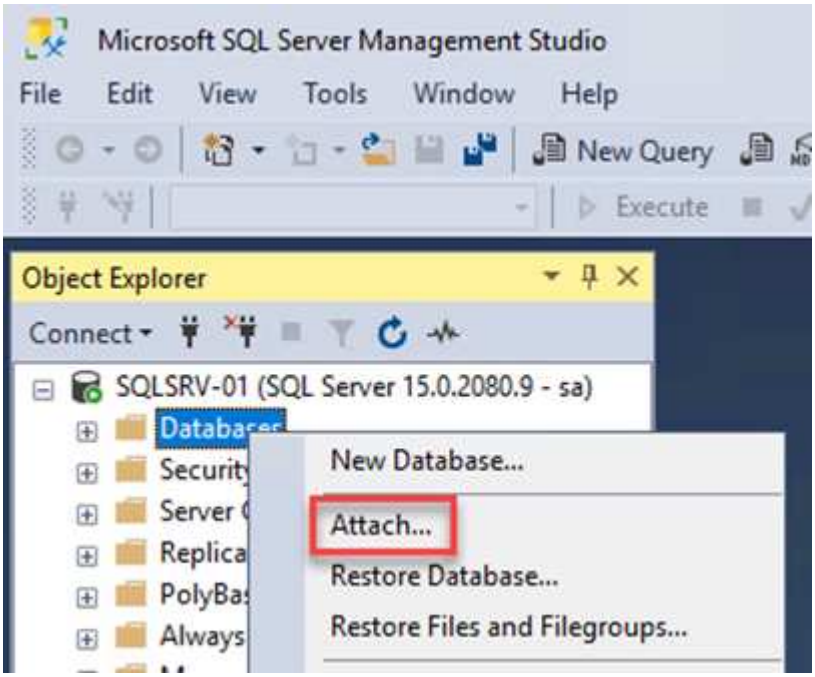


6. Abra la utilidad Administración de equipos y ponga los discos en línea. Compruebe que conservan las mismas letras de unidad que tenían anteriormente.

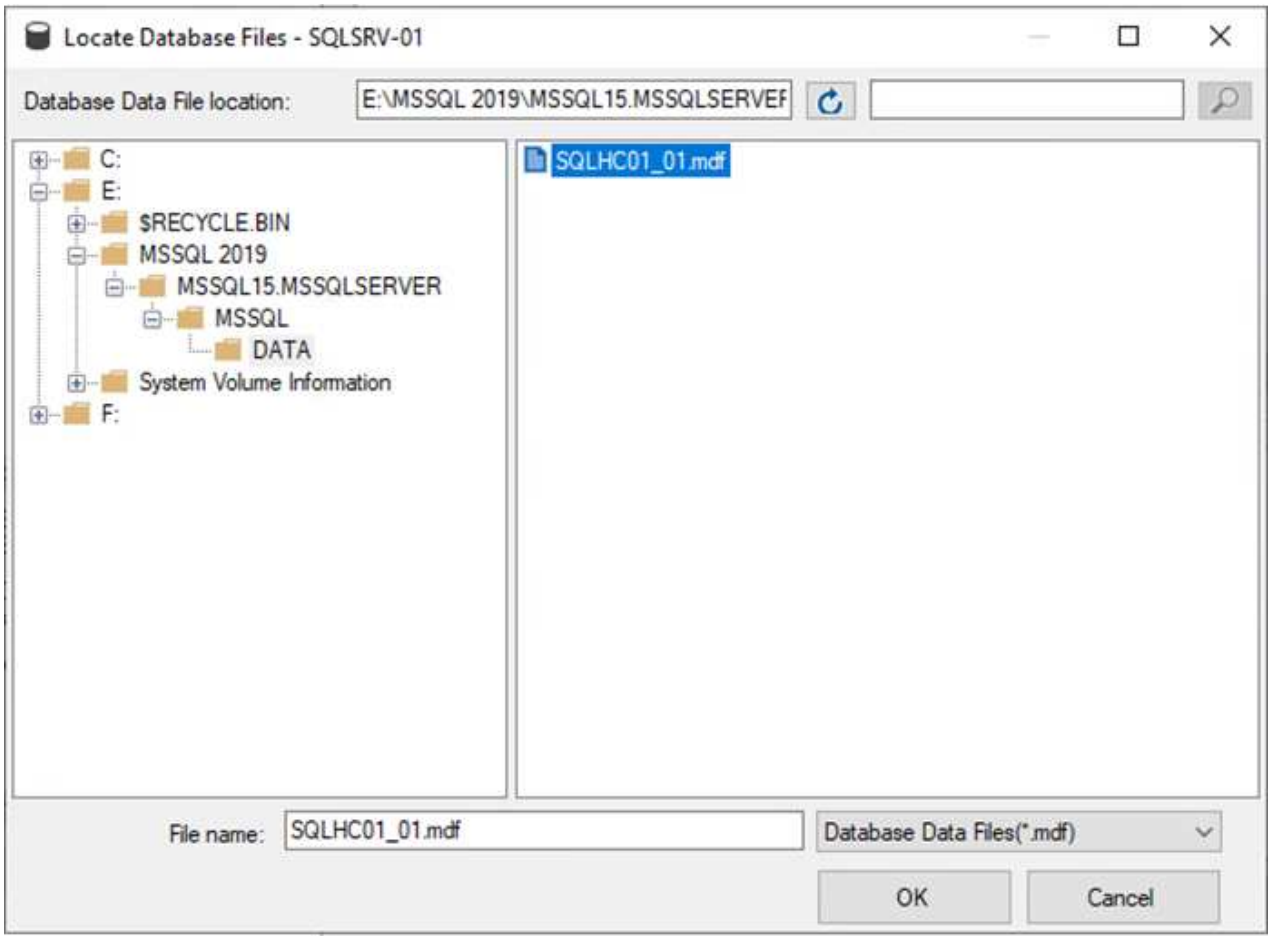

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Conecte las bases de datos de SQL Server

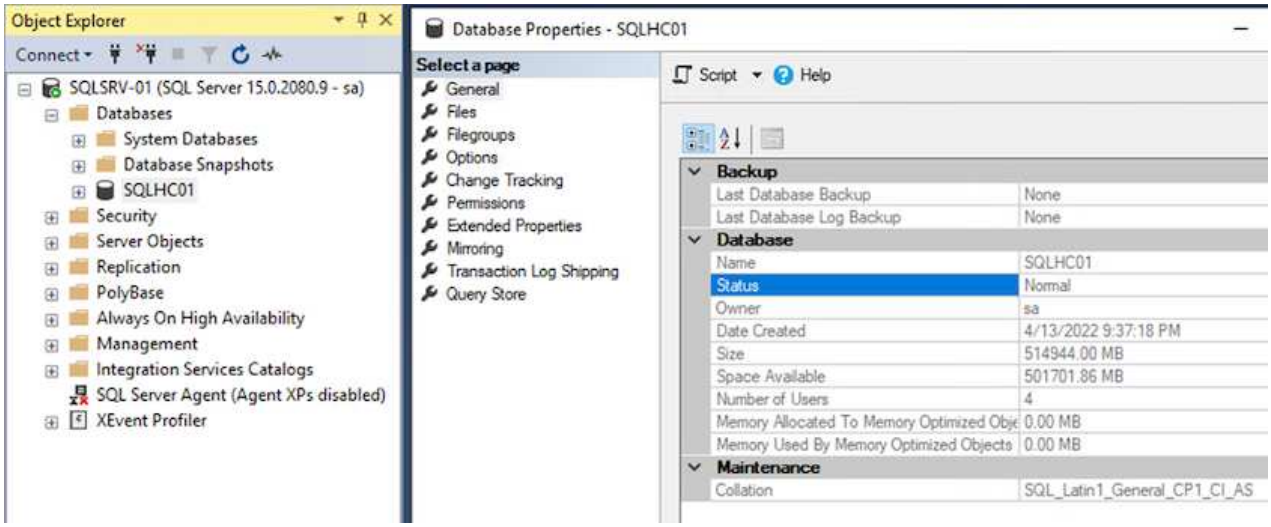
1. En la máquina virtual de SQL Server, abra Microsoft SQL Server Management Studio y seleccione Attach para iniciar el proceso de conexión a la base de datos.



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



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

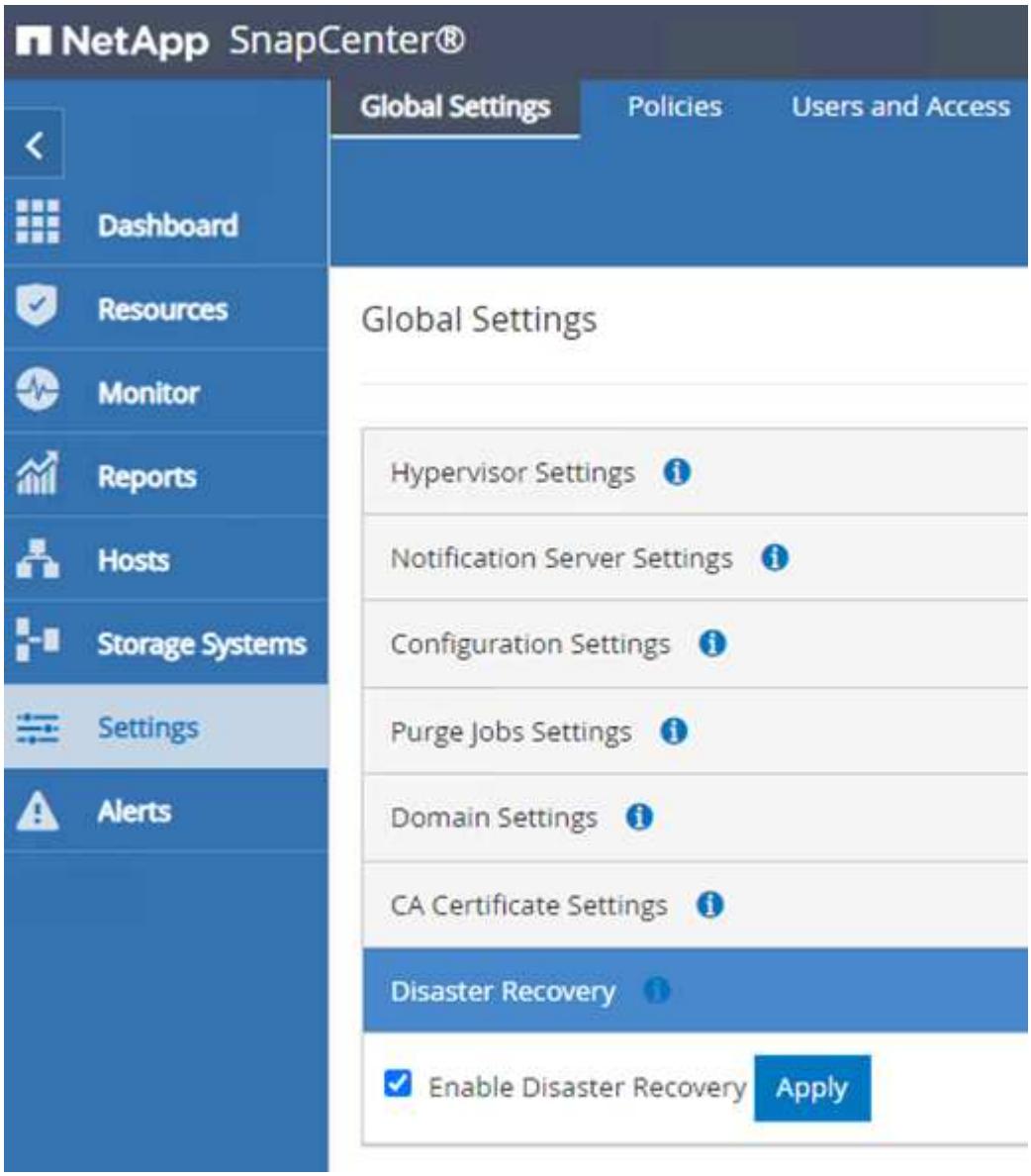


Confirme la comunicación de SnapCenter con el plugin de SQL Server

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

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

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



Restaure los datos de la aplicación Oracle

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

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

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

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

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

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

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

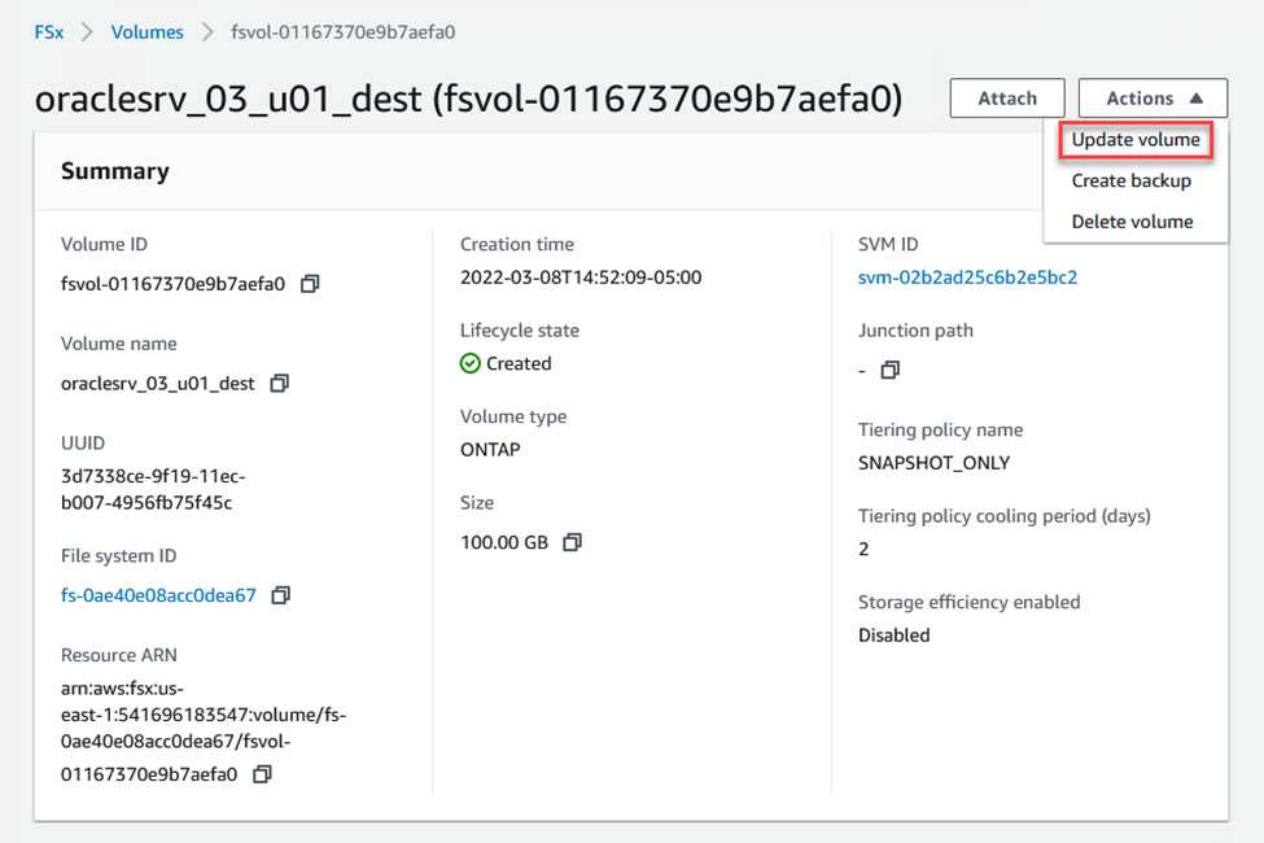
```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1   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

FsxId0ae40e08acc0dea67::>
```

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

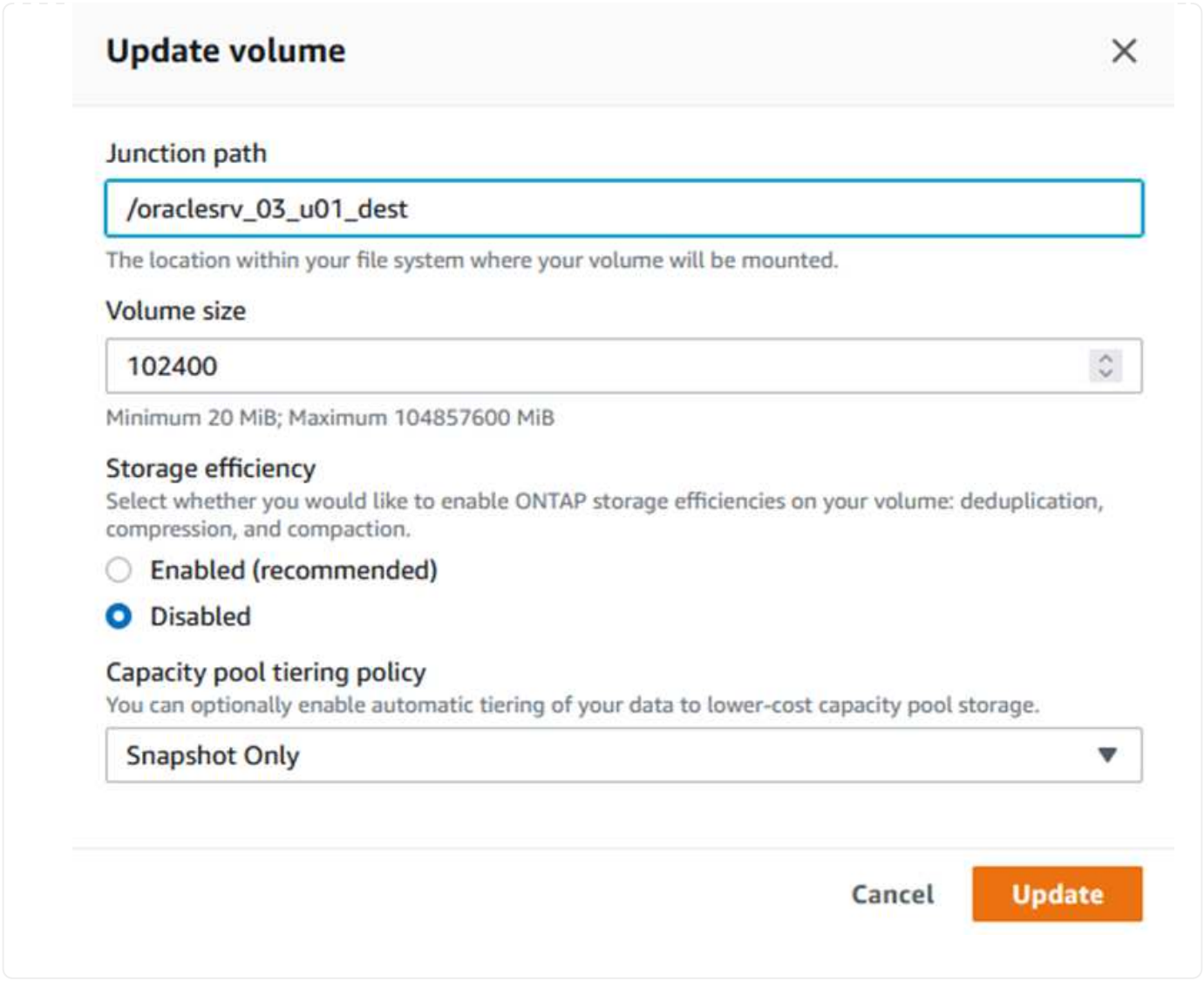
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

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

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

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



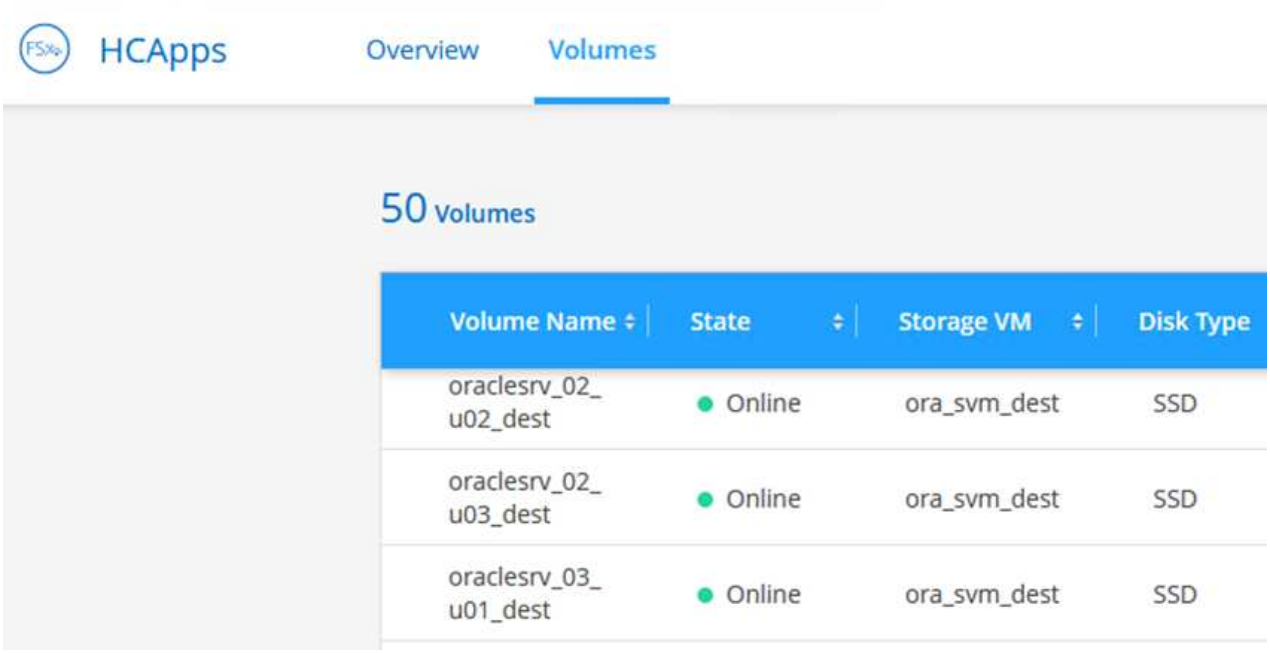
4. Añada el nombre de la ruta de unión y haga clic en Update. Especifique esta ruta de unión cuando monte el volumen NFS desde el servidor de Oracle.


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

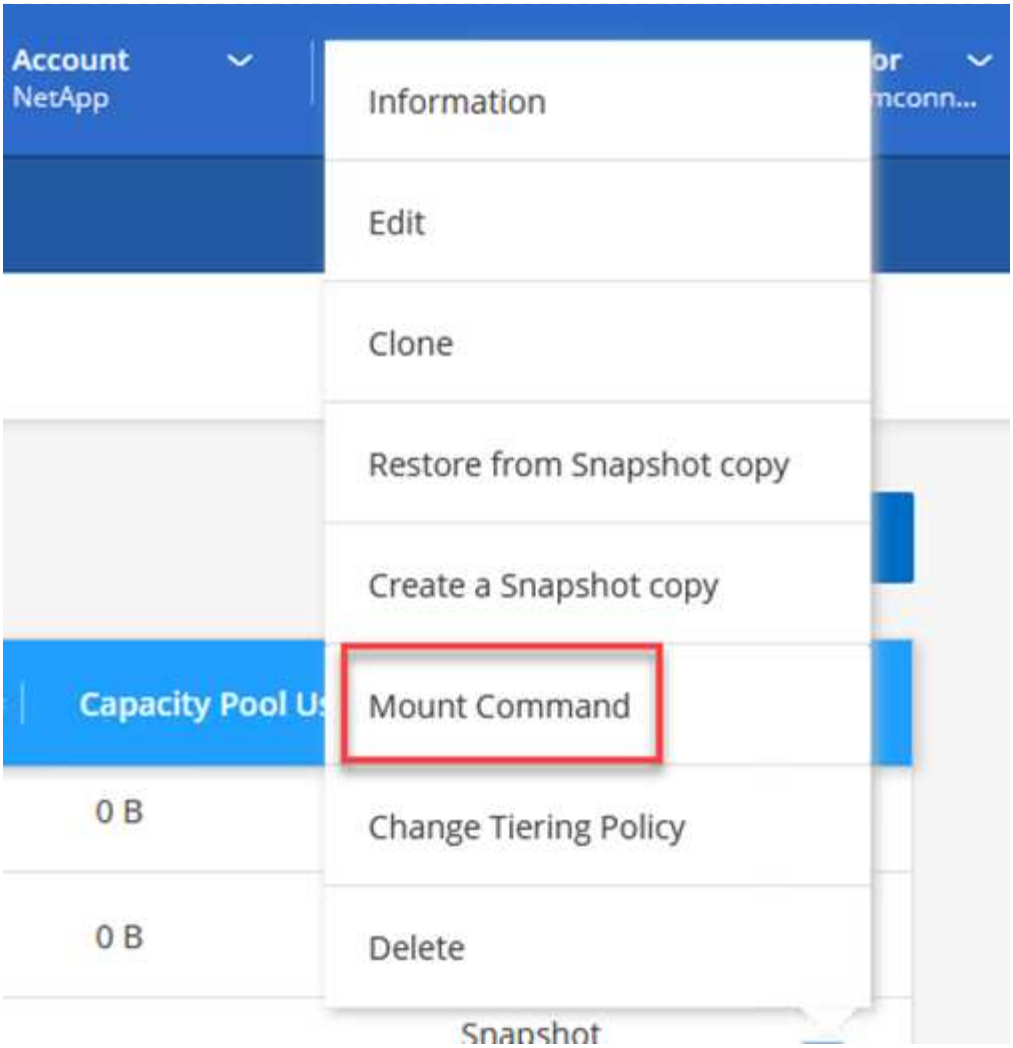
Montar volúmenes de NFS en Oracle Server

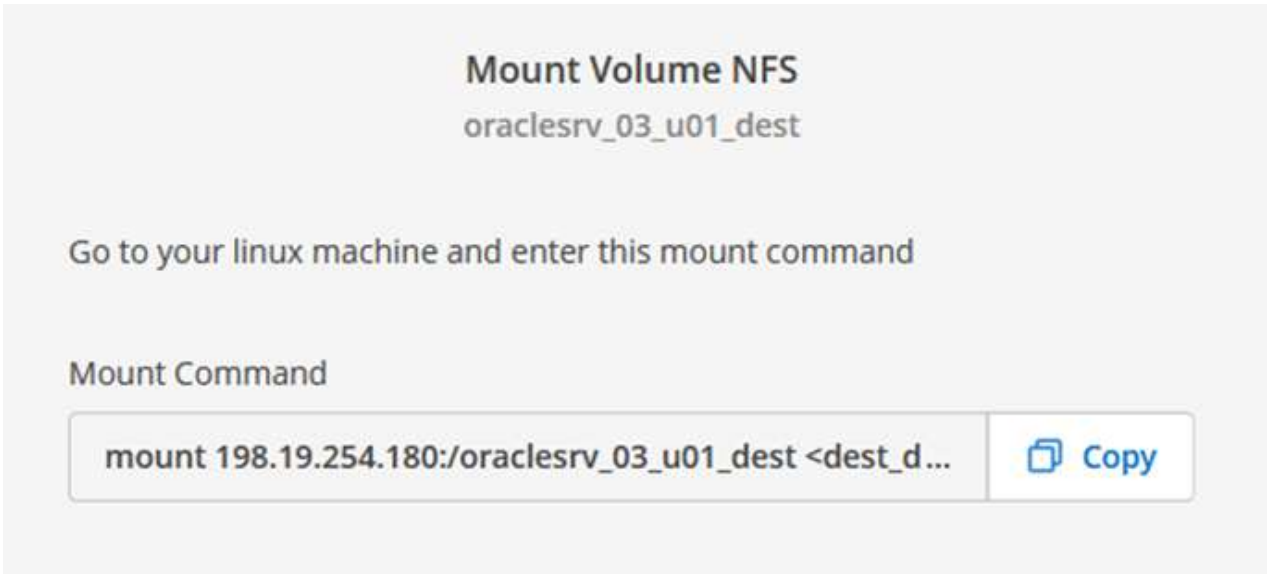
En Cloud Manager, puede obtener el comando de montaje con la dirección IP de LIF NFS correcta para montar los volúmenes NFS que contienen los registros y archivos de la base de datos de Oracle.

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



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





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

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

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

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

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

Conmutación tras recuperación

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

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

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

Conclusión

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

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

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

Dónde encontrar información adicional

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

web:

- Enlaces a la documentación de la solución

  "Multicloud híbrido de NetApp con soluciones de VMware"

  "Soluciones NetApp"

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

Autor: Josh Powell: Ingeniería de soluciones de NetApp

Descripción general

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

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

Casos de uso

Esta solución aborda los siguientes casos prácticos:

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

Almacenes de datos NFS mediante Amazon FSx para ONTAP

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

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

Descripción general de la puesta en marcha de soluciones

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

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

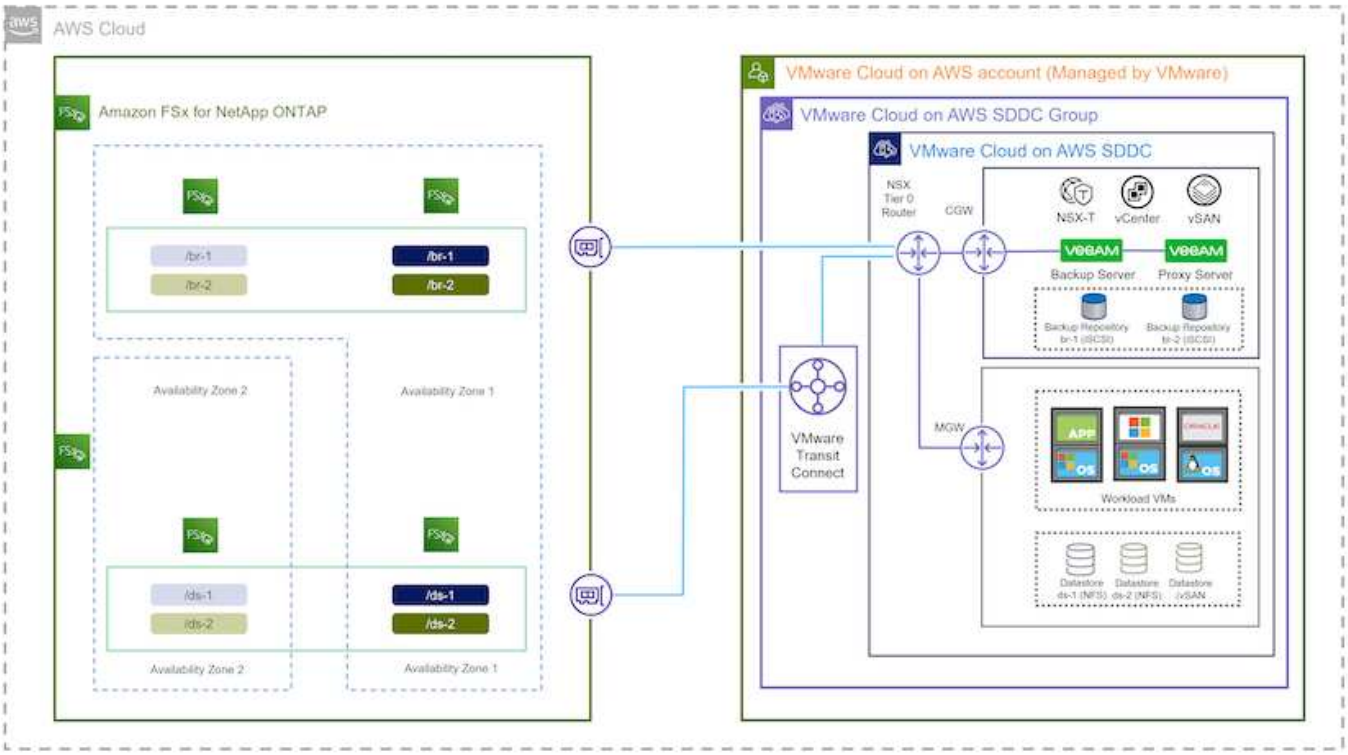
Requisitos previos

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

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

Arquitectura de alto nivel

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



Componentes de hardware/software

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

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

Puesta en marcha de la solución

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

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

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

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

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

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

Implemente el servidor proxy de Veeam

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

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

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

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

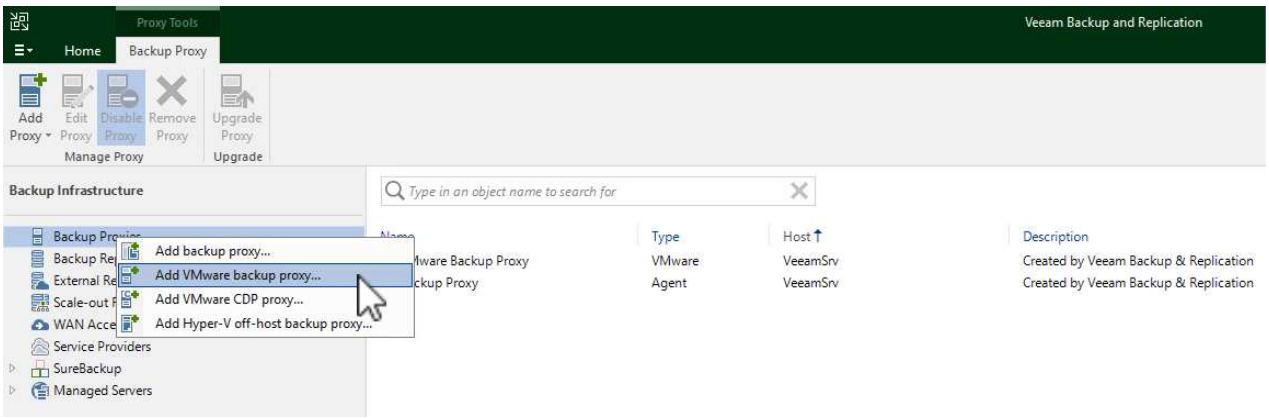
Para obtener más información sobre los modos de transporte, consulte la "Guía del usuario de backup y replicación de Veeam para VMware vSphere".

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

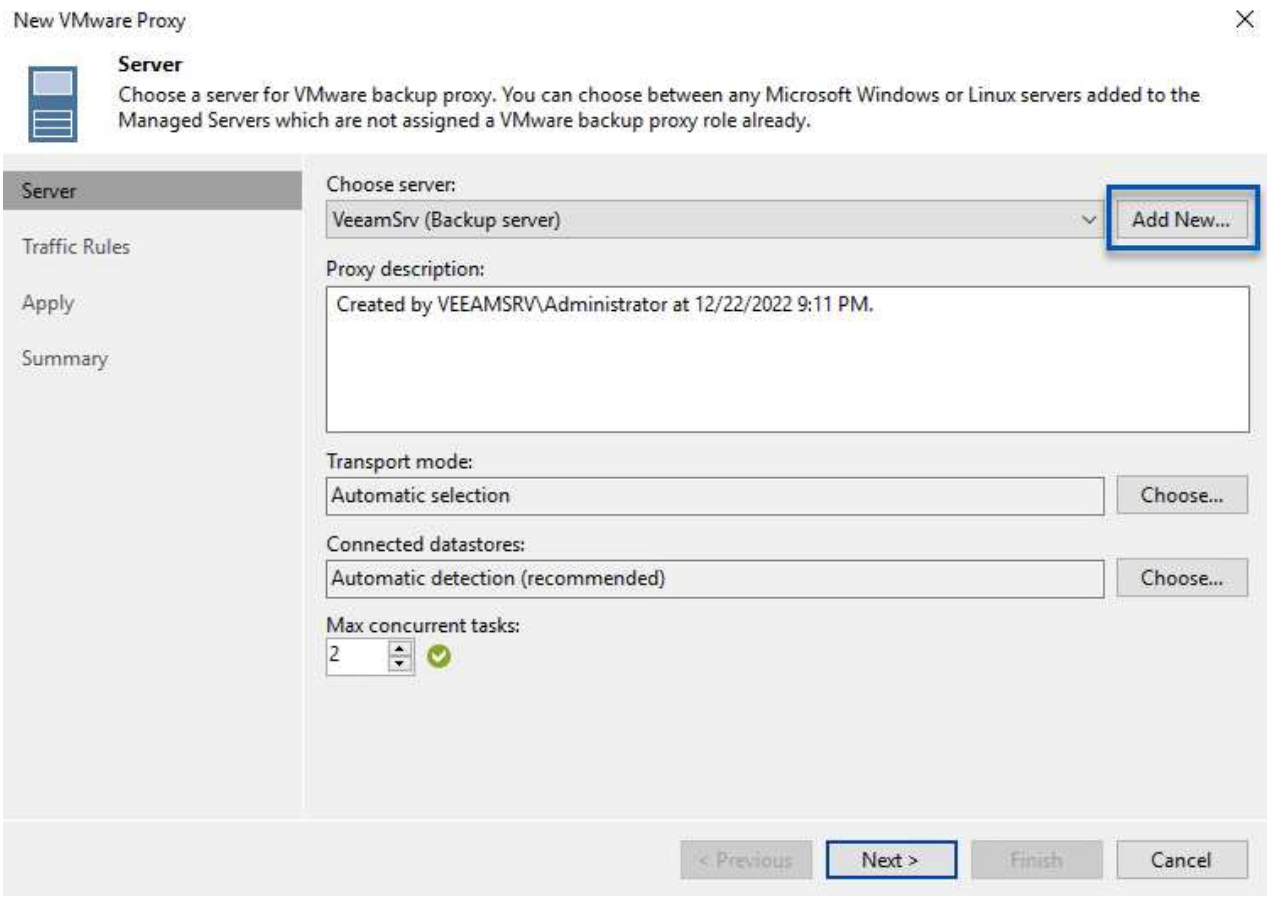
Implemente Veeam Proxy para distribuir las cargas de trabajo de backup

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

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

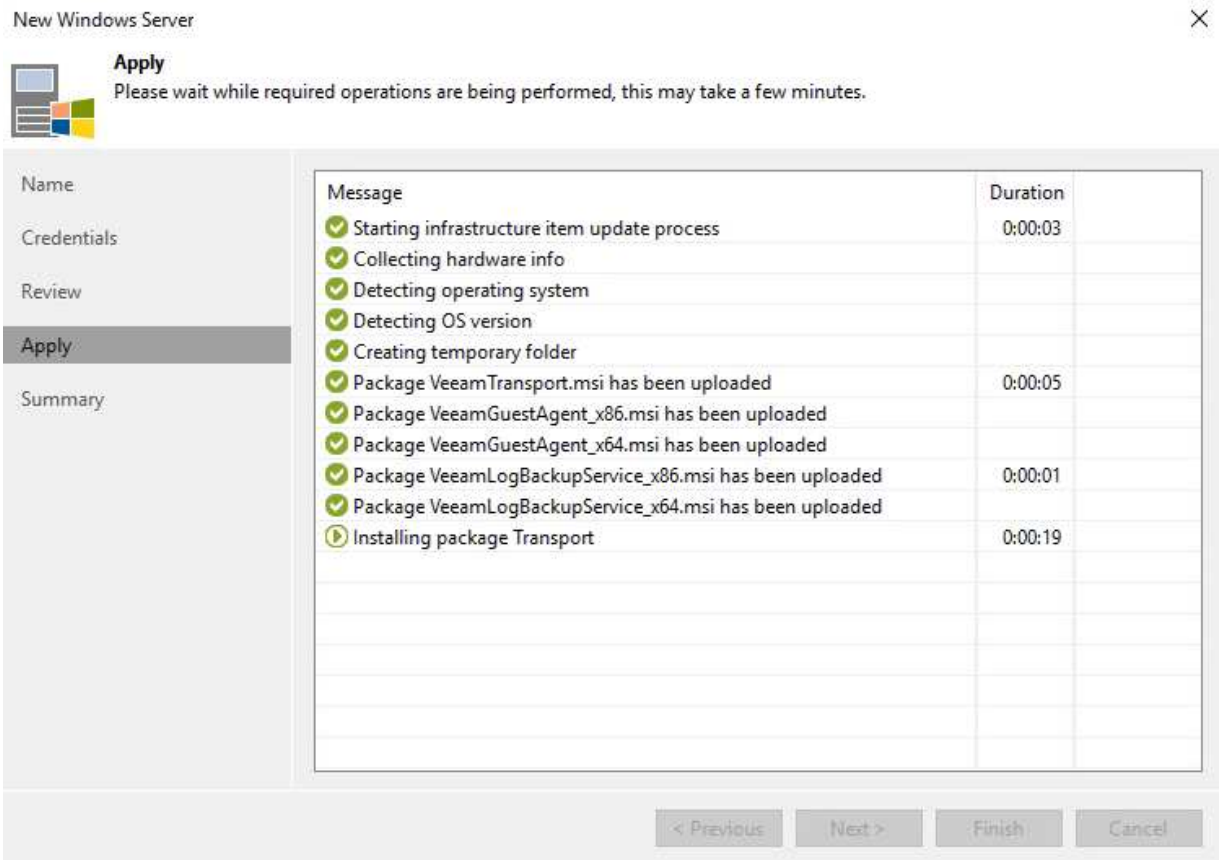


3. En el asistente de **Agregar proxy VMware**, haga clic en el botón **Agregar nuevo…** para agregar un nuevo servidor proxy.

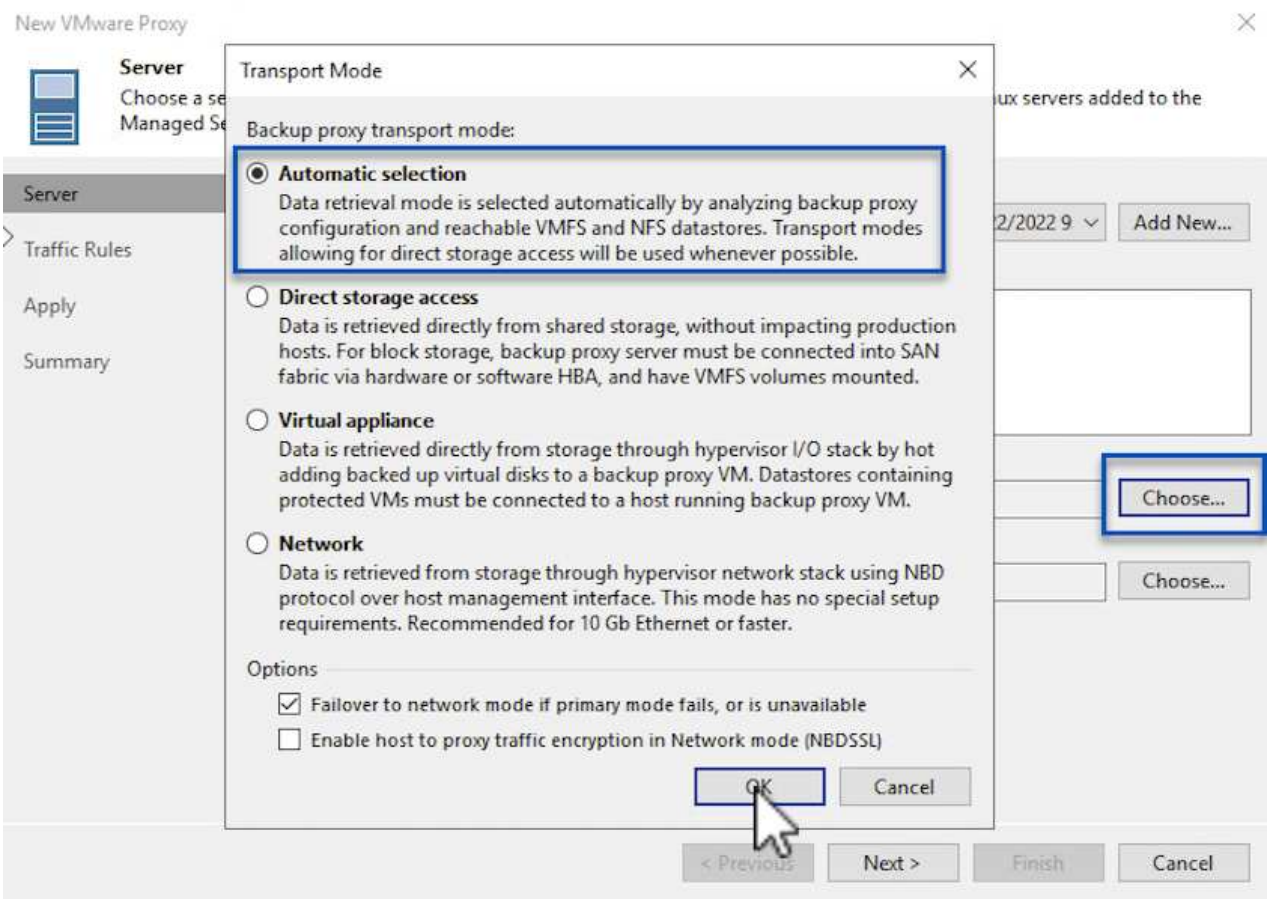


4. Seleccione para agregar Microsoft Windows y siga las indicaciones para agregar el servidor:

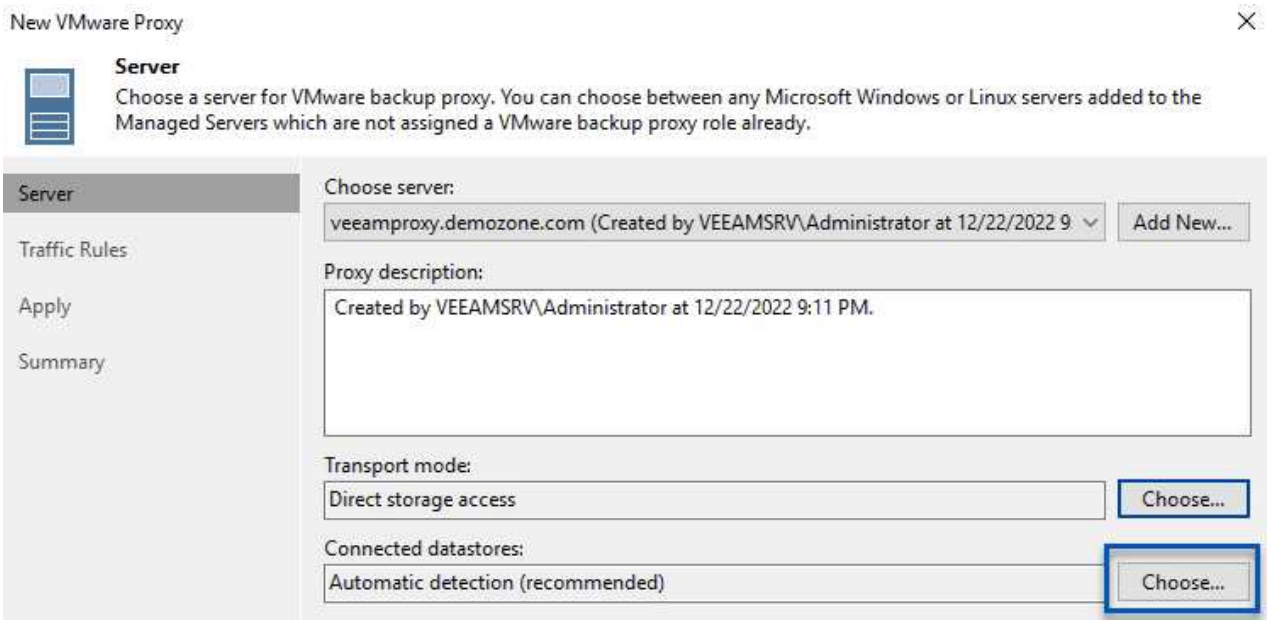
- Rellene el nombre DNS o la dirección IP
- Seleccione una cuenta para utilizar las credenciales en el nuevo sistema o agregue nuevas credenciales
- Revise los componentes que se van a instalar y luego haga clic en **Aplicar** para comenzar la implementación

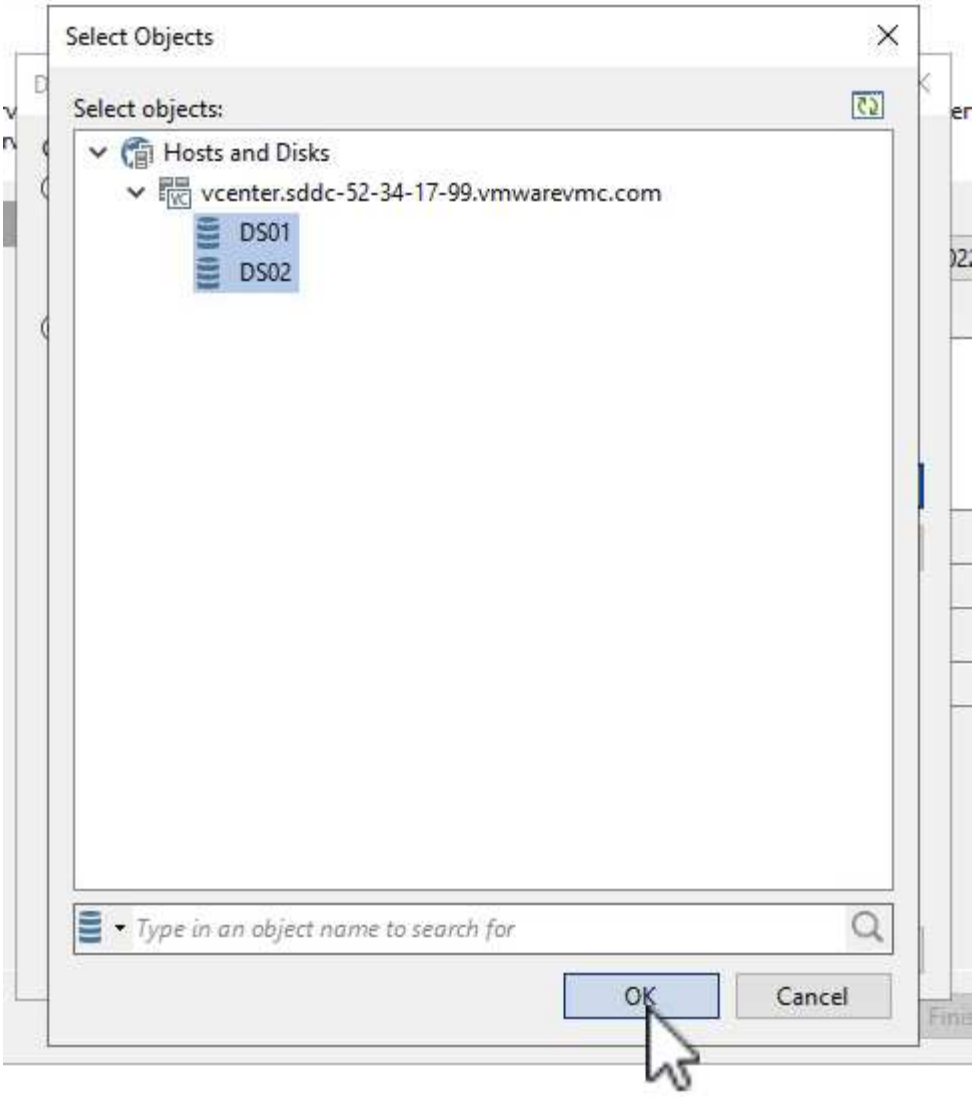


5. De nuevo en el asistente de **New VMware Proxy**, elija un modo de transporte. En nuestro caso elegimos **Selección Automática**.

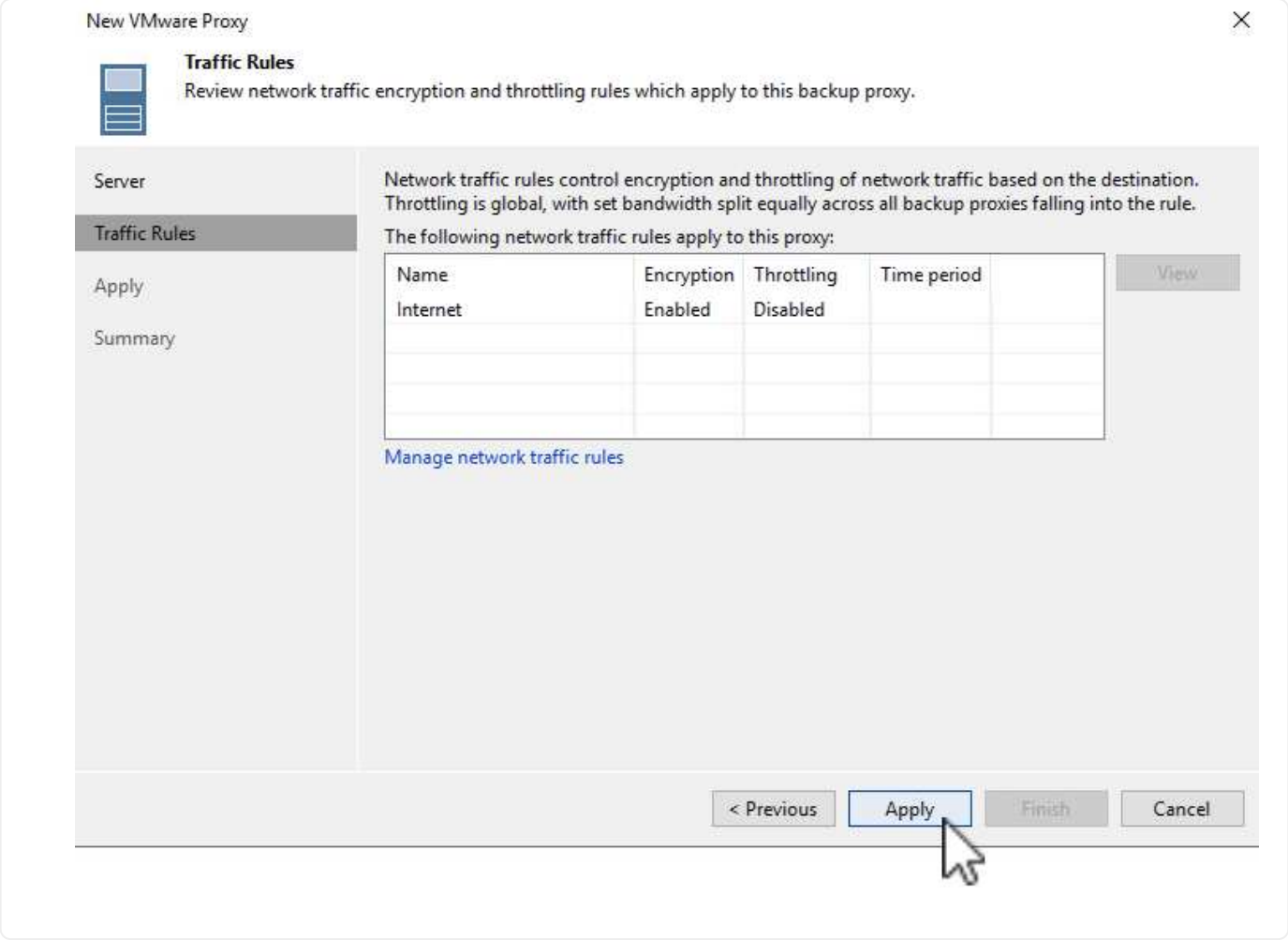


6. Seleccione los almacenes de datos conectados a los que desea que VMware Proxy tenga acceso directo.





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



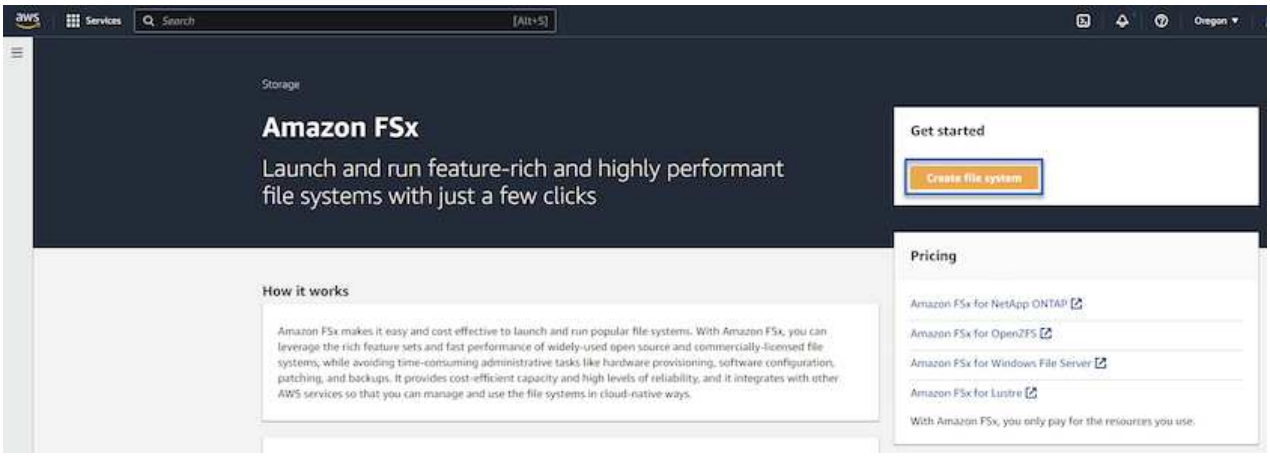
Configurar Repositorios de Almacenamiento y Copia de Seguridad

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

Crear FSX para el sistema de archivos ONTAP

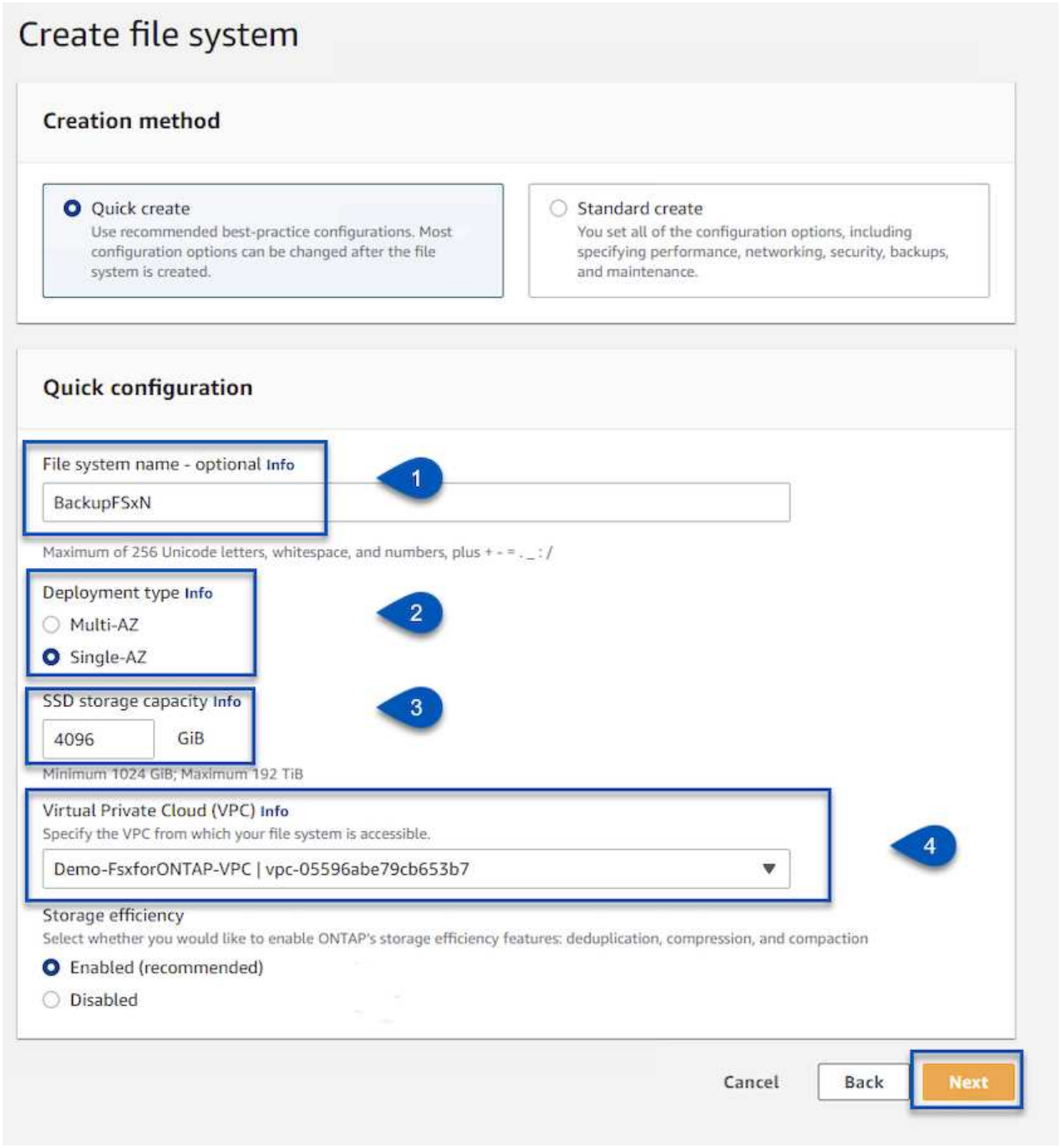
Cree un sistema de archivos FSx para ONTAP que se utilizará para alojar los volúmenes iSCSI para los repositorios de backup de Veeam.

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



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

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



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

Configuración y montaje de LUN iSCSI

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

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

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

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

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

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

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

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

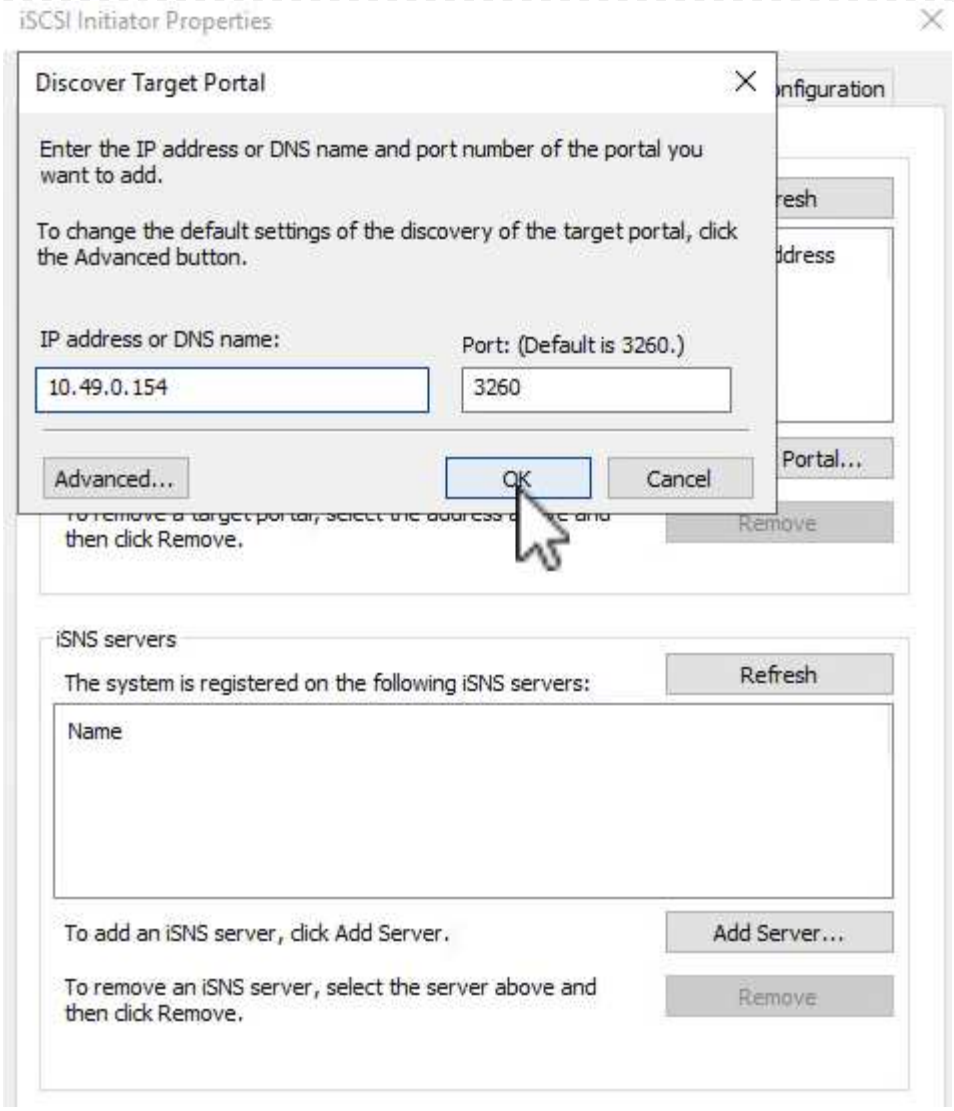
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

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

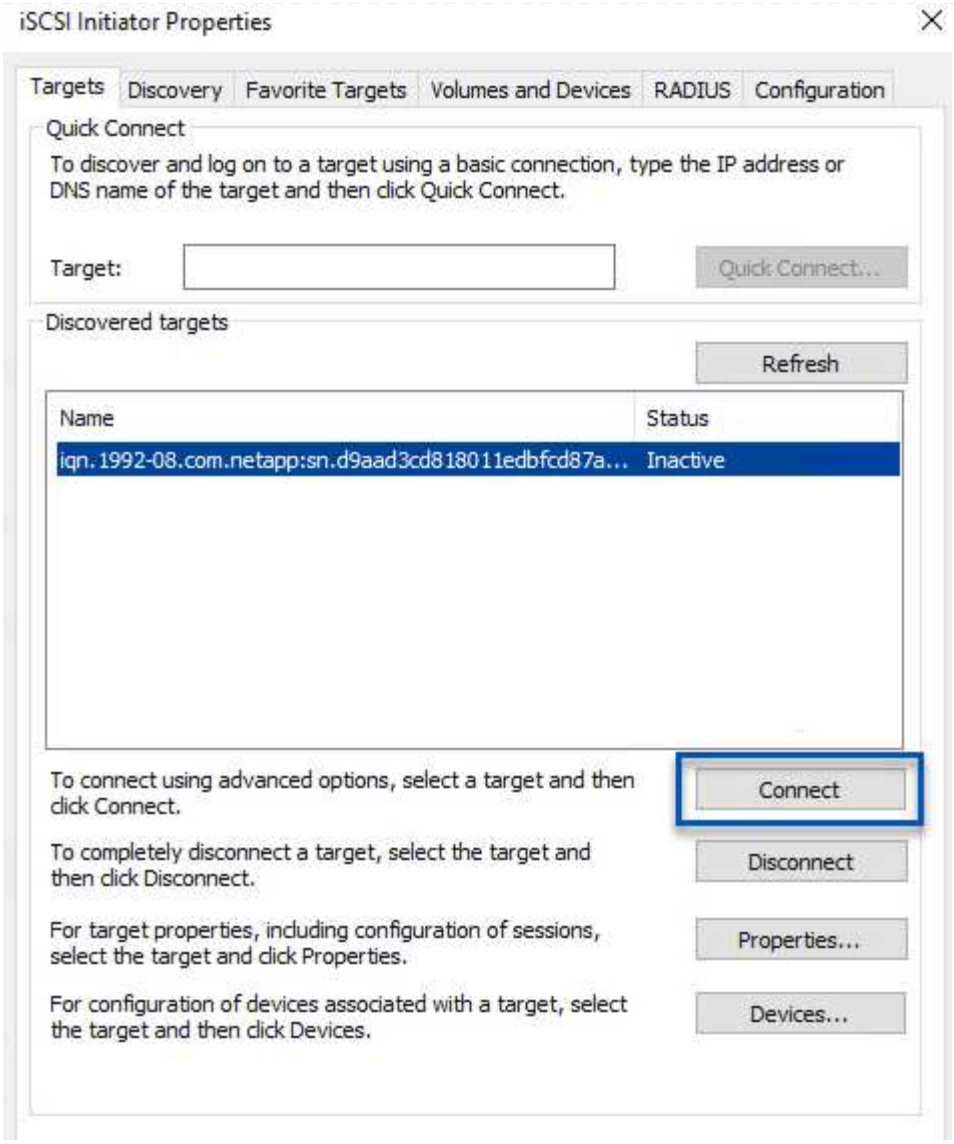
4. Finalmente, asigne las LUN al iGroup que acaba de crear:

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

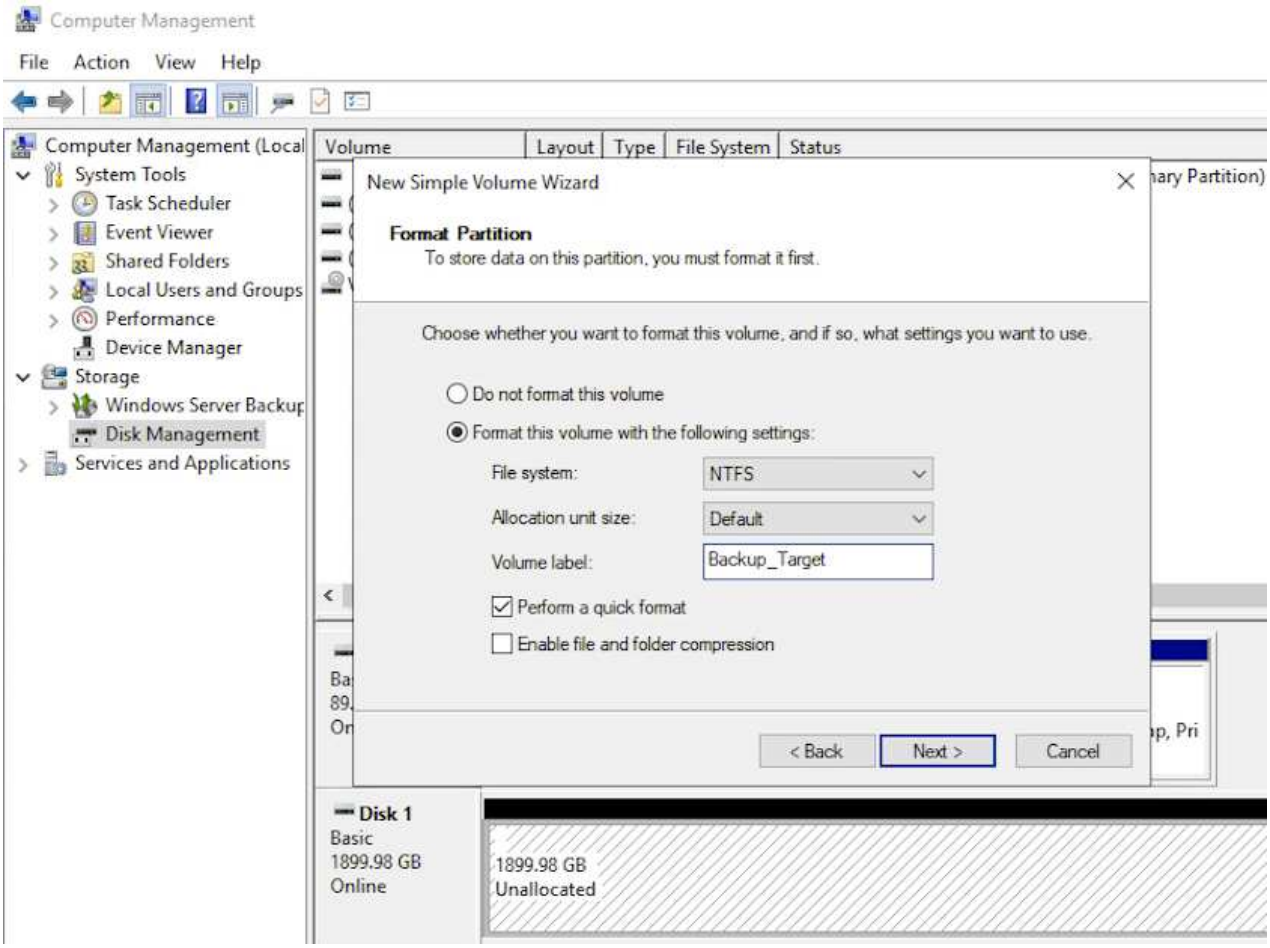
5. Para montar los LUN iSCSI, inicie sesión en Veeam Backup & Replication Server y abra Propiedades del iniciador iSCSI. Vaya a la pestaña **Discover** e introduzca la dirección IP de destino iSCSI.



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



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

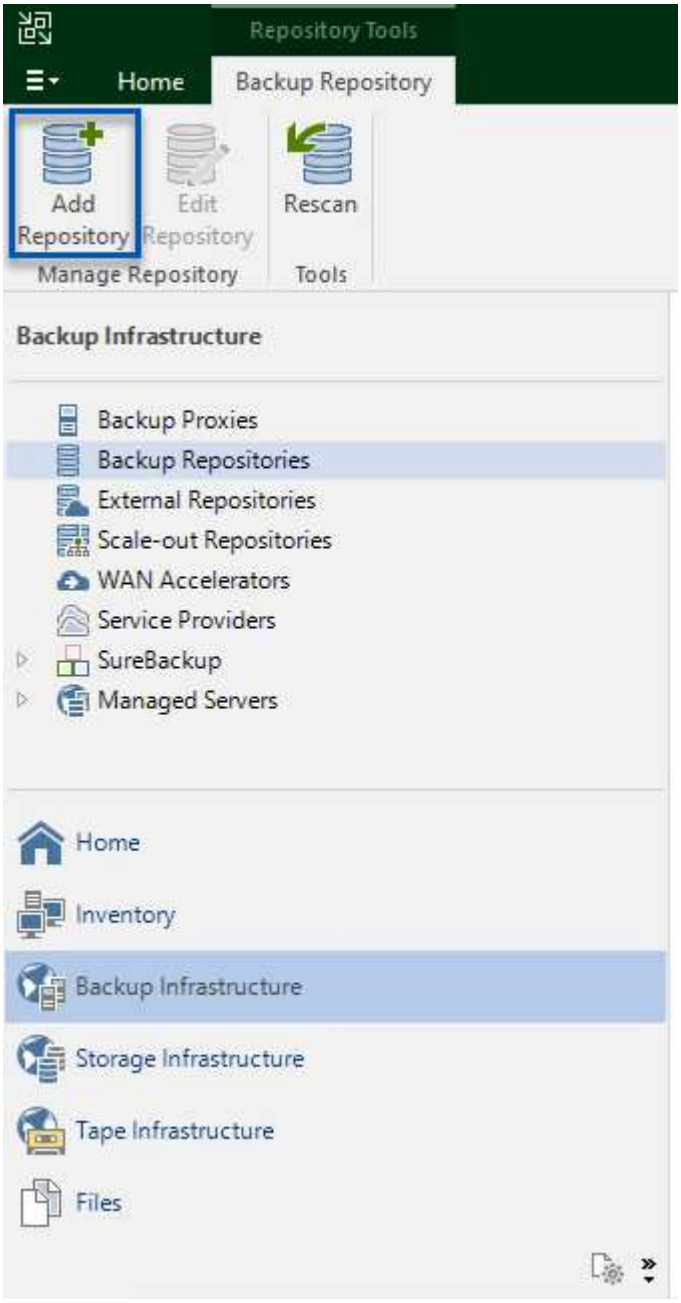


8. Repita estos pasos para montar los volúmenes iSCSI en el servidor proxy de Veeam.

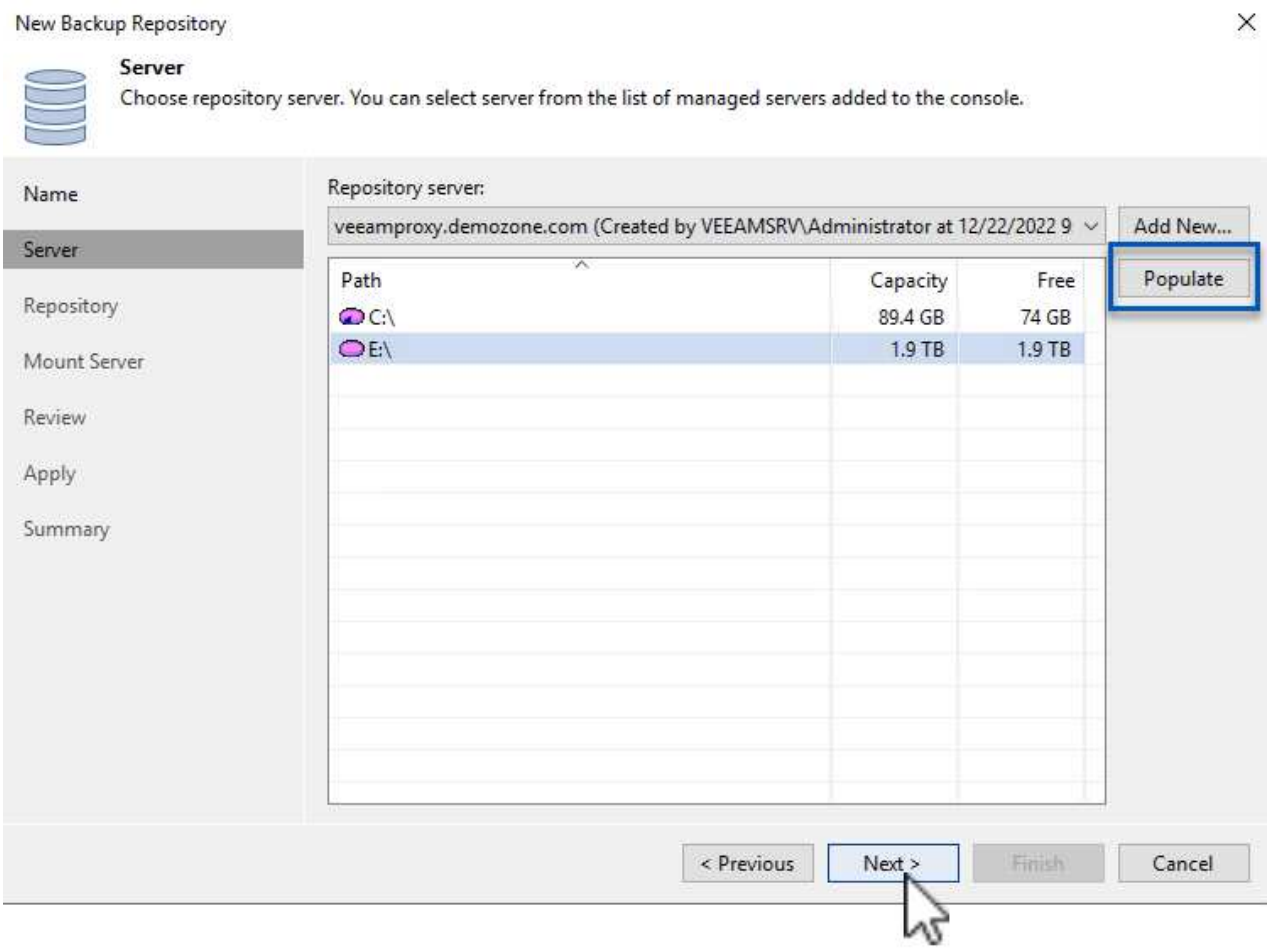
Crear repositorios de Veeam Backup

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

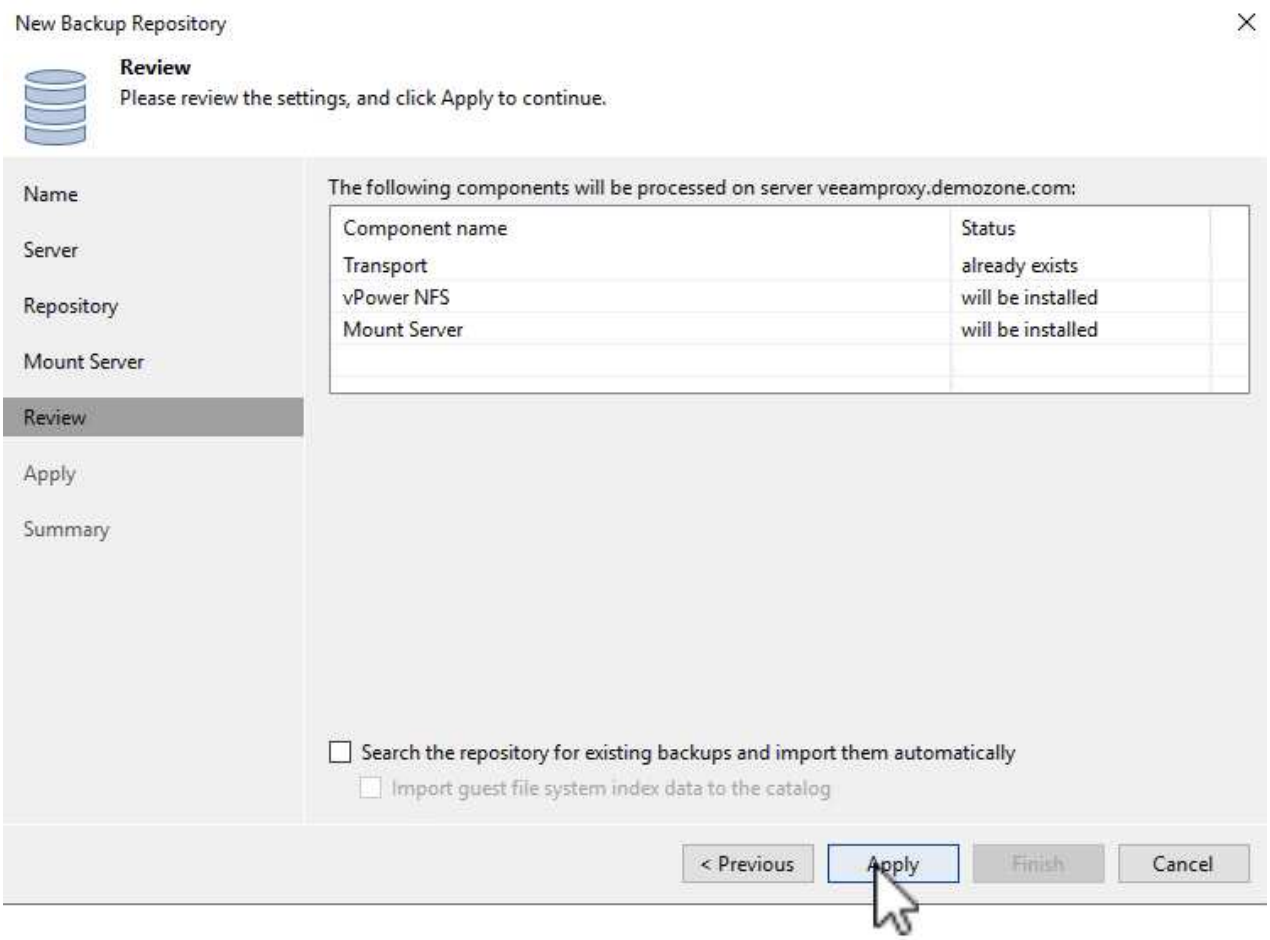
1. En la consola Veeam Backup and Replication, haga clic en **Backup Infrastructure** en la parte inferior izquierda y luego seleccione **Add Repository**



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



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



5. Repita estos pasos para cualquier servidor proxy adicional.

Configurar los trabajos de backup de Veeam

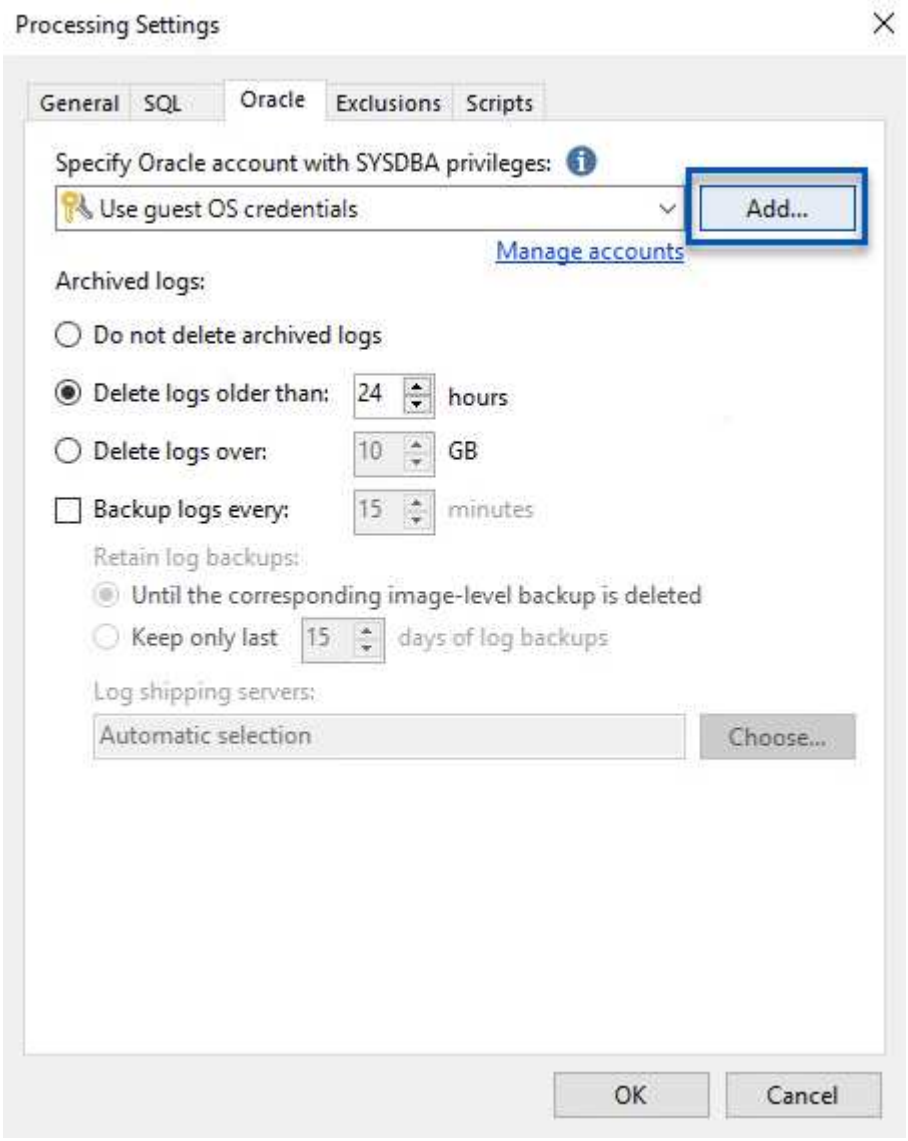
Los trabajos de copia de seguridad se deben crear utilizando los repositorios de copia de seguridad de la sección anterior. La creación de tareas de backup forma parte normal del repertorio de cualquier administrador de almacenamiento y no cubrimos todos los pasos aquí. Si desea obtener más información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

En esta solución se crearon tareas de backup independientes para:

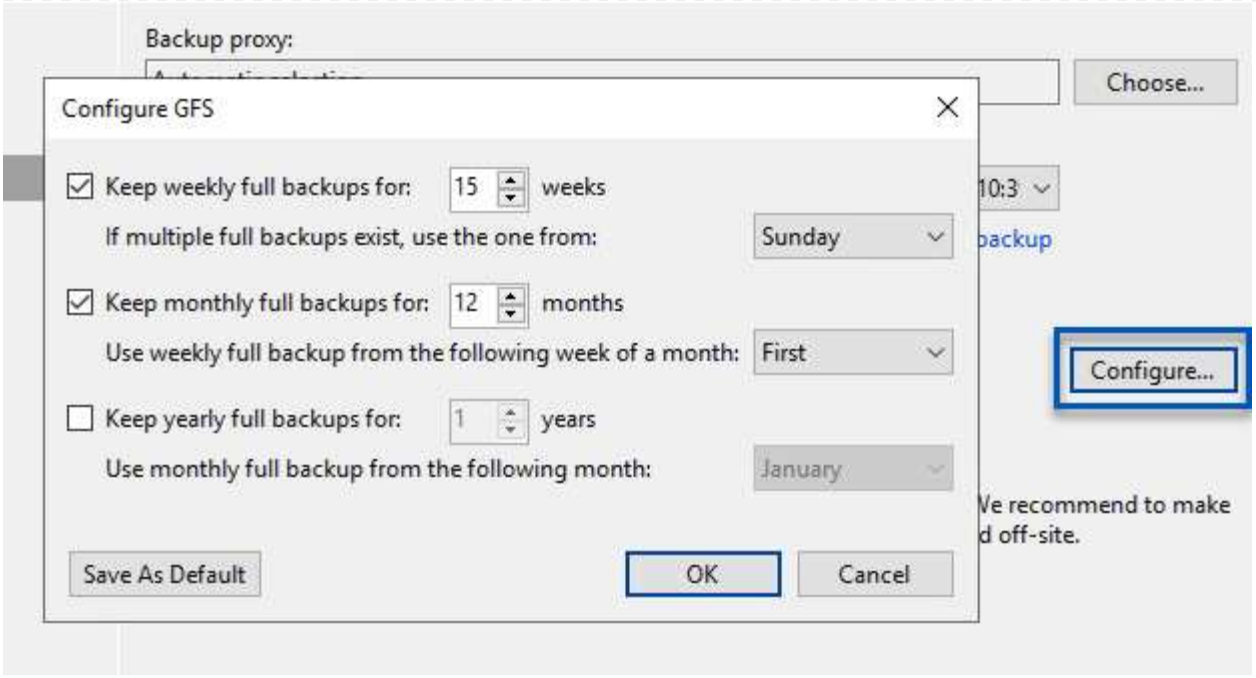
- Servidores Microsoft Windows SQL Server
- Servidores Oracle Database
- Servidores de archivo Windows
- Servidores de archivos Linux

Consideraciones generales al configurar trabajos de backup de Veeam

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



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



Restaure VMs de aplicaciones con la restauración completa de Veeam

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

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

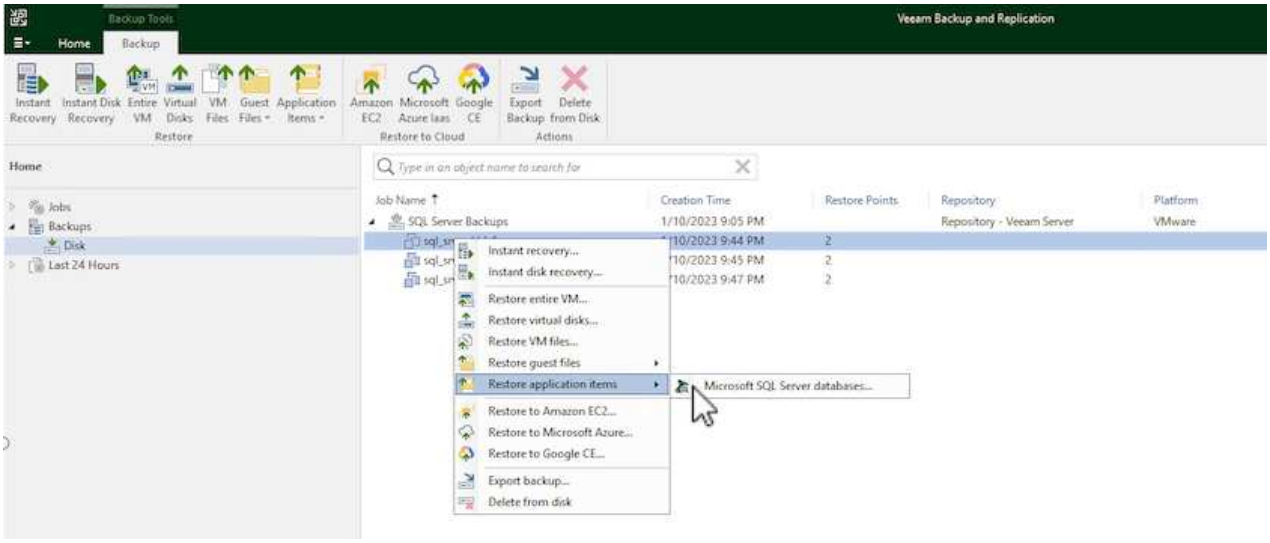
Restaure las bases de datos de SQL Server

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

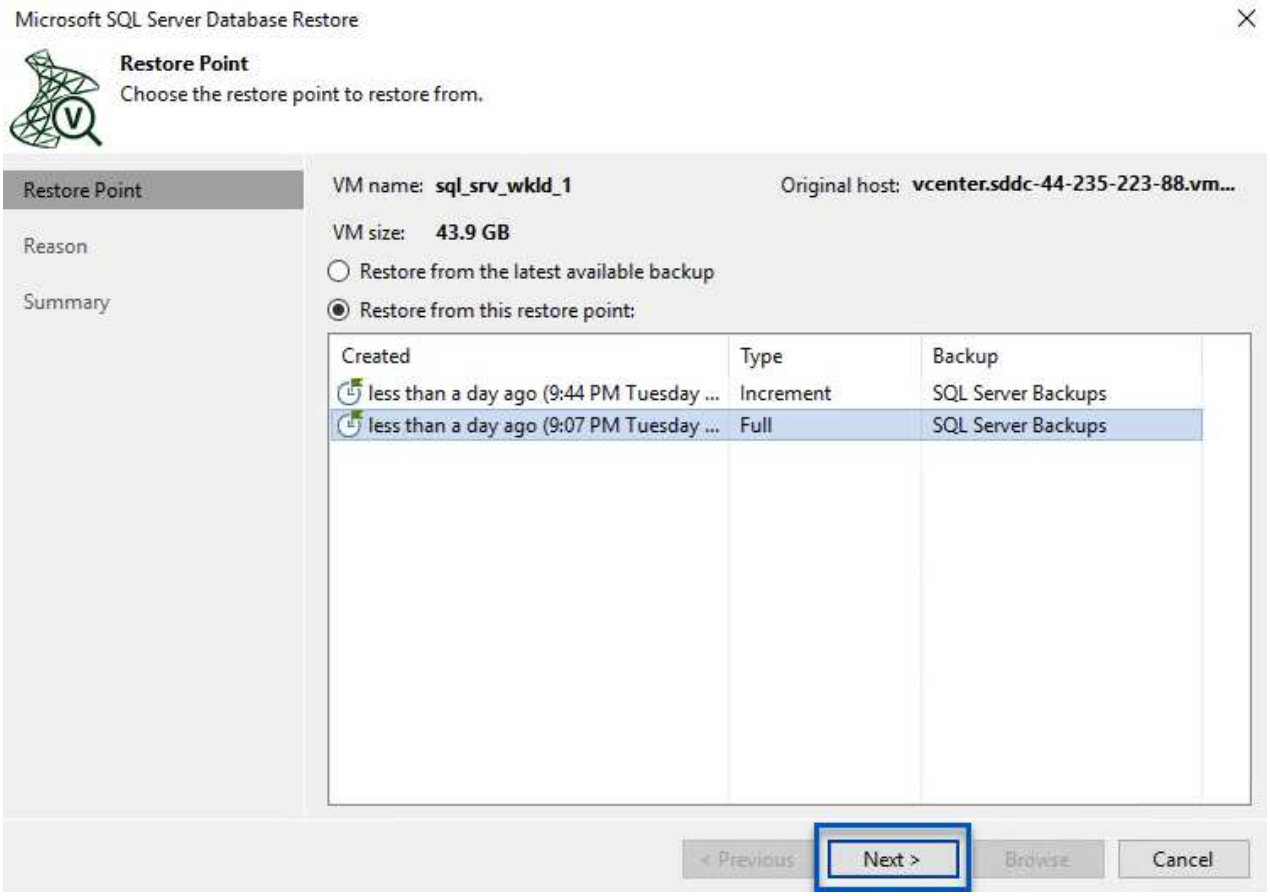
- Veeam Explorer **monta la copia de seguridad** que contiene la base de datos de SQL Server que se va a restaurar.
- El software **publica la base de datos** directamente desde los archivos montados, haciéndola accesible como base de datos temporal en la instancia de SQL Server de destino.
- Mientras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

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

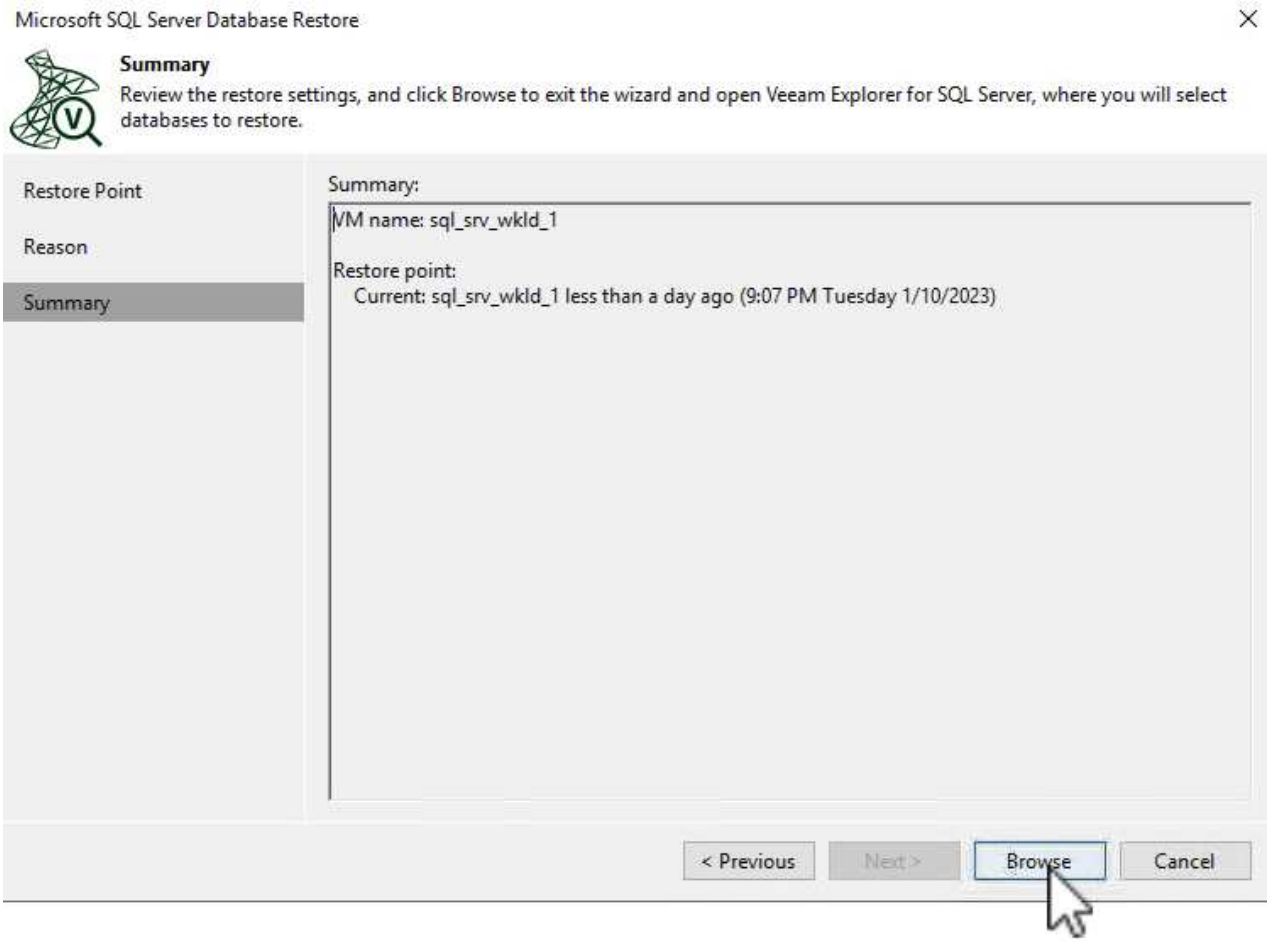
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de SQL Server, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de aplicación** y luego **Bases de datos de Microsoft SQL Server…**.



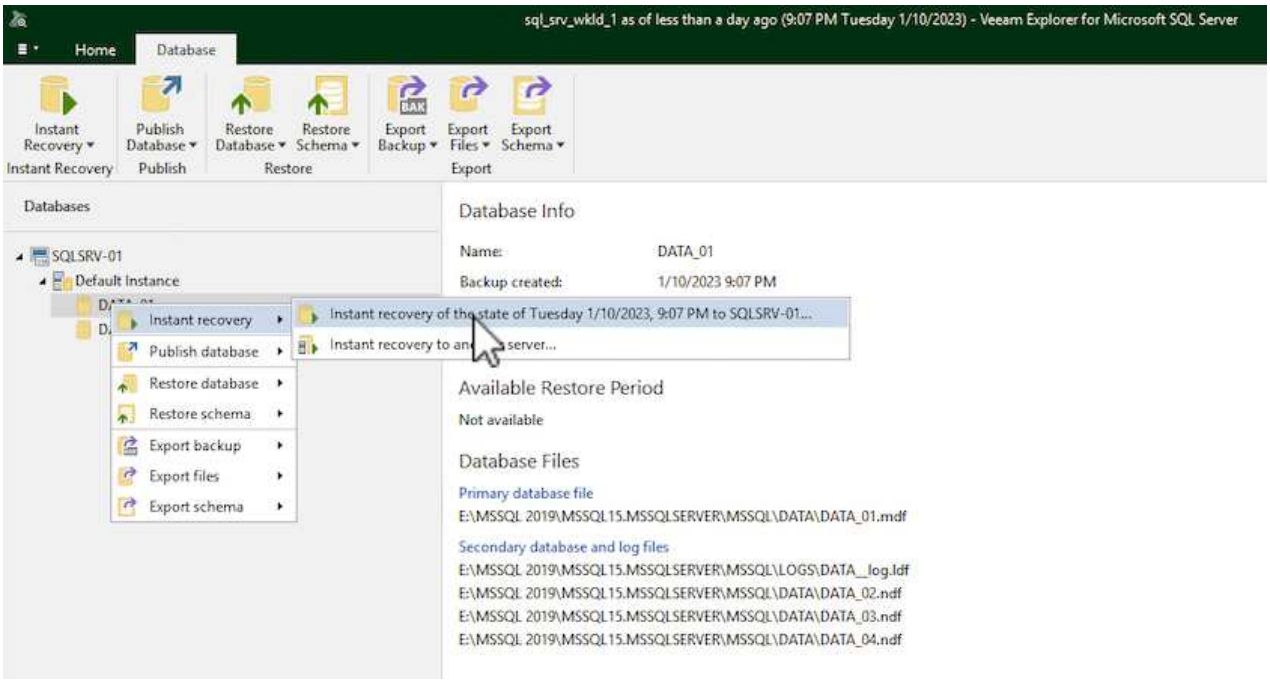
2. En el Asistente de restauración de bases de datos de Microsoft SQL Server, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.



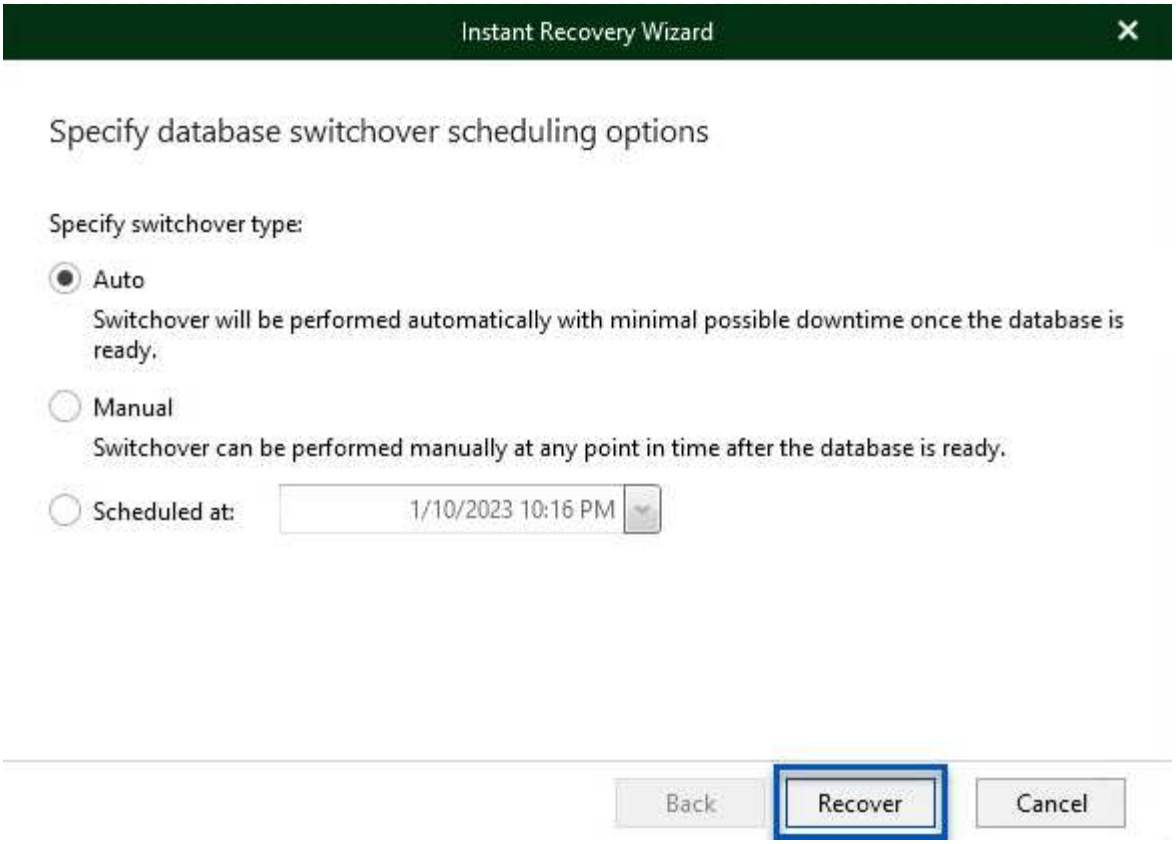
3. Introduzca un **Razón de restauración** si lo desea y, a continuación, en la página Resumen, haga clic en el botón **Examinar** para iniciar Veeam Explorer para Microsoft SQL Server.



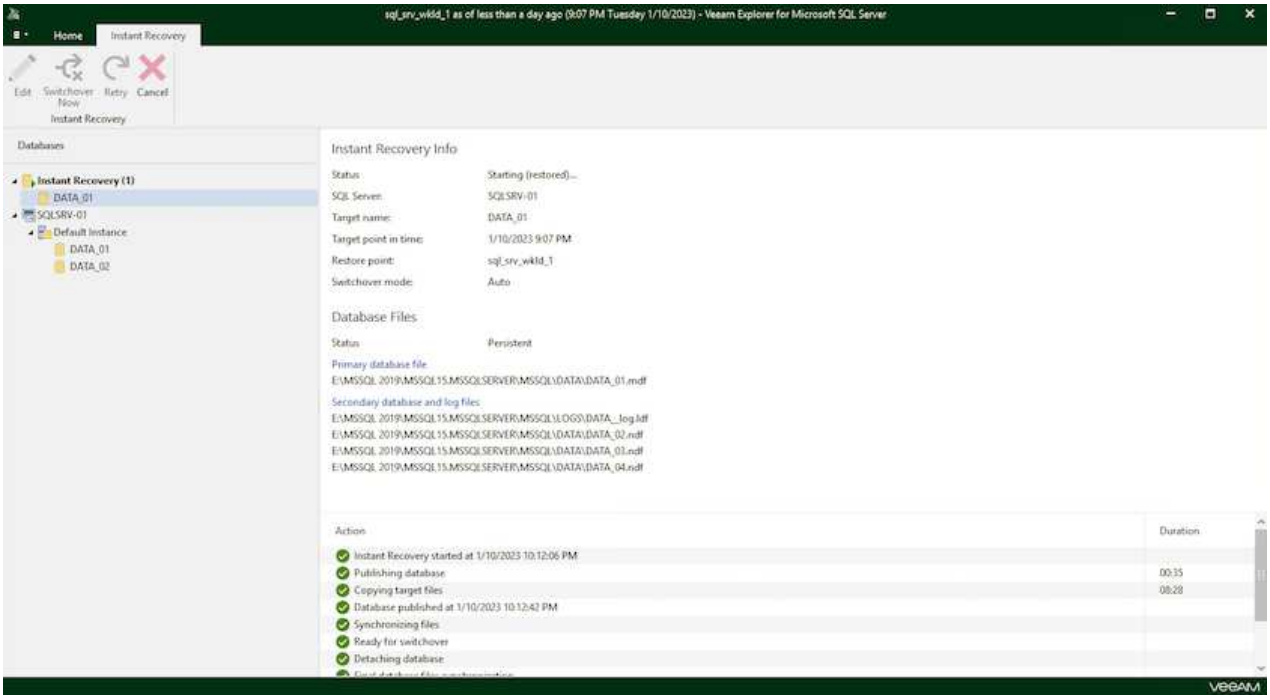
4. En Veeam Explorer expanda la lista de instancias de base de datos, haga clic derecho y seleccione **Recuperación instantánea** y luego el punto de restauración específico para recuperar.



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



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



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

Restaurar bases de datos de Oracle con Veeam Explorer

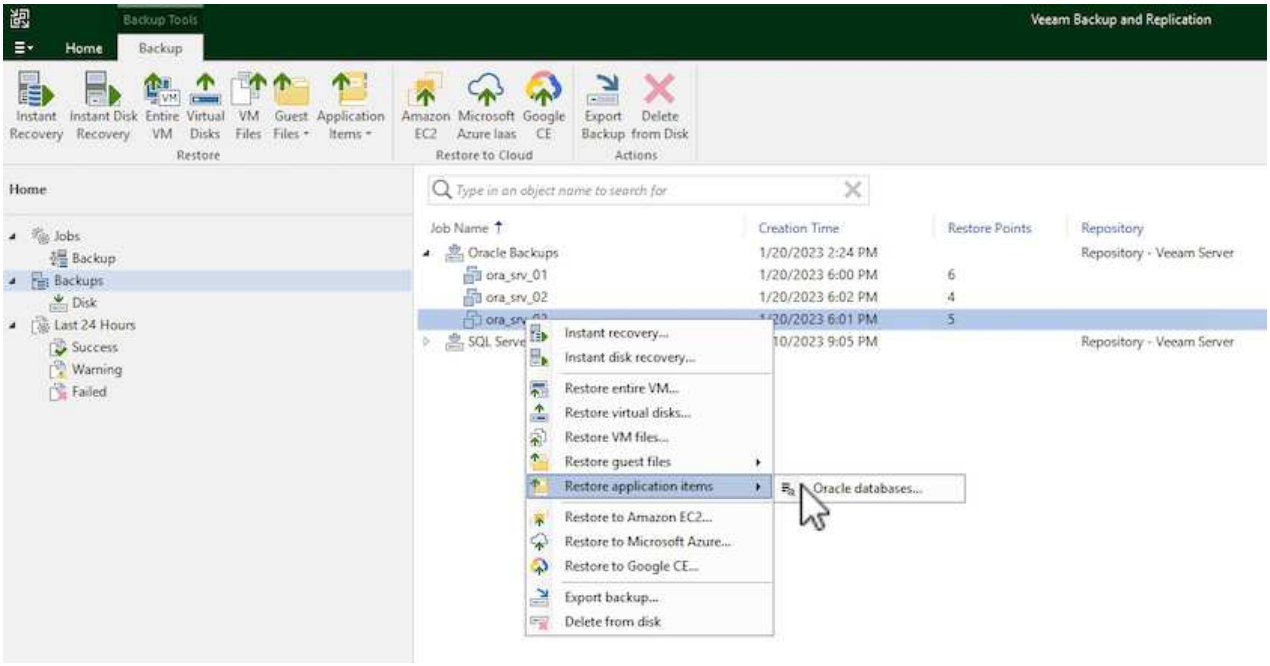
Veeam Explorer para la base de datos Oracle permite realizar una restauración estándar de la base de datos Oracle o una restauración sin interrupciones con Instant Recovery. También admite la publicación de bases de datos para un acceso rápido, la recuperación de bases de datos de Data Guard y las restauraciones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

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

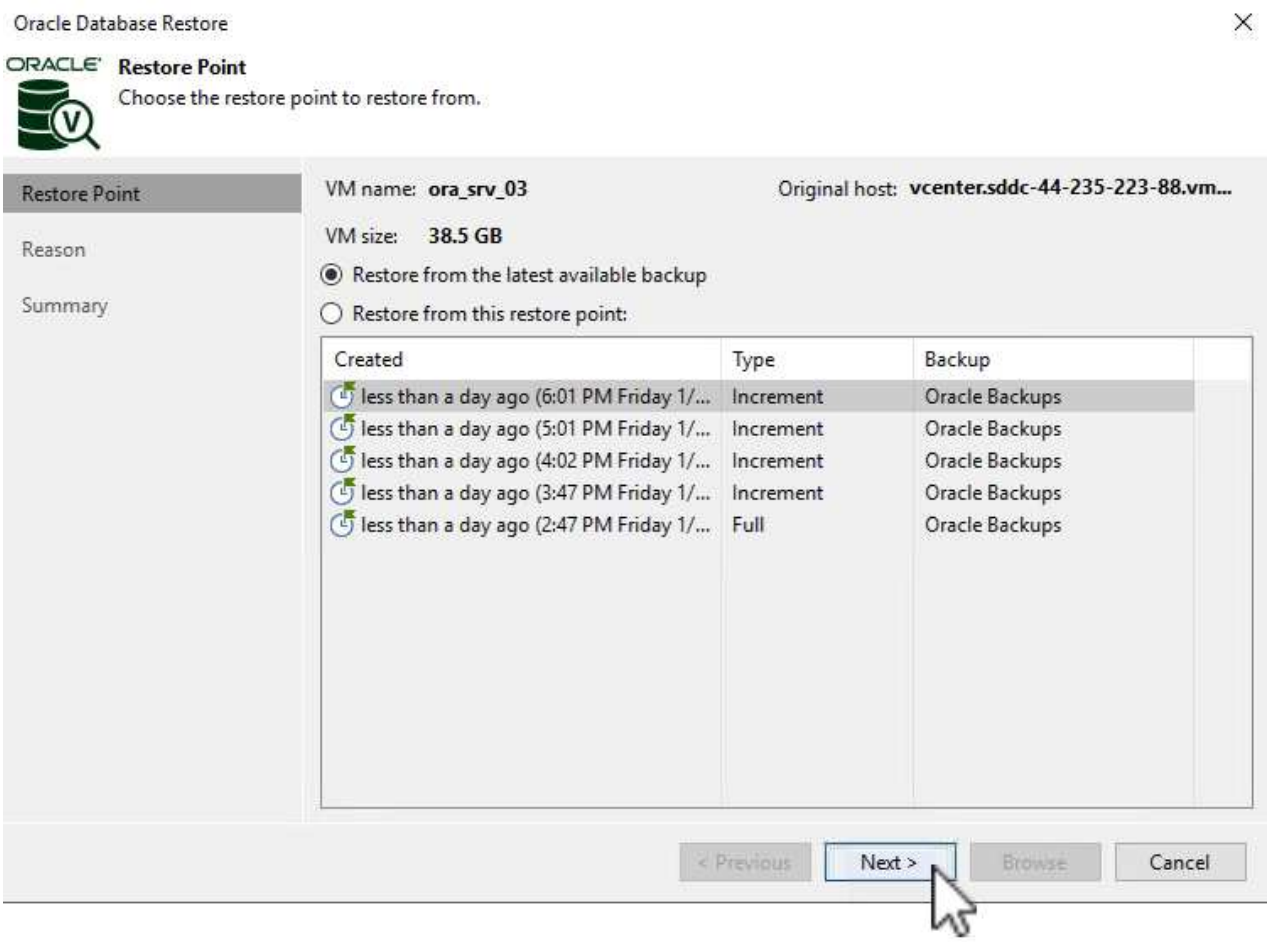
Restaurar base de datos de Oracle con Veeam Explorer

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

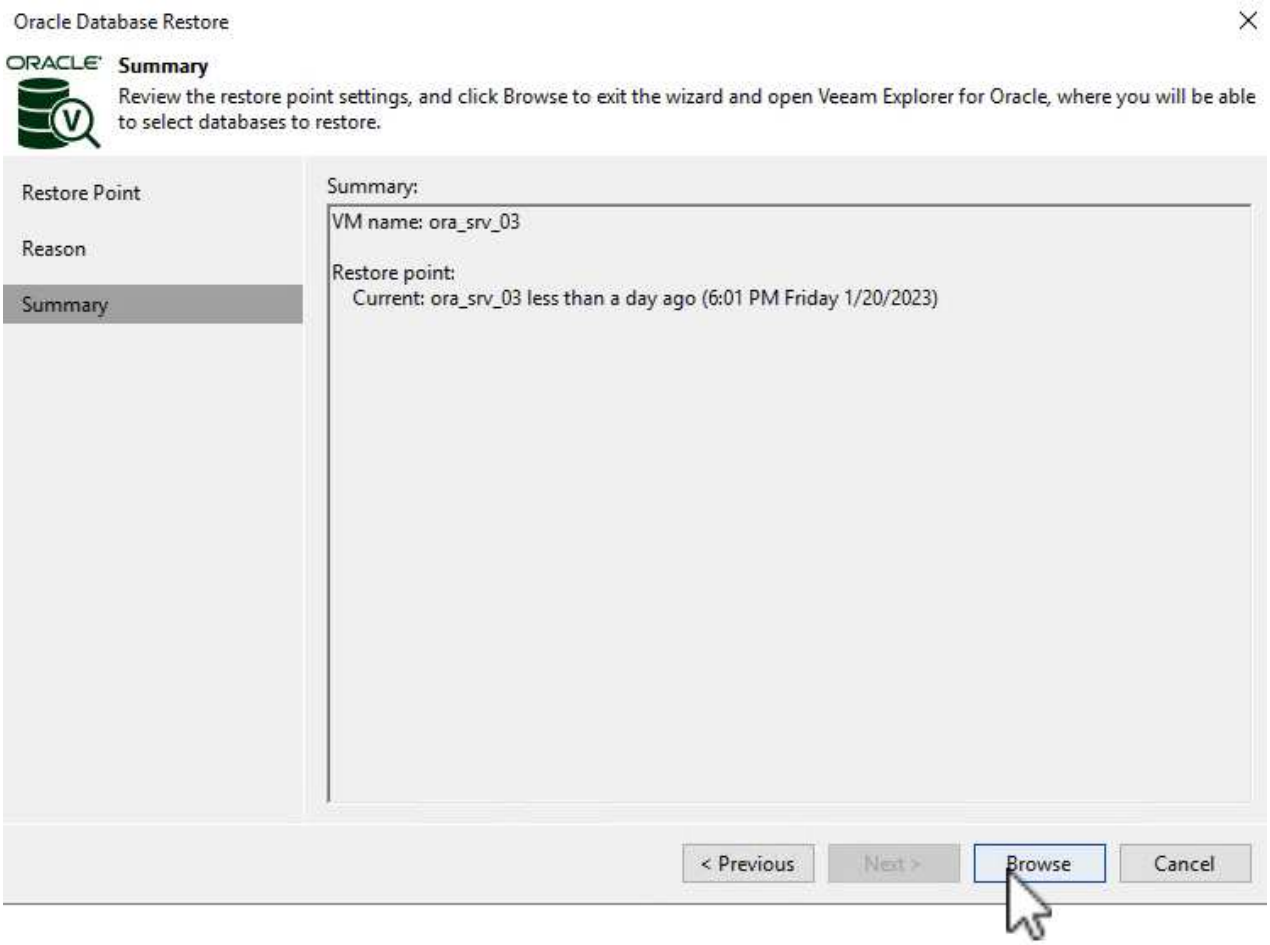
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de Oracle, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de aplicación** y luego **Bases de datos Oracle…**.



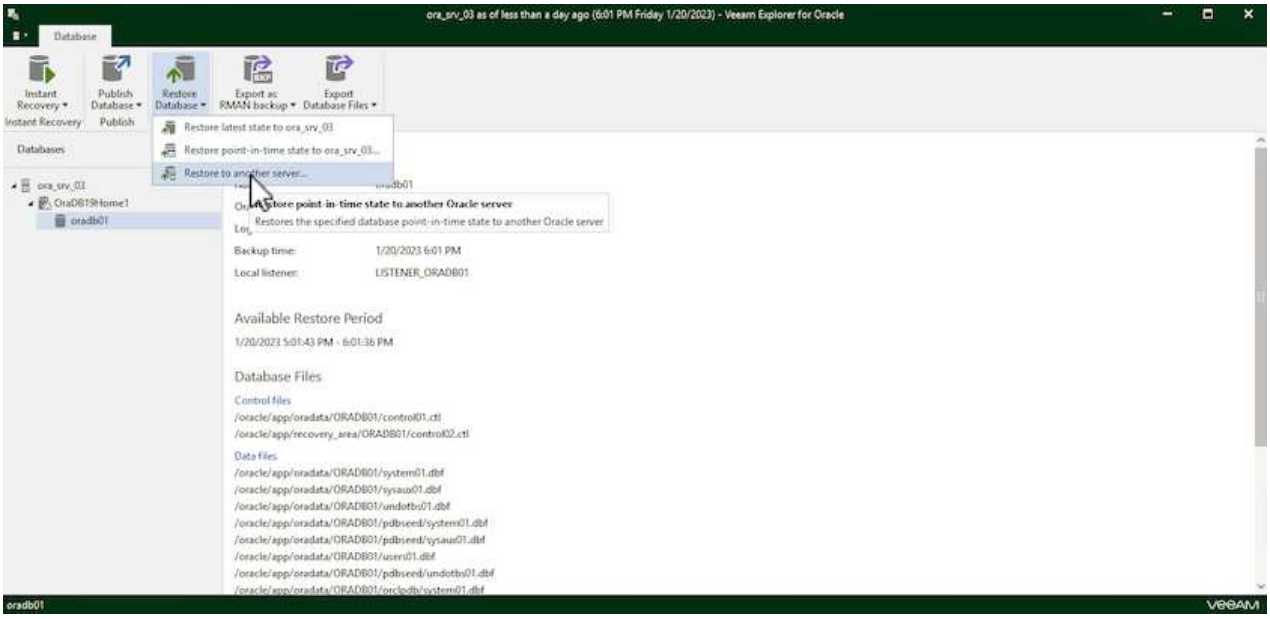
2. En el Asistente de restauración de bases de datos Oracle, seleccione un punto de restauración de la lista y haga clic en **Siguiente**.



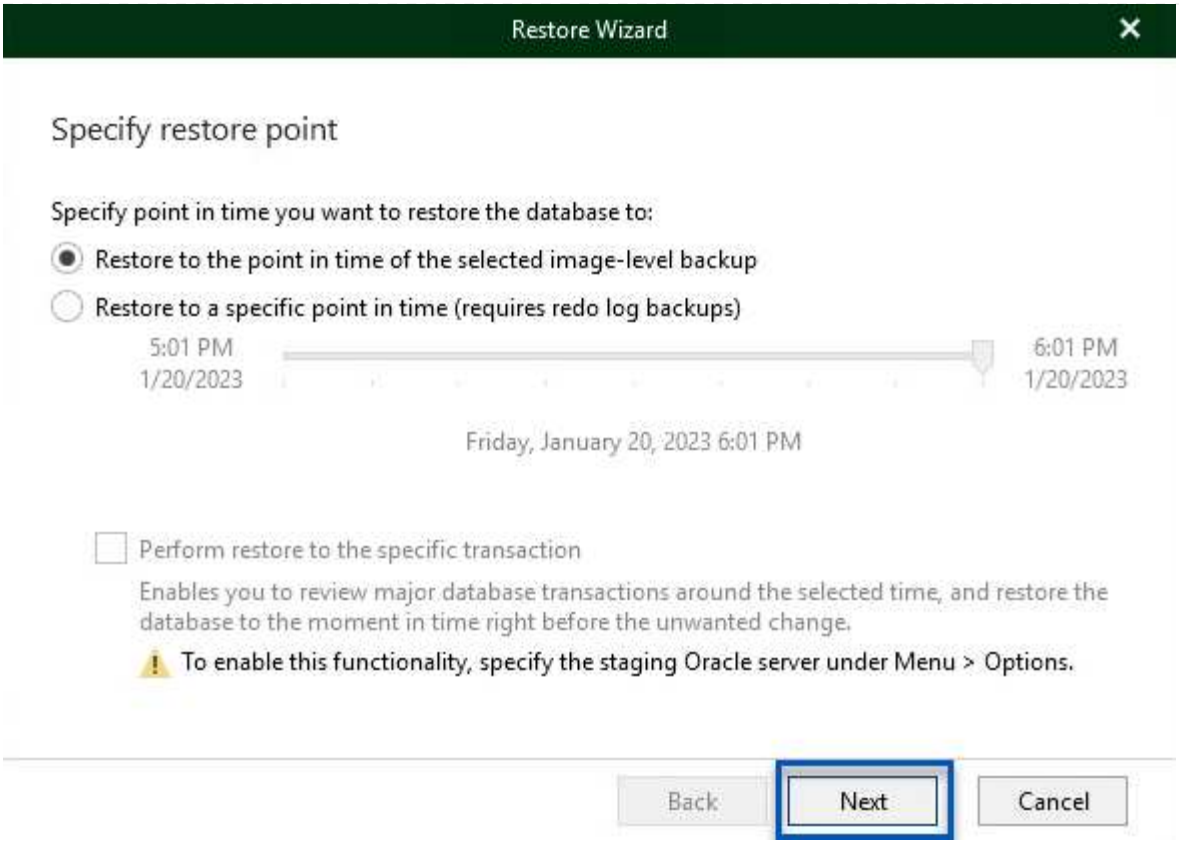
3. Introduzca un **Razón de restauración** si lo desea y, a continuación, en la página Resumen, haga clic en el botón **Examinar** para iniciar Veeam Explorer para Oracle.



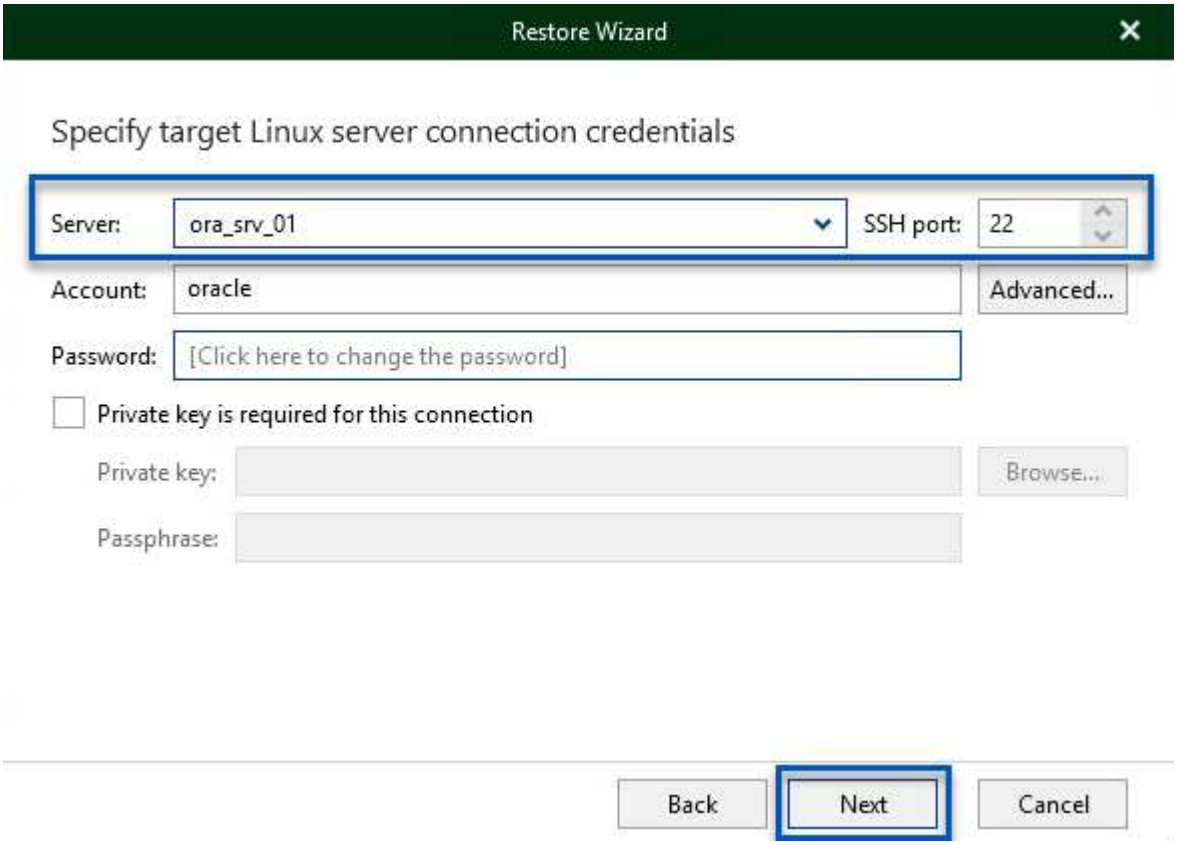
4. En Veeam Explorer expanda la lista de instancias de base de datos, haga clic en la base de datos que desea restaurar y luego en el menú desplegable **Restaurar base de datos** en la parte superior seleccione **Restaurar a otro servidor…**.



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

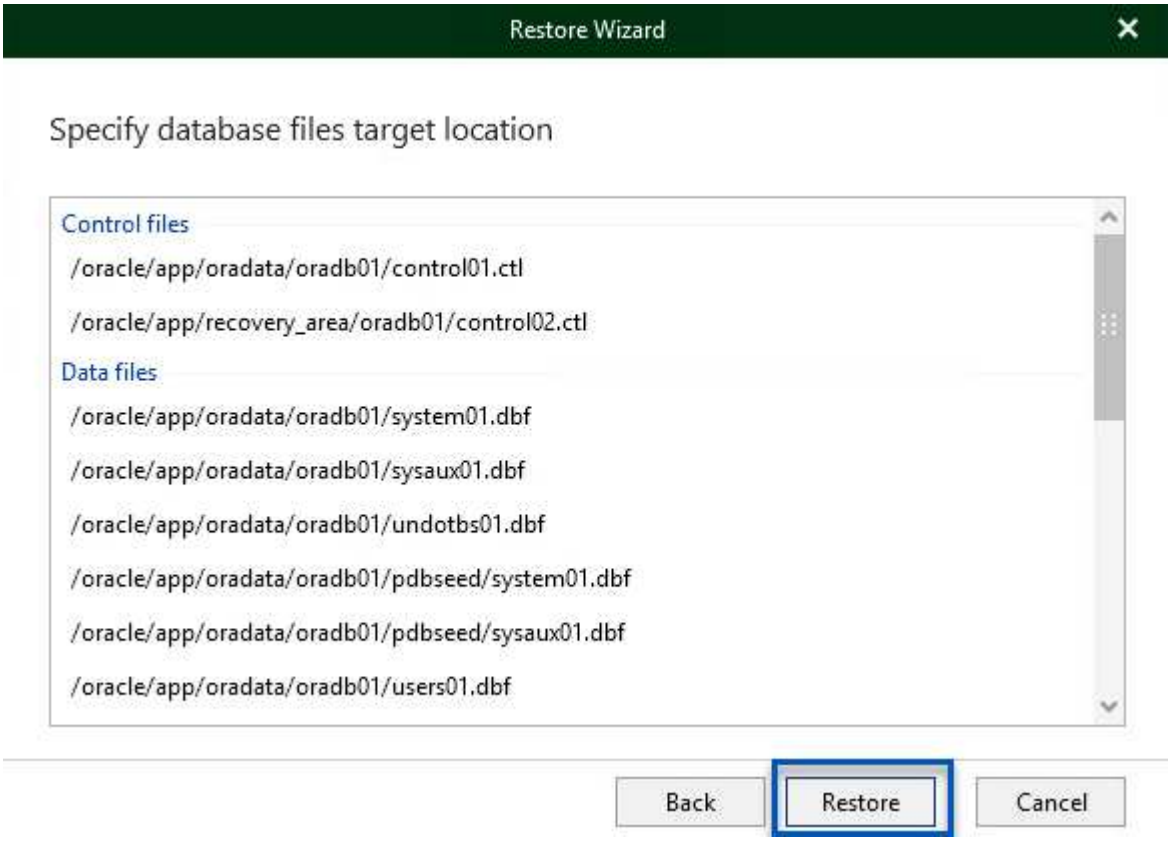


6. Especifique el servidor de destino al que se restaurará la base de datos y las credenciales de la cuenta y haga clic en **Siguiente**.



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

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

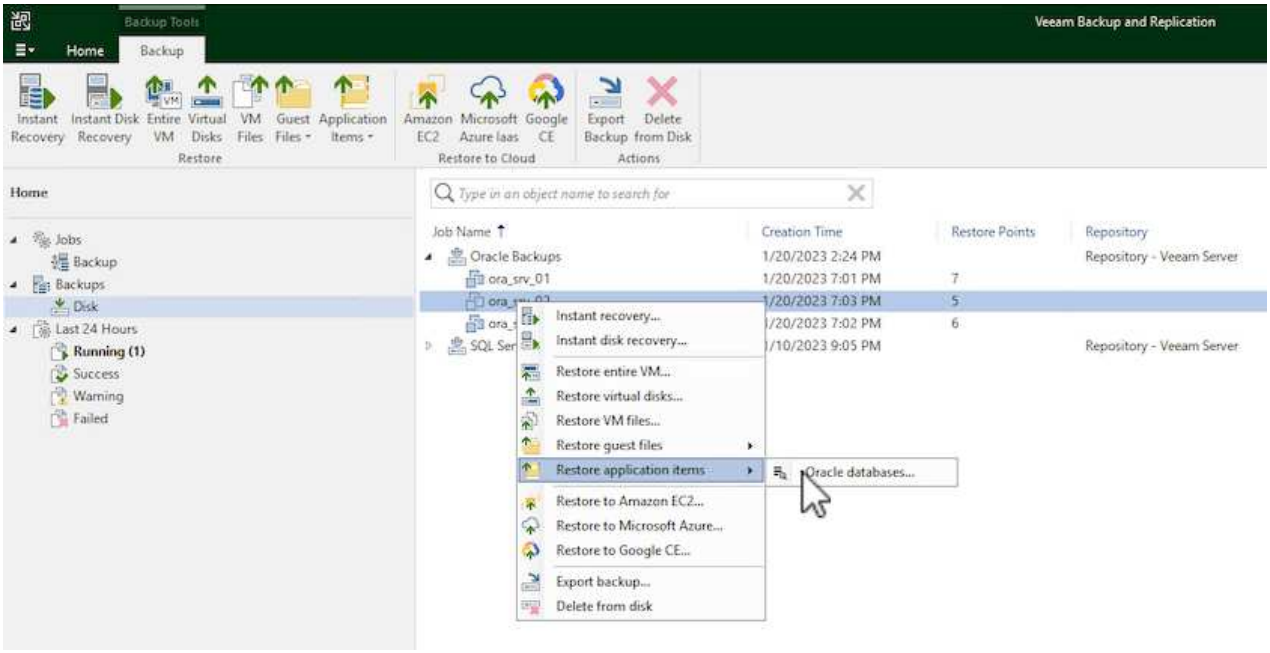


8. Una vez finalizada la recuperación de la base de datos, compruebe que la base de datos Oracle se inicia correctamente en el servidor.

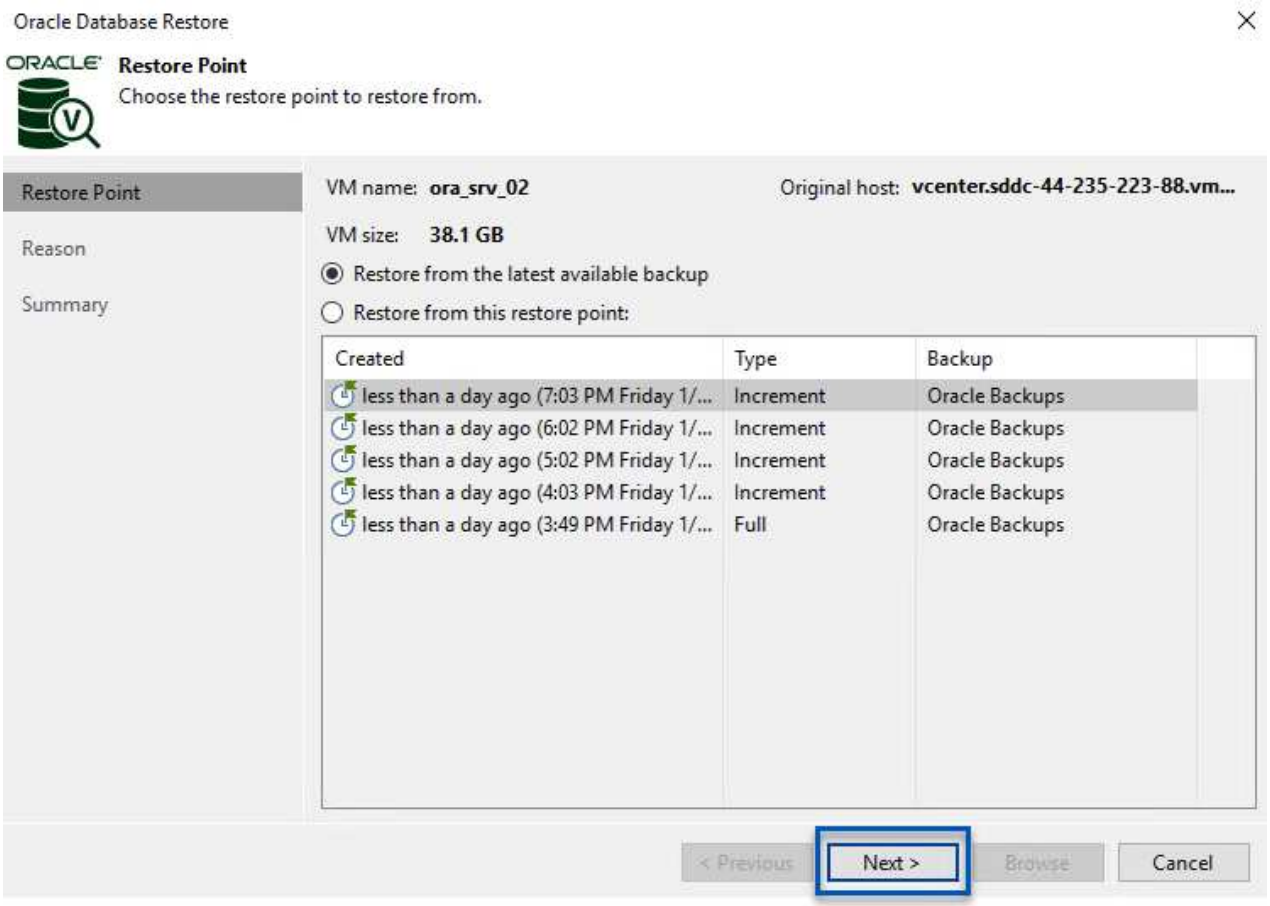
Publicar la base de datos Oracle en un servidor alternativo

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

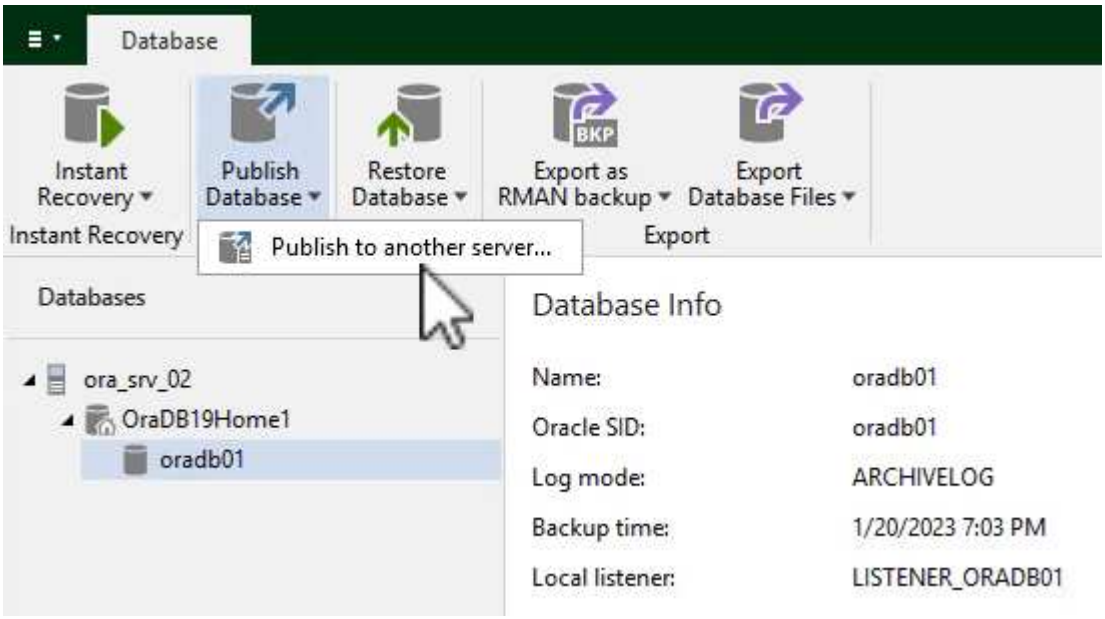
1. En la consola de Veeam Backup and Replication, navegue a la lista de copias de seguridad de Oracle, haga clic con el botón derecho en un servidor y seleccione **Restaurar elementos de aplicación** y luego **Bases de datos Oracle…**.



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

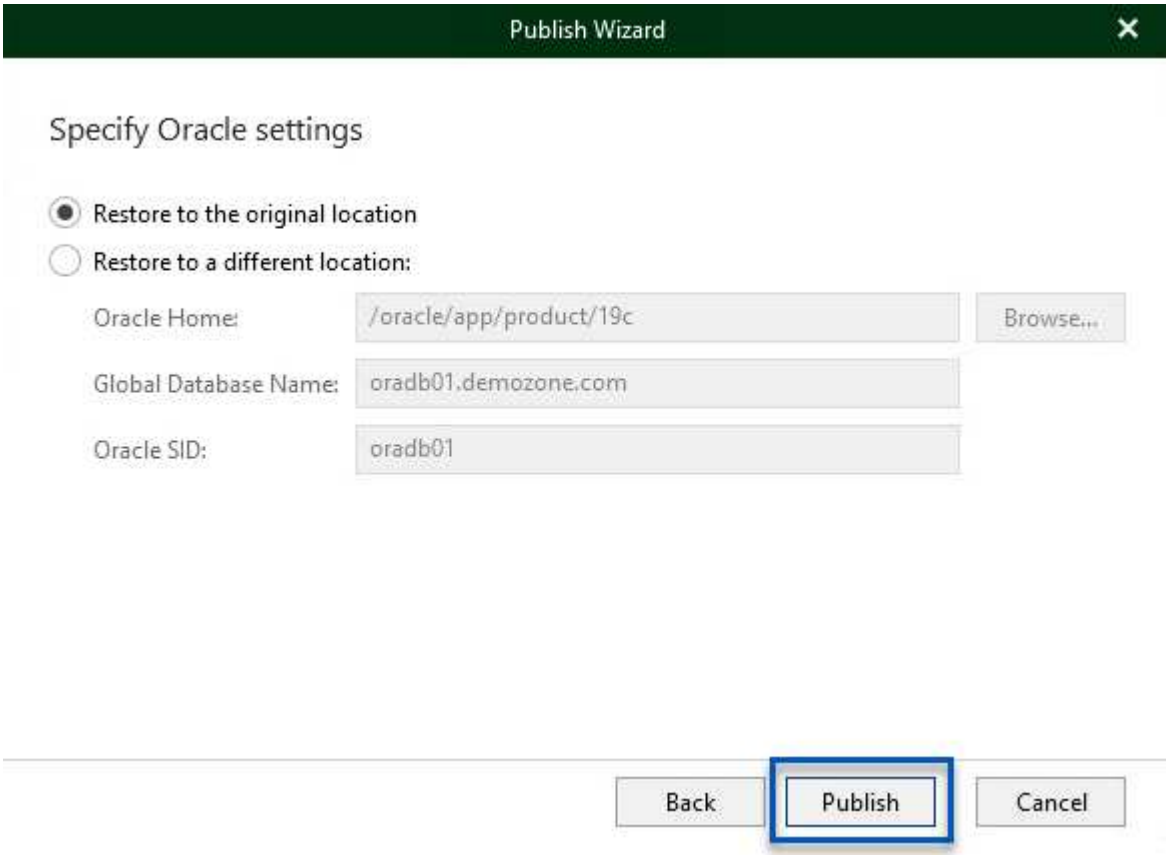


3. Introduzca un **Razón de restauración** si lo desea y, a continuación, en la página Resumen, haga clic en el botón **Examinar** para iniciar Veeam Explorer para Oracle.
4. En Veeam Explorer expanda la lista de instancias de base de datos, haga clic en la base de datos que desea restaurar y luego en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



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

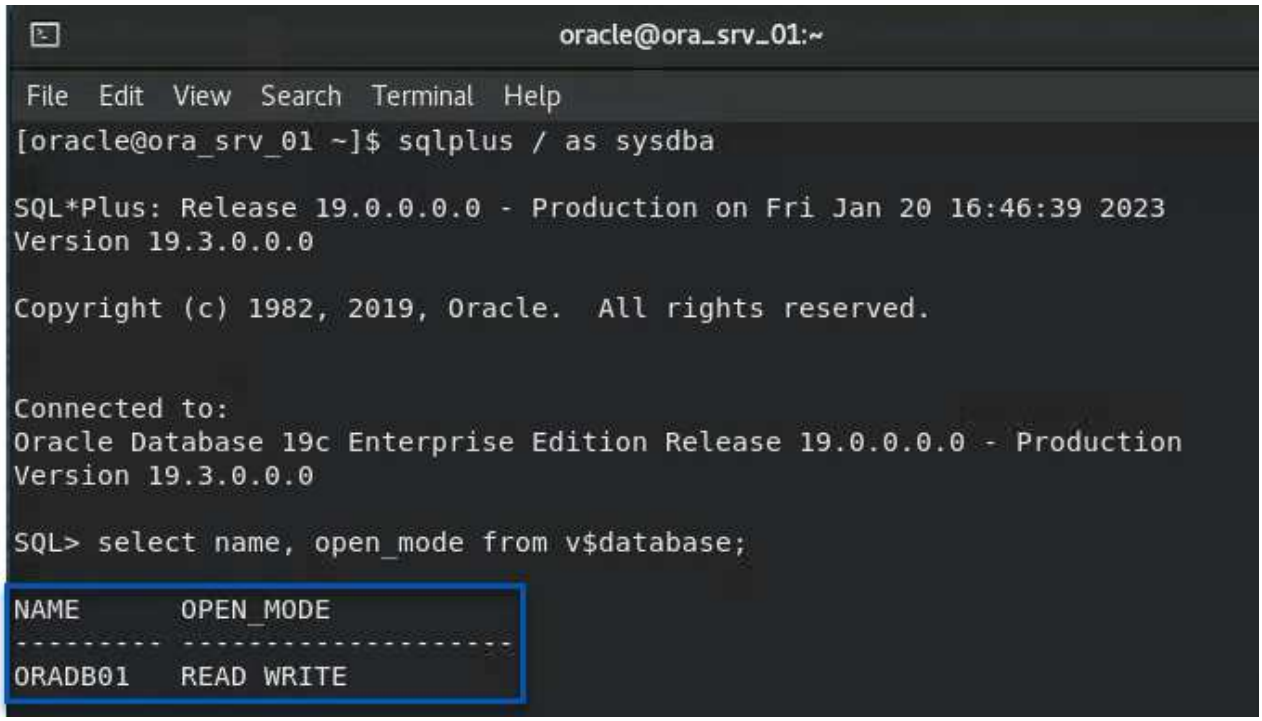
6. Por último, especifique la ubicación del sistema de archivos linux de destino y haga clic en **Publicar** para comenzar el proceso de restauración.



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

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

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



Conclusión

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

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

Información adicional

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

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

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

Niyaz Mohamed, NetApp

Descripción general

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

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

Primeros pasos

Implemente y configure VMware Cloud en AWS

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

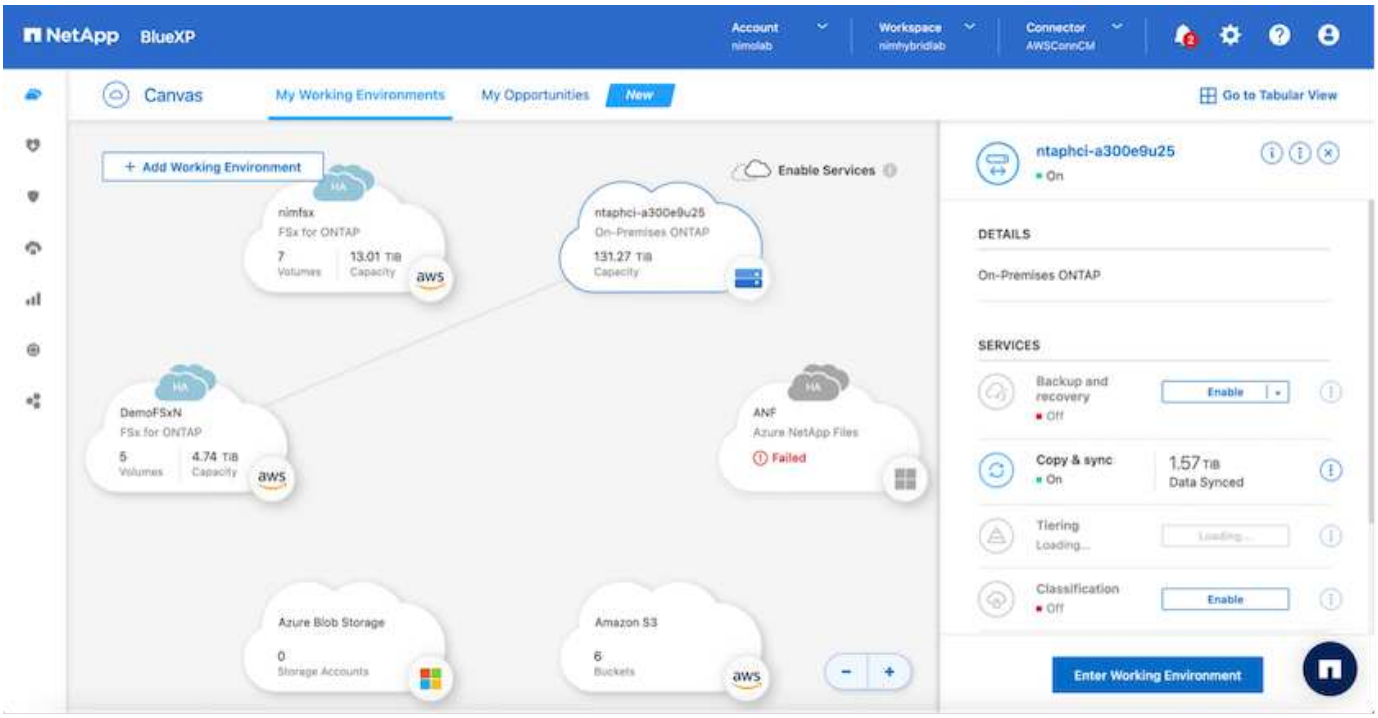
> En la versión inicial, DRO admite un clúster de luces piloto existente. La creación bajo demanda de SDDC estará disponible en una próxima versión.

Aprovisionar y configurar FSX para ONTAP

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

Poner en marcha y configurar SnapMirror a FSX para ONTAP

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



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

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

Instalación DE DRO

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

Requisitos previos

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

Requisitos de SO

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

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

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

Instale el paquete

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

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

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

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

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

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

```
sudo sh deploy.sh
```

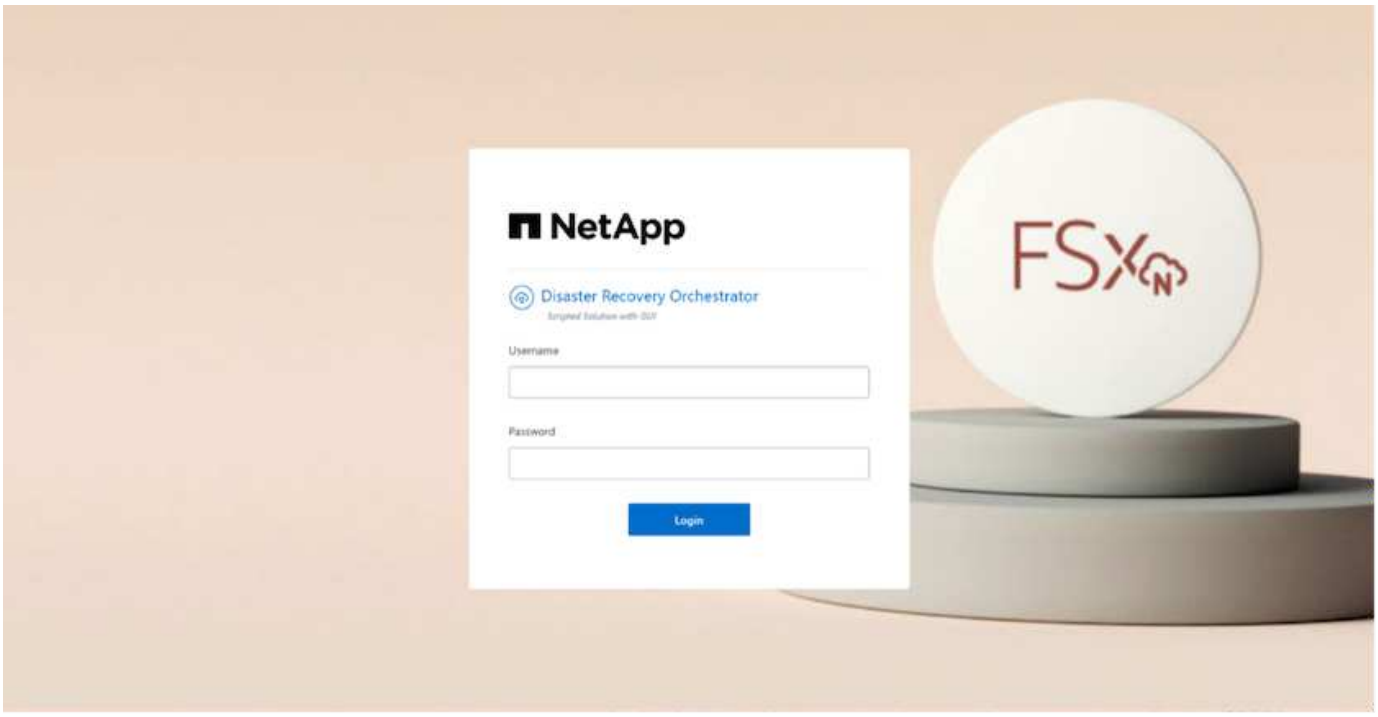
4. Acceda a la interfaz de usuario mediante:

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

   con las siguientes credenciales predeterminadas:

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

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



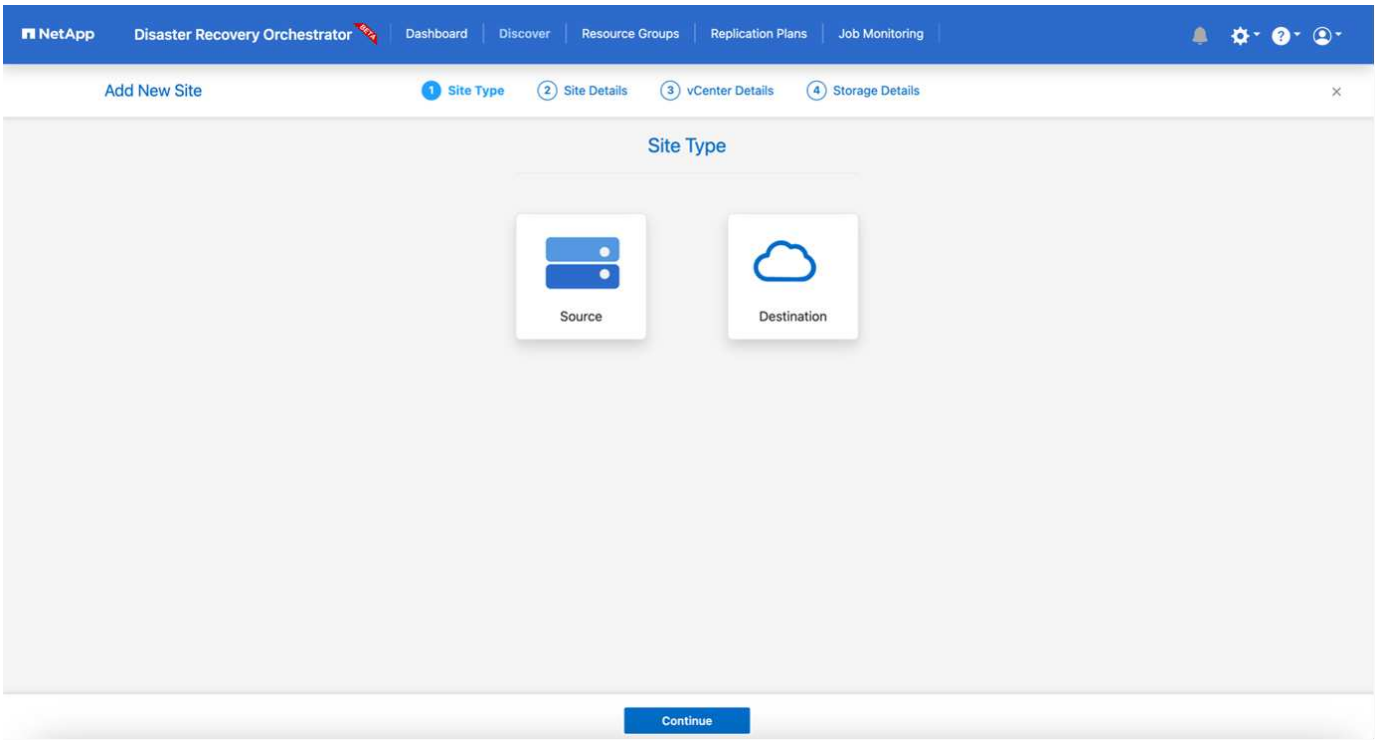
Configuración DE DRO

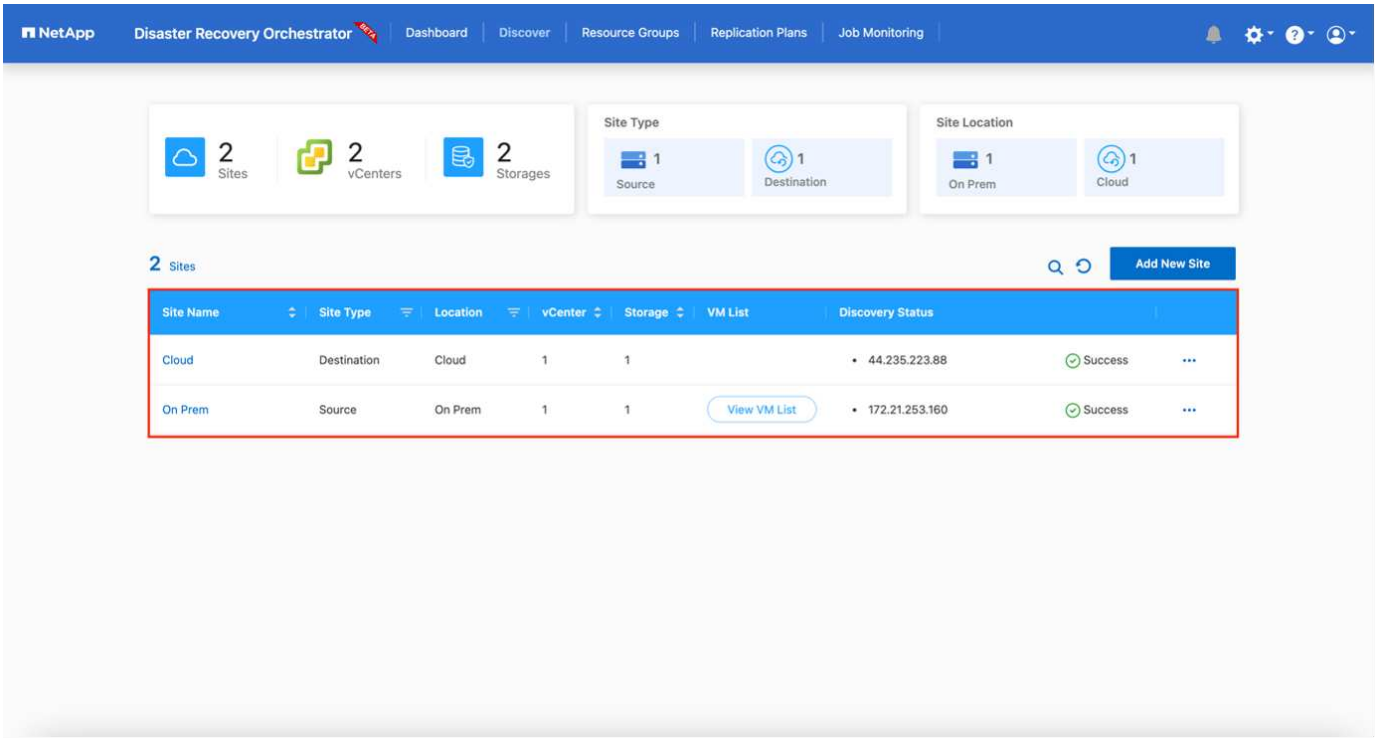
Después de que los FSX para ONTAP y VMC se hayan configurado correctamente, puede empezar a configurar DRO para automatizar la recuperación de las cargas de trabajo en las instalaciones a VMC usando las copias SnapMirror de solo lectura en FSX para ONTAP.

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

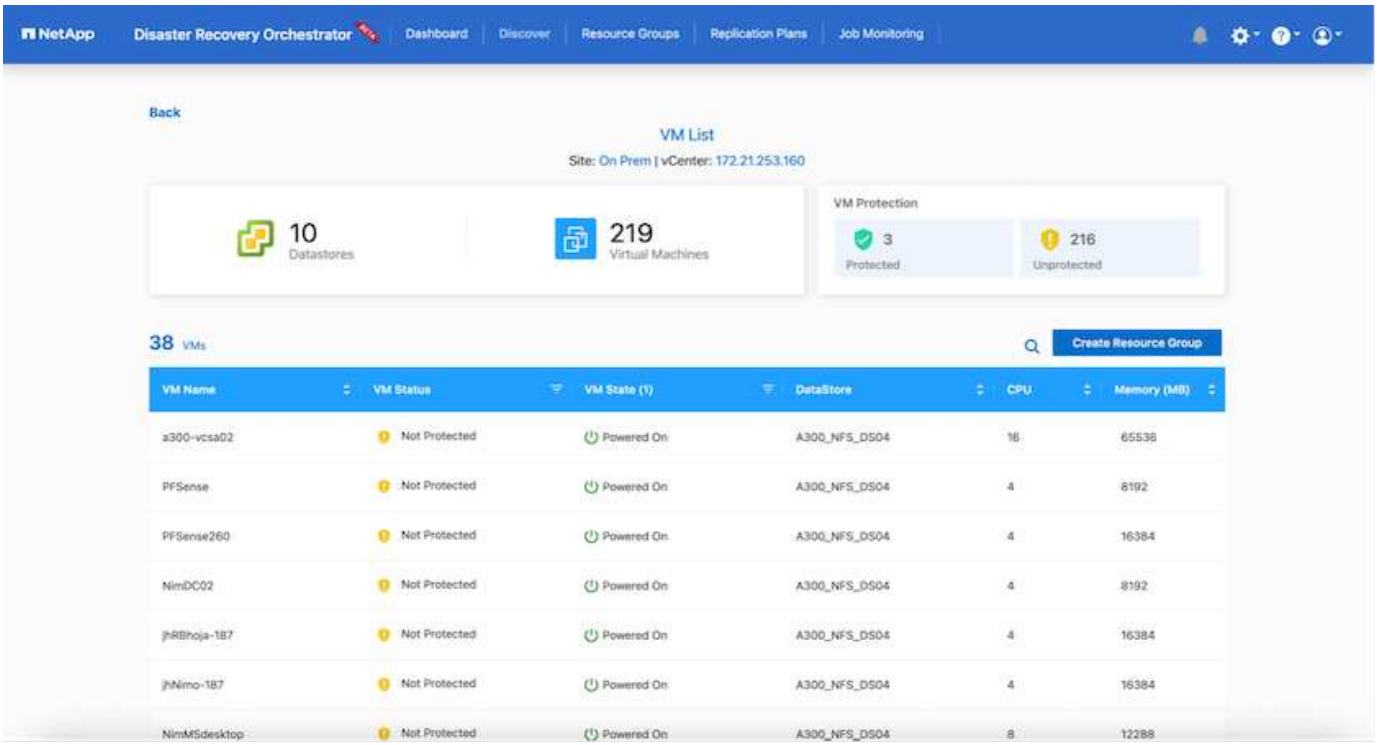
El primer paso es descubrir y añadir los recursos locales y cloud (tanto vCenter como almacenamiento) a la DRO. Abra DRO en un navegador compatible y utilice el nombre de usuario y la contraseña predeterminados (admin/admin) y Add Sites. También se pueden añadir sitios mediante la opción detectar. Añada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

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





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



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

Agrupaciones de recursos

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

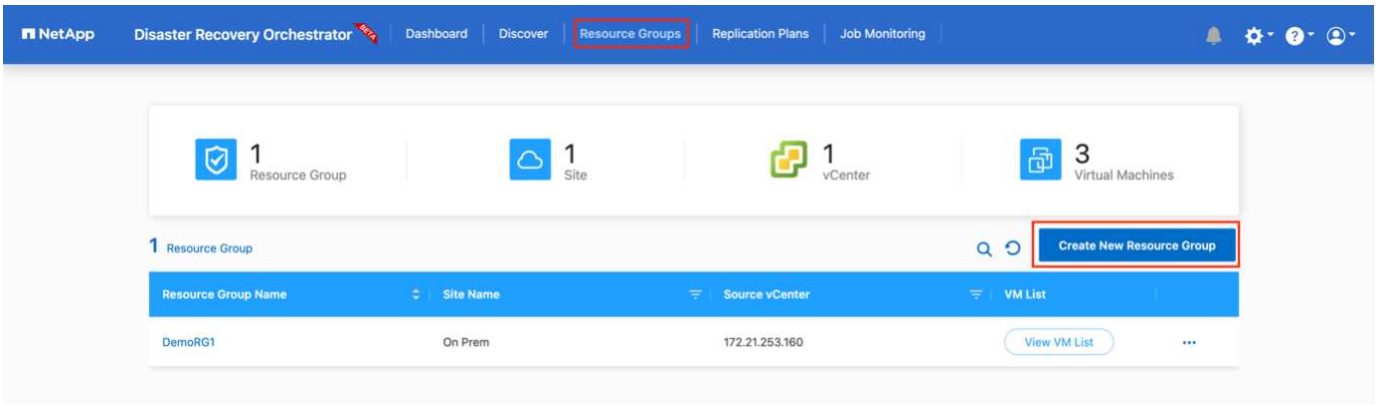
Para comenzar a crear grupos de recursos, complete los siguientes pasos:

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

   Las opciones son estas:

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

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

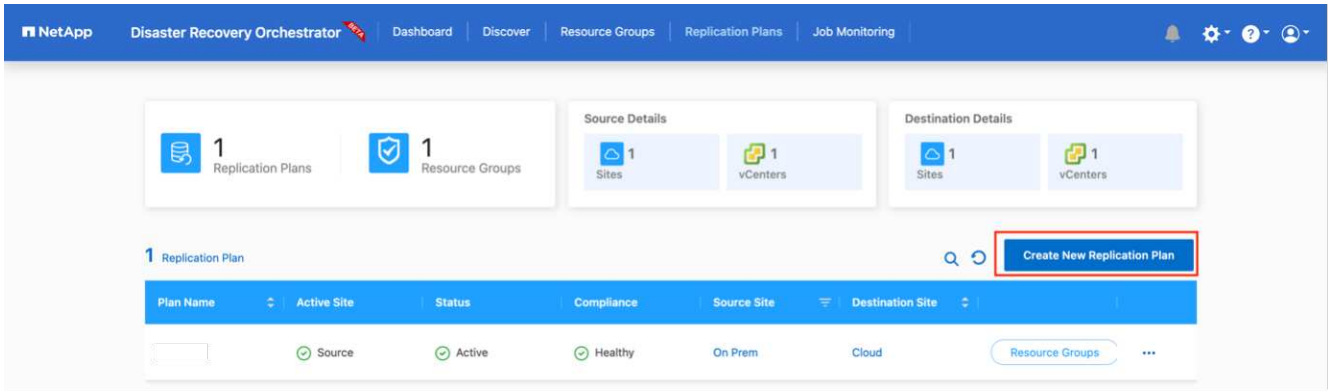


Planes de replicación

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

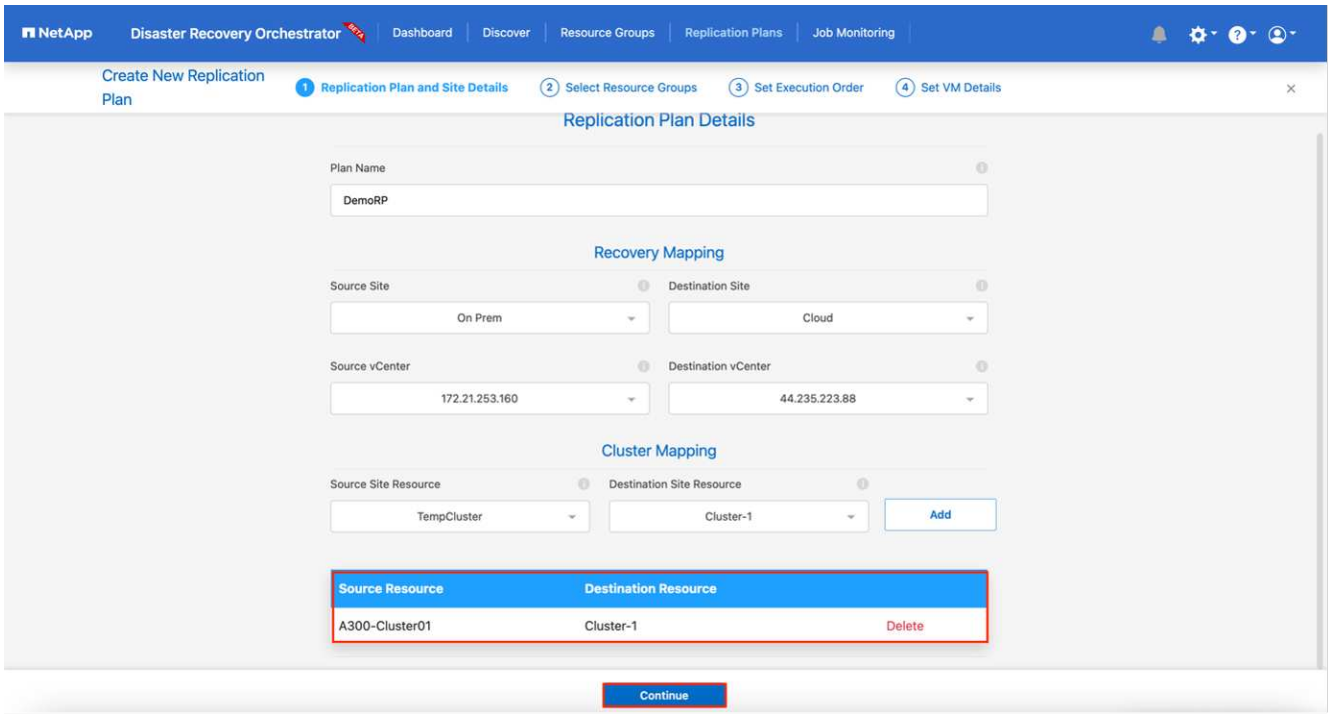
Para comenzar a crear un plan de replicación, lleve a cabo los siguientes pasos:

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



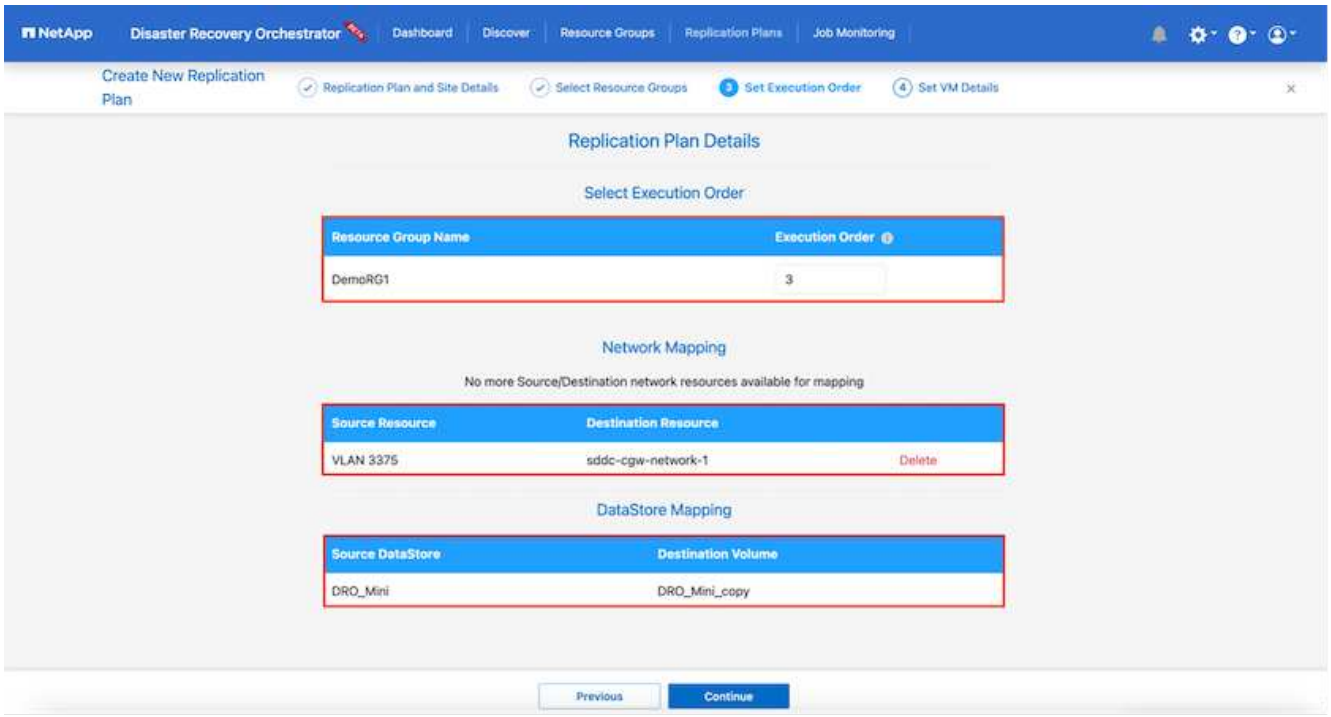
2. En **Nuevo Plan de replicación**, proporcione un nombre para el plan y agregue asignaciones de recuperación seleccionando el sitio de origen, vCenter asociada, sitio de destino y vCenter asociada.

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

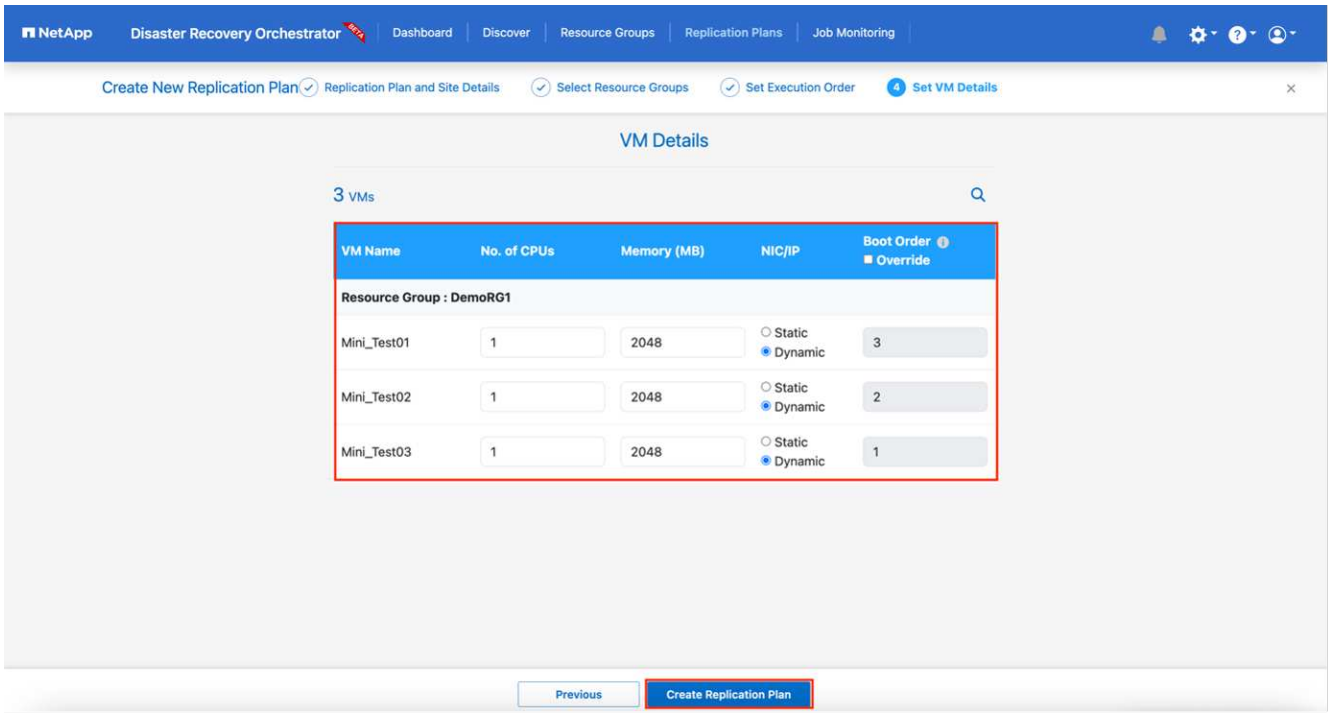


4. Seleccione **Detalles del grupo de recursos** y haga clic en **continuar**.
5. Establezca el orden de ejecución del grupo de recursos. Esta opción permite seleccionar la secuencia de operaciones cuando existen varios grupos de recursos.
6. Una vez que haya terminado, seleccione la asignación de red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

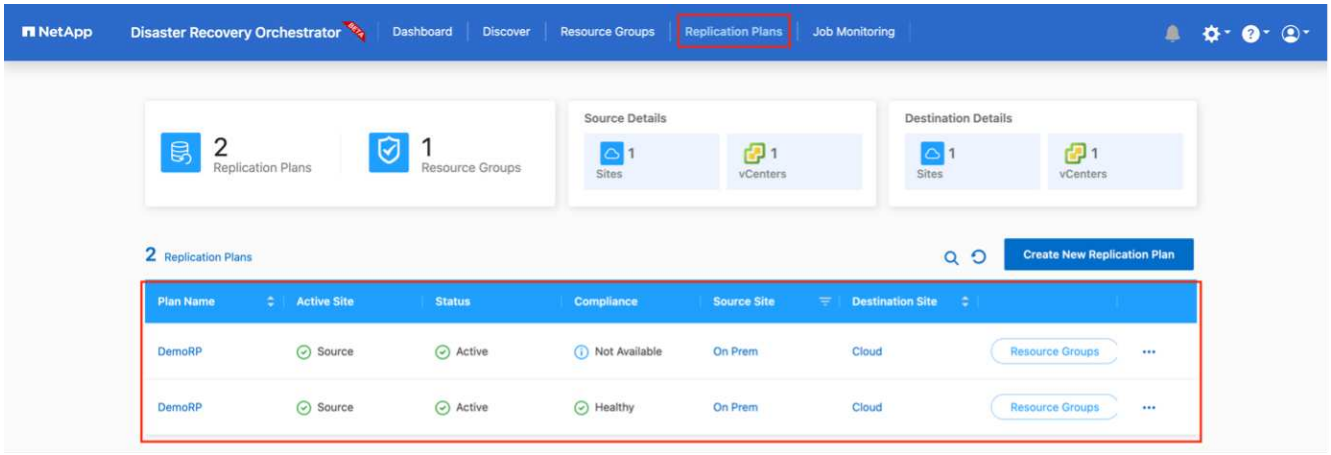
> SnapMirror se encuentra en el nivel de volumen. Por lo tanto, todas las máquinas virtuales se replican en el destino de replicación. Asegúrese de seleccionar todas las máquinas virtuales que forman parte del almacén de datos. Si no se seleccionan, solo se procesan las máquinas virtuales que forman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



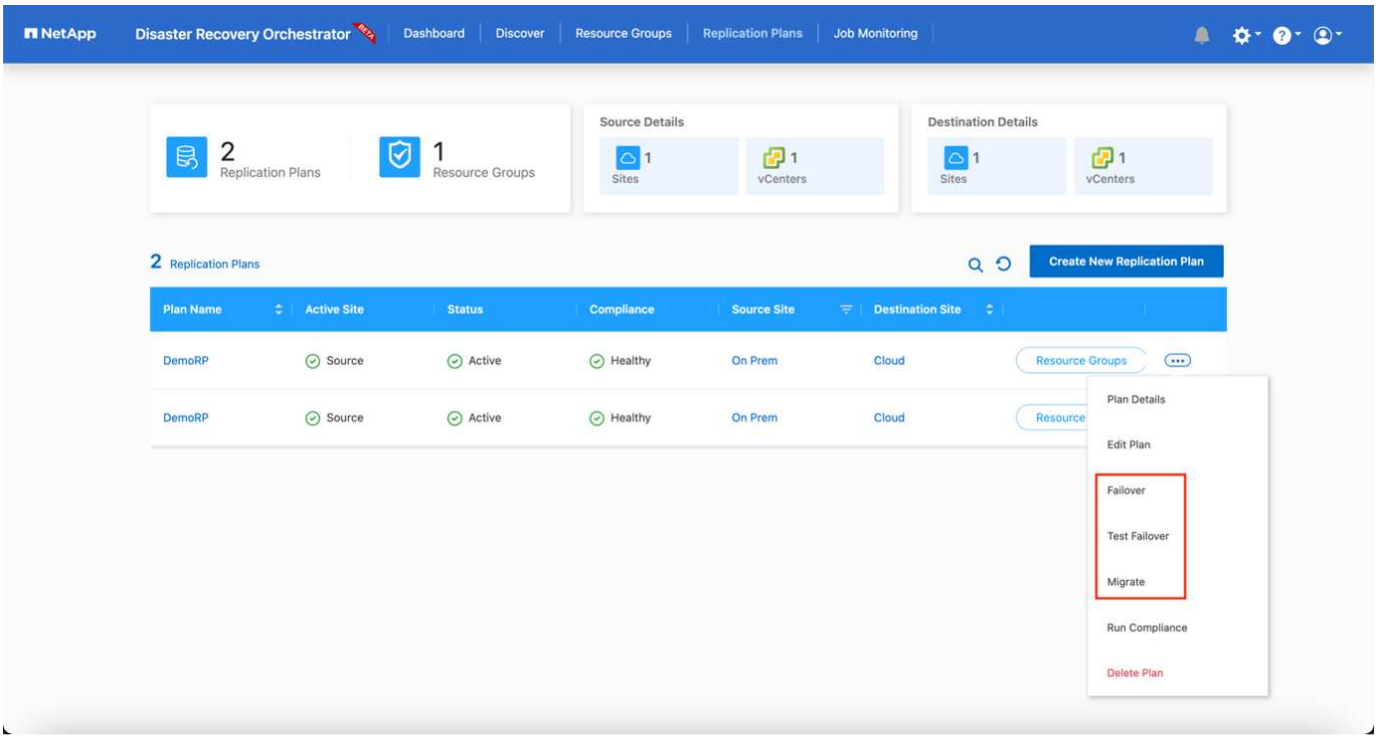
8. Si se especifican los datos del equipo virtual, se puede modificar de forma opcional el tamaño de los parámetros de RAM y CPU del equipo virtual; esto puede resultar muy útil a la hora de recuperar entornos de gran tamaño en clústeres de destino más pequeños o realizar pruebas de recuperación ante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



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

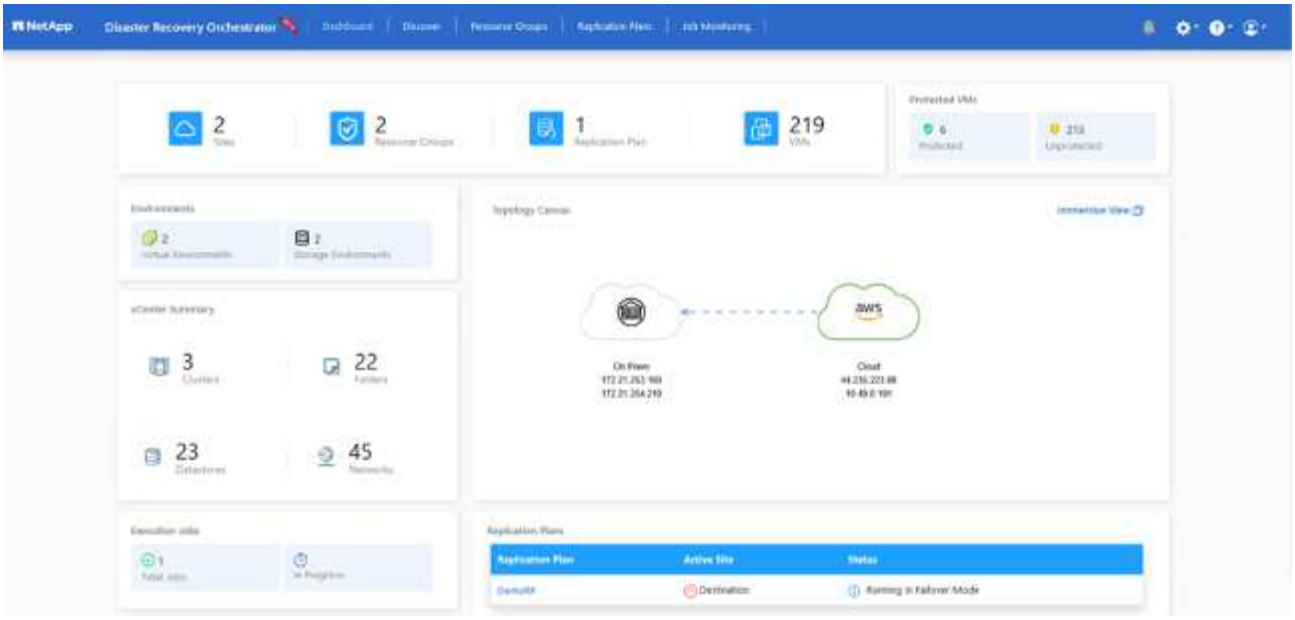


Una vez creado el plan de replicación, la opción de conmutación por error, la opción de conmutación por error de prueba o la opción de migración se pueden ejercer en función de los requisitos. Durante las opciones de conmutación por error y conmutación al nodo de respaldo, se utiliza la copia Snapshot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

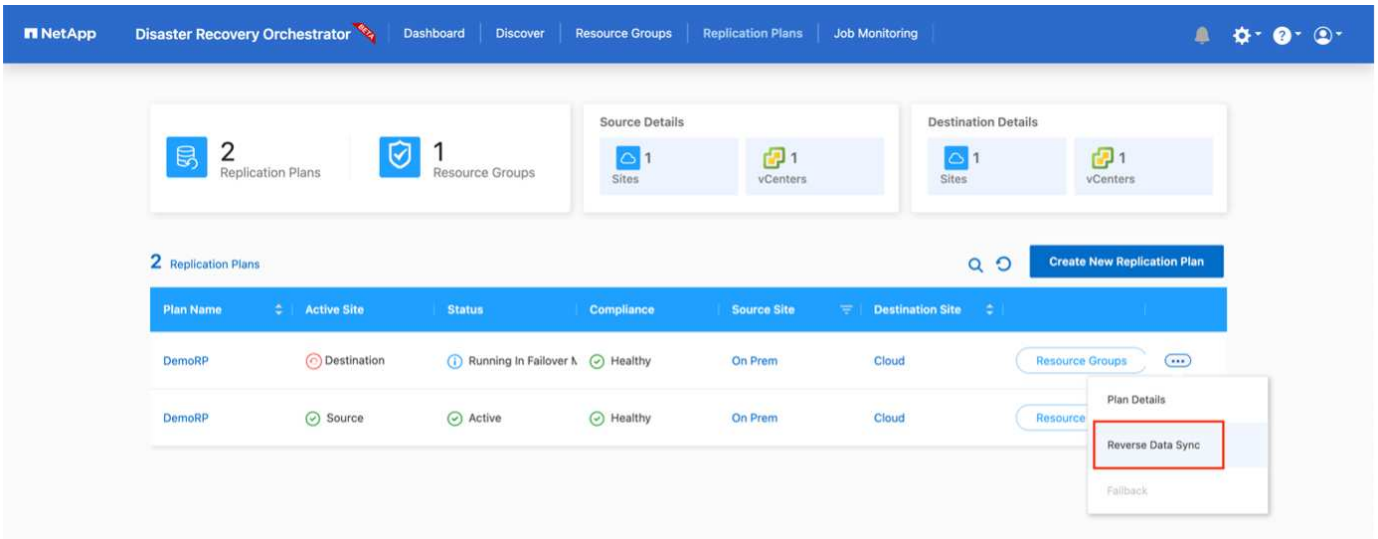


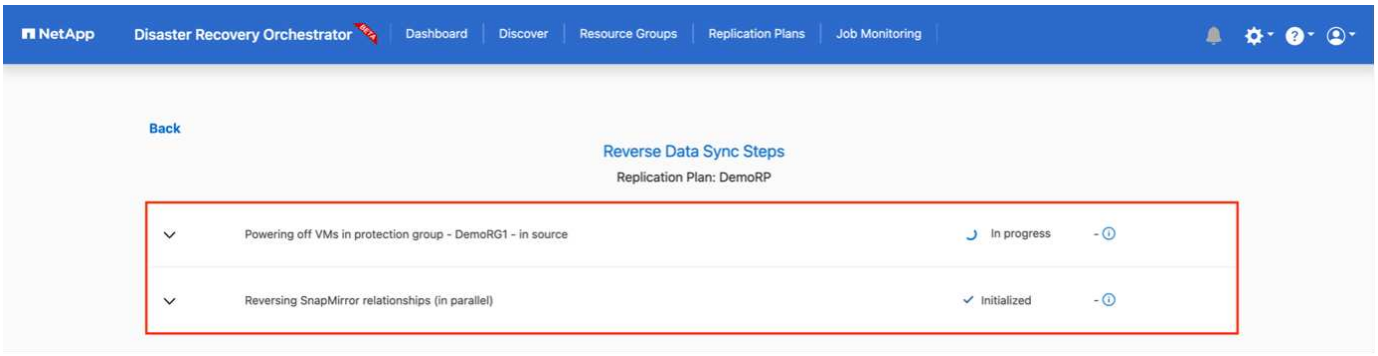
El plan de replicación se puede supervisar en el menú de tareas:

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

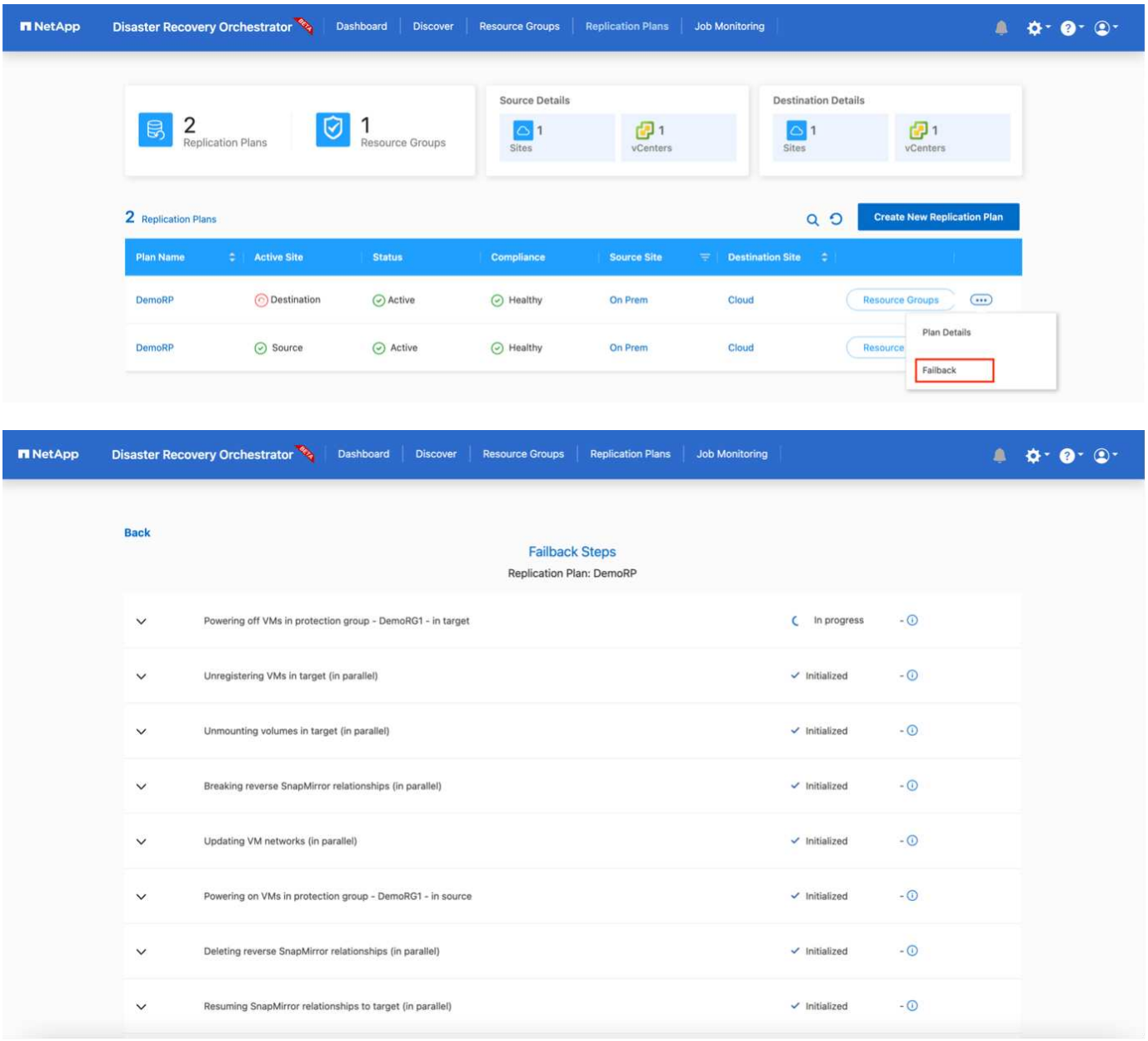


La conmutación por recuperación se puede activar en el nivel de plan de replicación. En el caso de una conmutación por error de prueba, se puede utilizar la opción de eliminación para revertir los cambios y eliminar la relación de FlexClone. La conmutación por recuperación relacionada con la conmutación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

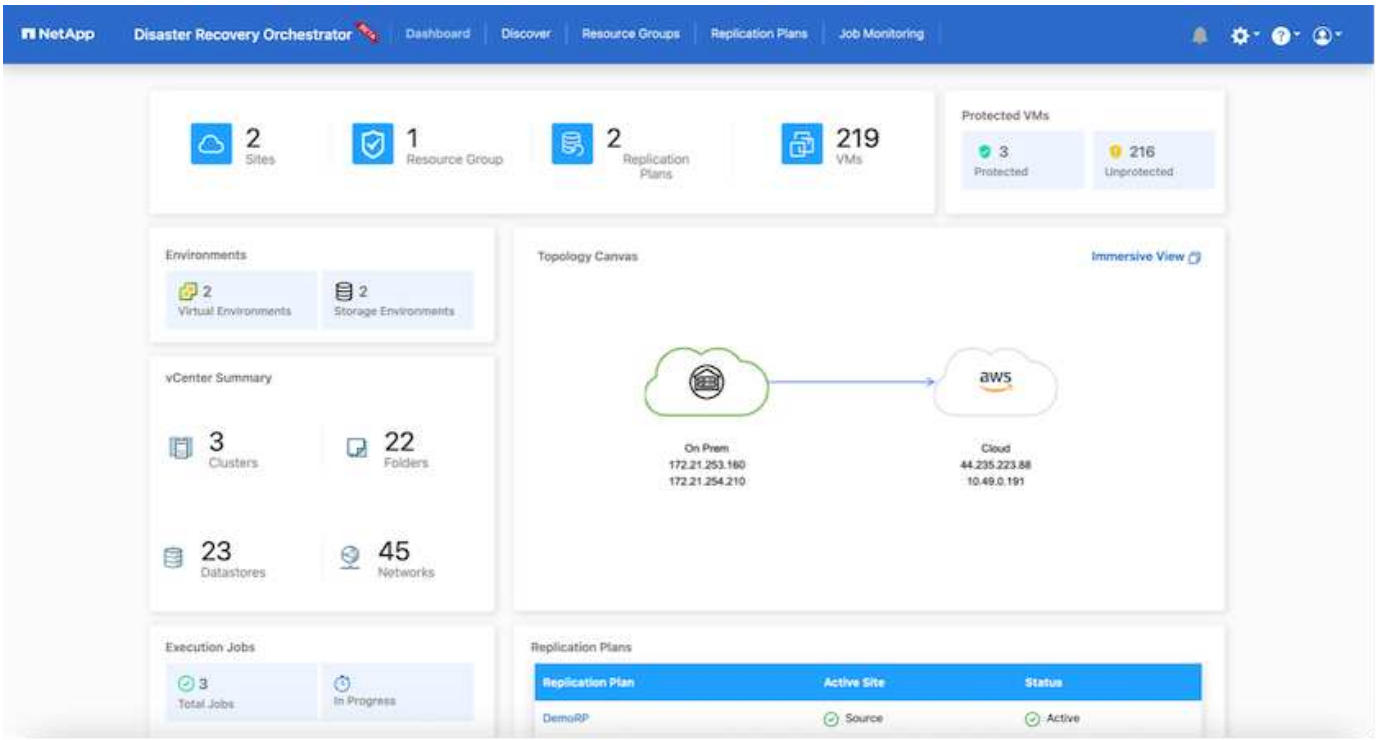




Una vez finalizada, puede activar la conmutación tras recuperación para volver a la instalación de producción original.



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



Recuperación de ransomware

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

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

Beneficios

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

Autor: Niyaz Mohamed - Ingeniería de Soluciones NetApp

Descripción general

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

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

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

Declaración del problema

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

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

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

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

Cuando se realiza una conmutación por error, una máquina virtual replicada asume el rol de la máquina virtual original. La conmutación por error se puede realizar en el estado más reciente de una réplica o en cualquiera de sus puntos de restauración conocidos. Esto permite la recuperación frente al ransomware o las pruebas aisladas según sea necesario. En Veeam Backup & Replication, la conmutación por error y la conmutación tras recuperación son pasos intermedios temporales que deberían completarse aún más. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.

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

Puesta en marcha de la solución

Escalones de alto nivel

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

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

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

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

Detalles de la implementación

Paso 1: Replicar máquinas virtuales

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

Para replicar equipos virtuales, siga los siguientes pasos:

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

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

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

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

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

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

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

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

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

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

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

Paso 2: Crear un plan de failover

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

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

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

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

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

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

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

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

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

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

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

Paso 3: Ejecute el plan de failover

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

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

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

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

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

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

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

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

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

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

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

Paso 4: Conmutación por recuperación al sitio de producción

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusión

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

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

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

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

Migrar cargas de trabajo en AWS / VMC

TR 4942: Migre cargas de trabajo al almacén de datos FSX ONTAP mediante VMware HCX

Autores: Ingeniería de soluciones de NetApp

Descripción general: Migración de máquinas virtuales con VMware HCX, almacenes de datos complementarios de FSX ONTAP y VMware Cloud

Un caso práctico común para VMware Cloud (VMC) en Amazon Web Services (AWS), con su almacén de datos NFS complementario en Amazon FSX para ONTAP de NetApp, es la migración de cargas de trabajo de VMware. VMware HCX es la opción preferida y proporciona diversos métodos de migración para mover máquinas virtuales (VM) locales y sus datos, ejecutándose en cualquier almacén de datos compatibles con VMware, a almacenes de datos VMC, lo que incluye almacenes de datos NFS complementarios en FSX para ONTAP.

VMware HCX es principalmente una plataforma de movilidad que está diseñada para simplificar la migración de cargas de trabajo, el reequilibrado de las cargas de trabajo y la continuidad empresarial entre clouds. Se incluye como parte de VMware Cloud en AWS y ofrece muchas formas de migrar cargas de trabajo y se puede usar para operaciones de recuperación ante desastres.

Este documento proporciona una guía paso a paso para la puesta en marcha y configuración de VMware HCX, incluidos todos sus componentes principales, tanto en las instalaciones como en el centro de datos de cloud, lo cual permite disponer de diversos mecanismos de migración de equipos virtuales.

Para obtener más información, consulte "Introducción a las implementaciones de HCX" y.. "Lista de comprobación de instalación B - HCX con VMware Cloud en el entorno de destino AWS SDDC".

Escalones 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 de OVA del conector HCX en la instancia local de vCenter Server.
3. Active HCX con una clave de licencia.
4. Emparejar el conector VMware HCX en las instalaciones con VMC HCX Cloud Manager.
5. Configure el perfil de red, el perfil de computación y la malla de servicio.
6. (Opcional) realice la extensión de red para ampliar la red y evitar la reIP.
7. Valide el estado del dispositivo y asegúrese de que la migración sea posible.
8. Migrar las cargas de trabajo de la máquina virtual.

Requisitos previos

Antes de empezar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte "Preparación para la instalación del HCX". Una vez que se hayan establecido los requisitos previos, incluida la conectividad, configure y active HCX generando una clave de licencia desde la consola VMware HCX en VMC. Después de activar HCX, se implementa el plugin de vCenter y es posible acceder a él mediante la consola de vCenter para la gestión.

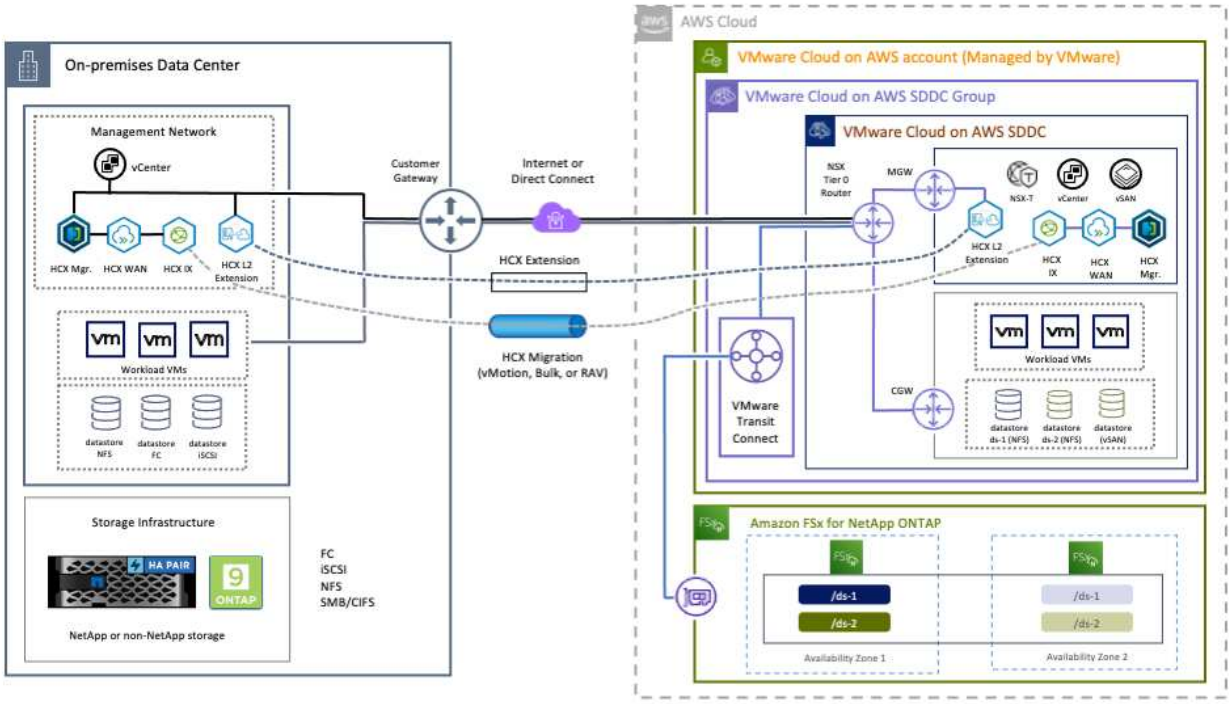
Antes de continuar con la activación e implementación de HCX, deben completarse los siguientes pasos de instalación:

1. Utilice un VMware SDDC existente o cree un nuevo SDDC a continuación "Enlace a NetApp" o esto "Enlace de VMware".
2. La ruta de red desde el entorno vCenter en las instalaciones al centro de datos definido por software de VMC debe admitir la migración de máquinas virtuales mediante vMotion.
3. Asegúrese de que es necesario "reglas y puertos del firewall" Se permiten para el tráfico de vMotion entre la instancia local de vCenter Server y SDDC vCenter.
4. El volumen NFS de FSX para ONTAP debe montarse como un almacén de datos complementario en el centro de datos VMC SDDC. Para conectar los almacenes de datos NFS al clúster adecuado, siga los pasos que se describen en este "Enlace a NetApp" o esto "Enlace de VMware".

Arquitectura de alto nivel

Para realizar las pruebas, el entorno de laboratorio local utilizado para esta validación se conectó mediante una VPN sitio a sitio a AWS VPC, que permitía la conectividad local con AWS y al centro de datos definido por software de cloud de VMware mediante una puerta de enlace de tránsito externa. La migración HCX y la extensión del tráfico de red fluyen por Internet entre el SDDC de destino en las instalaciones y el de cloud de VMware. Esta arquitectura se puede modificar para utilizar interfaces virtuales privadas de Direct Connect.

La siguiente imagen muestra la arquitectura de alto nivel.



Puesta en marcha de la solución

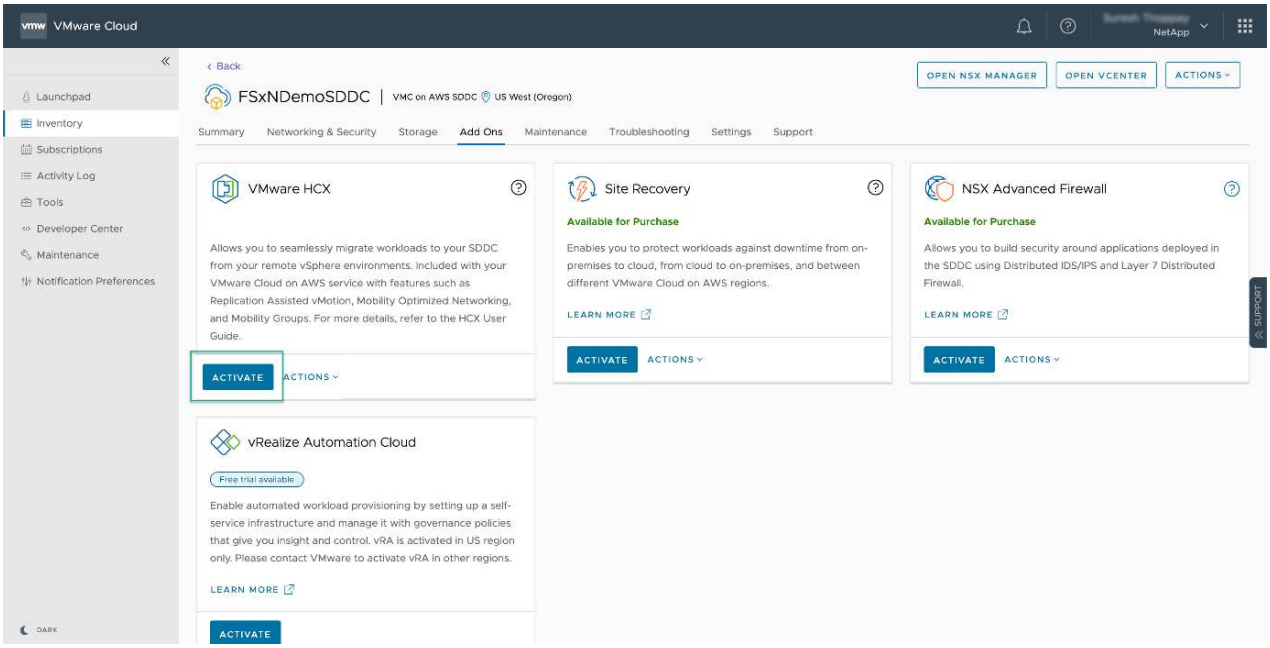
Siga la serie de pasos para completar la implementación de esta solución:

Paso 1: Active HCX mediante VMC SDDC mediante la opción Add-ons

Para realizar la instalación, lleve a cabo los siguientes pasos:

1. Inicie sesión en la consola VMC en "vmc.vmware.com" Y acceder al inventario.
2. Para seleccionar el SDDC adecuado y acceder a los Add- ons, haga clic en Ver detalles en SDDC y seleccione la pestaña Add Ons.
3. Haga clic en Activate for VMware HCX.

   Este paso tarda hasta 25 minutos en completarse.

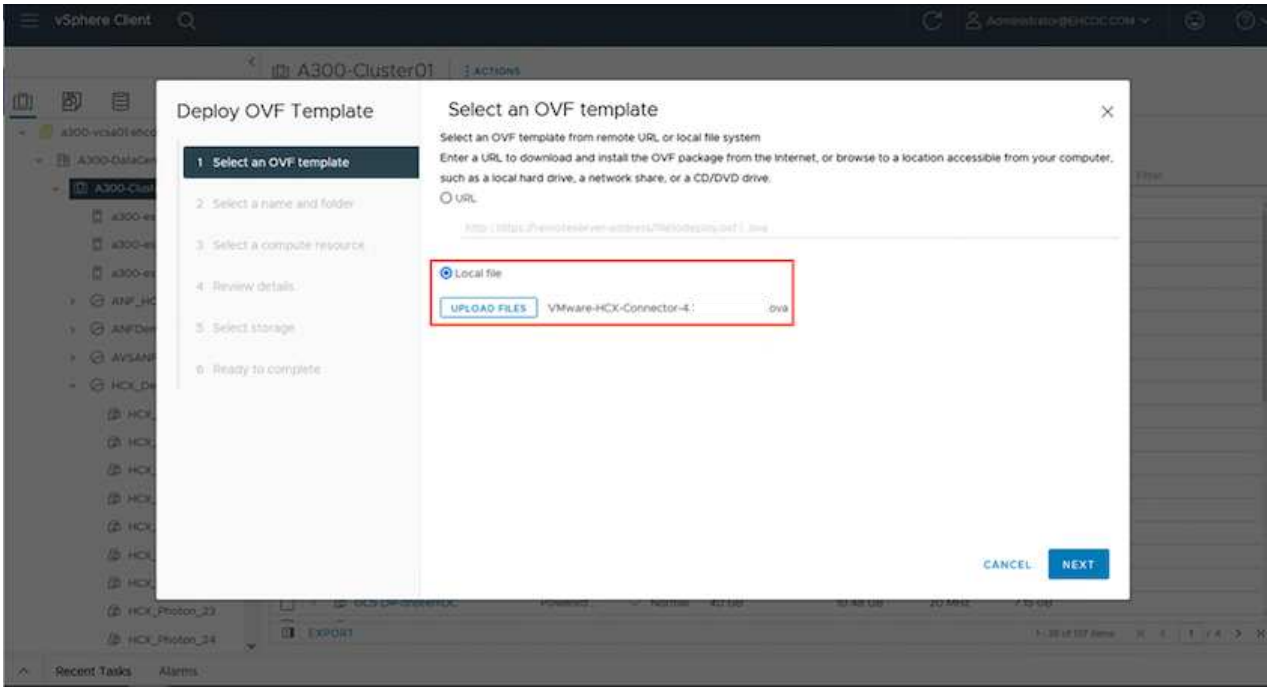


4. Una vez completada la implementación, valide la implementación confirmando que HCX Manager y sus plugins asociados están disponibles en vCenter Console.
5. Cree los firewalls de Management Gateway adecuados para abrir los puertos necesarios para acceder a HCX Cloud Manager.HCX Cloud Manager ahora está listo para operaciones HCX.

Paso 2: Ponga en marcha el OVA del instalador en la instancia local de vCenter Server

Para que el conector local se comunique con HCX Manager en VMC, asegúrese de que los puertos de firewall adecuados están abiertos en el entorno local.

1. Desde la consola VMC, vaya al panel HCX, vaya a Administración y seleccione la ficha 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 vCenter Server local. Haga clic con el botón derecho en vSphere Cluster y seleccione la opción Deploy OVF Template.

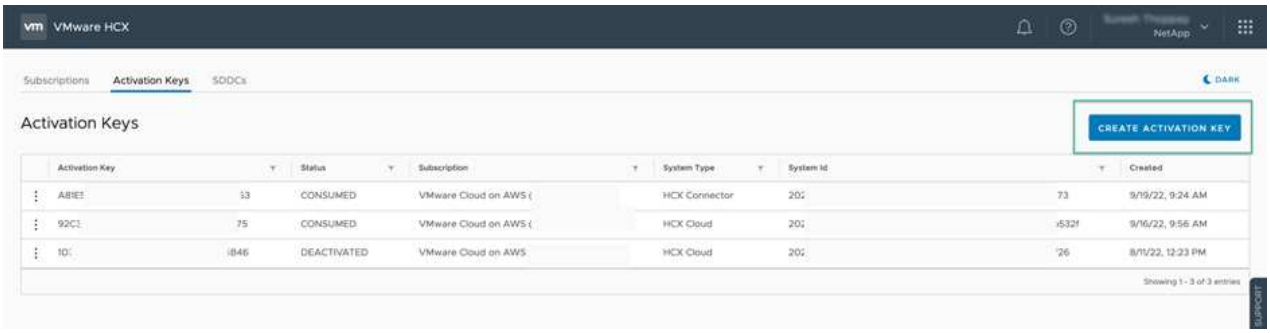


3. Introduzca la información necesaria en el asistente implementar plantilla OVF, haga clic en Siguiente y, a continuación, en Finalizar para implementar el OVA del conector HCX de VMware.
4. Encienda el dispositivo virtual manualmente.para obtener instrucciones paso a paso, vaya a. "Guía del usuario de VMware HCX".

Paso 3: Active el conector HCX con la clave de licencia

Después de implementar el OVA del conector HCX de VMware en las instalaciones e iniciar el dispositivo, lleve a cabo los siguientes pasos para activar el conector HCX. Genere la clave de licencia desde la consola VMware HCX en VMC e introduzca la licencia durante la configuración del conector VMware HCX.

1. En VMware Cloud Console, vaya a Inventory, seleccione el centro de datos definido por software y haga clic en View Details. En la pestaña Add Ons, en el icono VMware HCX, haga clic en Open HCX.
2. En la ficha 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. Copie la clave de activación.



> Se necesita una llave independiente para cada conector HCX desplegado en las instalaciones.

3. Inicie sesión en el conector VMware HCX local en "https://hcxconnectorIP:9443" uso de las credenciales de administrador.

> Utilice la contraseña definida durante la implementación de OVA.

4. En la sección licencias, introduzca la clave de activación copiada en el 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 Datacenter Location, proporcione la ubicación deseada para instalar VMware HCX Manager en las instalaciones. Haga clic en Continue.
6. En Nombre del sistema, actualice el nombre y haga clic en continuar.
7. Seleccione Sí y, a continuación, continúe.
8. En Connect your vCenter, proporcione la dirección IP o el nombre de dominio completo (FQDN) y las credenciales de vCenter Server y haga clic en Continue.

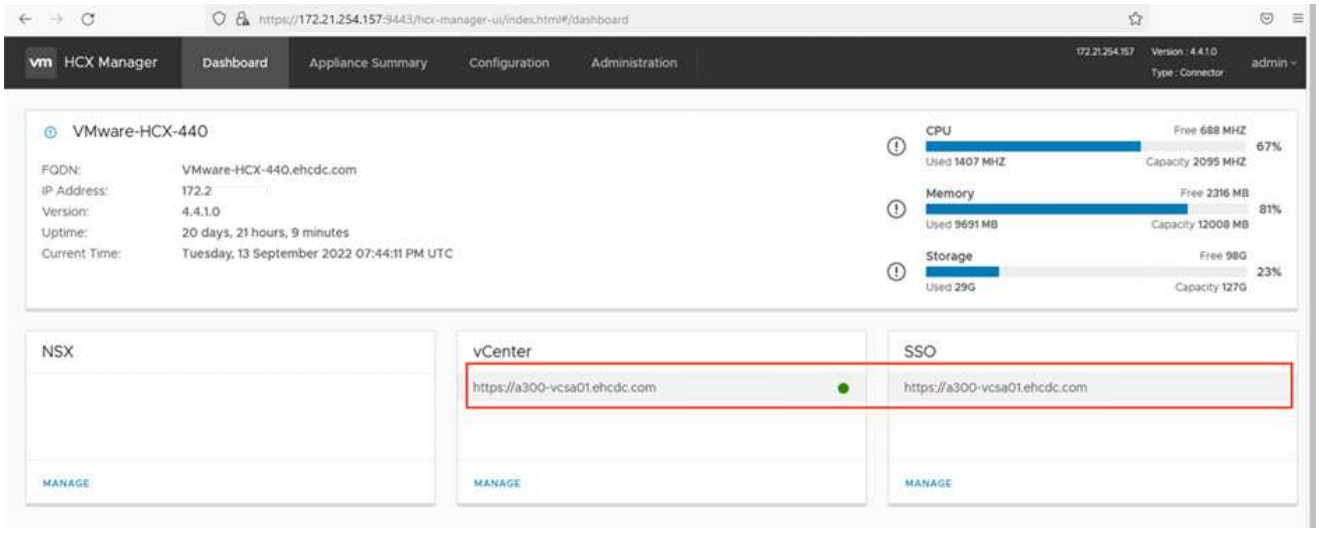
> Utilice el FQDN para evitar problemas de comunicación más adelante.

9. En Configure SSO/PSC, proporcione el FQDN o la dirección IP de Platform Services Controller y haga clic en Continue.

> Introduzca la dirección IP o el FQDN de vCenter Server.

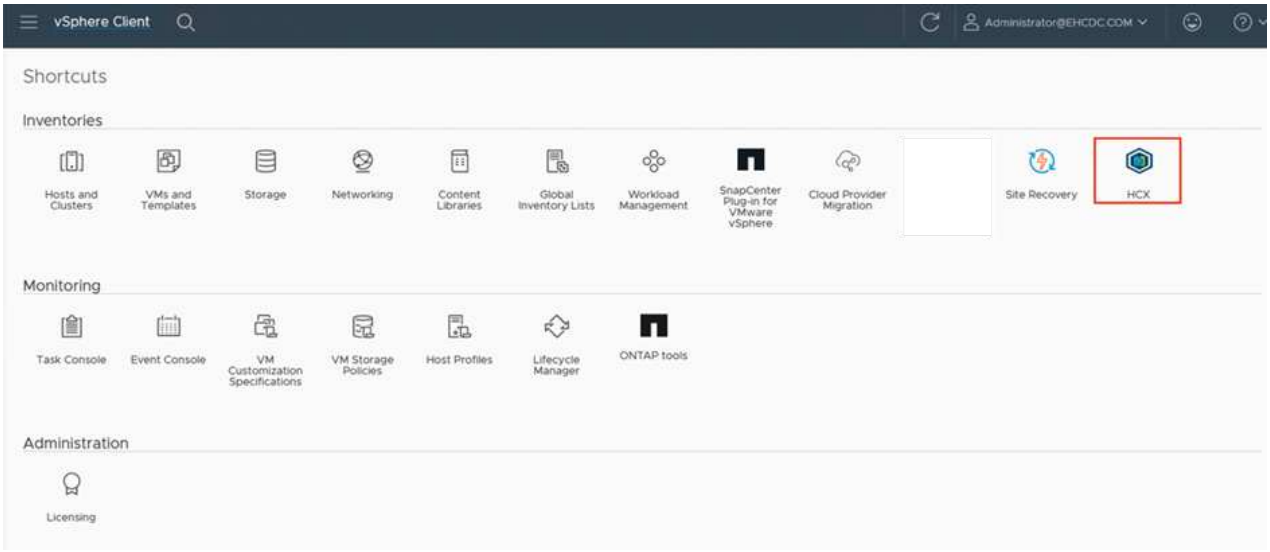
10. Compruebe que la información se haya introducido correctamente y haga clic en Restart.
11. Una vez completado, la instancia de vCenter Server se muestra como verde. Tanto la instancia de vCenter Server como el de SSO deben tener los parámetros de configuración correctos, que deben ser los mismos que la página anterior.

> Este proceso debe tardar aproximadamente de 10 a 20 minutos y el plugin se debe añadir a vCenter Server.

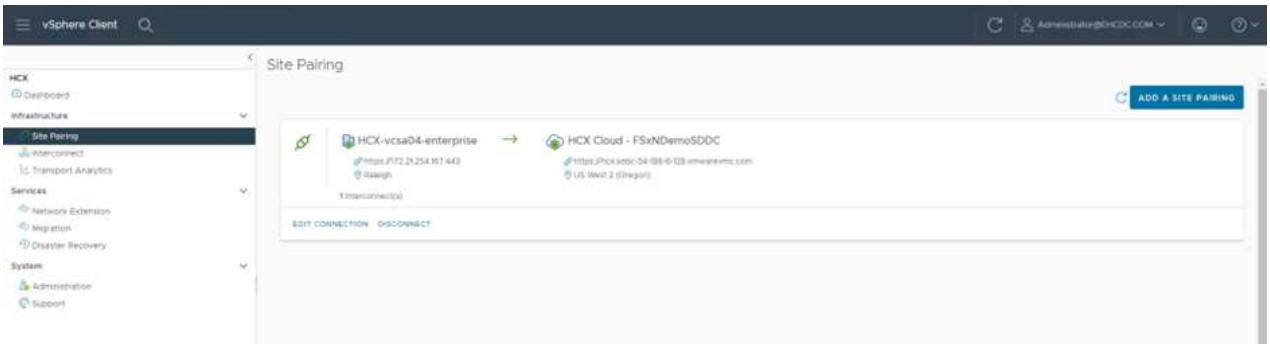


Paso 4: Emparejar el conector VMware HCX en las instalaciones con VMC HCX Cloud Manager

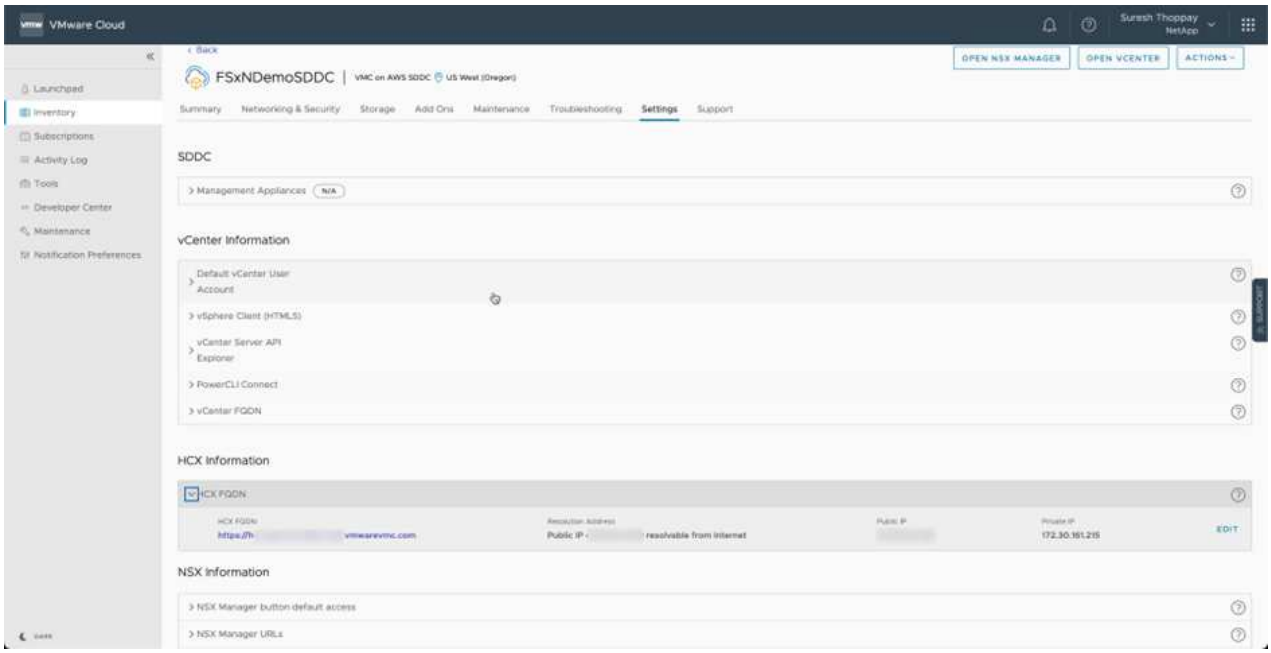
1. Para crear un par de sitios entre la instancia local de vCenter Server y el SDDC de VMC, inicie sesión en la instancia local de vCenter Server y acceda al plugin HCX vSphere Web Client.

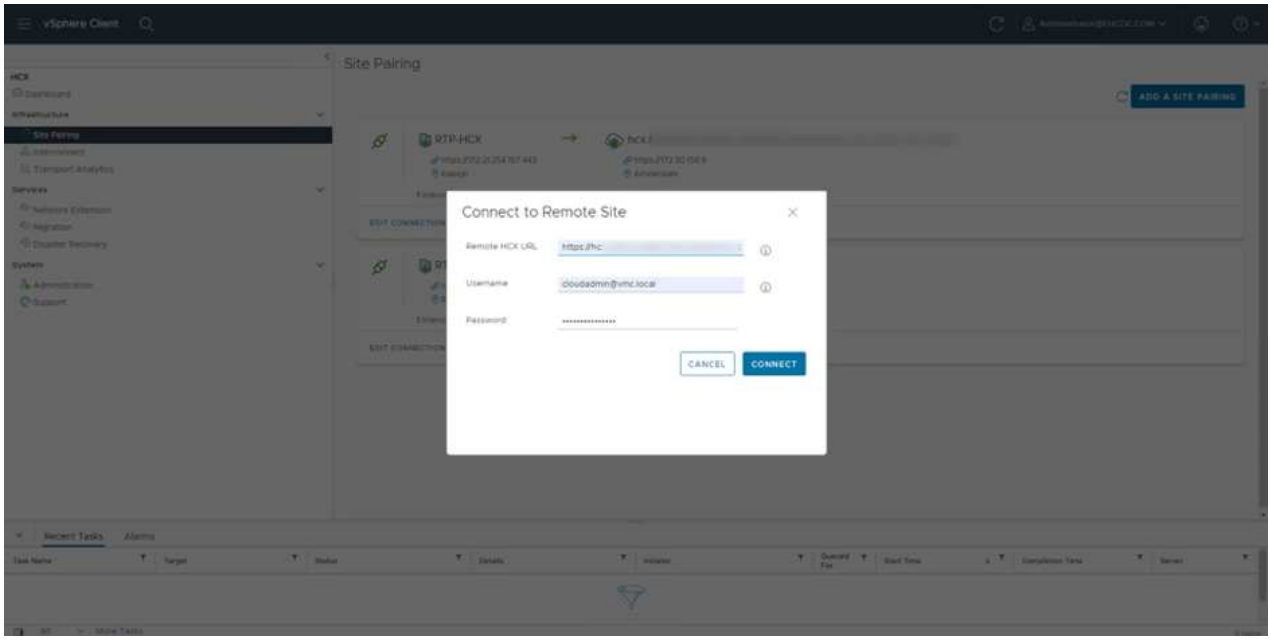


2. En Infraestructura, haga clic en Agregar un emparejamiento de sitios. Para autenticar el sitio remoto, introduzca la dirección IP o la URL de HCX Cloud Manager de VMC y las credenciales del rol CloudAdmin.



La información HCX se puede recuperar desde la página SDDC Settings.





3. Para iniciar el emparejamiento de sitios, haga clic en conectar.

> El conector HCX de VMware debe poder comunicarse con HCX Cloud Manager IP a través del puerto 443.

4. Una vez creado el emparejamiento, el emparejamiento de sitios recién configurado está disponible en el panel de HCX.

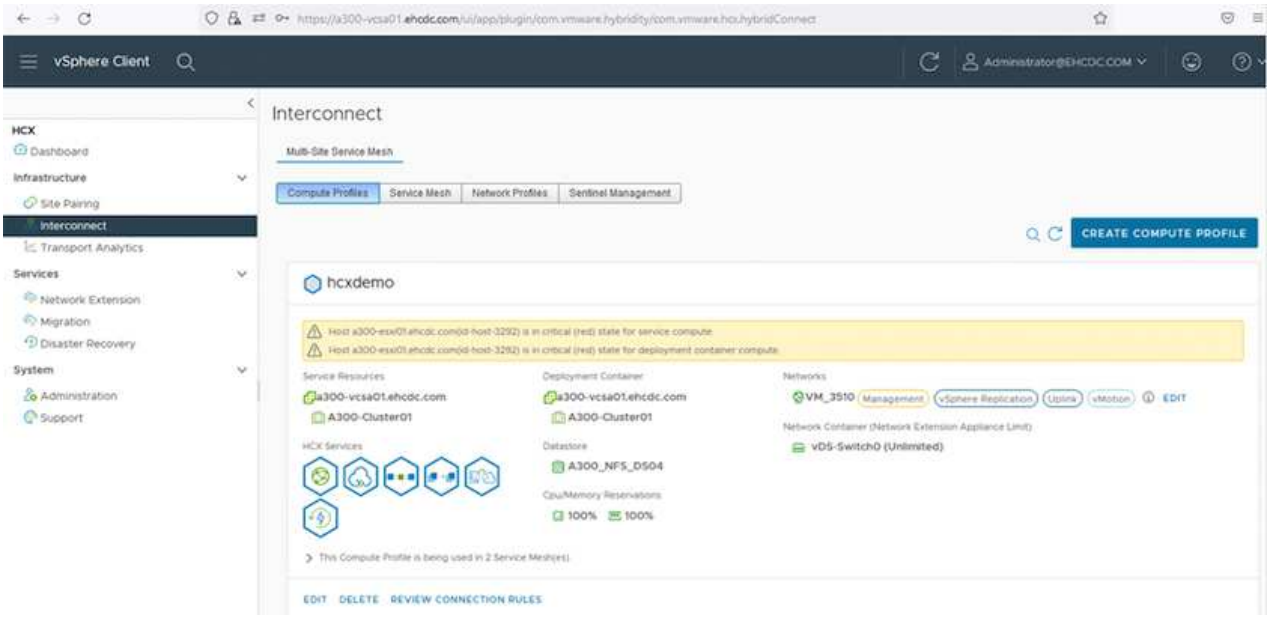
Paso 5: Configure el perfil de red, el perfil de computación y la malla de servicio

El dispositivo VMware HCX Interconnect (HCX-IX) proporciona capacidades de túnel seguro a través de Internet y conexiones privadas al sitio de destino que permiten 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, lleve a cabo los siguientes pasos:

1. En Infrastructure, seleccione Interconnect > malla de servicio multisitio > Compute Profiles > Create Compute Profile.

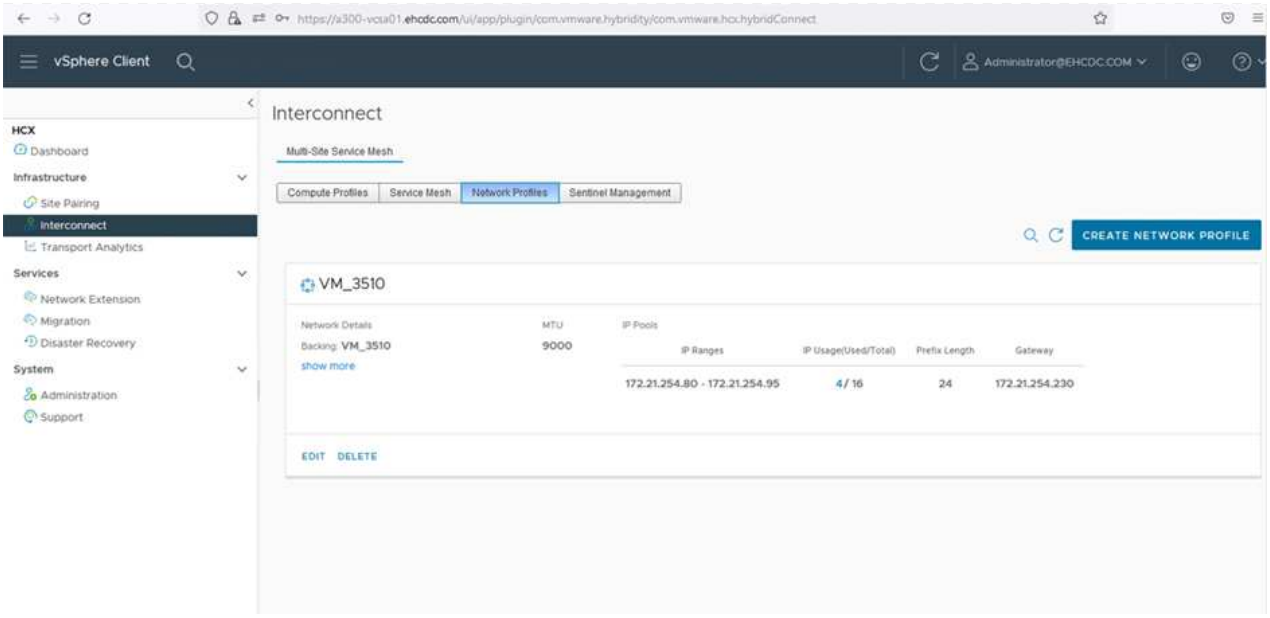
   Los perfiles de computación contienen los parámetros de puesta en marcha de computación, almacenamiento y red necesarios para poner en marcha un dispositivo virtual de interconexión. También especifican qué parte del centro de datos de VMware será accesible al servicio HCX.

   Para obtener instrucciones detalladas, consulte "Crear un perfil de computación".



2. Una vez creado el perfil de computación, cree el perfil de red seleccionando malla de servicio multisitio > Perfiles de red > Crear perfil de red.
3. El perfil de red define un rango de direcciones IP y redes que utilizará HCX para sus dispositivos virtuales.

   Esto requerirá dos o más direcciones IP. Estas direcciones IP se asignarán desde la red de gestión a los dispositivos virtuales.

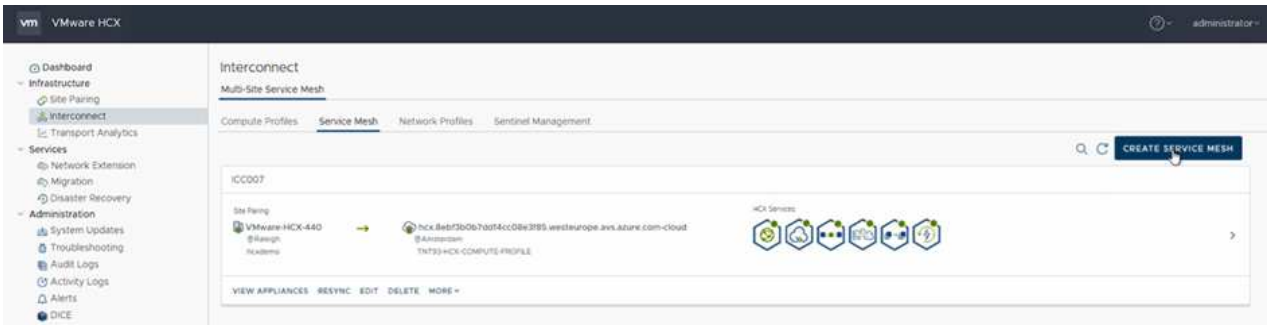


Para obtener instrucciones detalladas, consulte "Creación de un perfil de red".

> Si está conectando con una SD-WAN a través de Internet, tiene que reservar IP públicas en la sección redes y seguridad.

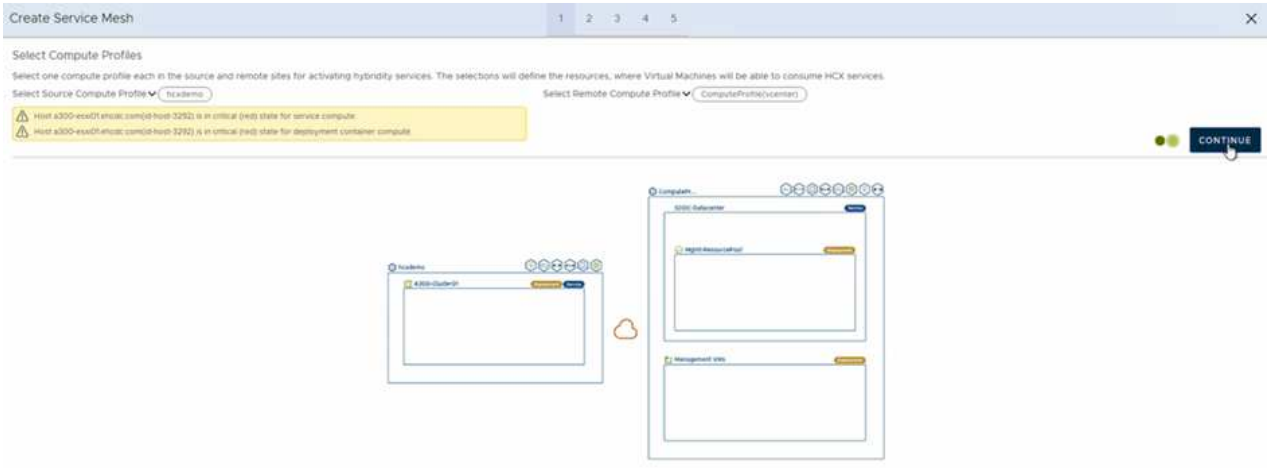
4. Para crear una malla de servicio, seleccione la pestaña malla de servicio dentro de la opción Interconnect (interconexión) y seleccione sites in situ y VMC SDDC.

   La malla de servicio establece un par de perfiles de red y de computación local y remota.

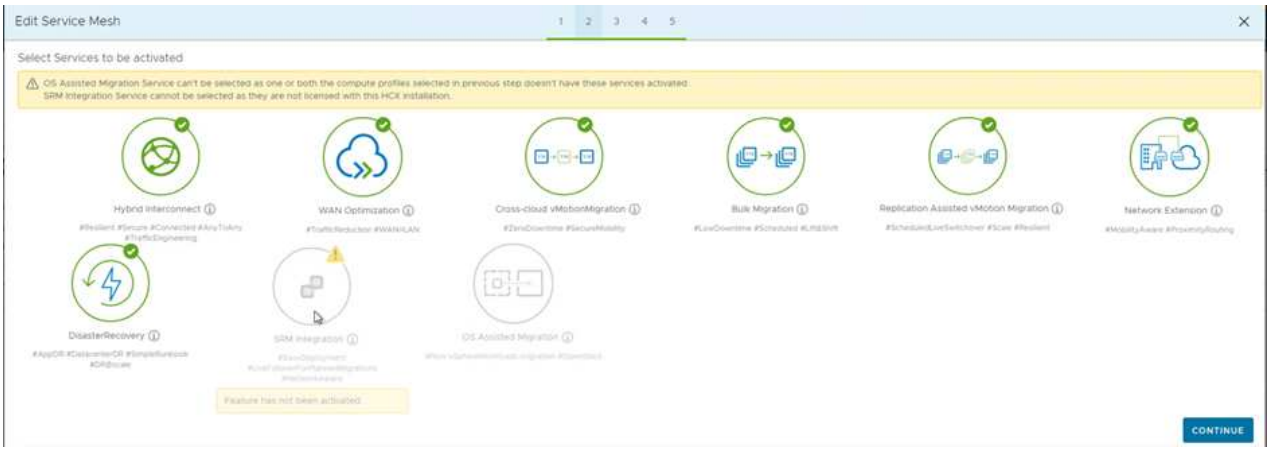


> Parte de este proceso implica la implementación de dispositivos HCX que se configurarán automáticamente tanto en los sitios de origen como en los de destino, con lo que se creará una estructura de transporte segura.

5. Seleccione los perfiles de computación de origen y remoto y haga clic en Continue.

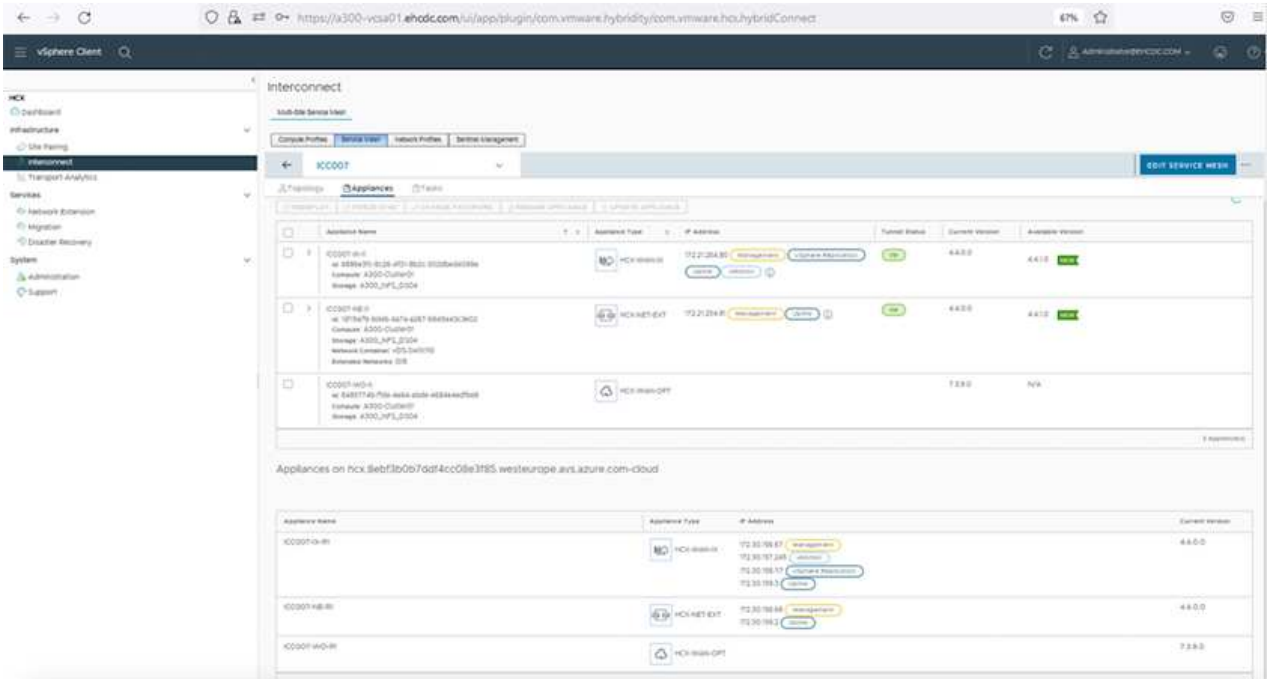


6. Seleccione el servicio que desea activar y haga clic en continuar.



> Se requiere una licencia HCX Enterprise para la migración de vMotion asistida con 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 puesta en marcha tardará aproximadamente 30 minutos en completarse. Una vez configurada la malla de servicio, se crean las máquinas virtuales y las redes necesarias para migrar las máquinas virtuales de carga de trabajo.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

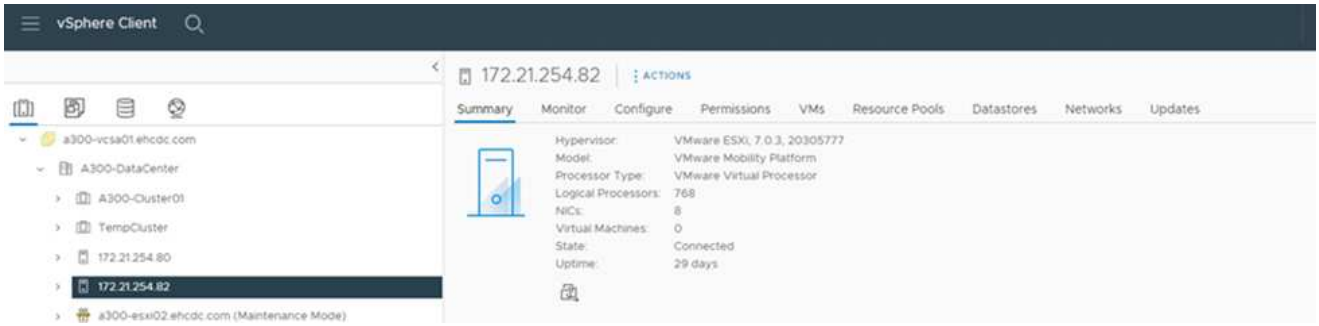
Paso 6: Migrar cargas de trabajo

HCX proporciona servicios de migración bidireccionales entre dos o más entornos diferentes, como los centros de datos SDDC en las instalaciones y los VMC. Las cargas de trabajo de aplicaciones se pueden migrar a y desde sitios activados por HCX mediante diversas tecnologías de migración como la migración masiva de HCX, HCX vMotion, migración en frío de HCX, vMotion asistido con replicación de HCX (disponible con la edición de HCX Enterprise) y la migración asistida por HCX OS (disponible con la edición de HCX Enterprise).

Para obtener más información sobre las tecnologías de migración HCX disponibles, consulte "Tipos de migración HCX de VMware"

El dispositivo HCX-IX utiliza el servicio de agente de movilidad para realizar migraciones vMotion, de frío y de replicación asistida (RAV).

> El dispositivo HCX-IX agrega el servicio Mobility Agent como un objeto host en vCenter Server. El procesador, la memoria, los recursos de almacenamiento y redes que se muestran en este objeto no representan el consumo real en el hipervisor físico que aloja el dispositivo IX.

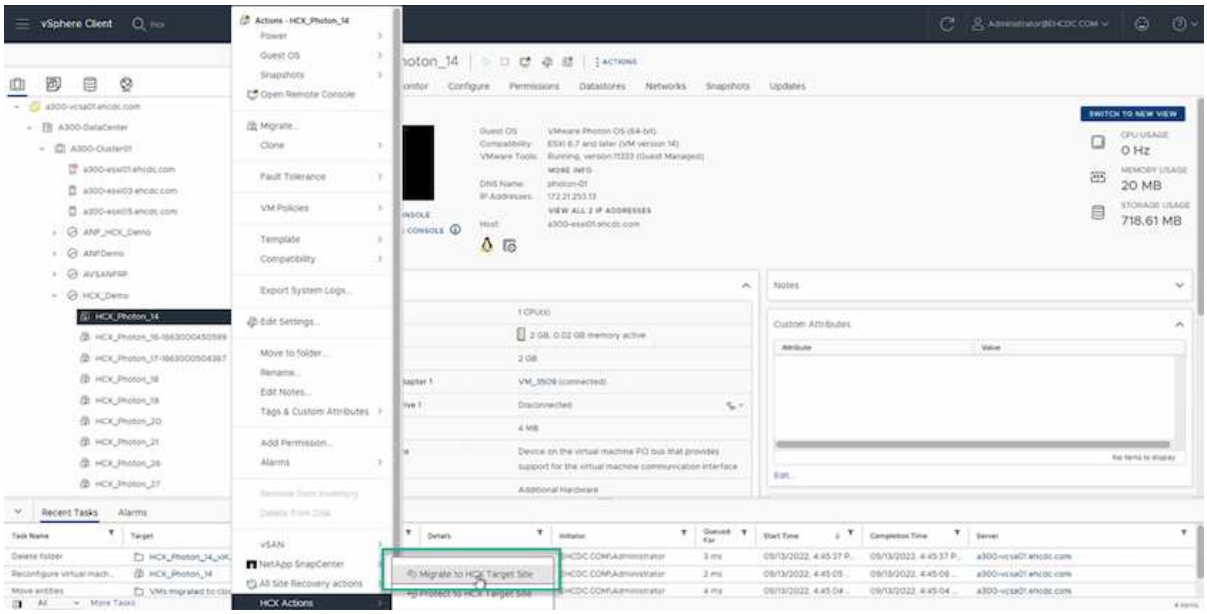


HCX vMotion de VMware

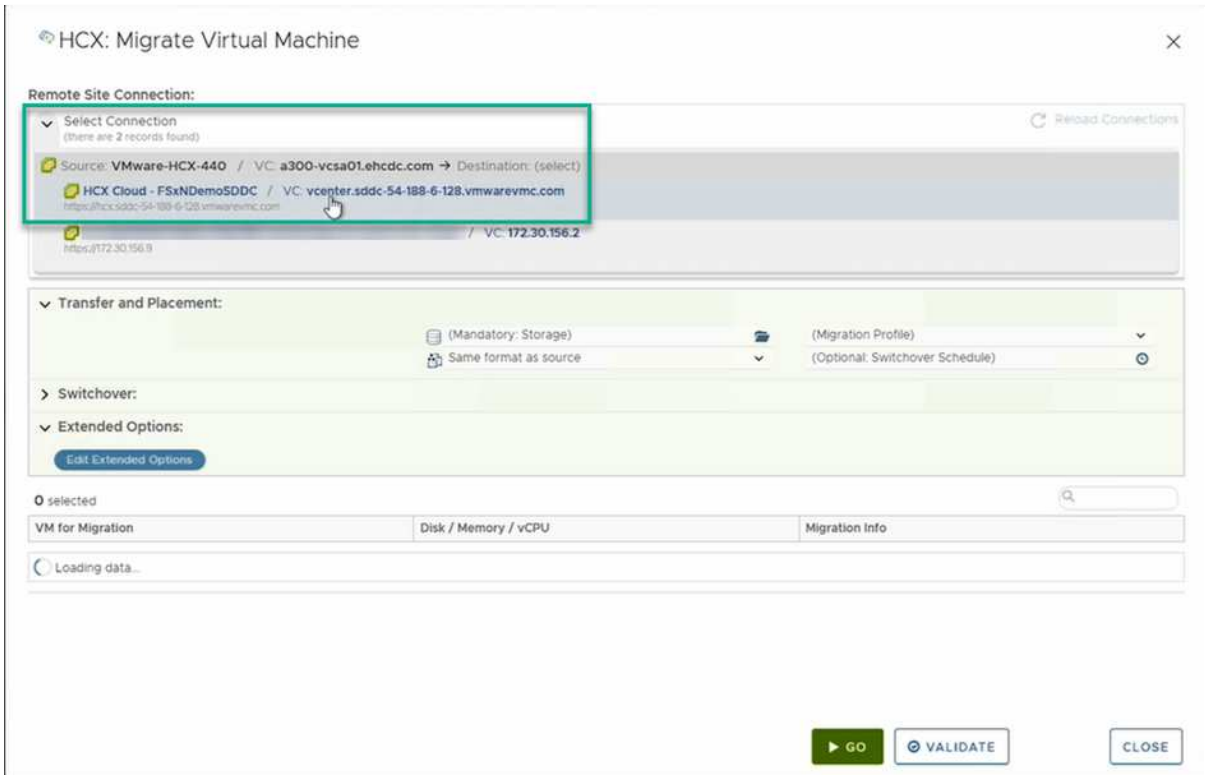
En esta sección se describe el mecanismo HCX vMotion. Esta tecnología de migración utiliza el protocolo VMware vMotion para migrar una máquina virtual a VMC SDDC. La opción de migración de vMotion se utiliza para migrar el estado de las máquinas virtuales de una única máquina virtual a la vez. No se produce ninguna 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 máquina virtual) para migrar la máquina virtual sin necesidad de modificar la dirección IP.

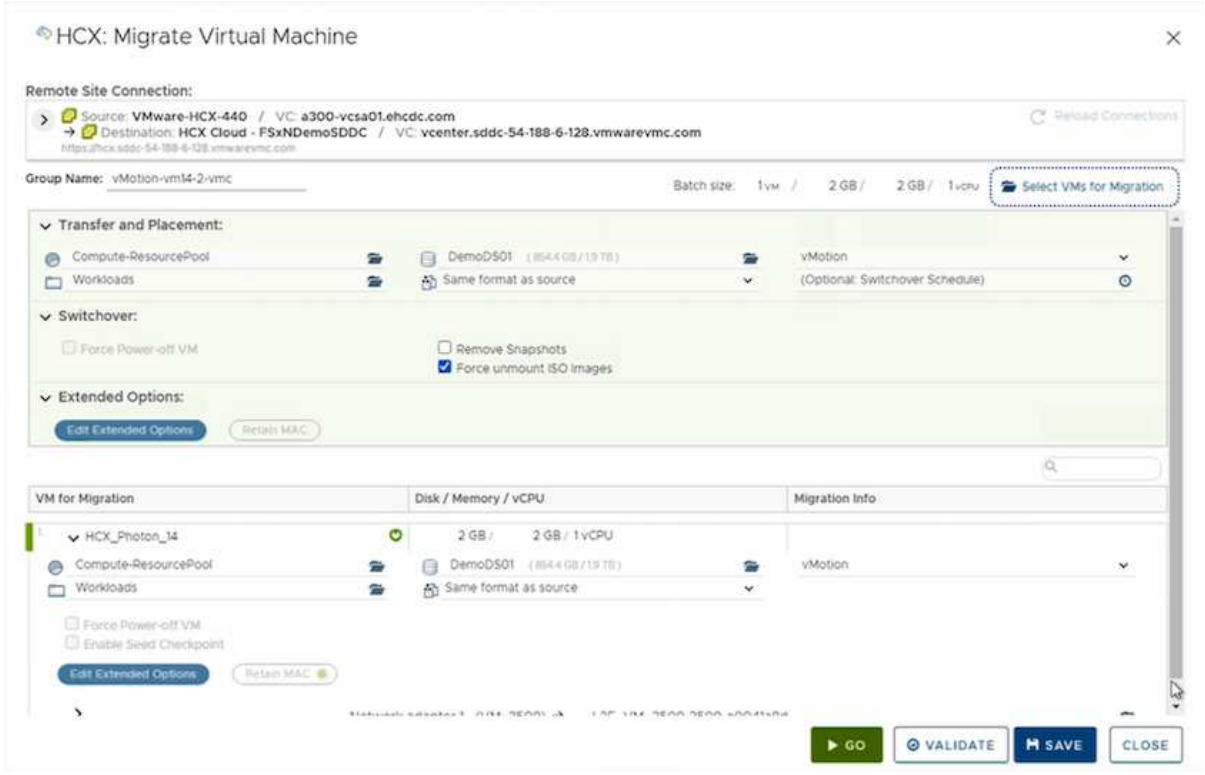
1. Desde el cliente vSphere local, vaya a Inventory, haga clic con el botón derecho en la máquina virtual que se va a migrar y seleccione HCX Actions > Migrate to HCX Target Site.



2. En el asistente Migrate Virtual Machine, seleccione Remote Site Connection (VMC SDDC de destino).



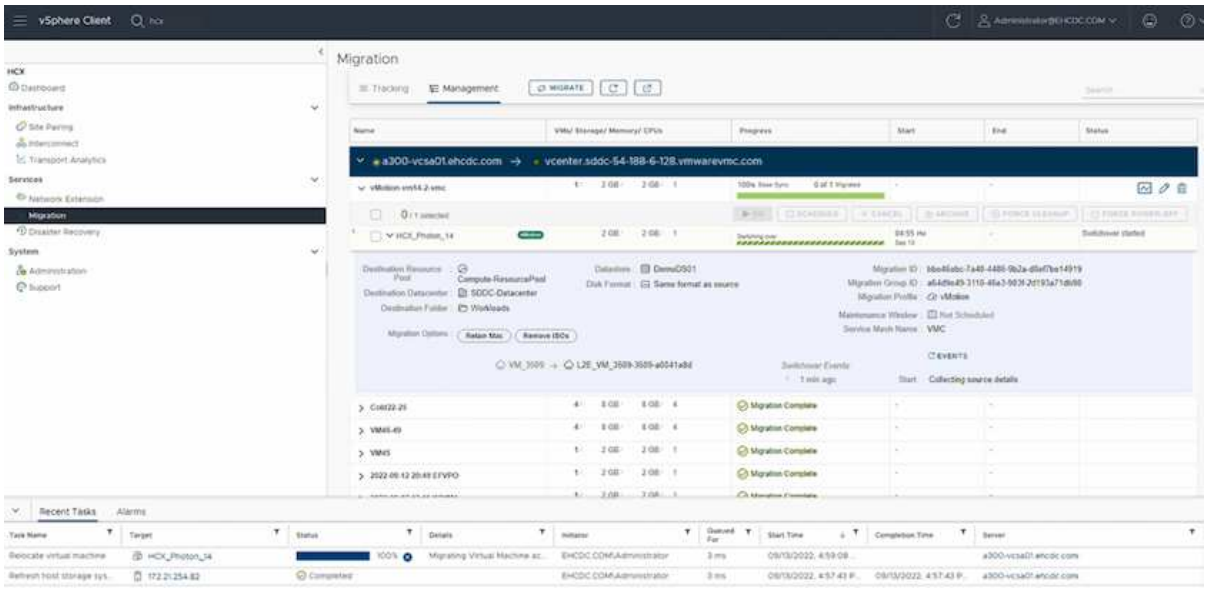
3. Agregue un nombre de grupo y, en transferencia y colocación, actualice los campos obligatorios (clúster, almacenamiento y red de destino) y haga clic en Validar.



4. Una vez finalizadas las comprobaciones de validación, haga clic en Ir para iniciar la migración.

La transferencia de vMotion captura la memoria activa de la máquina virtual, su estado de ejecución, su dirección IP y su dirección MAC. Para obtener más información sobre los requisitos y las limitaciones de HCX vMotion, consulte "Comprender vMotion y la migración de datos fríos de VMware HCX".

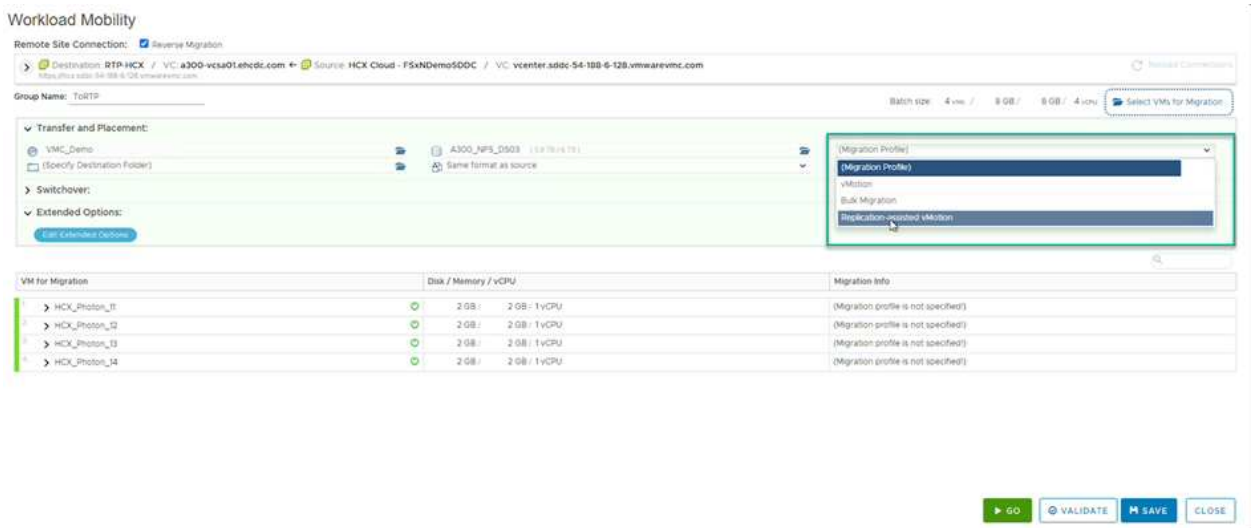
5. Es posible supervisar el progreso y la finalización de vMotion desde el panel HCX > Migration.



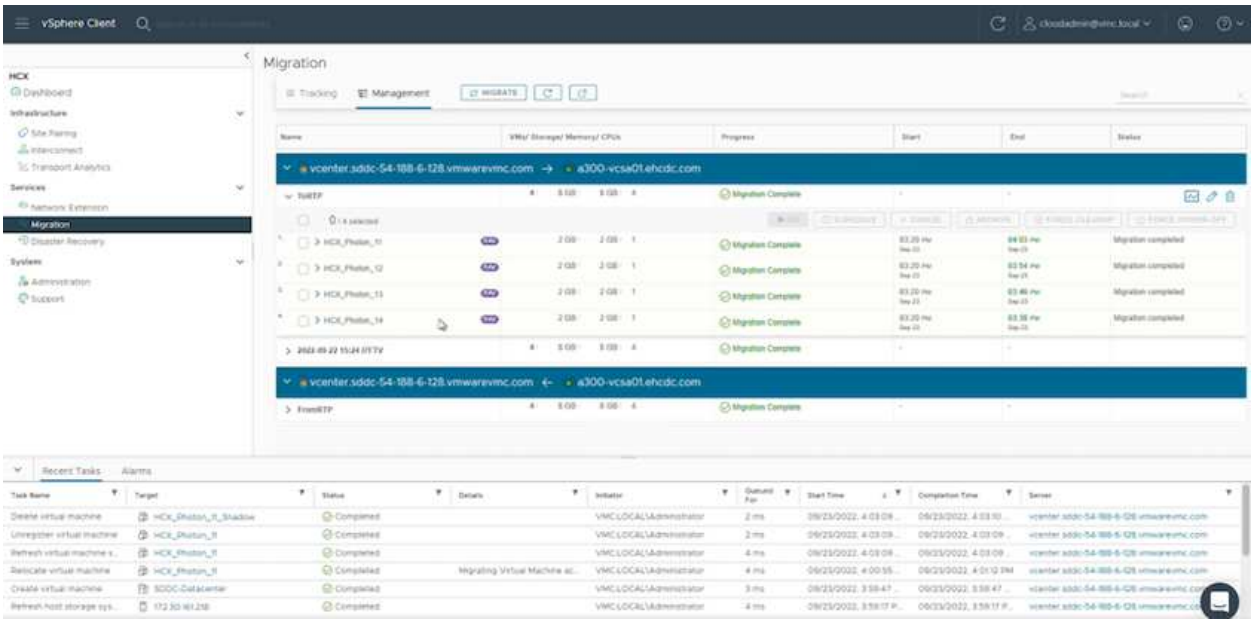
VMotion asistido con replicación de VMware

Como ya se ha visto en la documentación de VMware, VMware HCX Replication Assisted vMotion (RAV) combina las ventajas de la migración masiva y vMotion. La migración masiva usa replicación de vSphere para migrar varias máquinas virtuales en paralelo: El equipo virtual se reinicia durante la conmutación de sitios. HCX vMotion migra sin tiempo de inactividad, pero se ejecuta en serie una máquina virtual a la vez en un grupo de replicación. RAV replica el equipo virtual en paralelo y lo mantiene sincronizado hasta la ventana de cambio. Durante el proceso de conmutación de sitios, migra un equipo virtual a la vez sin tiempo de inactividad de dicho equipo.

La siguiente captura de pantalla muestra el perfil de migración como Replication Assisted vMotion.



La duración de la replicación puede ser más larga en comparación con vMotion de un pequeño número de máquinas virtuales. Con RAV, sólo sincronice los deltas e incluya el contenido de la memoria. A continuación se muestra 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 equipo virtual.



Si quiere más información acerca de las opciones de migración a HCX y sobre cómo migrar cargas de trabajo de las instalaciones a VMware Cloud en AWS mediante HCX, consulte la "Guía del usuario de VMware HCX".

VMware HCX vMotion requiere 100 Mbps o más capacidad de rendimiento.

La VMC FSX de destino para el almacén de datos ONTAP debe tener espacio suficiente para acomodar la migración.

Conclusión

Tanto si su objetivo es llegar a un cloud híbrido o un cloud, como si los datos residen en almacenamiento de cualquier tipo o proveedor en las instalaciones, Amazon FSX para ONTAP de NetApp y HCX proporcionan opciones excelentes para poner en marcha y migrar las cargas de trabajo, a la vez que reduce el TCO y permite que los requisitos de datos se adaptan perfectamente a la capa de la aplicación. Sea cual sea el caso de uso, elija VMC junto con FSX para el almacén de datos ONTAP para comprender rápidamente las ventajas del cloud, una infraestructura consistente y operaciones en las instalaciones y varios clouds, la portabilidad bidireccional de las cargas de trabajo, y la capacidad y el rendimiento de clase empresarial. Es el mismo proceso y procedimientos que ya conoce que se utiliza para conectar el almacenamiento y migrar máquinas virtuales mediante la replicación de VMware vSphere, VMware vMotion o incluso una copia NFC.

Puntos

Los puntos clave de este documento son:

- Ahora puede usar Amazon FSX ONTAP como almacén de datos con VMC SDDC.
- Puede migrar datos fácilmente desde cualquier centro de datos local a una instancia de VMC que se ejecute con FSX para almacén de datos ONTAP
- Puede aumentar y reducir fácilmente el almacén de datos ONTAP de FSX para satisfacer los requisitos de capacidad y rendimiento durante la actividad de migración.

Dónde encontrar información adicional

Si quiere más información sobre la información descrita en este documento, consulte los siguientes enlaces a sitios web:

- Documentación de VMware Cloud

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Documentación de Amazon FSX para ONTAP de NetApp

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  Guía del usuario de VMware HCX

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Region Availability – almacén de datos NFS suplementario para VMC

Amazon define la disponibilidad de almacenes de datos NFS complementarios en

AWS/VMC. Primero, debe determinar si tanto VMC como FSxN están disponibles en una región específica. A continuación, debe determinar si el almacén de datos NFS complementario FSxN es compatible en esa región.

- Compruebe la disponibilidad del VMC "aquí".
- La guía de precios de Amazon ofrece información sobre dónde está disponible FSxN (FSX ONTAP). Usted puede encontrar esa información "aquí".
- La disponibilidad del almacén de datos NFS complementario FSxN para VMC estará disponible próximamente.

Aunque aún se dispone de información, el siguiente gráfico identifica el soporte actual de VMC, FSxN y FSxN como almacén de datos NFS complementario.

América

Región de AWS	Disponibilidad VMC	Disponibilidad de ONTAP FSX	Disponibilidad del almacén de datos NFS
Este DE EE. UU. (Virginia del Norte)	Sí	Sí	Sí
Este DE EE. UU. (Ohio)	Sí	Sí	Sí
Oeste DE EE. UU. (Norte de California)	Sí	No	No
Oeste DE EE. UU. (Oregón)	Sí	Sí	Sí
GovCloud (oeste de EE. UU.)	Sí	Sí	Sí
Canadá (Central)	Sí	Sí	Sí
Sudamérica (São Paulo)	Sí	Sí	Sí

Última actualización el: 2 de junio de 2022.

EMEA

Región de AWS	Disponibilidad VMC	Disponibilidad de ONTAP FSX	Disponibilidad del almacén de datos NFS
Europa (Irlanda)	Sí	Sí	Sí
Europa (Londres)	Sí	Sí	Sí
Europa (Frankfurt)	Sí	Sí	Sí
Europa (París)	Sí	Sí	Sí
Europa (Milán)	Sí	Sí	Sí
Europa (Estocolmo)	Sí	Sí	Sí

Última actualización el: 2 de junio de 2022.

Asia-Pacífico

Región de AWS	Disponibilidad VMC	Disponibilidad de ONTAP FSX	Disponibilidad del almacén de datos NFS
APAC (Sidney)	Sí	Sí	Sí
APAC (Tokio)	Sí	Sí	Sí
APAC (Osaka)	Sí	No	No
APAC (Singapur)	Sí	Sí	Sí
APAC (Seúl)	Sí	Sí	Sí
APAC (Bombay)	Sí	Sí	Sí
APAC (Yakarta)	No	No	No

APAC (Hong Kong)	Sí	Sí	Sí

Última actualización el: 28 de septiembre de 2022.

Funcionalidades de NetApp para Azure AVS

Obtenga más información acerca de las funcionalidades que NetApp aporta a la solución VMware de Azure (AVS): Desde NetApp como dispositivo de almacenamiento conectado a invitado o un almacén de datos NFS complementario a la migración de flujos de trabajo, ampliando o rebosando al cloud, backup/restauración y recuperación ante desastres.

Para ir a la sección del contenido deseado, seleccione una de las siguientes opciones:

- "Configuración de AVS en Azure"
- "Opciones de almacenamiento de NetApp para AVS"
- "Soluciones cloud de NetApp/VMware"

Configuración de AVS en Azure

Al igual que en las instalaciones, la planificación de un entorno de virtualización basado en cloud es crucial para tener un entorno preparado para la producción con éxito a la hora de crear equipos virtuales y migración.

En esta sección se describe cómo configurar y gestionar la solución VMware de Azure y utilizarla en combinación con las opciones disponibles para conectar el almacenamiento de NetApp.

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

El proceso de configuración puede dividirse en los siguientes pasos:

- Registre el proveedor de recursos y cree un cloud privado
- Conéctese a una puerta de enlace de red virtual ExpressRoute nueva o existente
- Validar la conectividad de red y acceder al cloud privado

Vea el detalles "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 de datos NFS complementario o conectado, en Azure AVS.

Visite "Opciones de almacenamiento de NetApp admitidas" si quiere más información.

Azure admite almacenamiento de NetApp en las siguientes configuraciones:

- Azure NetApp Files (ANF) como almacenamiento conectado como invitado
- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado

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

Vea el detalles "Opciones de almacenamiento de Guest Connect para AVS". Vea el detalles "Opciones complementarias de almacén de datos NFS para AVS".

Casos de uso de soluciones

Con las soluciones cloud de NetApp y VMware, la puesta en marcha en Azure AVS resulta sencilla en muchos casos de uso. Los casos de ingenieros de sistemas se definen para cada una de las áreas cloud definidas de VMware:

- Protect (incluye recuperación ante desastres y backup/restauración)
- Extender
- Migración

"Examine las soluciones de NetApp para Azure AVS"

Proteger cargas de trabajo en Azure/AVS

Recuperación ante desastres con ANF y JetStream

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por los datos (por ejemplo, ransomware). Gracias al marco de trabajo VAIO de VMware, las cargas de trabajo de VMware locales se pueden replicar en el almacenamiento Azure Blob y recuperarse, lo que permite una pérdida de datos mínima o casi nula, y el objetivo de tiempo de recuperación casi nulo.

JetStream DR se puede utilizar para recuperar sin problemas las cargas de trabajo replicadas de las instalaciones a AVS y específicamente a Azure NetApp Files. Permite una recuperación ante desastres rentable usando unos recursos mínimos en el sitio de recuperación ante desastres y un almacenamiento en cloud rentable. Jetstream DR automatiza la recuperación en almacenes de datos de ANF mediante el almacenamiento BLOB de Azure. JetStream DR recupera máquinas virtuales independientes o grupos de máquinas virtuales relacionadas en la infraestructura de sitio de recuperación según su asignación de red y proporciona recuperación de un momento específico para la protección de ransomware.

Este documento proporciona una comprensión de los principios de operaciones de JetStream DR y sus principales componentes.

Información general sobre la puesta en marcha de la

1. Instale el software JetStream DR en el centro de datos local.
   a. Descargue el paquete de software de recuperación ante desastres JetStream desde Azure Marketplace (ZIP) y ponga en marcha 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 de recuperación ante desastres AVS.
   d. Ponga en marcha dispositivos DRVA y asigne volúmenes de registro de replicación (VMDK a partir de un almacén de datos existente o almacenamiento iSCSI compartido).
   e. Cree dominios protegidos (grupos de máquinas virtuales relacionadas) y asigne DRVAs y Azure Blob Storage/ANF.
   f. Inicie la protección.
2. Instalar el software de recuperación ante desastres JetStream en el cloud privado de Azure VMware Solution.
   a. Utilice el comando Run para instalar y configurar JetStream DR.
   b. Agregue el mismo contenedor de Azure Blob y descubra dominios mediante la opción Scan Domains.
   c. Implementar los dispositivos DRVA necesarios.
   d. Cree volúmenes de registros de replicación con almacenes de datos VSAN o ANF disponibles.
   e. Importe dominios protegidos y configure ROCvA (recuperación va) para utilizar el almacén de datos ANF en las ubicaciones de los equipos virtuales.
   f. Seleccione la opción de conmutación por error adecuada y inicie una rehidratación continua para dominios de objetivo de tiempo de recuperación casi cero o máquinas virtuales.
3. Durante un evento de desastre, active la conmutación por error en los almacenes de datos de Azure NetApp Files en el sitio de recuperación ante desastres AVS designado.
4. Invoque la conmutación por recuperación al sitio protegido después de haber recuperado el sitio protegido.antes de comenzar, asegúrese de que se cumplen los requisitos previos tal y como se indica en este "enlace" Además, ejecute Bandwidth Testing Tool (BWT) de JetStream Software para evaluar el rendimiento potencial del almacenamiento de Azure Blob y su ancho de banda de replicación cuando se utiliza con el software JetStream DR. Tras los requisitos previos, incluida la conectividad, se han establecido, se han establecido y se han suscrito a JetStream DR para AVS de la "Azure Marketplace". Después de descargar el paquete de software, continúe con el proceso de instalación descrito anteriormente.

Cuando planifique e inicie la protección de un gran número de equipos virtuales (por ejemplo, 100+), utilice la herramienta de planificación de capacidad (CPT) del kit de herramientas de automatización de recuperación ante desastres JetStream. Proporcionar una lista de equipos virtuales que se protegerán junto a sus preferencias de grupo de recuperación y tiempo de recuperación, y luego ejecutar CPT.

CPT realiza las siguientes funciones:

- Combinación de máquinas virtuales en dominios de protección según su objetivo de tiempo de recuperación.
- Definir el número óptimo de DRVAs y sus recursos.

- Calcular el ancho de banda de replicación requerido.
- Identificación de las características del volumen de registro de replicación (capacidad, ancho de banda, etc.).
- Calculando la capacidad de almacenamiento de objetos requerida, etc.

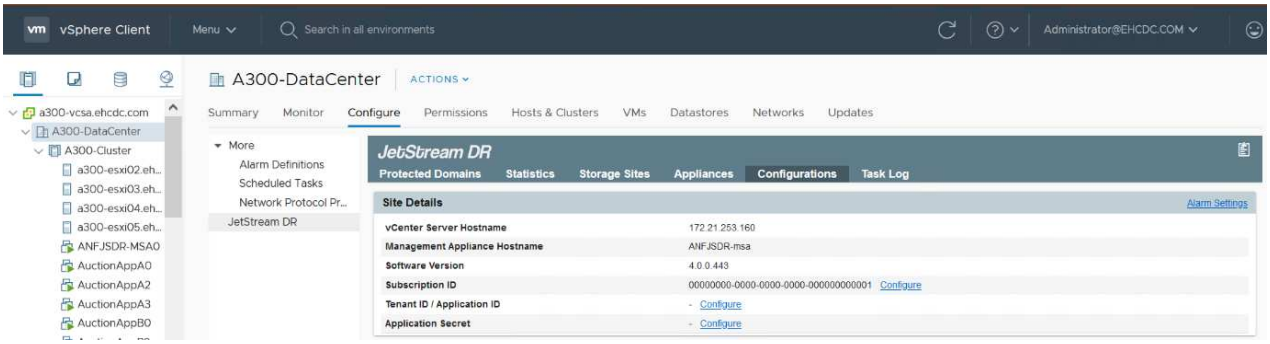
> La cantidad y el contenido de los dominios prescritos dependen de diversas características de los equipos virtuales, como la tasa media de IOPS, la capacidad total, la prioridad (que define el orden de conmutación por error), el objetivo de tiempo de recuperación, etc.

Instalar JetStream DR en el centro de datos local

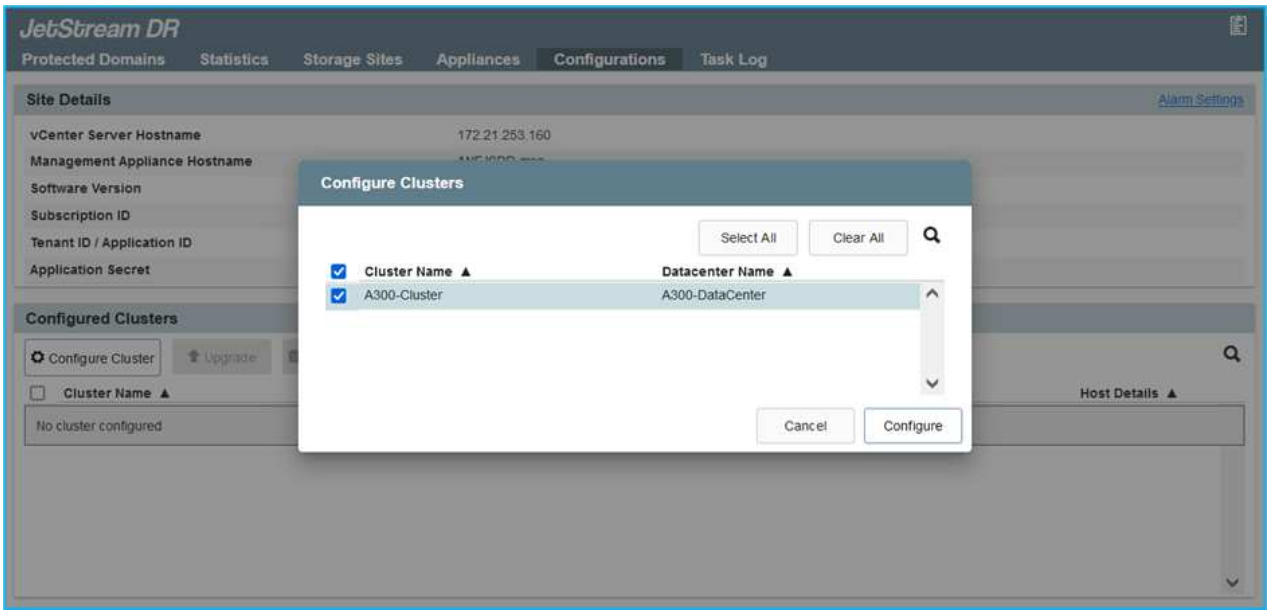
El software Jetstream DR consta de tres componentes principales: Jetstream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) y componentes host (paquetes de filtros de I/o). MSA se utiliza para instalar y configurar componentes host en el cluster informático y, a continuación, administrar el software de recuperación ante desastres JetStream. La siguiente lista proporciona una descripción de alto nivel del proceso de instalación:

Cómo instalar JetStream DR para las instalaciones

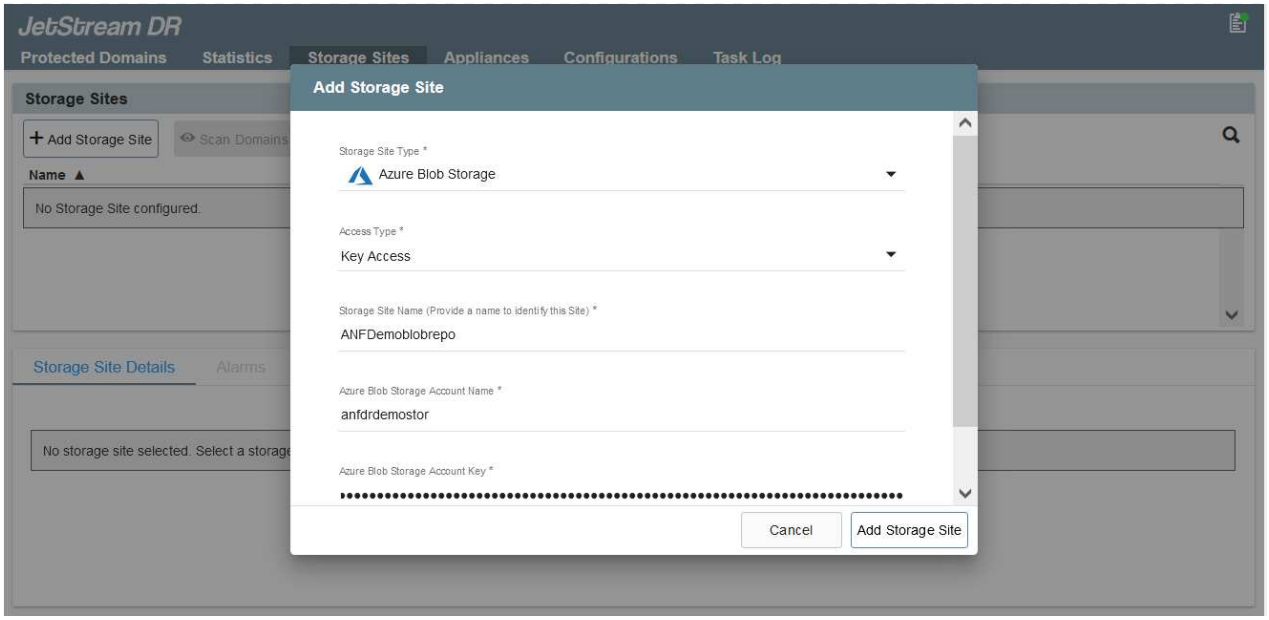
1. Compruebe los requisitos previos.
2. Ejecute la herramienta de planificación de la capacidad para realizar recomendaciones de recursos y configuración (opcional pero recomendado para pruebas de concepto).
3. Implemente JetStream DR MSA en un host de vSphere en el clúster designado.
4. Inicie MSA usando su nombre DNS en un explorador.
5. Registre el servidor vCenter con MSA.para realizar la instalación, complete los siguientes pasos detallados:
6. Una vez que se haya puesto en marcha JetStream DR MSA y se haya registrado vCenter Server, acceda al complemento de recuperación ante desastres JetStream mediante vSphere Web Client. Para ello, vaya a Datacenter > Configure > JetStream DR.



7. En la interfaz DR de JetStream, seleccione el clúster adecuado.



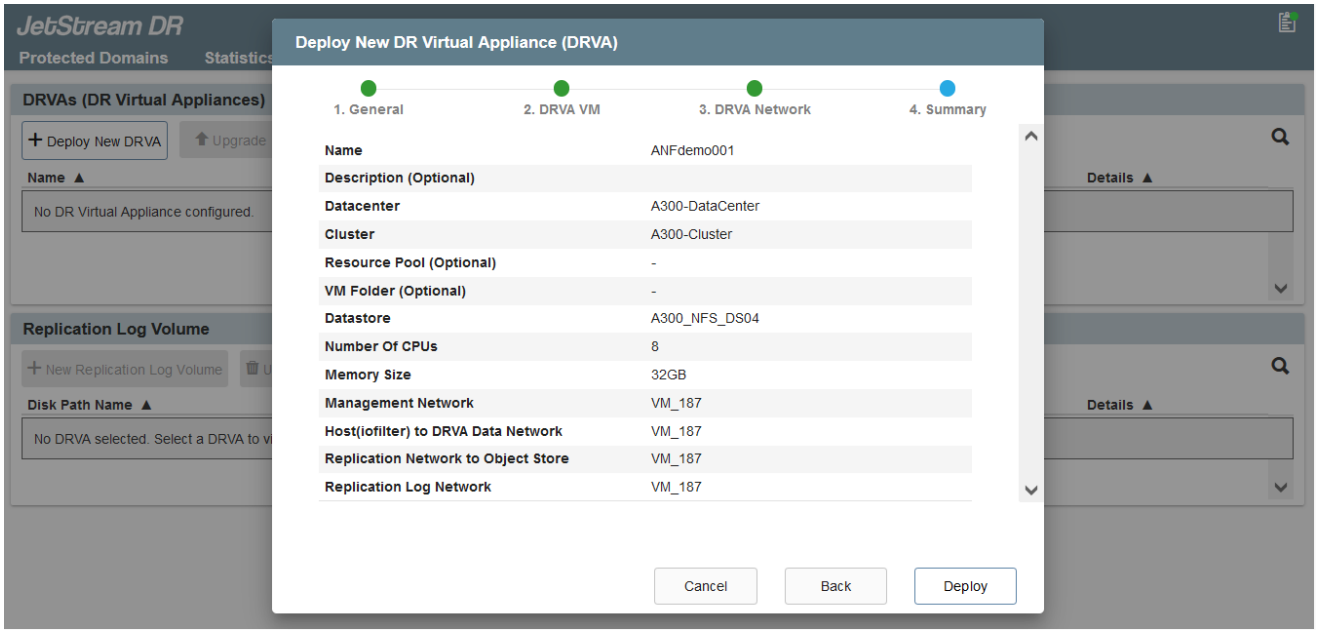
8. Configure el clúster con el paquete de filtro de I/O.



9. Añada Azure Blob Storage ubicado en el sitio de recuperación.
10. Implemente un dispositivo virtual de recuperación ante desastres (DRVA) desde la ficha Appliances (dispositivos).

> Los DRVAs se pueden crear automáticamente mediante CPT, pero para las pruebas POC recomendamos configurar y ejecutar manualmente el ciclo DR (iniciar protección > failover > conmutación por recuperación).

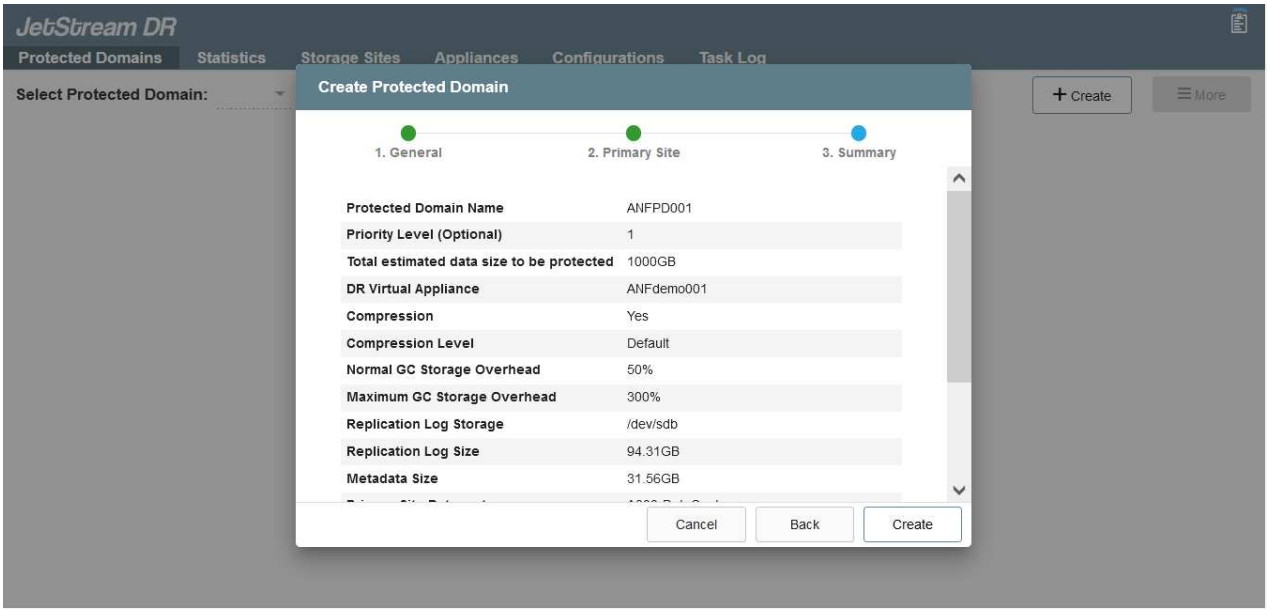
JetStream DRVA es un dispositivo virtual que facilita las funciones clave del proceso de replicación de datos. Un clúster protegido debe contener al menos un DVAD y, normalmente, un DVAD se configura por host. Cada DRVA puede gestionar varios dominios protegidos.



En este ejemplo, se crearon cuatro DRVA para 80 máquinas virtuales.

1. Crear volúmenes de registro de replicación para cada DRVA utilizando VMDK desde los almacenes de datos disponibles o grupos de almacenamiento iSCSI compartidos independientes.

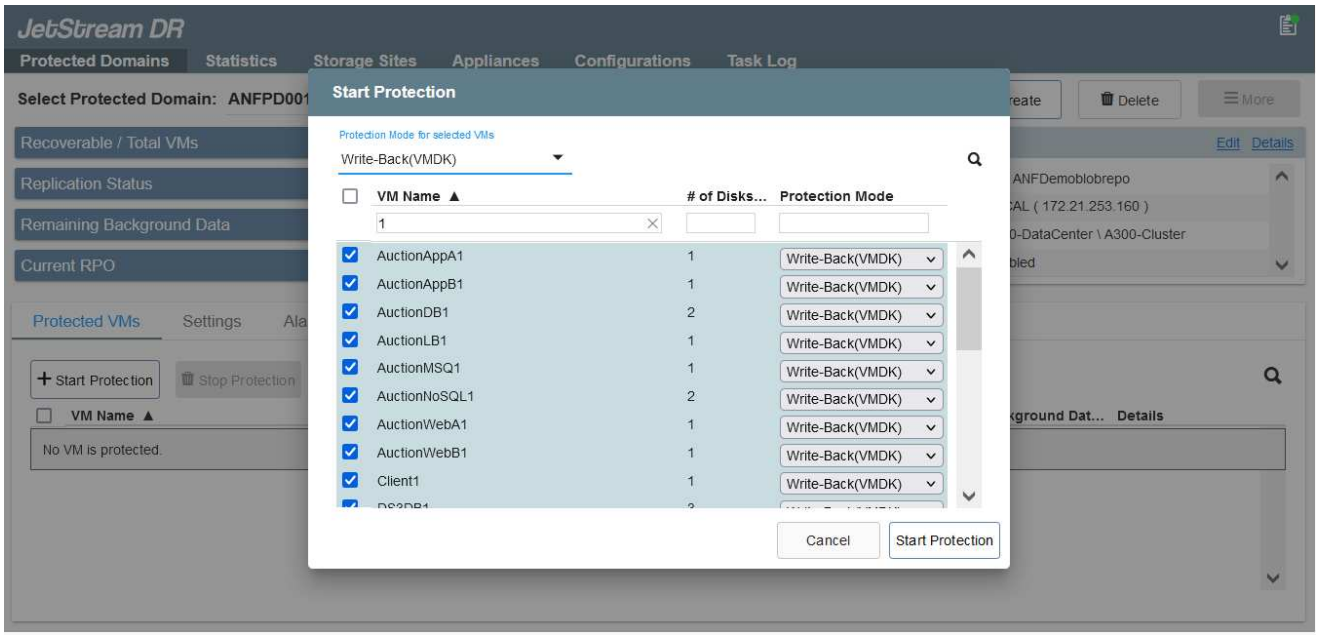
2. En la pestaña protected Domains, cree la cantidad necesaria de dominios protegidos utilizando información acerca del sitio de Azure Blob Storage, la instancia de DRVA y el registro de replicación. Un dominio protegido define una máquina virtual o un conjunto de máquinas virtuales específicos del clúster que se protegen en conjunto y asignó un orden de prioridad a las operaciones de conmutación por error y conmutación tras recuperación.



3. Seleccione las máquinas virtuales que desea proteger e iniciar la protección de máquinas virtuales del dominio protegido. Esto comienza la replicación de datos en el almacén BLOB designado.

Compruebe que se utilice el mismo modo de protección para todas las máquinas virtuales de un dominio protegido.

El modo Write- Back (VMDK) puede ofrecer un mayor rendimiento.



Compruebe que los volúmenes de registro de replicación se colocan en un almacenamiento de alto

rendimiento.

> Los libros de ejecución de conmutación por error se pueden configurar para agrupar los equipos virtuales (denominado Grupo de recuperación), establecer la secuencia de órdenes de arranque y modificar los ajustes de CPU/memoria junto con las configuraciones de IP.

Instalar JetStream DR para AVS en un cloud privado de Azure VMware Solution mediante el comando Run

Una práctica recomendada para un sitio de recuperación (AVS) es crear un clúster de tres nodos de luz piloto con antelación. Esto permite configurar la infraestructura del centro de recuperación, incluidos los siguientes elementos:

- Segmentos de red de destino, firewalls, servicios como DHCP y DNS, etc.
- Instalación de JetStream DR para AVS
- La configuración de volúmenes ANF como almacenes de datos y la recuperación ante desastres más moreJetStream admite un modo de objetivo de tiempo de recuperación casi cero para dominios críticos de negocio. Para estos dominios, el almacenamiento de destino debe estar preinstalado. ANF es un tipo de almacenamiento recomendado en este caso.

> La configuración de la red, incluida la creación de segmentos, se debe configurar en el clúster AVS para que coincida con los requisitos en las instalaciones.

En función de los requisitos de SLA y RTO, se puede usar el modo de conmutación por error continua o el modo de conmutación por error regular (estándar). Para lograr un objetivo de tiempo de recuperación cercano a cero, es necesario iniciar una rehidratación continua en el sitio de recuperación.

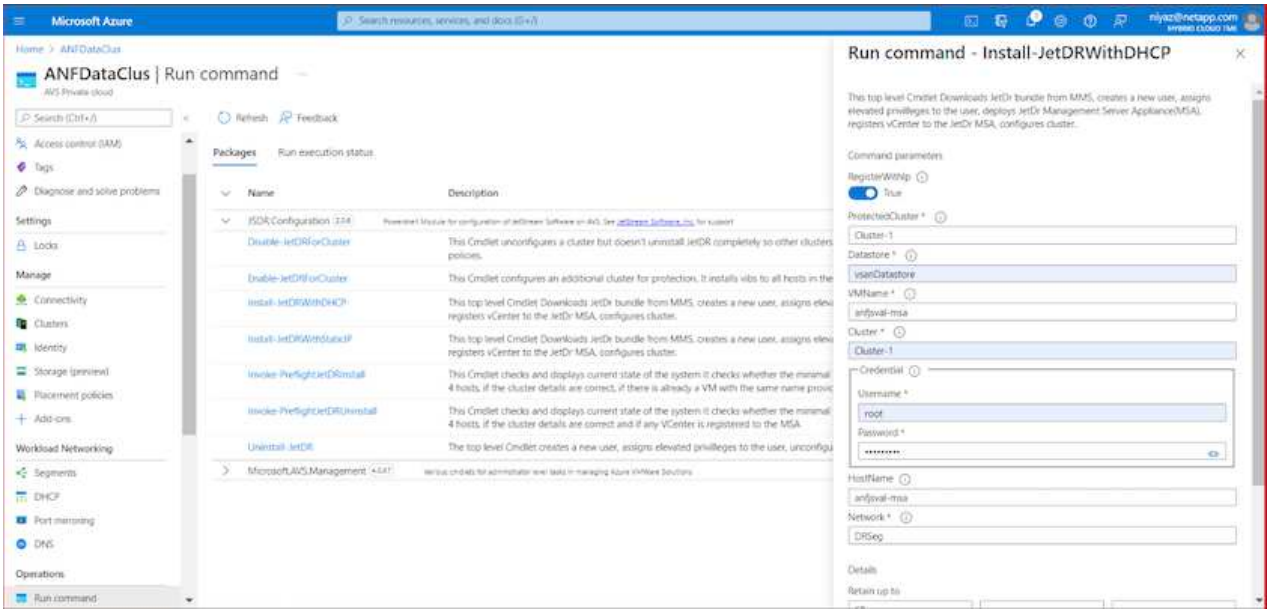
Cómo instalar JetStream DR para AVS en una nube privada

Para instalar JetStream DR para AVS en un cloud privado con Azure VMware Solution, realice los siguientes pasos:

1. En el portal de Azure, vaya a la solución Azure VMware, seleccione la nube privada y seleccione Ejecutar comando > Paquetes > JSDR.Configuration.

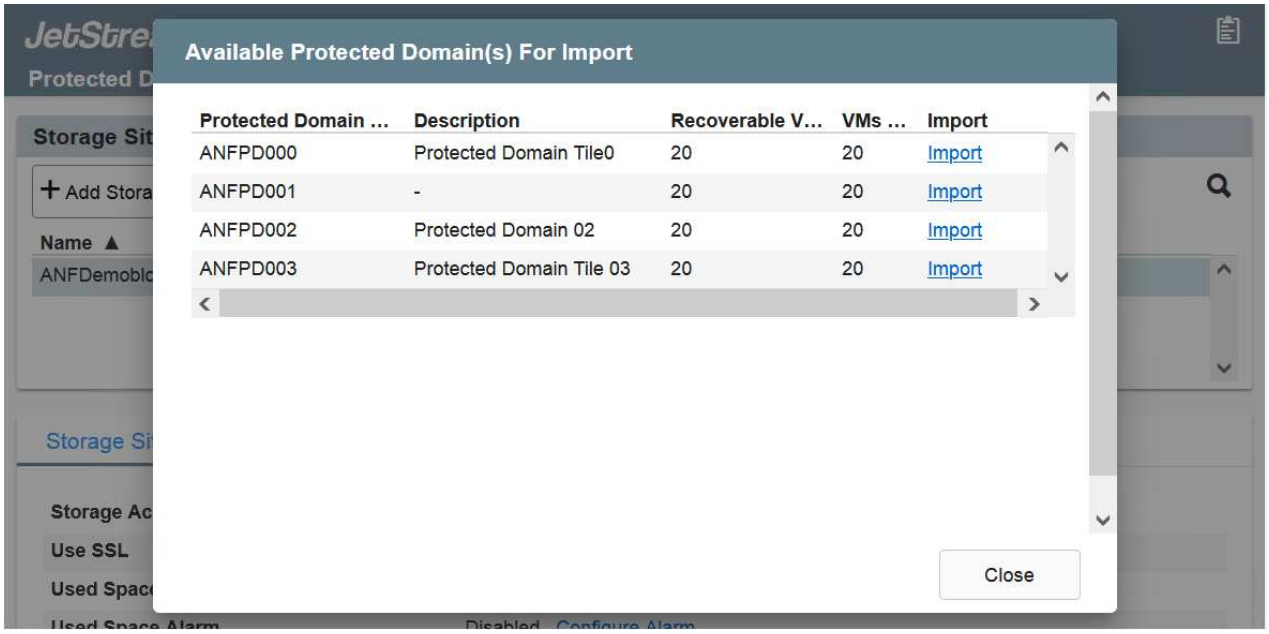
> El usuario de CloudAdmin predeterminado en la solución VMware de Azure no tiene suficientes privilegios para instalar JetStream DR para AVS. La solución VMware Azure permite una instalación simplificada y automatizada de la recuperación ante desastres de JetStream mediante la llamada al comando Azure VMware Solution Run para la recuperación ante desastres de JetStream.

La siguiente captura de pantalla muestra la instalación mediante una dirección IP basada en DHCP.



2. Una vez finalizada la instalación de JetStream DR para AVS, actualice el explorador. Para acceder a la interfaz de usuario de recuperación ante desastres de JetStream, vaya a SDDC Datacenter > Configure > JetStream DR.

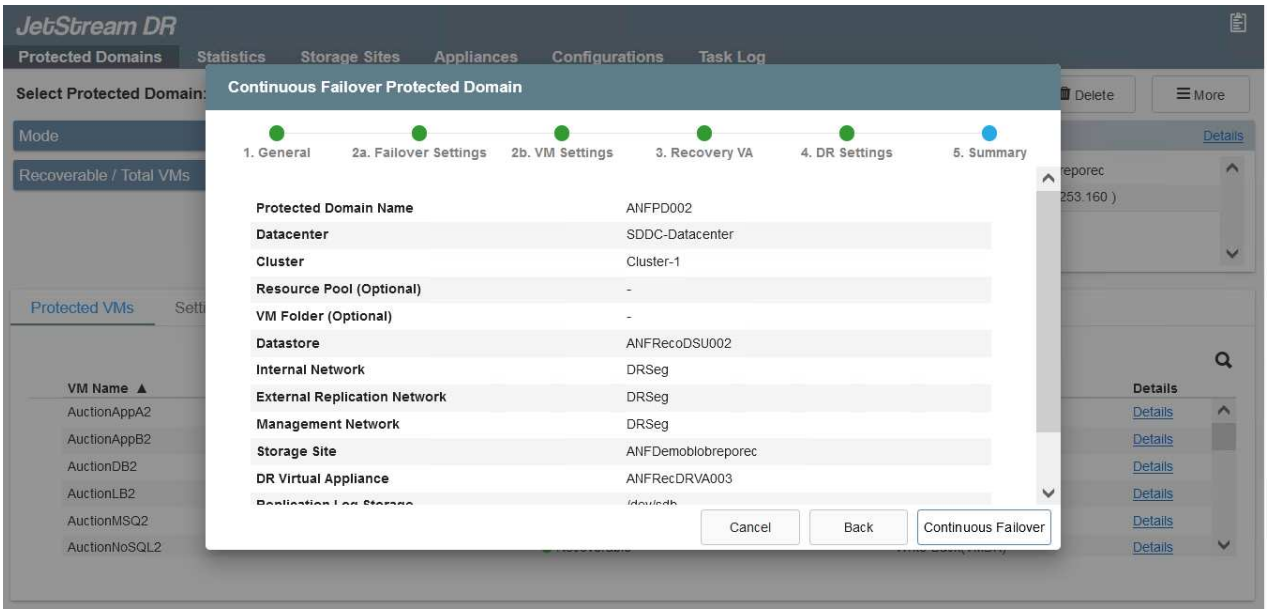
3. Desde la interfaz DR de JetStream, añada la cuenta de almacenamiento BLOB de Azure que se utilizó para proteger el clúster local como sitio de almacenamiento y, a continuación, ejecute la opción Scan Domains.



4. Después de importar los dominios protegidos, implemente dispositivos DRVA. En este ejemplo, la rehidratación continua se inicia manualmente desde el sitio de recuperación mediante la IU de recuperación ante desastres de JetStream.

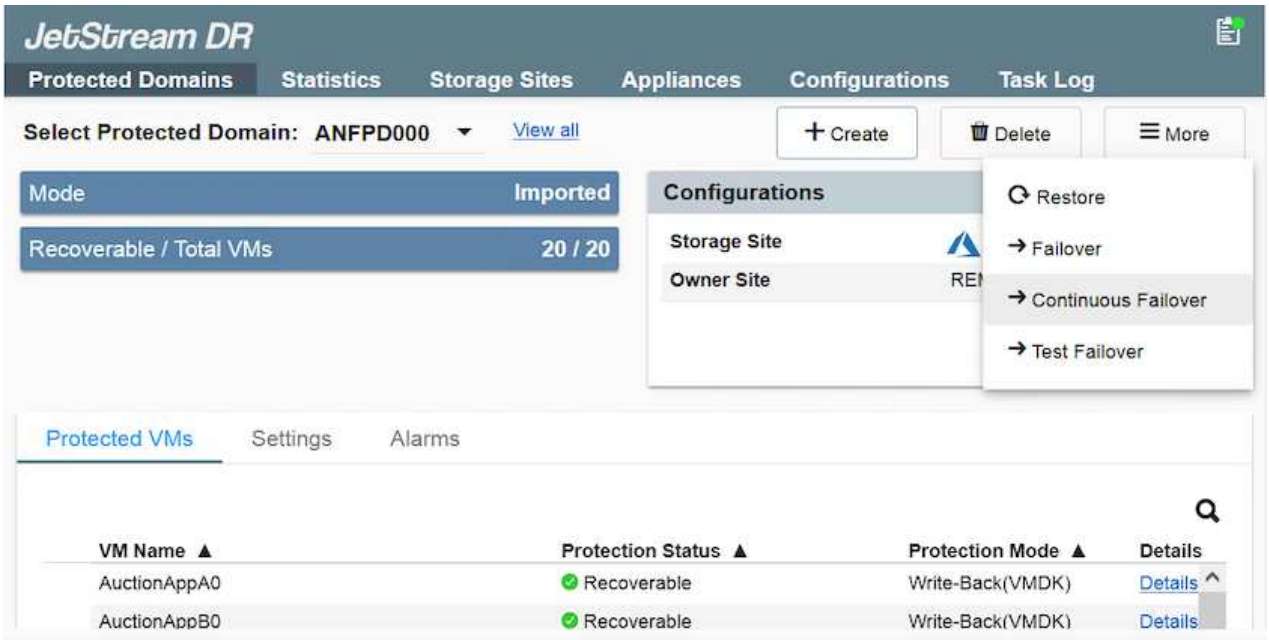
> Estos pasos también se pueden automatizar mediante planes creados por CPT.

5. Cree volúmenes de registros de replicación con almacenes de datos VSAN o ANF disponibles.
6. Importe los dominios protegidos y configure Recovery VA para utilizar el almacén de datos ANF en las ubicaciones de las máquinas virtuales.



Asegúrese de que DHCP esté habilitado en el segmento seleccionado y haya suficientes IP disponibles. Las IP dinámicas se utilizan temporalmente mientras se recuperan los dominios. Cada VM que se recupera (incluida la rehidratación continua) requiere una IP dinámica individual. Una vez finalizada la recuperación, se libera la IP y se puede volver a utilizar.

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).



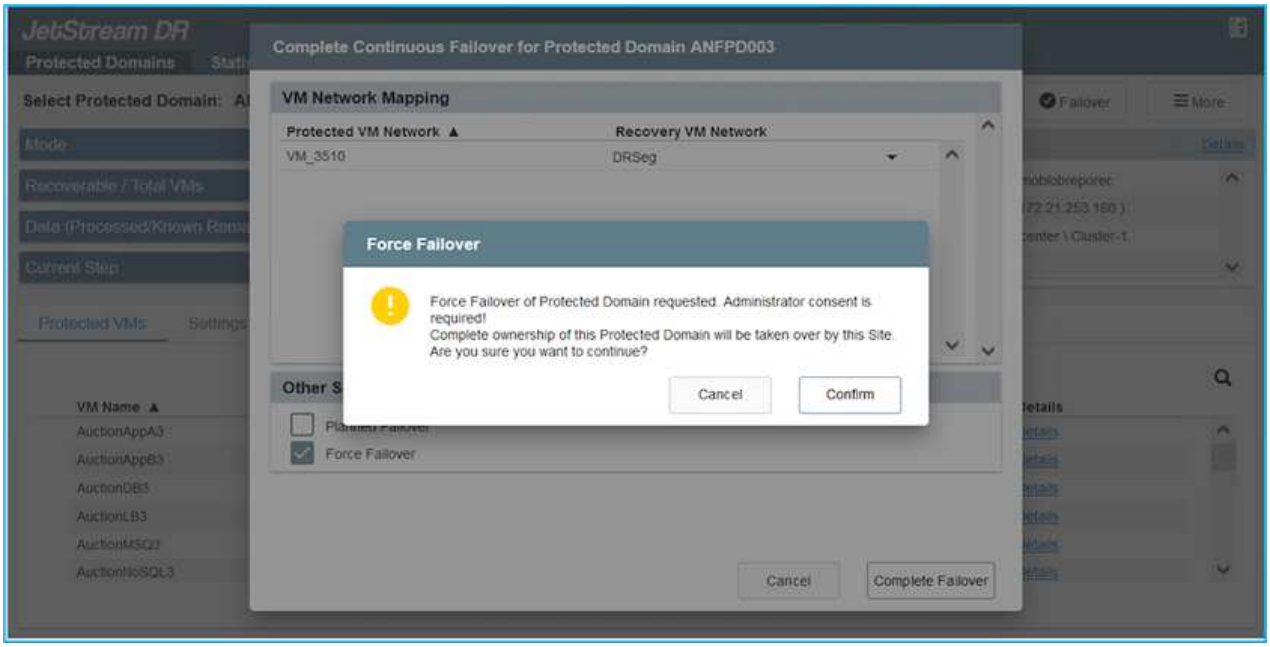
Realizar conmutación por error/conmutación por error

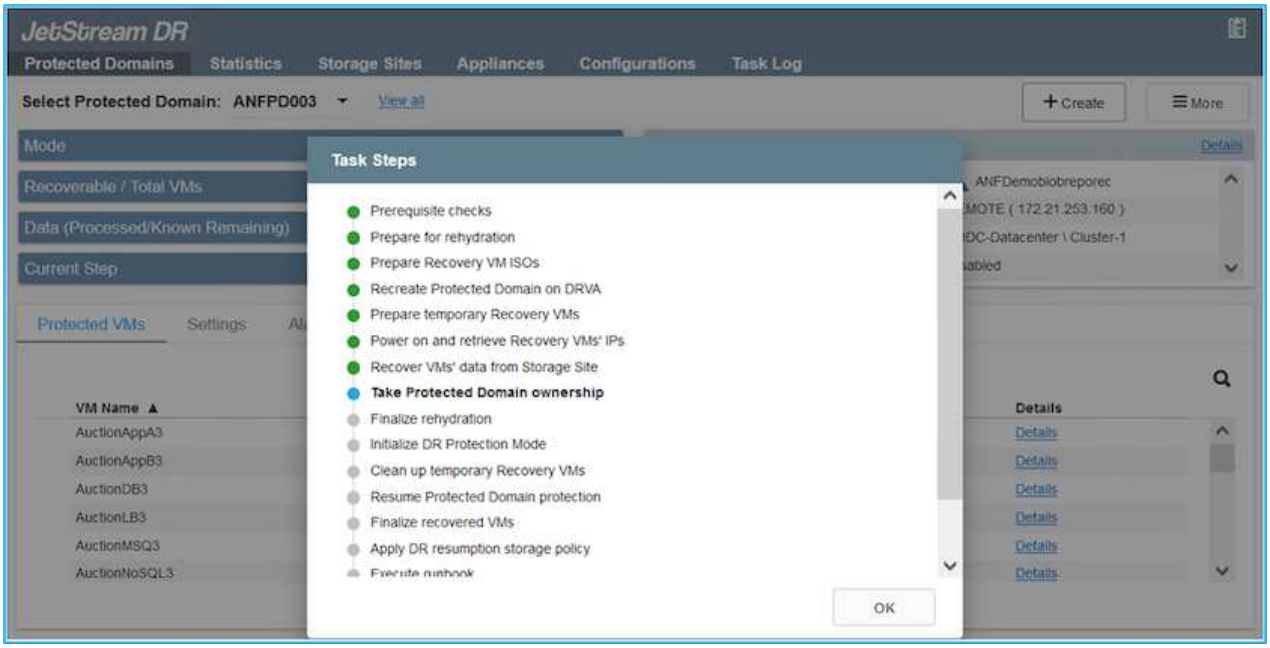
Cómo realizar una conmutación por error/conmutación por recuperación

1. Cuando se produce un desastre en el clúster protegido del entorno local (fallo parcial o total), active la conmutación al respaldo.

   CPT se puede usar para ejecutar el plan de conmutación por error y recuperar las máquinas virtuales de Azure Blob Storage en el sitio de recuperación del clúster AVS.

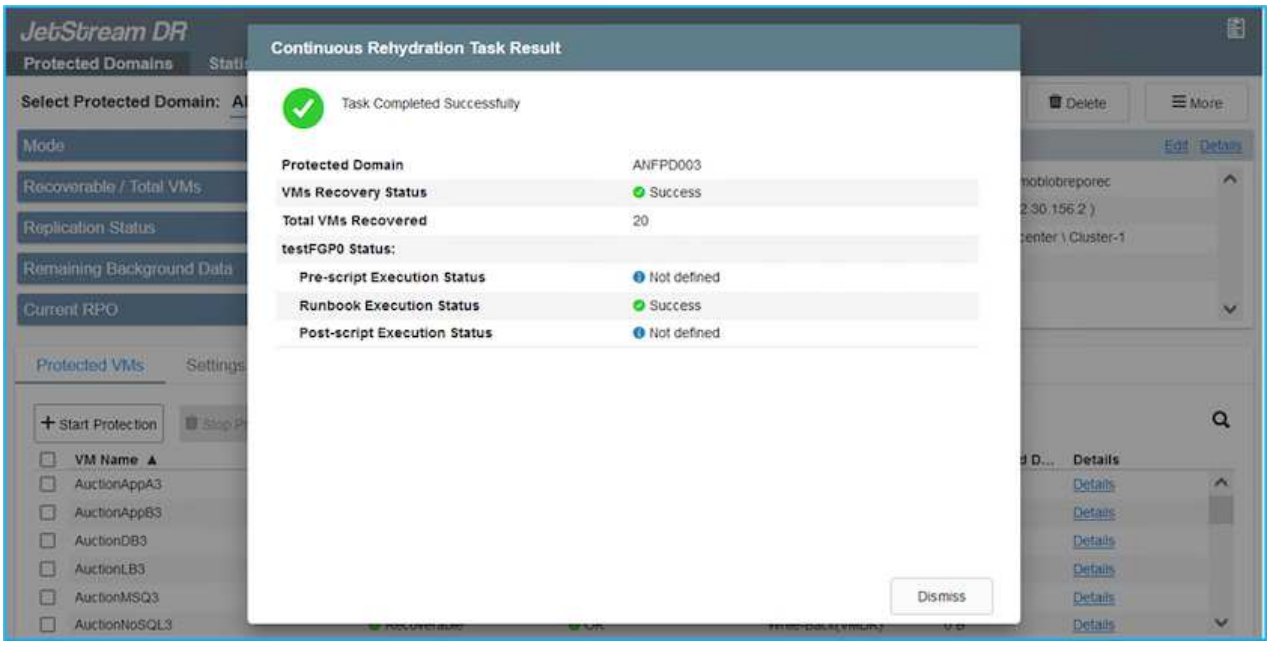
   Después de la conmutación al nodo de respaldo (para una rehidratación continua o estándar), cuando se iniciaron las máquinas virtuales protegidas en AVS, la protección se reanuda automáticamente y JetStream DR sigue replicando sus datos en los contenedores originales o adecuados en Azure Blob Storage.





   La barra de tareas muestra el progreso de las actividades de failover.

2. Una vez finalizada la tarea, el acceso al equipo virtual recuperado y al negocio continúa de forma normal.

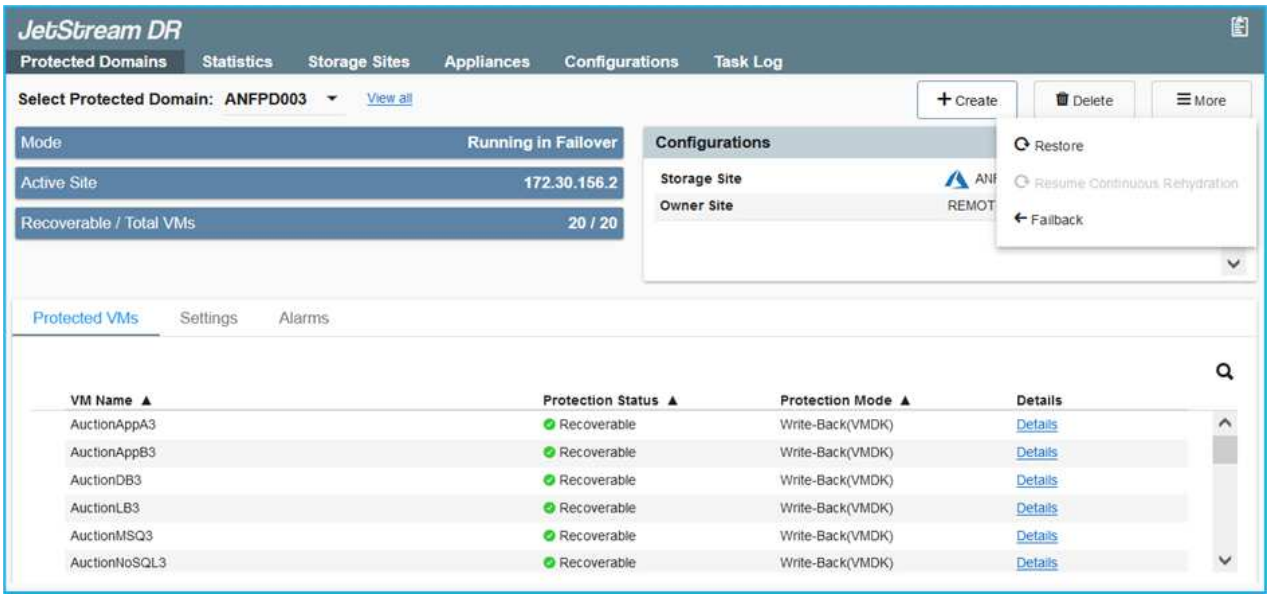


Una vez que el sitio principal esté activo y en funcionamiento de nuevo, es posible realizar la conmutación tras recuperación. La protección de equipos virtuales se reanuda y se debe comprobar la consistencia de los datos.

3. Restaure el entorno de sus instalaciones. En función del tipo de incidente de desastre, podría ser necesario restaurar o verificar la configuración del clúster protegido. Si es necesario, puede que sea necesario volver a instalar el software JetStream DR.

> Nota: La `recovery_utility_prepare_failback` El script que se proporciona en el kit de herramientas de automatización se puede utilizar 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 recuperación ante desastres de Jetstream y seleccione el dominio protegido adecuado. Una vez que el sitio protegido esté listo para la conmutación tras recuperación, seleccione la opción de conmutación por recuperación en la interfaz de usuario.



El plan de conmutación por recuperación generado por CPT también se puede usar para iniciar la devolución de los equipos virtuales y sus datos del almacén de objetos al entorno de VMware original.

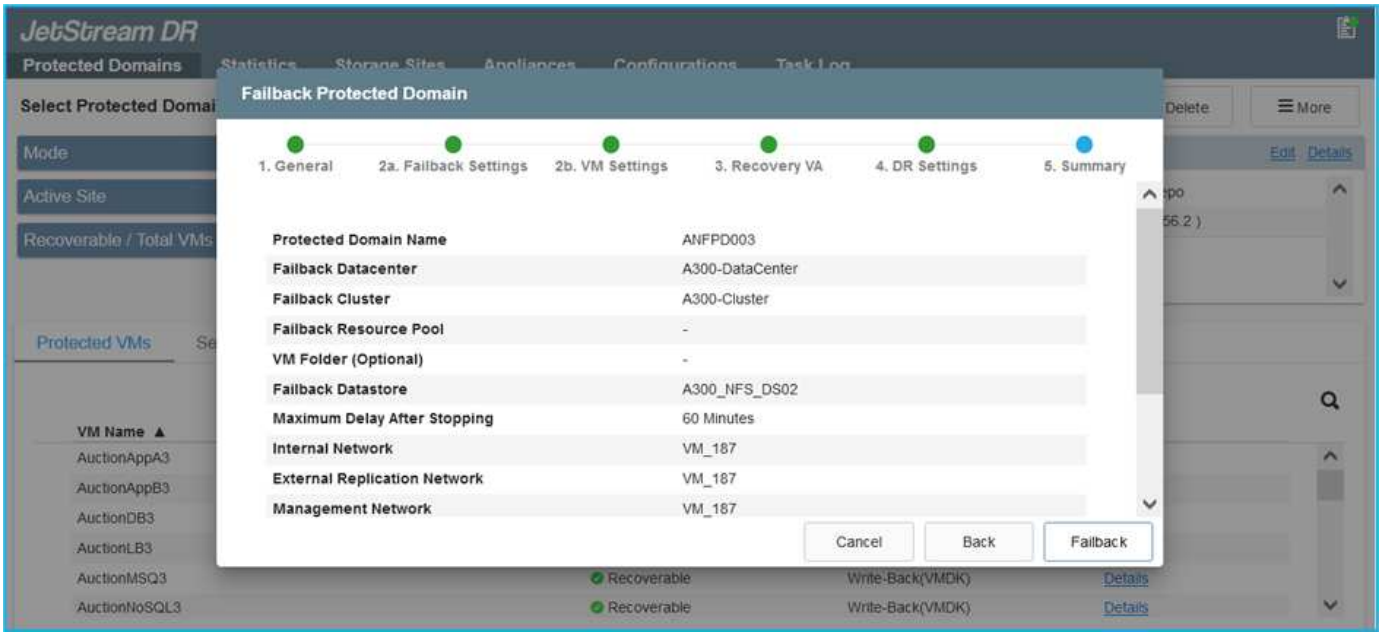
Especifique la demora máxima después de pausar las máquinas virtuales en el sitio de recuperación y reiniciar en el sitio protegido. Esta vez incluye completar la replicación después de detener las máquinas virtuales en caso de fallo, el tiempo para limpiar el sitio de recuperación y el tiempo para recrear las máquinas virtuales en el sitio protegido. El valor recomendado por NetApp es de 10 minutos.

Completar el proceso de conmutación tras recuperación y, a continuación, confirmar la reanudación de la protección de los equipos virtuales y la consistencia de datos.

Recuperación de Ransomeware

Recuperarse del ransomware puede ser una tarea abrumadora. Específicamente, puede resultar difícil para las organizaciones TECNOLÓGICAS determinar el punto de retorno seguro y, una vez determinado, cómo garantizar que las cargas de trabajo recuperadas se protejan de los ataques que vuelvan a producirse (de malware en suspensión o de aplicaciones vulnerables).

Jetstream DR para AVS junto con los almacenes de datos de Azure NetApp Files pueden resolver estos problemas al permitir que las organizaciones se recuperen de puntos disponibles en el tiempo, de modo que las cargas de trabajo se recuperen en una red funcional y aislada, en caso necesario. La recuperación permite que las aplicaciones funcionen y se comuniquen entre sí mientras no las exponen al tráfico norte-sur, dando así a los equipos de seguridad un lugar seguro para realizar el análisis forense y otra reparación necesaria.



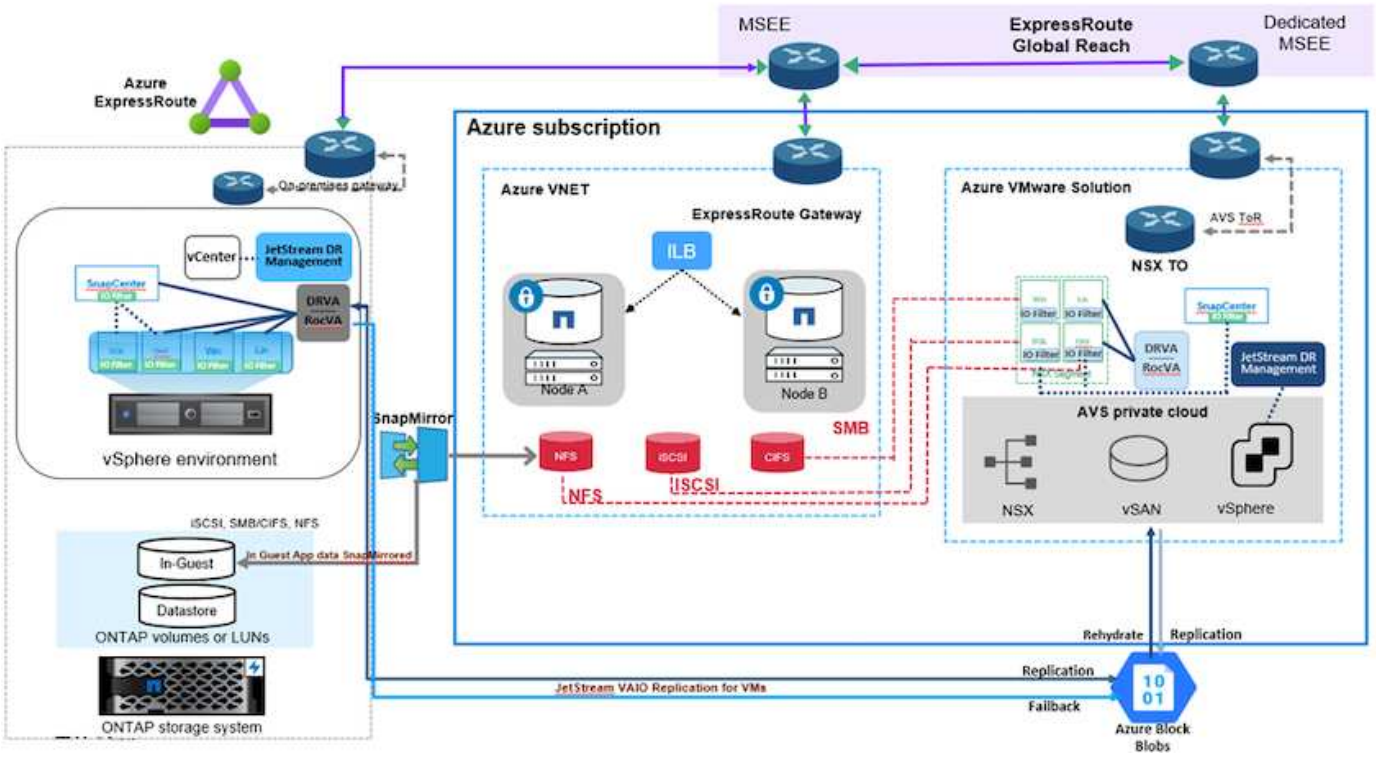
Recuperación ante desastres con CVO y AVS (almacenamiento conectado a invitado)

Descripción general

Autores: Ravi BCB y Niyaz Mohamed, NetApp

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por datos como ransomware. Con SnapMirror de NetApp, las cargas de trabajo de VMware en las instalaciones que utilizan el almacenamiento conectado a invitado se pueden replicar a Cloud Volumes ONTAP de NetApp que se ejecuta en Azure. Así se tratan los datos de aplicaciones; sin embargo, ¿qué ocurre con los equipos virtuales mismos? La recuperación ante desastres debería cubrir todos los componentes dependientes, incluidos equipos virtuales, VMDK, datos de aplicaciones, etc. Para ello, SnapMirror y JetStream pueden utilizarse para recuperar sin problemas cargas de trabajo replicadas de las instalaciones a Cloud Volumes ONTAP utilizando almacenamiento VSAN para VMDK de VM.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, JetStream y la solución Azure VMware (AVS) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con las aplicaciones.

> Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para obtener conectividad entre el entorno local y la red virtual de Azure, utilice el alcance global de la ruta Express o una WAN virtual con una puerta de enlace VPN. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Azure, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Azure para conocer el método de conectividad apropiado entre las instalaciones y Azure.

Implementar la solución DR

Descripción general de la puesta en marcha de soluciones

1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisione Cloud Volumes ONTAP con el tamaño de instancia correcto usando Cloud Manager dentro de la suscripción y la red virtual adecuadas.
    a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.

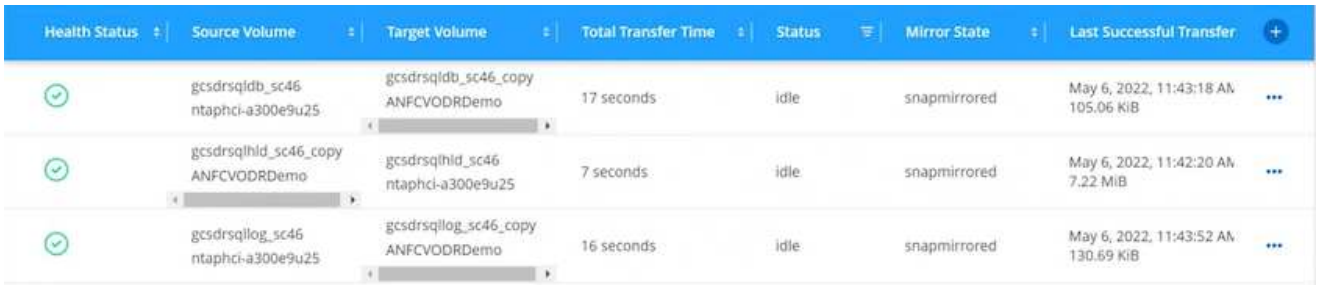
b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.

3. Instale el software de recuperación ante desastres JetStream en el centro de datos local y comience la protección de las máquinas virtuales.
4. Instalar el software de recuperación ante desastres JetStream en el cloud privado de Azure VMware Solution.
5. Durante un evento de desastre, rompa la relación de SnapMirror con Cloud Manager y active la conmutación por error de máquinas virtuales a Azure NetApp Files o a almacenes de datos VSAN en el sitio de recuperación ante desastres AVS designado.
   a. Vuelva a conectar las LUN ISCSI y los montajes NFS para los equipos virtuales de la aplicación.
6. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Azure y replicar volúmenes a CVO

El primer paso es configurar Cloud Volumes ONTAP en Azure ("Enlace") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.



Configurar los hosts AVS y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar el SDDC son el tamaño del clúster en la solución Azure VMware y el tiempo que se debe mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

La decisión de poner en marcha un clúster AVS se basa principalmente en los requisitos de RPO/RTO. Con la solución para Azure VMware, el SDDC se puede aprovisionar justo a tiempo como preparación para pruebas o ante un desastre real. Un SDDC implementado en el tiempo ahorra en costes de host ESXi cuando no se enfrenta a un desastre. Sin embargo, esta forma de puesta en marcha afecta al objetivo de tiempo de recuperación en unas pocas horas, mientras que se aprovisiona SDDC.

La opción más común implementada es tener SDDC en funcionamiento en un modo de funcionamiento siempre activo y con luz piloto. Esta opción proporciona una huella pequeña de tres hosts siempre disponibles y también acelera las operaciones de recuperación, ya que proporciona una línea de base en ejecución para las actividades de simulación y comprobaciones de cumplimiento de normativas, lo que evita el riesgo de que se produzca una desviación operativa entre los sitios de producción y de recuperación ante desastres. El grupo piloto se puede escalar verticalmente rápidamente hasta el nivel deseado cuando es necesario para gestionar un evento de recuperación ante desastres real.

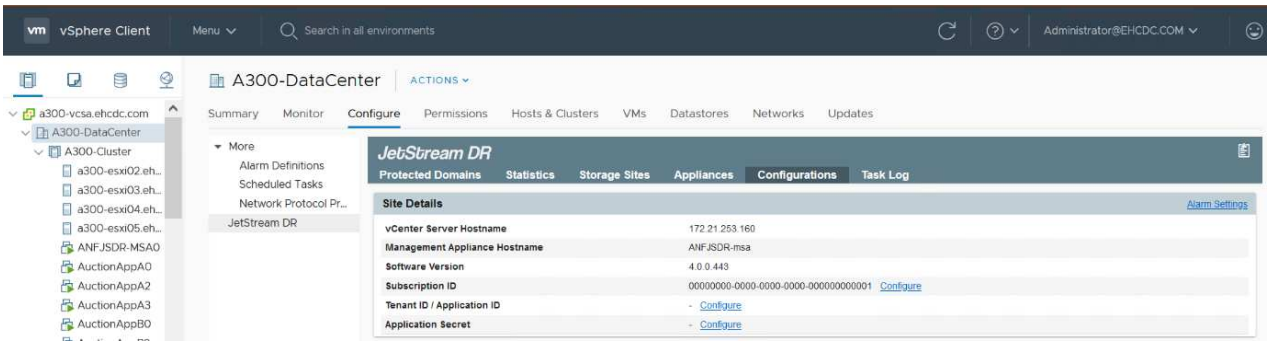
Para configurar AVS SDDC (ya sea a petición o en modo piloto), consulte "Ponga en marcha y configure el entorno de virtualización en Azure". Como requisito previo, verifique que los equipos virtuales invitados que residen en los hosts AVS pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y AVS se hayan configurado correctamente, comience a configurar JetStream para automatizar la recuperación de las cargas de trabajo en las instalaciones en AVS (VM con VMDK de aplicación y equipos virtuales con almacenamiento en invitado) mediante el mecanismo VAIO y aprovechando SnapMirror para copias de volúmenes de aplicación en Cloud Volumes ONTAP.

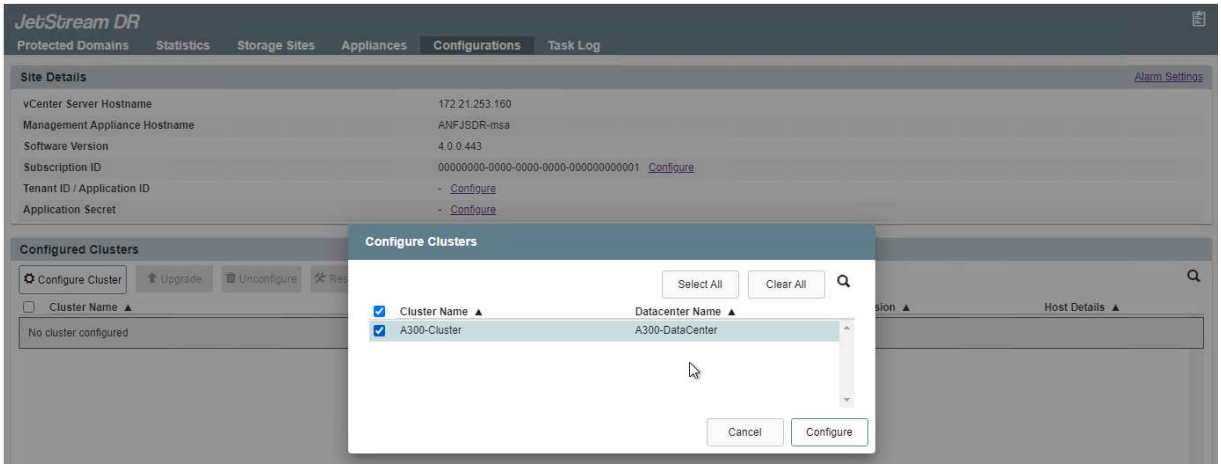
Instalar JetStream DR en el centro de datos local

El software JetStream DR consta de tres componentes principales: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) y componentes host (paquetes de filtros de I/o). MSA se utiliza para instalar y configurar componentes host en el cluster informático y, a continuación, administrar el software JetStream DR. El proceso de instalación es el siguiente:

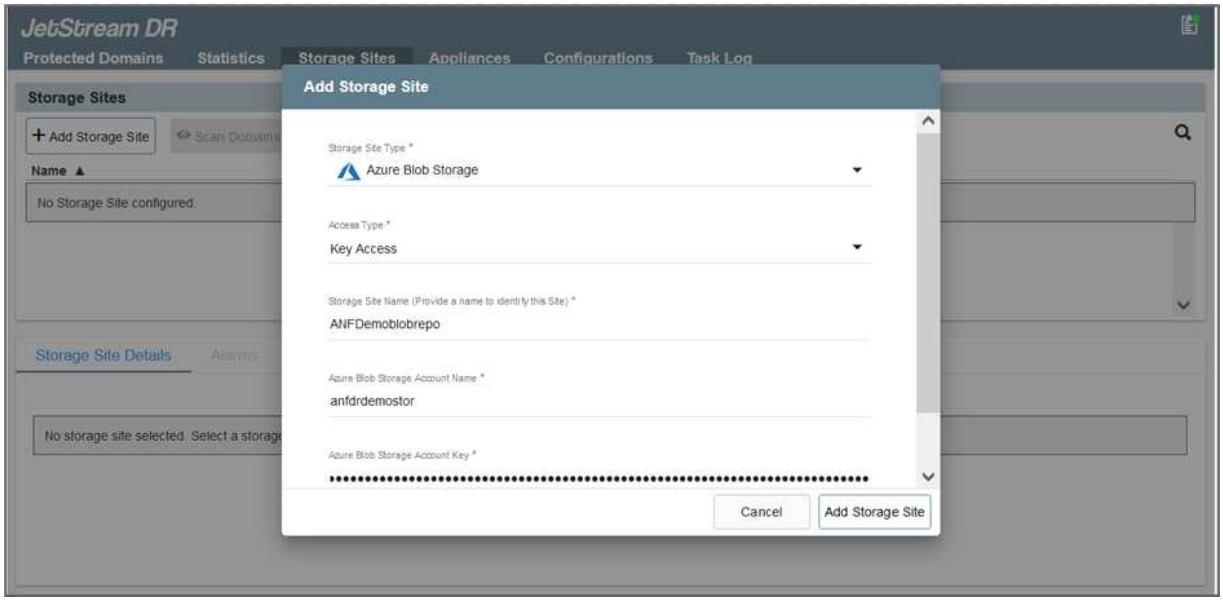
1. Compruebe los requisitos previos.
2. Ejecute la herramienta de planificación de la capacidad para realizar recomendaciones de recursos y configuración.
3. Implemente JetStream DR MSA en cada host de vSphere en el clúster designado.
4. Inicie MSA usando su nombre DNS en un explorador.
5. Registre el servidor vCenter con el MSA.
6. Una vez que se haya puesto en marcha JetStream DR MSA y se haya registrado vCenter Server, desplácese hasta el complemento de recuperación ante desastres JetStream con vSphere Web Client. Para ello, vaya a Datacenter > Configure > JetStream DR.



7. Desde la interfaz DR de JetStream, realice las siguientes tareas:
   a. Configure el clúster con el paquete de filtro de I/O.

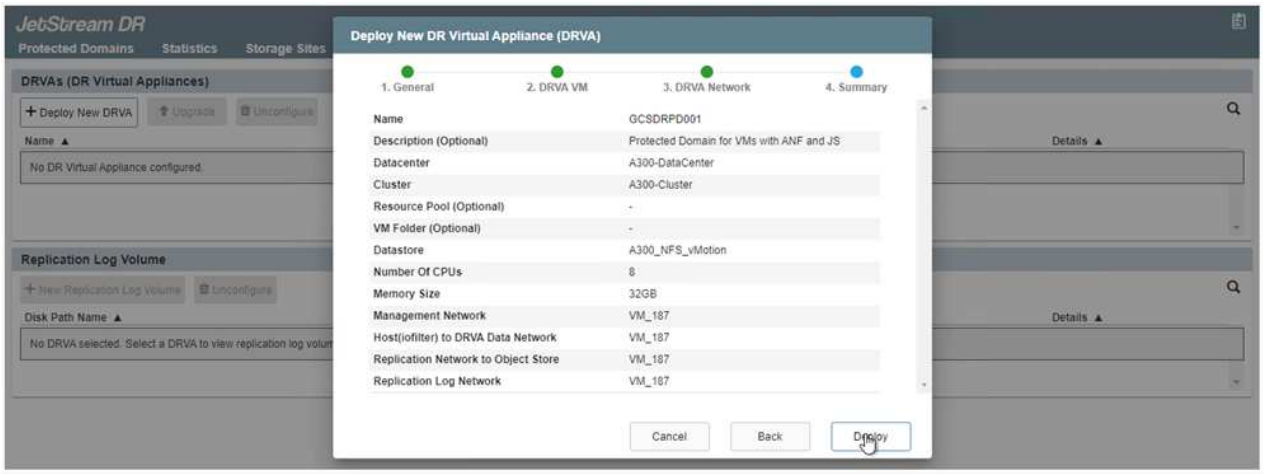


   b. Añada el almacenamiento de Azure Blob que está situado en el sitio de recuperación.

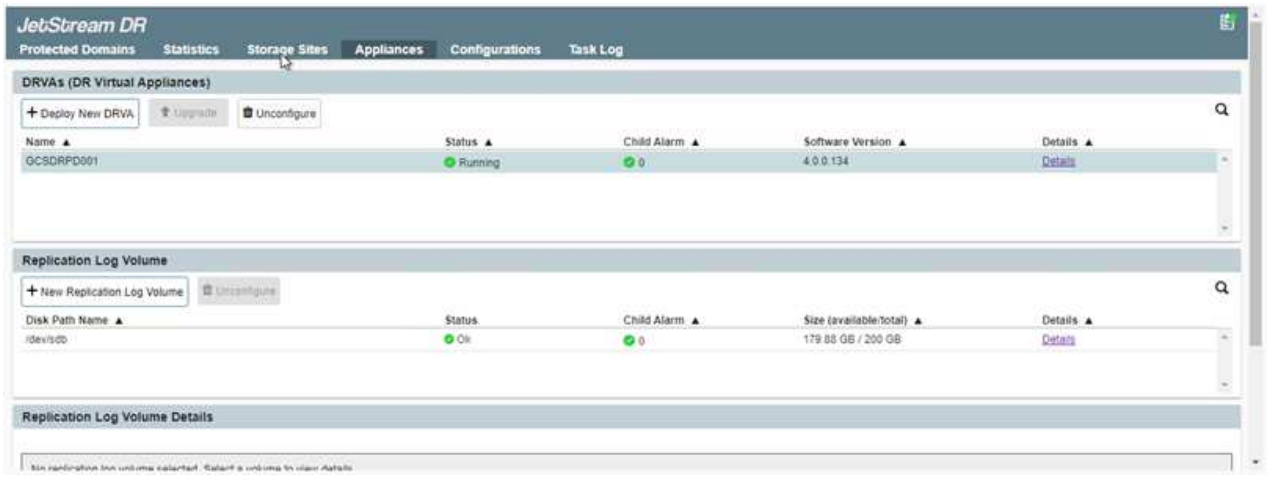


8. Implemente el número necesario de dispositivos virtuales de recuperación ante desastres (DRVAs) desde la ficha Appliances (dispositivos virtuales).

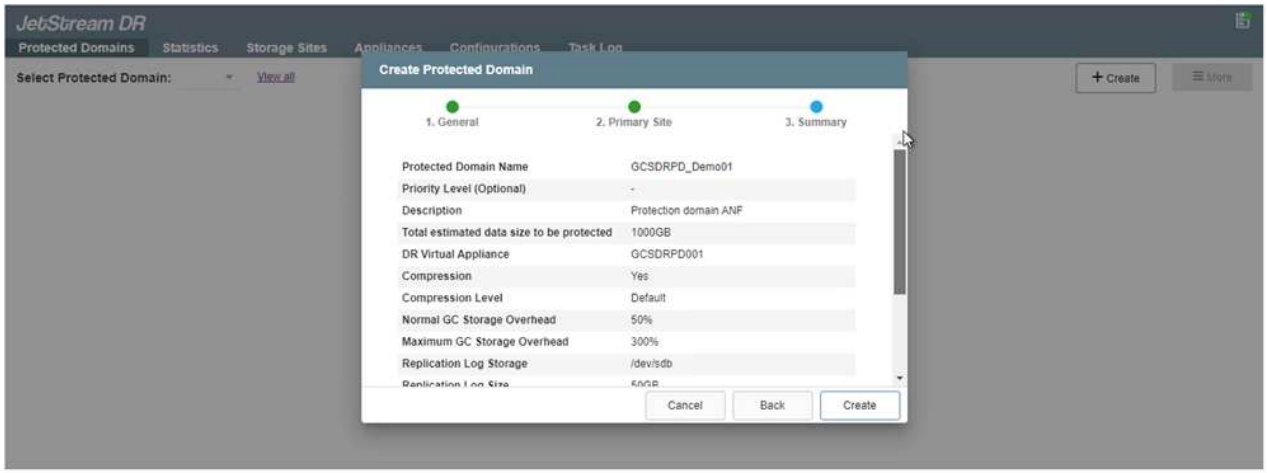
> Utilice la herramienta de planificación de la capacidad para calcular el número de DRVAs necesarios.

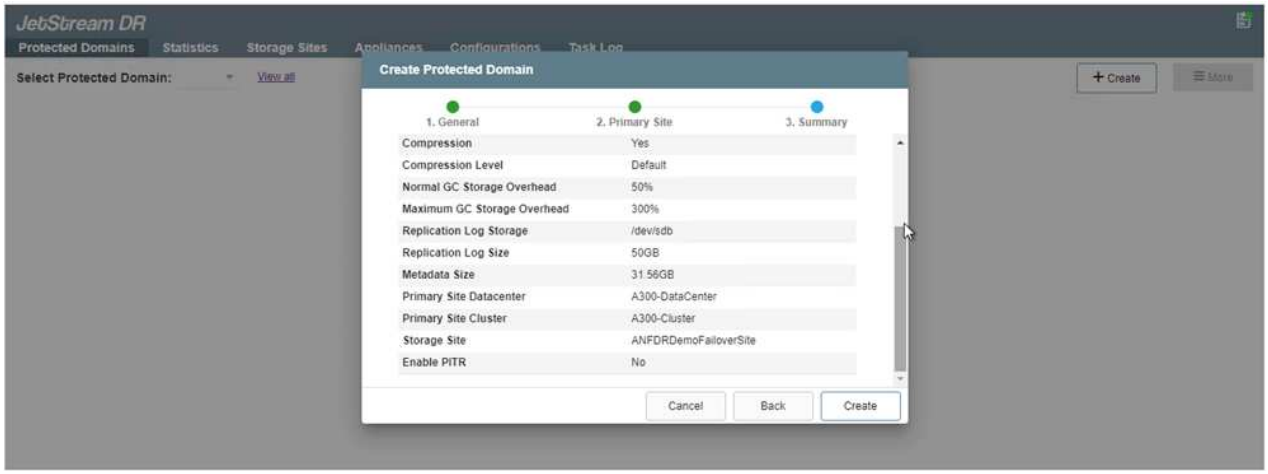


9. Cree volúmenes de registro de replicación para cada DRVA utilizando el VMDK desde los almacenes de datos disponibles o el pool de almacenamiento iSCSI compartido independiente.



10. En la pestaña Protected Domains, cree la cantidad necesaria de dominios protegidos utilizando información acerca del sitio de Azure Blob Storage, la instancia de DRVA y el registro de replicación. Un dominio protegido define una máquina virtual o un conjunto específico de máquinas virtuales de aplicación dentro del clúster que se protegen en conjunto y asignó un orden de prioridad para las operaciones de conmutación por error y conmutación tras recuperación.

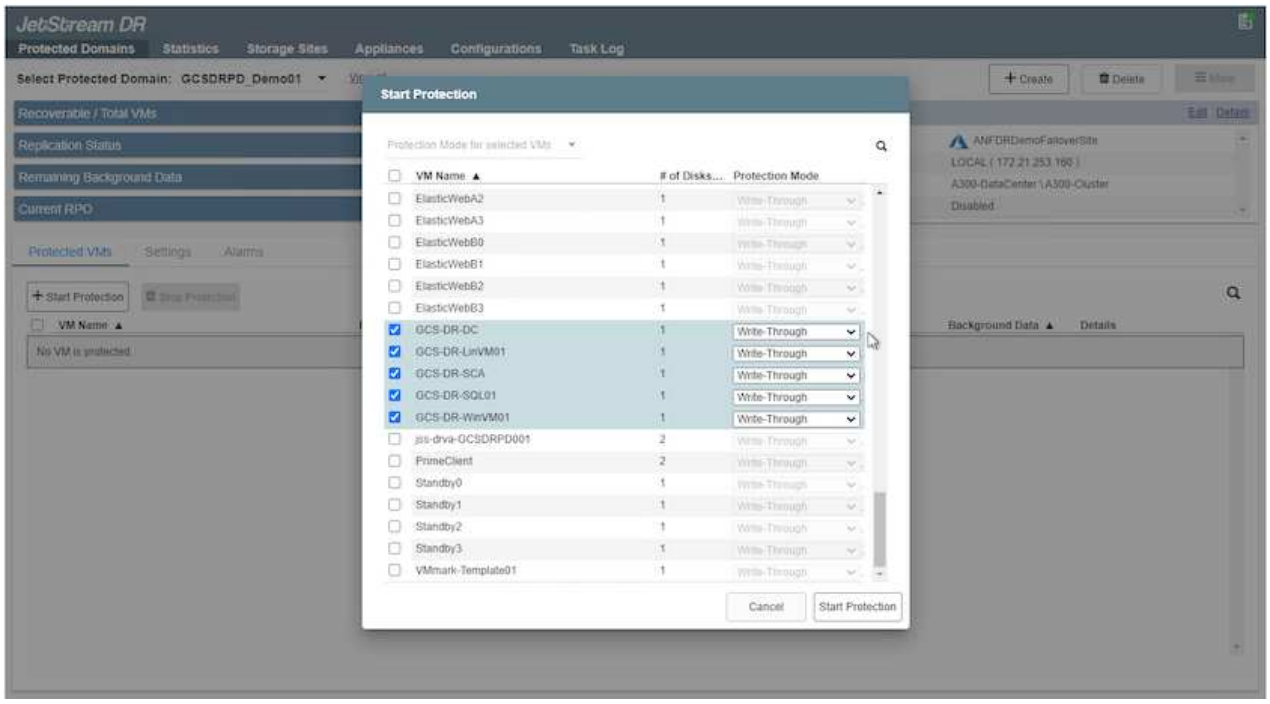




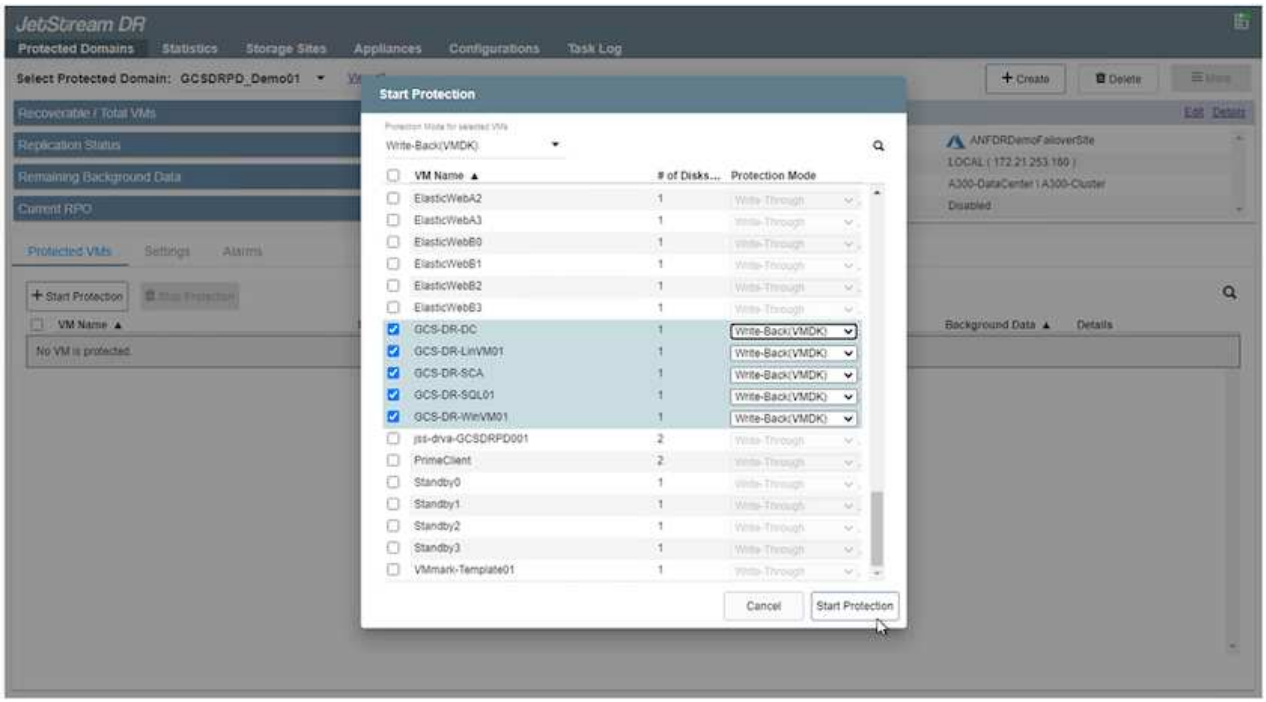
11. Seleccione las máquinas virtuales que se van a proteger y agrupe las máquinas virtuales en grupos de aplicaciones en función de la dependencia. Las definiciones de aplicaciones le permiten agrupar conjuntos de máquinas virtuales en grupos lógicos que contengan sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones opcionales que se pueden ejecutar tras la recuperación.

Asegúrese de que se utilice el mismo modo de protección para todas las máquinas virtuales de un dominio protegido.

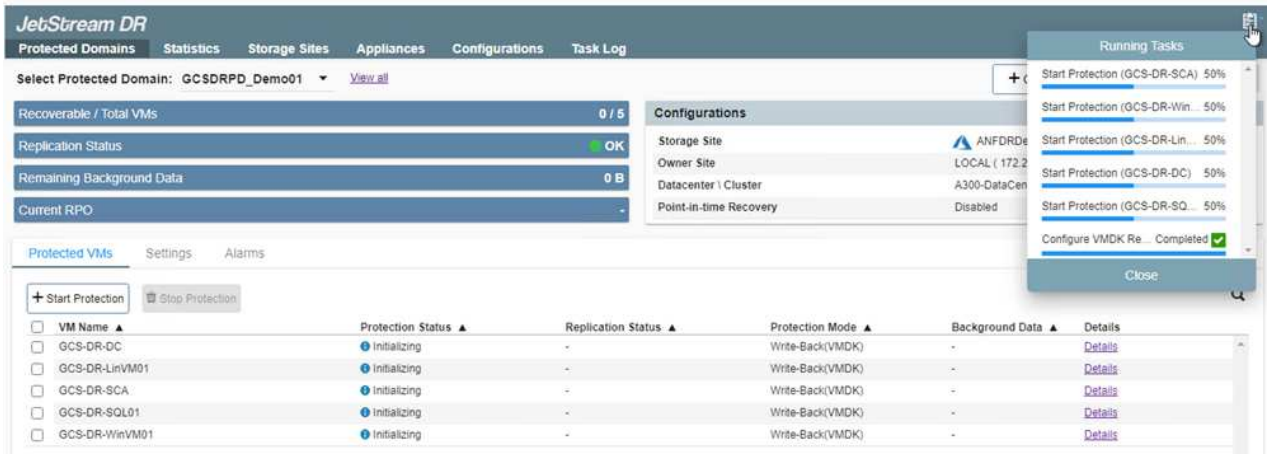
El modo Write-Back (VMDK) ofrece un mayor rendimiento.



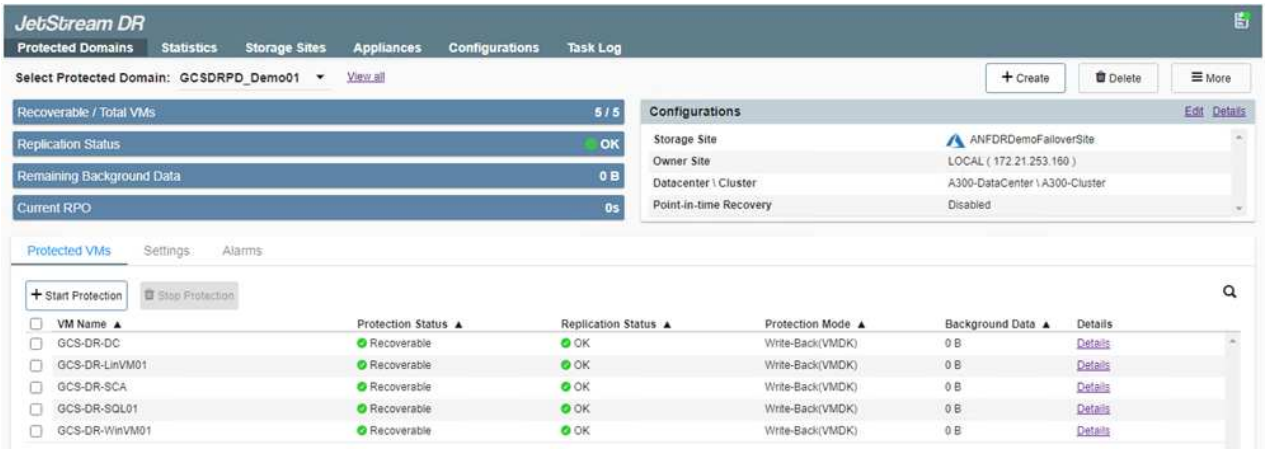
12. Asegúrese de que los volúmenes de registros de replicación se colocan en un almacenamiento de alto rendimiento.



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 BLOB designado.



14. Una vez finalizada la replicación, el estado de protección del equipo virtual se Marca como recuperable.

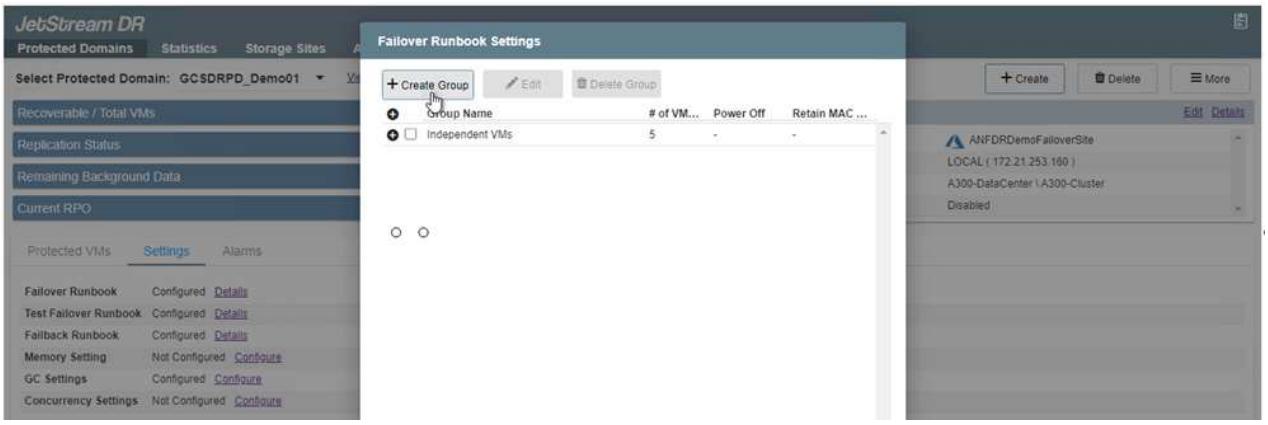


> Los runbooks pueden configurarse para agrupar los equipos virtuales (denominados «grupo de recuperación»), establecer la secuencia de órdenes de arranque y modificar la configuración de CPU/memoria junto con las configuraciones de IP.

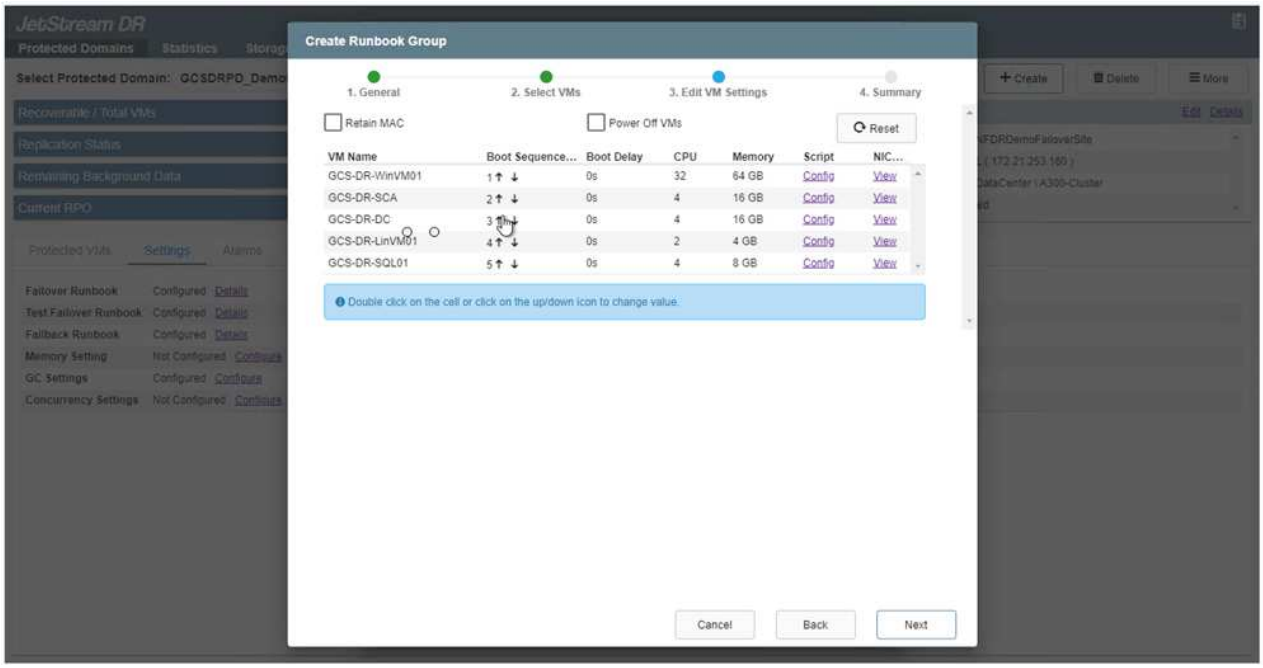
15. Haga clic en Configuración y, a continuación, en el enlace Configurar libro de ejecución para configurar el grupo de libro de ejecución.

16. Haga clic en el botón Crear grupo para comenzar a crear un nuevo grupo runbook.

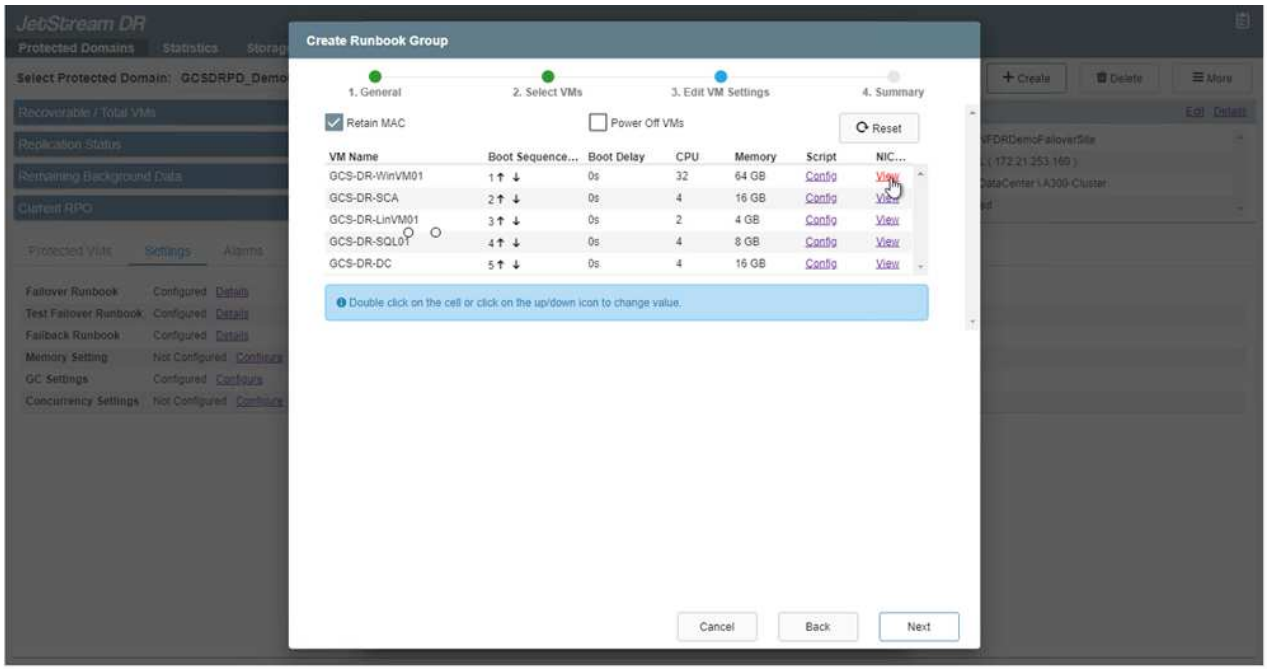
Si es necesario, en la parte inferior de la pantalla, aplique scripts previos y posteriores personalizados para que se ejecuten automáticamente antes y después del funcionamiento del grupo runbook. Asegúrese de que los scripts de Runbook residen en el servidor de administración.



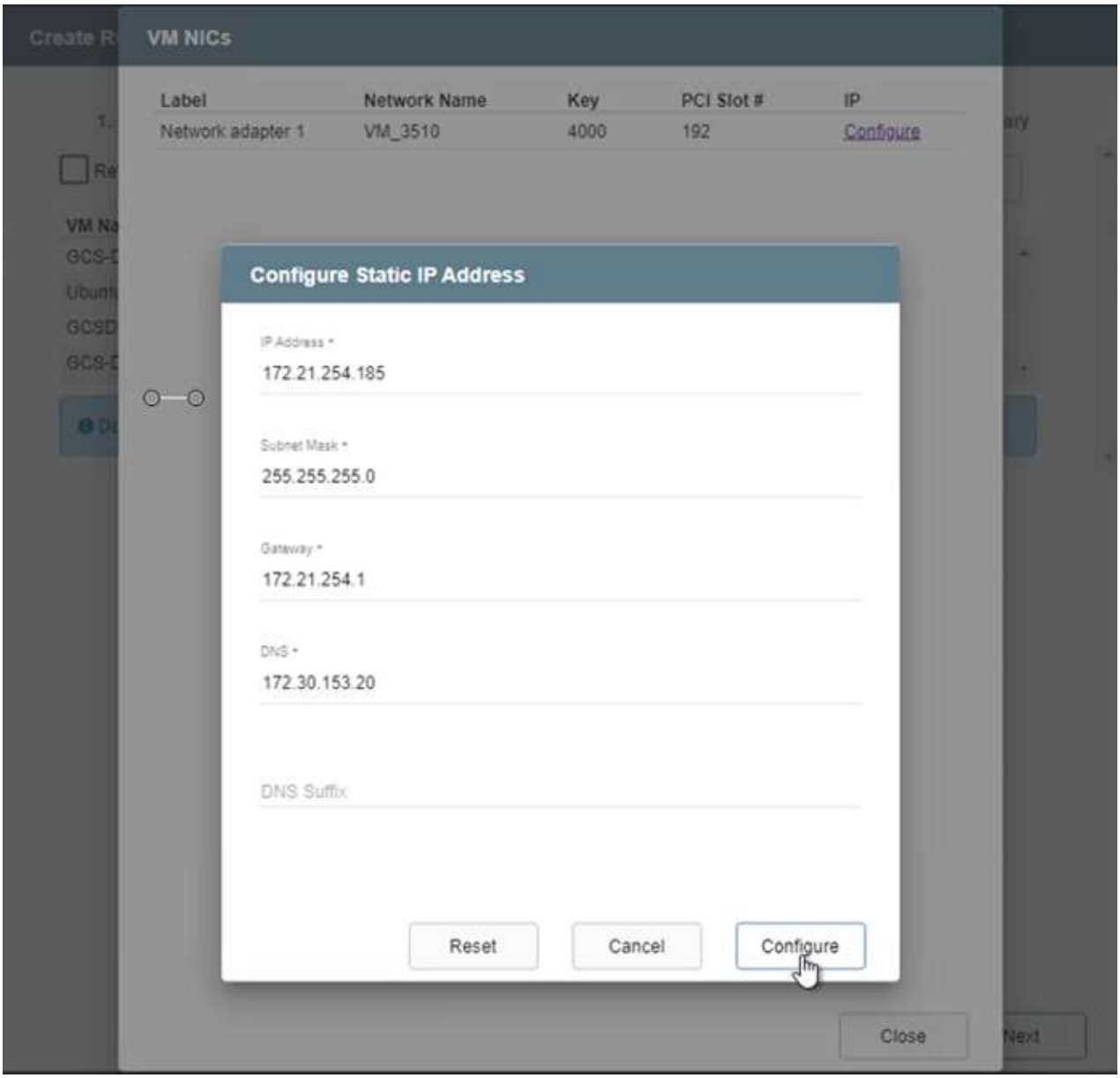
17. Edite la configuración de la máquina virtual según sea necesario. Especifique los parámetros para recuperar las VM, incluida la secuencia de arranque, el retraso de arranque (especificado en segundos), el número de CPU y la cantidad de memoria que se debe asignar. Cambie la secuencia de arranque de las VM haciendo clic en las flechas arriba o abajo. También se proporcionan opciones para conservar MAC.

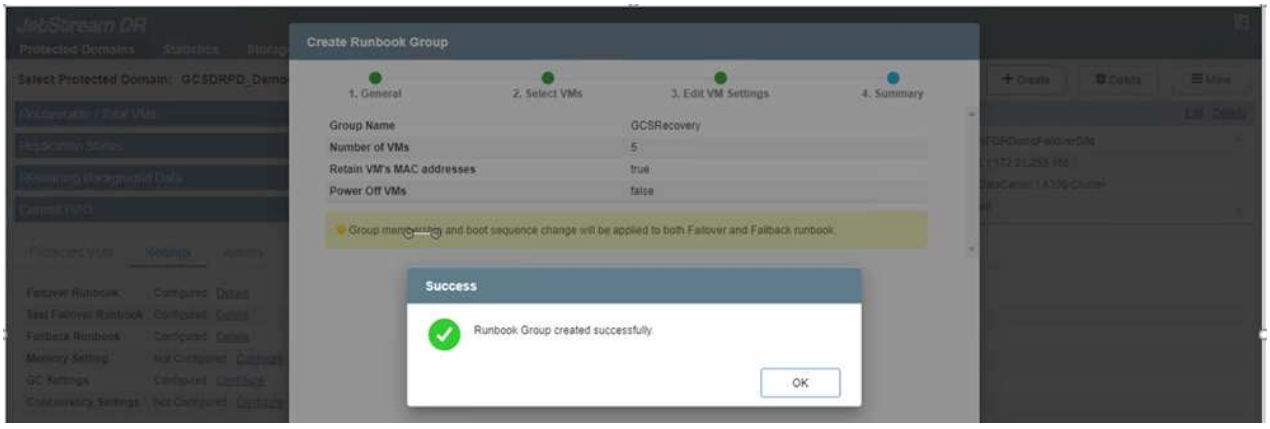


18. Las direcciones IP estáticas pueden configurarse manualmente para las máquinas virtuales individuales del grupo. Haga clic en el enlace NIC View de una máquina virtual para configurar manualmente las opciones de su dirección IP.



19. Haga clic en el botón Configure para guardar los ajustes de NIC de los equipos virtuales correspondientes.





El estado de los runbooks de conmutación por error y conmutación por recuperación se muestra ahora como configurado. Los grupos de runbooks de conmutación por error y conmutación tras recuperación se crean en parejas utilizando el mismo grupo inicial de máquinas virtuales y configuraciones. Si es necesario, la configuración de cualquier grupo runbook se puede personalizar individualmente haciendo

clic en el vínculo Detalles correspondiente y realizando cambios.

Instale JetStream DR para AVS en la nube privada

Una práctica recomendada para un sitio de recuperación (AVS) es crear un clúster de tres nodos de luz piloto con antelación. Esto permite configurar la infraestructura del centro de recuperación, lo que incluye lo siguiente:

- Segmentos de red de destino, firewalls, servicios como DHCP y DNS, etc.
- Instalación de JetStream DR para AVS
- La configuración de volúmenes ANF como almacenes de datos y mucho más

Jetstream DR admite un modo RTO casi cero para los dominios de misión crítica. Para estos dominios, el almacenamiento de destino debe estar preinstalado. ANF es un tipo de almacenamiento recomendado en este caso.

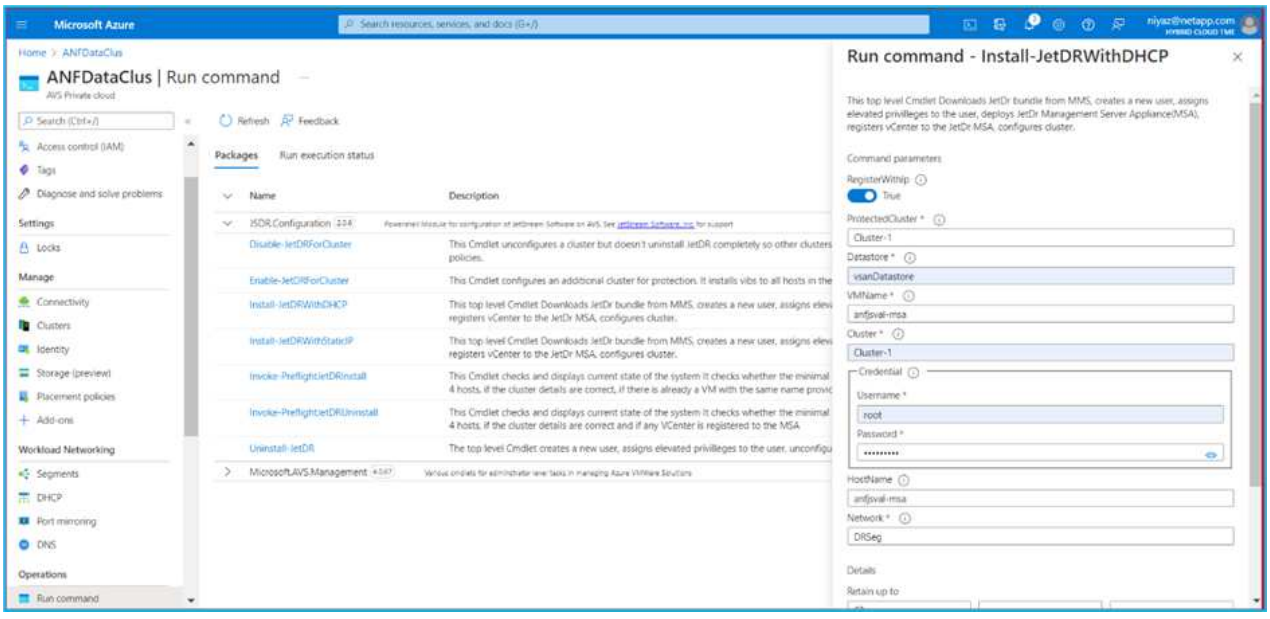
> La configuración de la red, incluida la creación de segmentos, se debe configurar en el clúster AVS para que coincida con los requisitos en las instalaciones.

> Según los requisitos del acuerdo de nivel de servicio y el objetivo de tiempo de recuperación, puede utilizar la conmutación por error continua o el modo de conmutación por error normal (estándar). Para lograr un objetivo de tiempo de recuperación cercano a cero, debe comenzar una rehidratación continua en el sitio de recuperación.

1. Para instalar JetStream DR para AVS en un cloud privado de Azure VMware Solution, utilice el comando Run. En el portal de Azure, vaya a la solución VMware de Azure, seleccione la nube privada y seleccione Ejecutar comando > Paquetes > JSDR.Configuration.

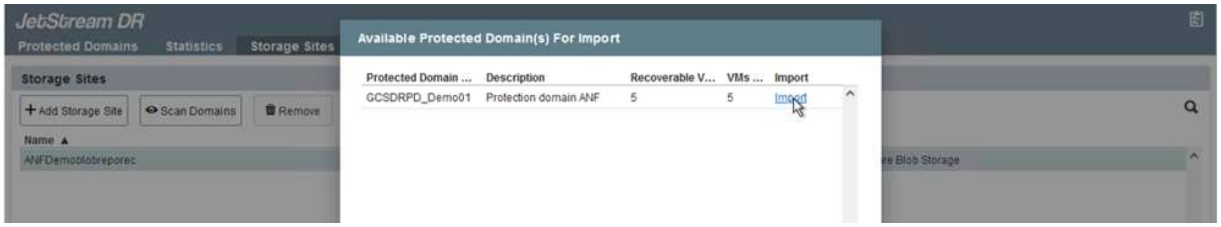
   > El usuario CloudAdmin predeterminado de la solución VMware de Azure no tiene suficientes privilegios para instalar JetStream DR para AVS. La solución Azure VMware permite una instalación simplificada y automatizada de la recuperación ante desastres de JetStream mediante la llamada al comando Azure VMware Solution Run para la recuperación ante desastres de JetStream.

   La siguiente captura de pantalla muestra la instalación mediante una dirección IP basada en DHCP.



2. Una vez finalizada la instalación de JetStream DR para AVS, actualice el explorador. Para acceder a la interfaz de usuario de recuperación ante desastres de JetStream, vaya a SDDC Datacenter > Configure > JetStream DR.

3. Desde la interfaz DR de JetStream, realice las siguientes tareas:
   a. Añada la cuenta de Azure Blob Storage que se utilizó para proteger el clúster local como sitio de almacenamiento y, a continuación, ejecute la opción Scan Domains.
   b. En la ventana emergente de diálogo que aparece, seleccione el dominio protegido que desea importar y, a continuación, haga clic en el vínculo Importar.

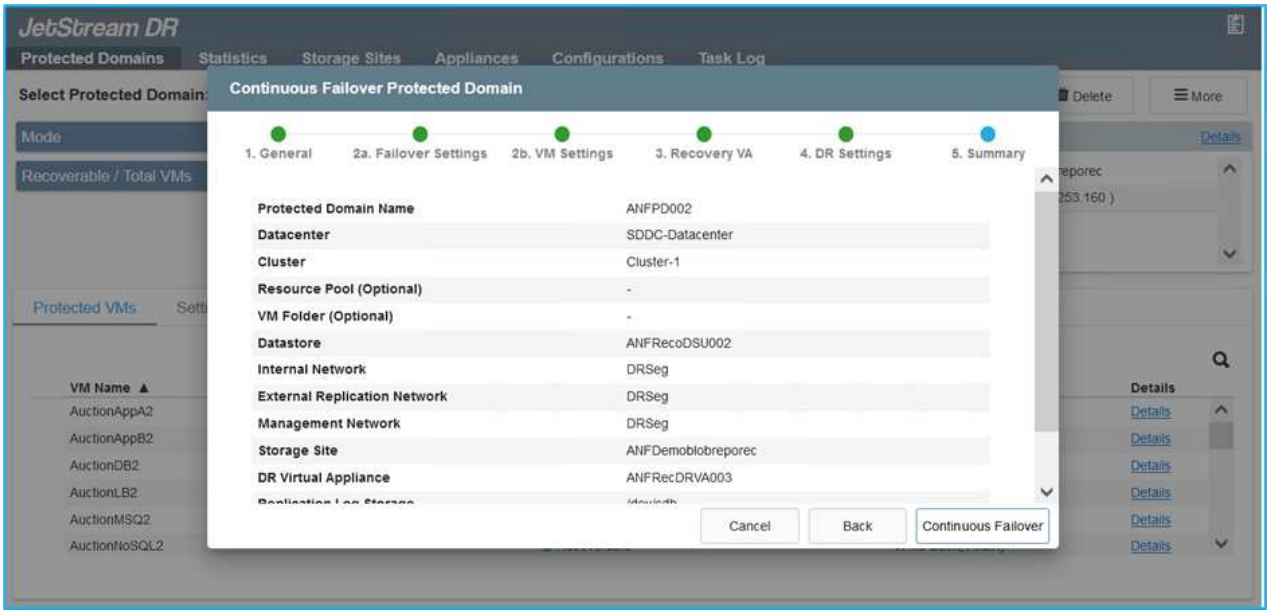


4. El dominio se importa para la recuperación. Vaya a la ficha Dominios protegidos y compruebe que el dominio deseado se ha seleccionado o elija el que desee en el menú Seleccionar dominio protegido. Se muestra una lista de las máquinas virtuales recuperables del dominio protegido.

5. Después de importar los dominios protegidos, implemente dispositivos DRVA.

Estos pasos también se pueden automatizar mediante planes creados por CPT.

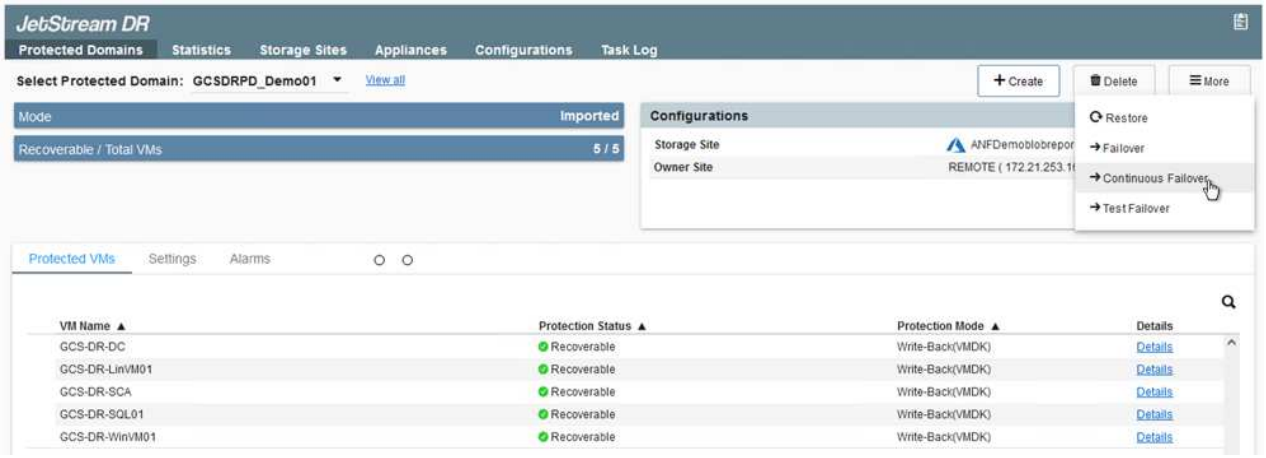
6. Cree volúmenes de registros de replicación con almacenes de datos VSAN o ANF disponibles.
7. Importe los dominios protegidos y configure el va de recuperación para utilizar un almacén de datos ANF para las ubicaciones de las máquinas virtuales.



Asegúrese de que DHCP está habilitado en el segmento seleccionado y de que hay suficientes IP disponibles. Las IP dinámicas se utilizan temporalmente mientras se recuperan los dominios. Cada VM que se recupera (incluida la rehidratación continua) requiere una IP dinámica individual. Una vez finalizada la recuperación, se libera la IP y se puede volver a utilizar.

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).

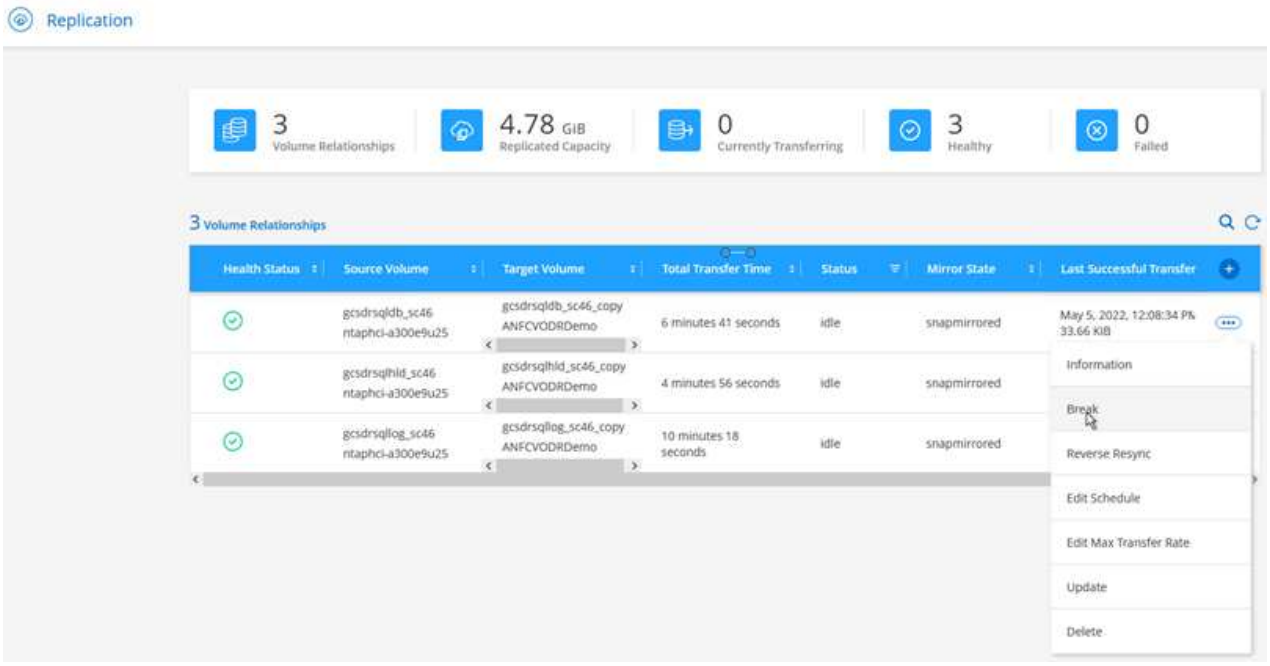
Aunque los modos de conmutación por error continua y conmutación por error varían cuando se realiza la configuración, ambos modos de conmutación por error se configuran siguiendo los mismos pasos. Los pasos de conmutación por error se configuran y se realizan de forma conjunta en respuesta a un evento de desastre. La conmutación por error continua se puede configurar en cualquier momento y luego se puede ejecutar en segundo plano durante el funcionamiento normal del sistema. Una vez ocurrido un evento de desastre, la conmutación al respaldo continua se completa para transferir inmediatamente la propiedad de las máquinas virtuales protegidas al sitio de recuperación (objetivo de tiempo de recuperación cercano a cero).

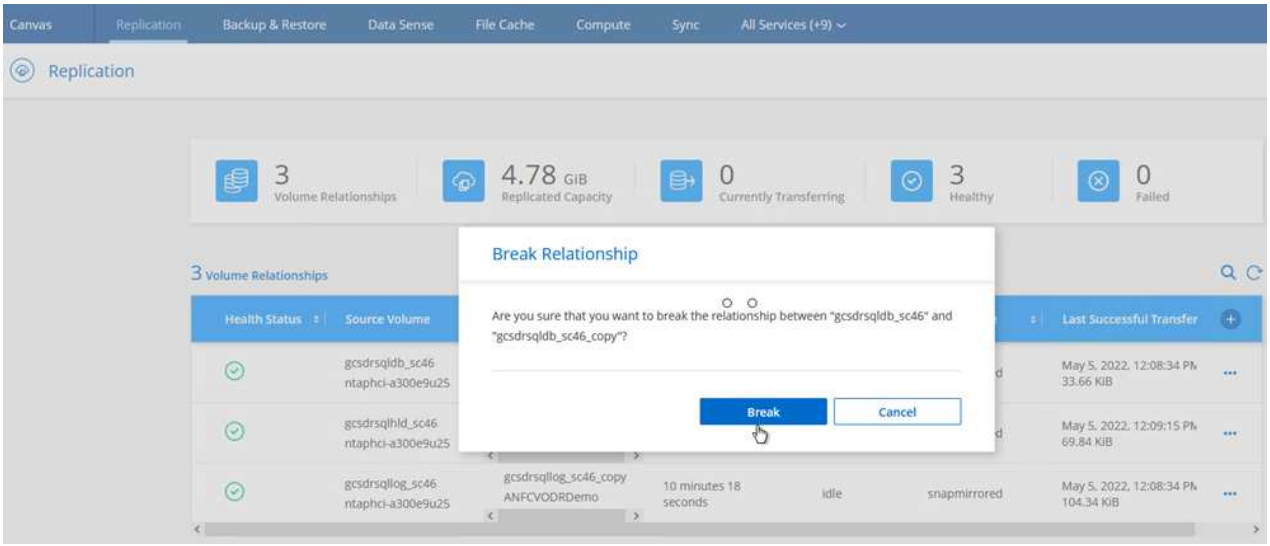


El proceso de conmutación al respaldo continua comienza y su progreso se puede supervisar desde la interfaz de usuario. Al hacer clic en el icono azul de la sección Paso actual se muestra una ventana emergente que muestra los detalles del paso actual del proceso de conmutación por error.

Conmutación por error y conmutación por recuperación

1. Cuando se produce un desastre en el clúster protegido del entorno local (fallo parcial o completo), puede activarse la conmutación por error para máquinas virtuales mediante Jetstream tras romper la relación de SnapMirror con los volúmenes de aplicaciones correspondientes.

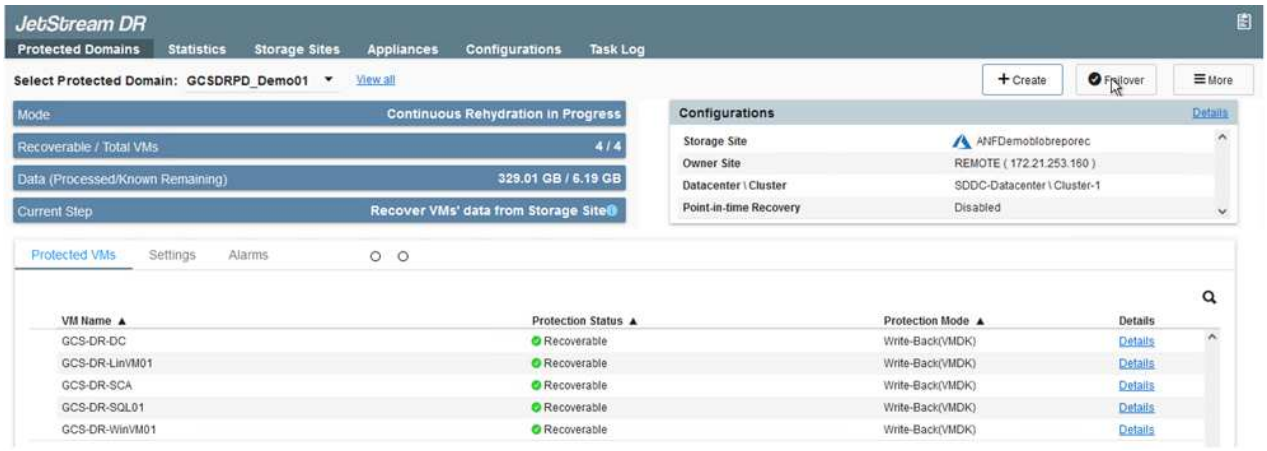


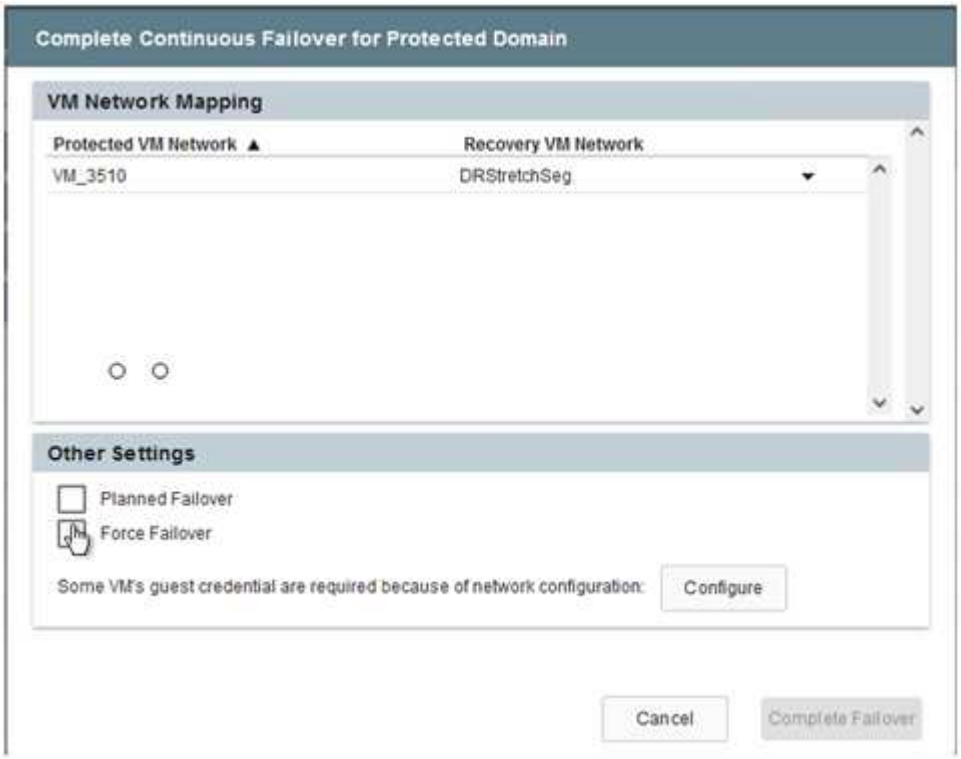


Este paso puede automatizarse fácilmente para facilitar el proceso de recuperación.

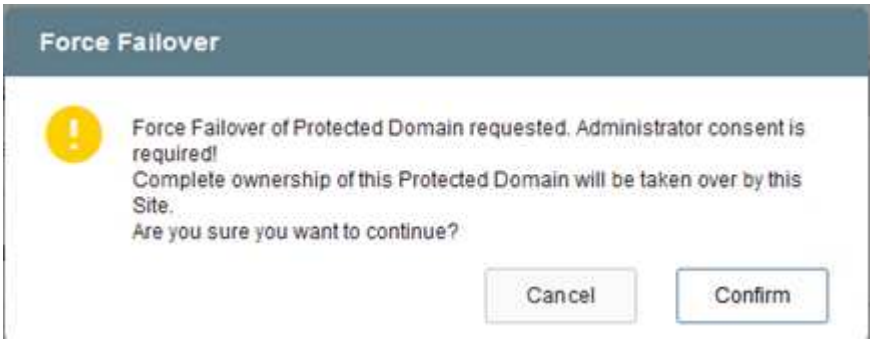
2. Acceda a Jetstream UI en AVS SDDC (destino) y active la opción de recuperación tras fallos para completar la recuperación tras fallos. La barra de tareas muestra el progreso de las actividades de failover.

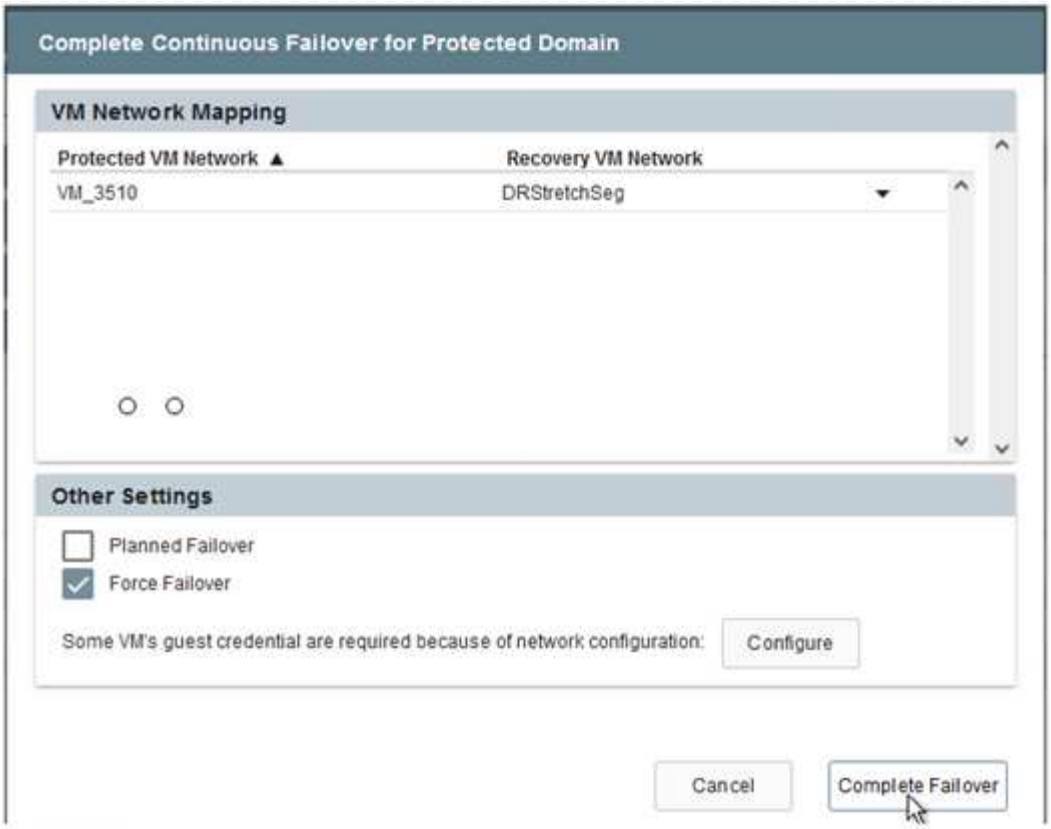
   En la ventana de diálogo que aparece al finalizar la conmutación por error, la tarea de conmutación por error se puede especificar como planificada o se supone que se fuerza.





La conmutación por error forzada asume que el sitio principal ya no está accesible y que el sitio de recuperación debería asumir directamente la propiedad del dominio protegido.



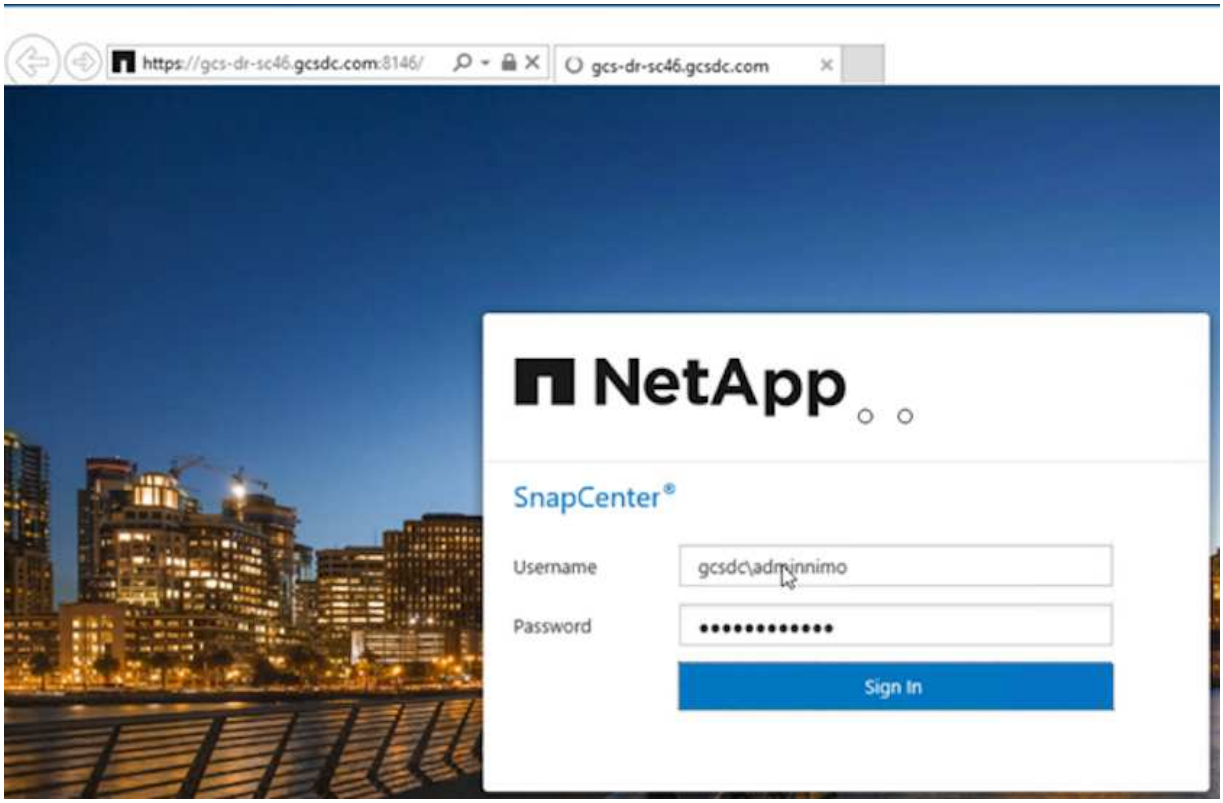


3. Una vez finalizada la conmutación por error continua, aparece un mensaje que confirma la finalización de la tarea. Una vez finalizada la tarea, acceda a los equipos virtuales recuperados para configurar sesiones ISCSI o NFS.

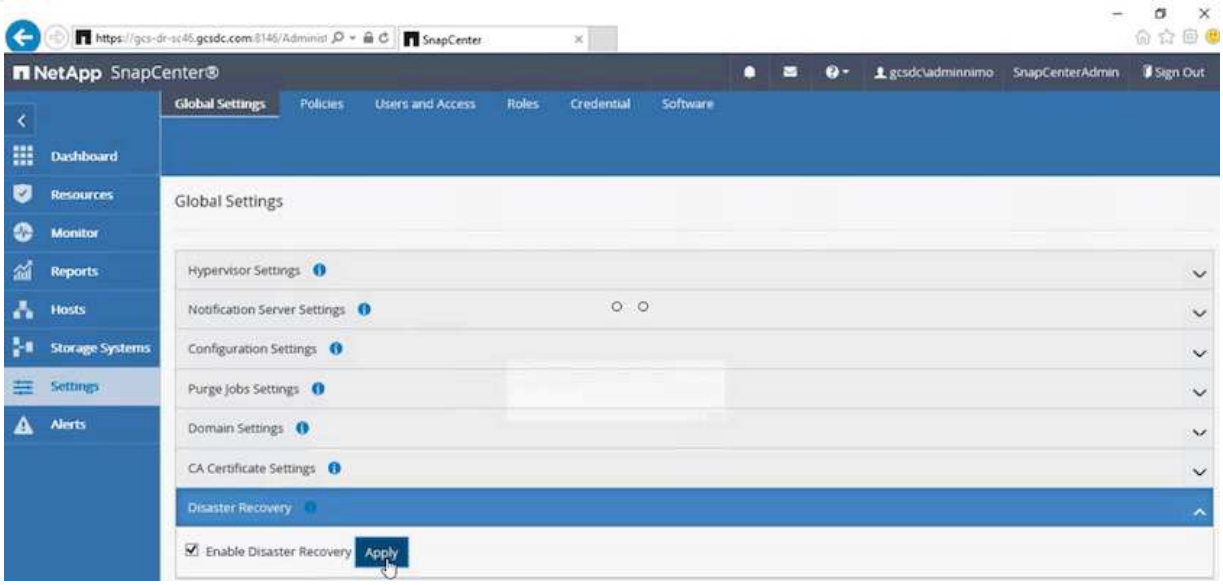
El modo de recuperación tras fallos cambia a ejecutarse en Failover y el estado del equipo virtual es recuperable. Todas las máquinas virtuales del dominio protegido ahora se ejecutan en el sitio de recuperación con el estado especificado por la configuración de runbook para conmutación por error.

Para verificar la configuración de recuperación tras fallos y la infraestructura, JetStream puede utilizarse en modo de prueba (opción de conmutación por error de prueba) para observar la recuperación de máquinas virtuales y sus datos desde el almacén de objetos en un entorno de recuperación de pruebas. Cuando se ejecuta un procedimiento de conmutación por error en el modo de prueba, su operación se asemeja a un proceso de conmutación por error real.

4. Después de recuperar las máquinas virtuales, utilice la recuperación ante desastres de almacenamiento para el almacenamiento invitado. Para demostrar este proceso, se utiliza SQL Server en este ejemplo.
5. Inicie sesión en el SnapCenter VM recuperado en AVS SDDC y habilite el modo de recuperación ante desastres.
   a. Acceda a la interfaz de usuario de SnapCenter mediante el comando browserN.



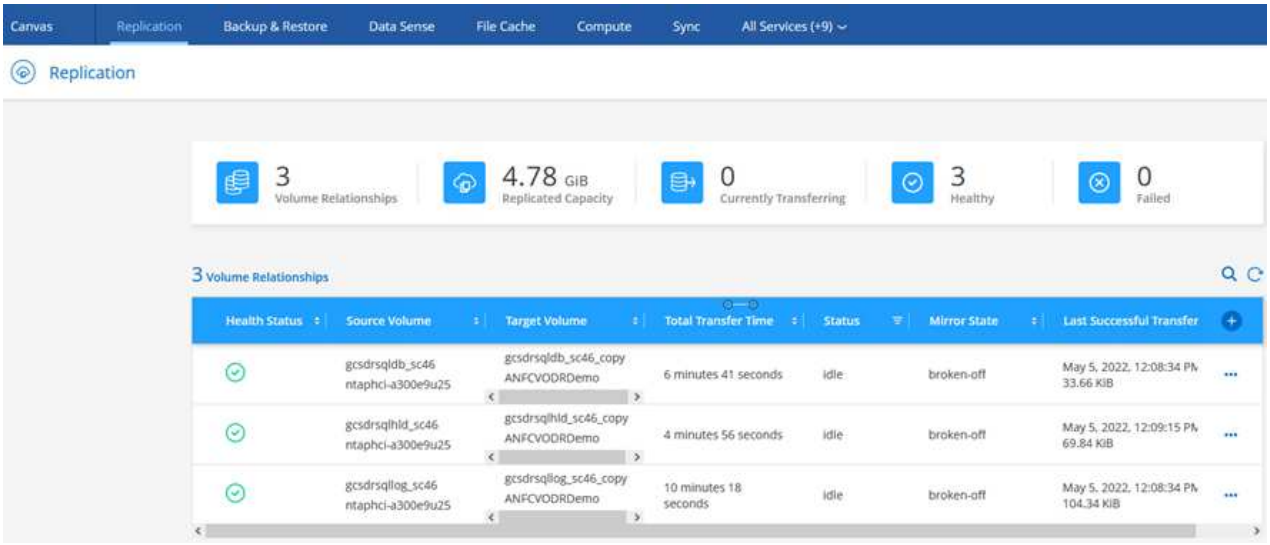
   b. En la página Settings, vaya a Settings > Global Settings > Disaster Recovery.
   c. Seleccione Enable Disaster Recovery.
   d. Haga clic en Apply.



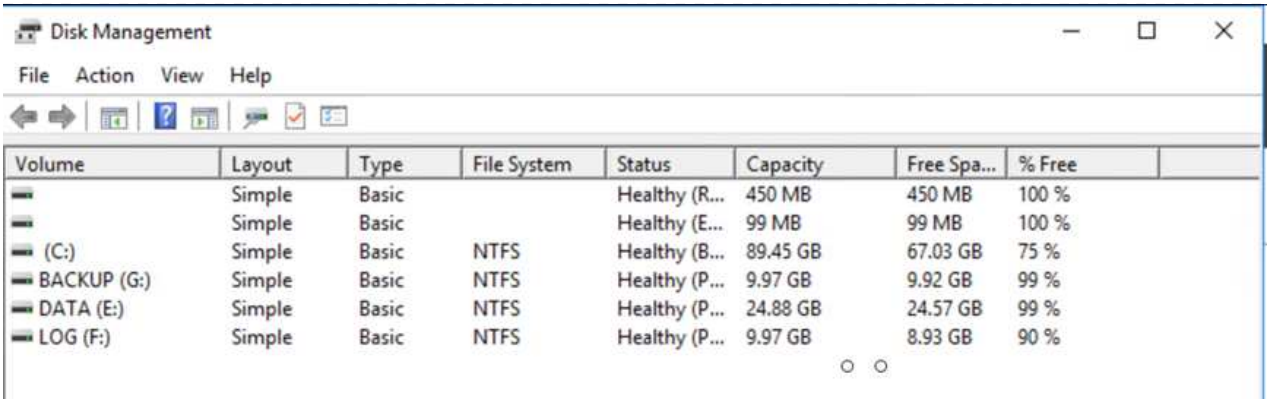
e. Compruebe si el trabajo de recuperación ante desastres está habilitado. Para ello, haga clic en Monitor > Jobs.

> NetApp SnapCenter 4.6 o posterior deben utilizarse para la recuperación ante desastres de almacenamiento. En las versiones anteriores, se deben utilizar snapshots coherentes con la aplicación (replicados mediante SnapMirror) y se debe ejecutar la recuperación manual en caso de que los backups anteriores se recuperen en el centro de recuperación ante desastres.

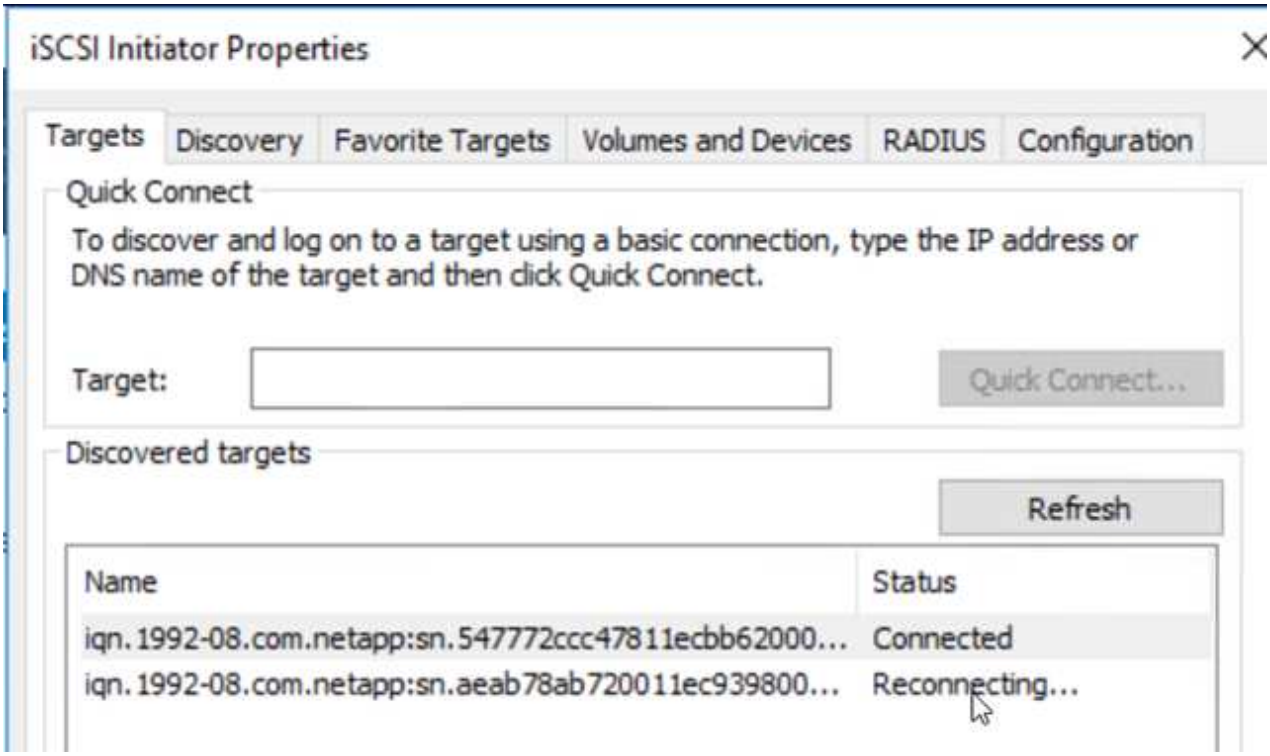
6. Asegúrese de que la relación de SnapMirror esté rota.



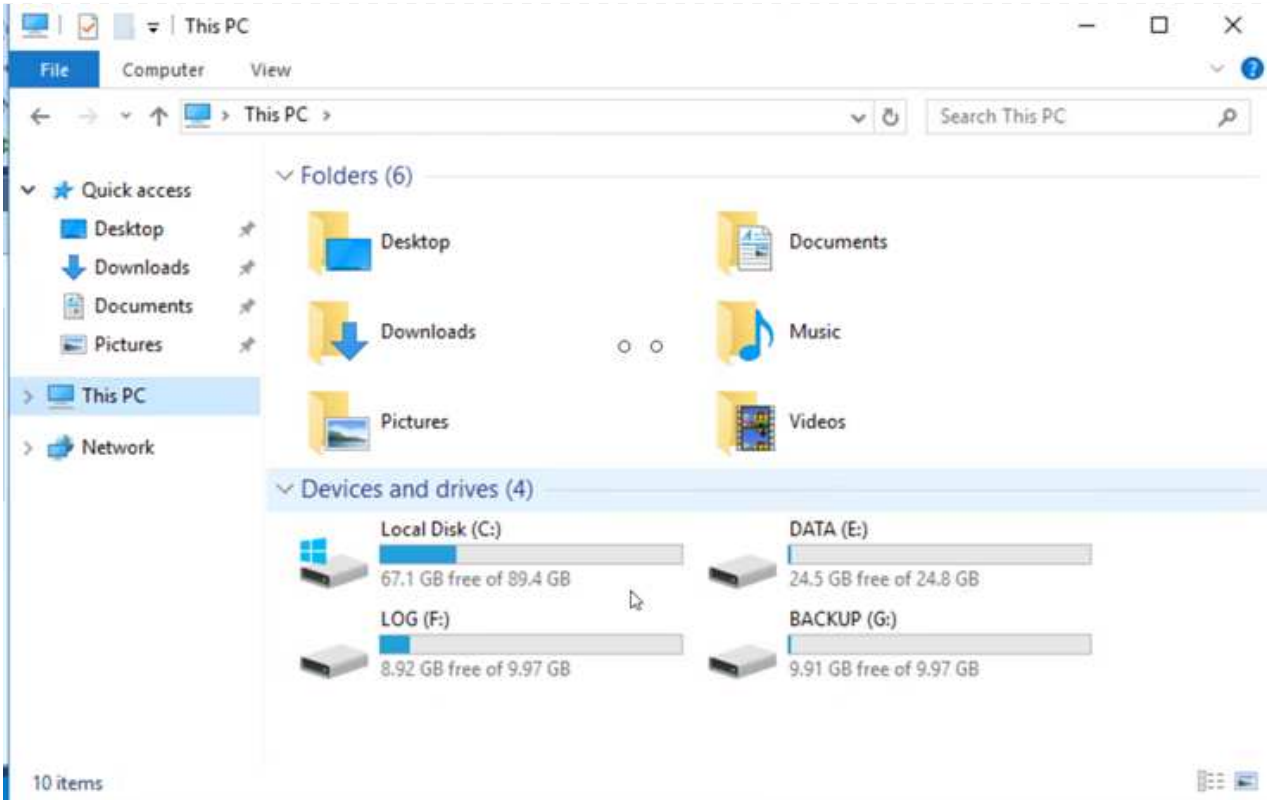
7. Asociar la LUN de Cloud Volumes ONTAP a la máquina virtual invitada de SQL recuperada con las mismas letras de unidad.



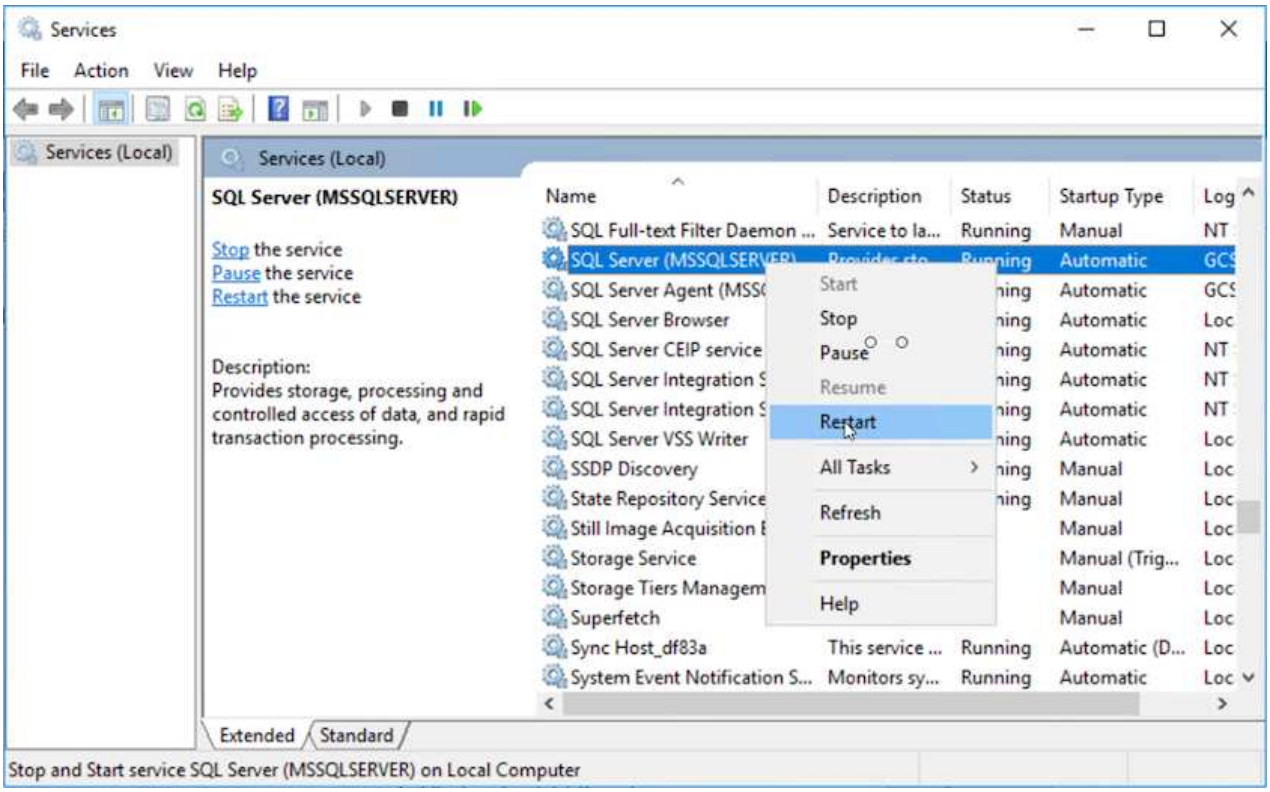
8. Abra el iniciador iSCSI, borre la sesión desconectada anterior y añada el nuevo destino junto con la multivía para los volúmenes Cloud Volumes ONTAP replicados.



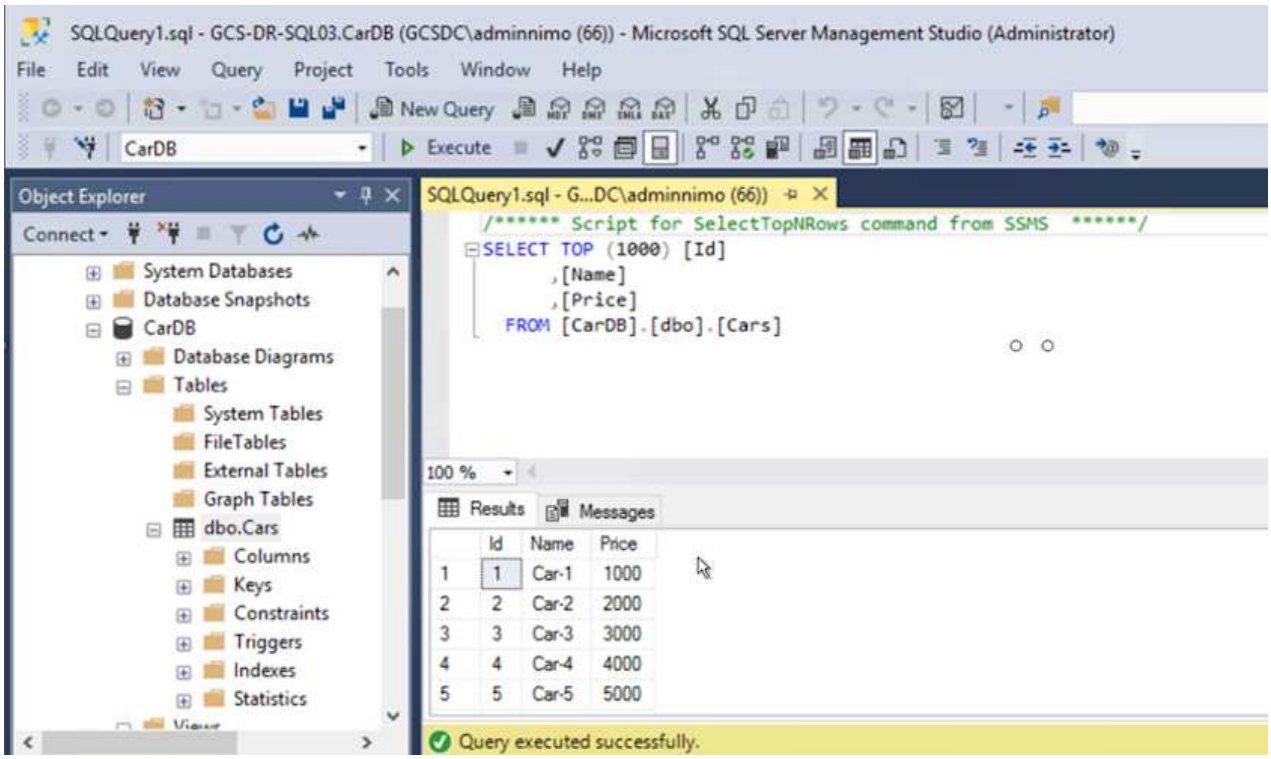
9. Asegúrese de que todos los discos están conectados utilizando las mismas letras de unidad que se usaron antes de la recuperación ante desastres.



10. Reinicie el servicio del servidor MSSQL.



11. Asegúrese de que los recursos SQL vuelven a estar en línea.



En el caso de NFS, asocie los volúmenes con el comando Mount y actualice el `/etc/fstab` entradas.

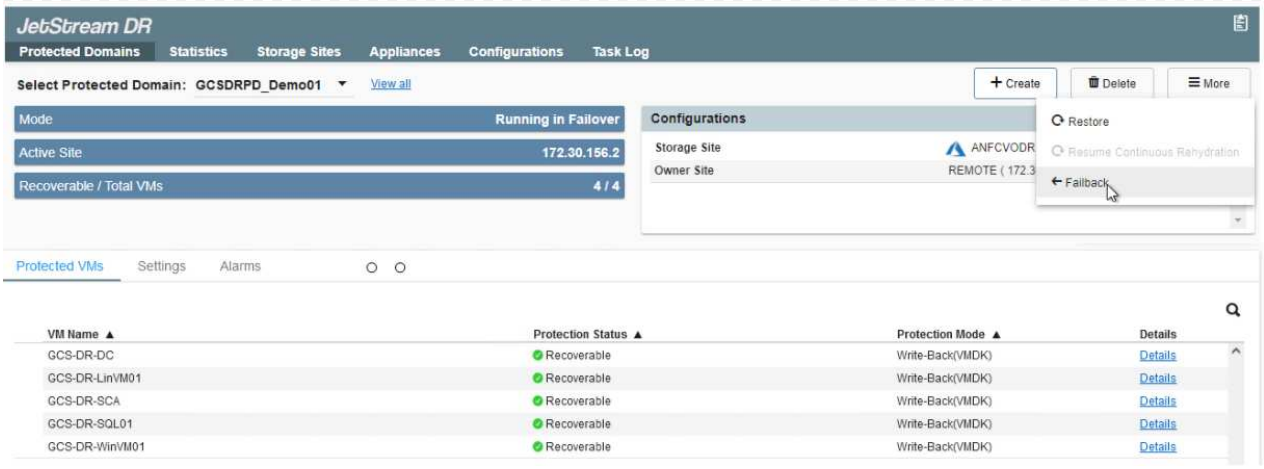
En este momento, pueden ejecutarse las operaciones y el negocio continúa de forma normal.

En el extremo de NSX-T, es posible crear una pasarela de nivel 1 dedicada separada para simular escenarios de conmutación por error. De este modo, se garantiza que todas las cargas de trabajo se puedan comunicar entre sí, pero que ningún tráfico pueda enrutarse tanto dentro como fuera del entorno, de modo que las tareas de clasificación, contención o endurecimiento se puedan realizar sin riesgo de contaminación cruzada. Esta operación se encuentra fuera del alcance de este documento, pero se puede realizar fácilmente para simular el aislamiento.

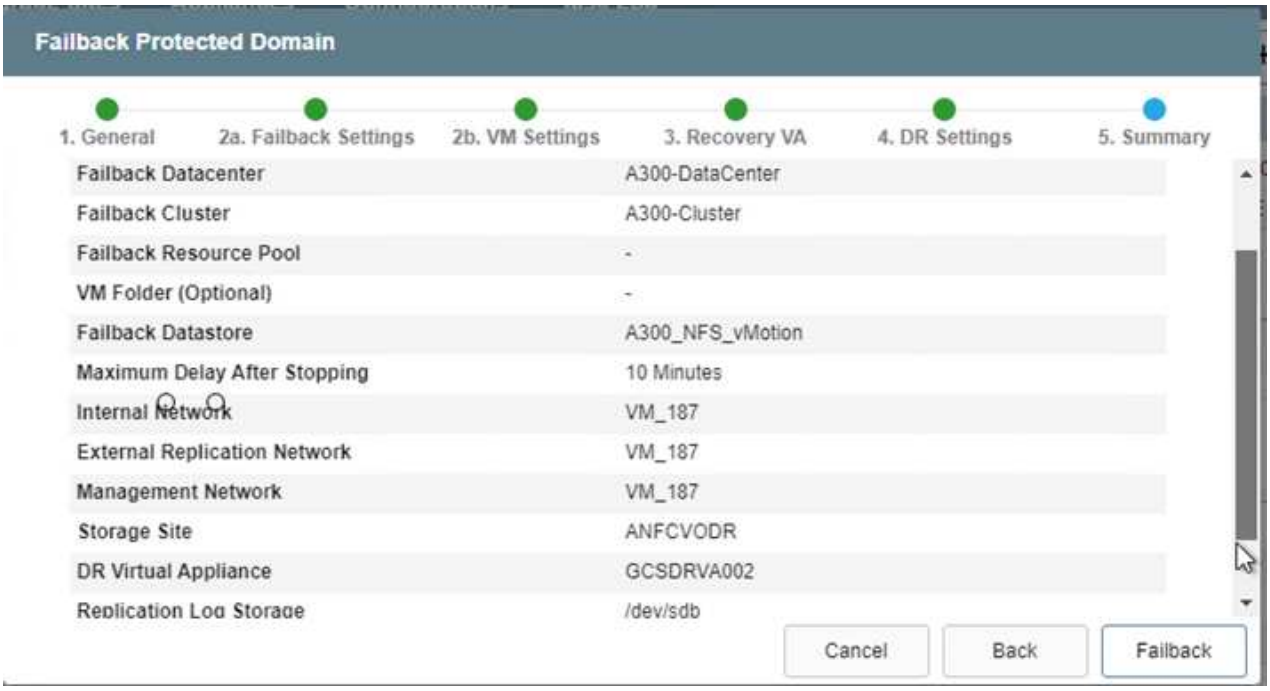
Una vez que la instalación principal esté activa y en funcionamiento de nuevo, puede realizar la conmutación tras recuperación. JetStream reanuda la protección de máquinas virtuales y debe revertirse la relación de SnapMirror.

1. Restaure el entorno de sus instalaciones. En función del tipo de incidente de desastre, podría ser necesario restaurar o verificar la configuración del clúster protegido. Si es necesario, puede que sea necesario volver a instalar el software JetStream DR.
2. Acceda al entorno local restaurado, vaya a la interfaz de usuario de recuperación ante desastres de Jetstream y seleccione el dominio protegido adecuado. Una vez que el sitio protegido esté listo para la conmutación tras recuperación, seleccione la opción de conmutación por recuperación en la interfaz de usuario.

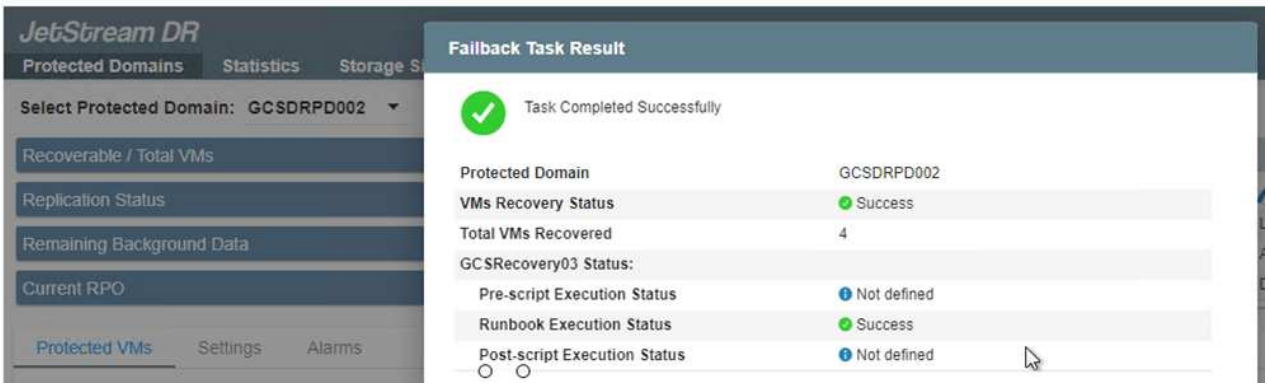
El plan de conmutación por recuperación generado por CPT también se puede usar para iniciar la devolución de los equipos virtuales y sus datos del almacén de objetos al entorno VMware original.



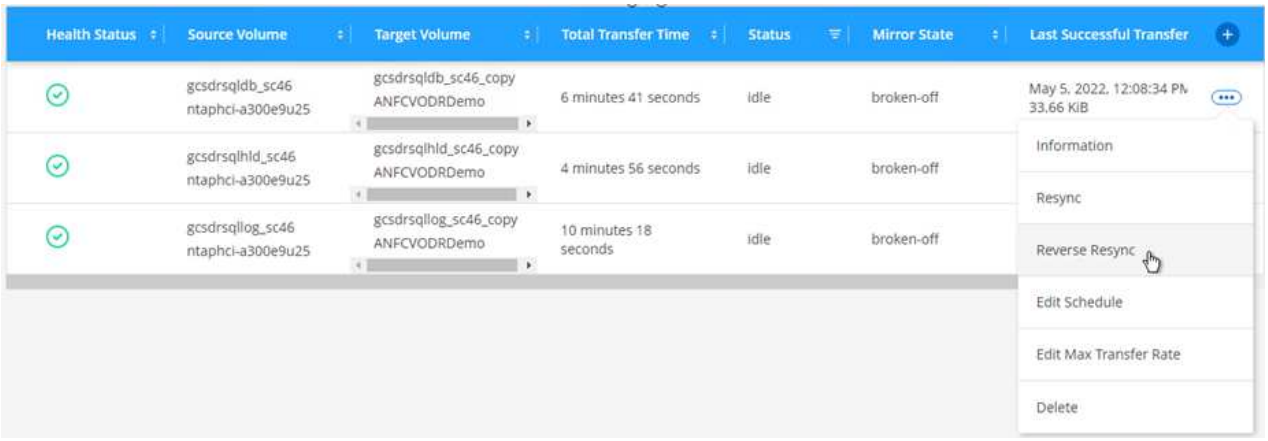
Especifique la demora máxima después de pausar las máquinas virtuales en el sitio de recuperación y reiniciarlas en el sitio protegido. El tiempo necesario para completar este proceso incluye la finalización de la replicación tras detener la conmutación por error de las máquinas virtuales, el tiempo necesario para limpiar el sitio de recuperación y el tiempo necesario para recrear las máquinas virtuales en el sitio protegido. NetApp recomienda 10 minutos.

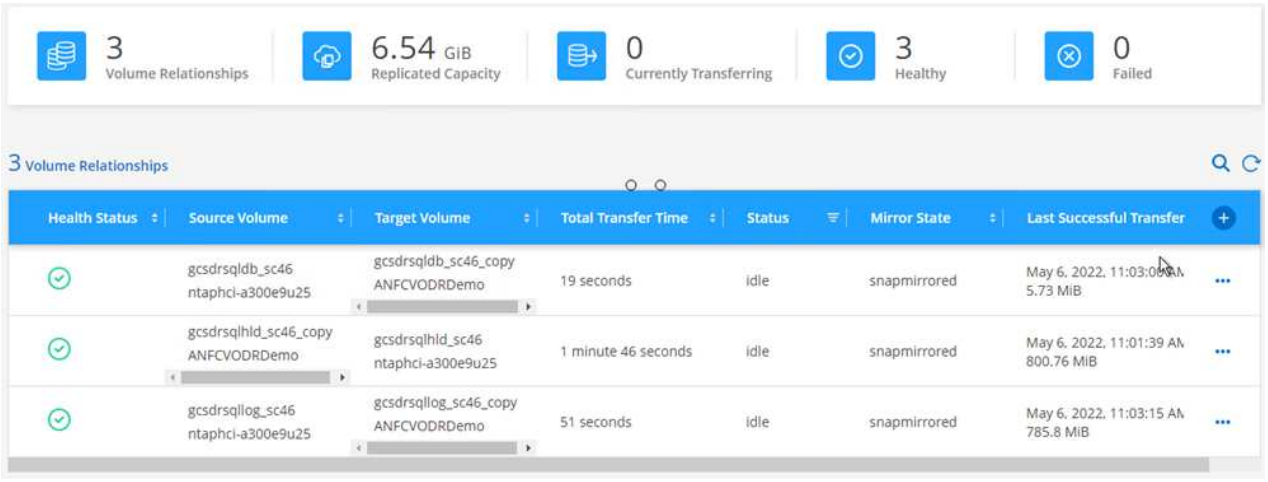


3. Completar el proceso de conmutación tras recuperación y, a continuación, confirmar la reanudación de la protección de los equipos virtuales y la consistencia de datos.

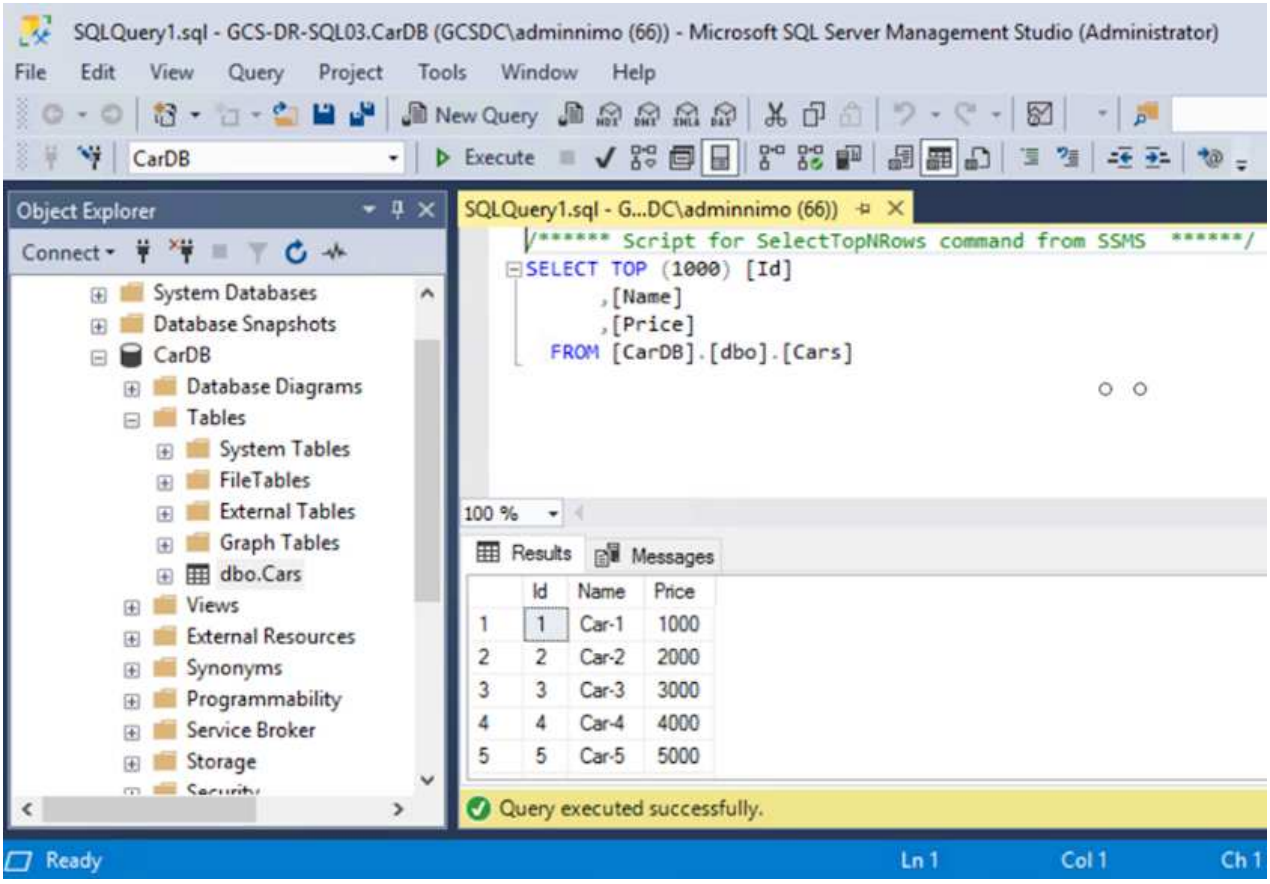


4. Una vez recuperados los equipos virtuales, desconecte el almacenamiento secundario del host y conéctelo al almacenamiento principal.





5. Reinicie el servicio del servidor MSSQL.
6. Compruebe que los recursos de SQL vuelven a estar en línea.



Para volver a realizar la conmutación tras recuperación al almacenamiento principal, asegúrese de que la dirección de la relación sigue 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, vuelva a realizar la operación de resincronización inversa.

Este proceso es aplicable a otras aplicaciones como Oracle, tipos de base de datos similares y cualquier otra aplicación que utilice almacenamiento conectado a «guest».

Como siempre, probar los pasos necesarios para recuperar las cargas de trabajo críticas antes de ponerlas en producción.

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.
- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
  - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.

- Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
- Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.

- La optimización de la CPU y la RAM puede ayudar a reducir los costes del cloud al permitir la recuperación en clústeres informáticos más pequeños.

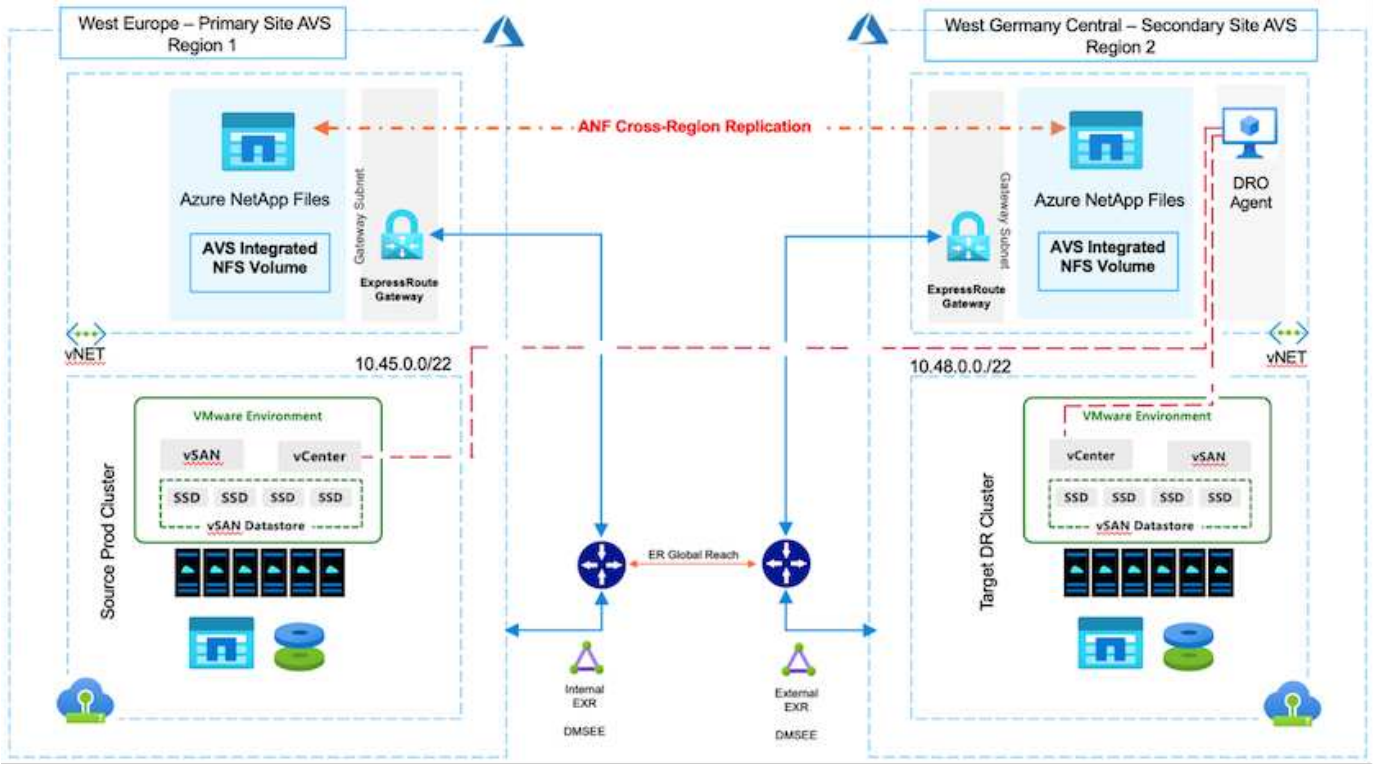
TR-4955: Recuperación ante desastres con Azure NetApp Files (ANF) y la solución VMware de Azure (AVS)

Autor(es): Niyaz Mohamed, Ingeniería de Soluciones NetApp

Descripción general

La recuperación ante desastres mediante replicación a nivel de bloques entre regiones del cloud es un método resiliente y rentable de proteger las cargas de trabajo frente a interrupciones del servicio del sitio y eventos de corrupción de datos (por ejemplo, ransomware). Con la replicación de volúmenes entre regiones de Azure NetApp Files (ANF), las cargas de trabajo de VMware que se ejecutan en un sitio SDDC de Azure VMware Solution (AVS) usando Azure NetApp Files Volumes como almacén de datos NFS en el sitio de AVS principal se pueden replicar en un sitio de AVS secundario designado en la región de recuperación de destino.

El orquestador de recuperación ante desastres (DRO) (una solución basada en secuencia de comandos con una interfaz de usuario) puede utilizarse para recuperar sin problemas las cargas de trabajo replicadas desde un SDDC de AVS a otro. DRO automatiza la recuperación rompiendo la paridad de replicación y luego montando el volumen de destino como almacén de datos, a través del registro de VM en AVS, a las asignaciones de red directamente en NSX-T (incluido con todos los clouds privados de AVS).



Requisitos previos y recomendaciones generales

- Compruebe que ha habilitado la replicación entre regiones mediante la creación de pares de replicación.

Consulte "Crear replicación de volúmenes para Azure NetApp Files".

- Debe configurar ExpressRoute Global Reach entre los clouds privados de Azure VMware Solution de origen y destino.
- Debe tener un principal de servicio que pueda acceder a los recursos.
- Se admite la siguiente topología: Sitio AVS primario al sitio AVS secundario.
- Configure el "replicación" programe cada volumen de forma apropiada según las necesidades empresariales y la tasa de cambio de datos.

No se admiten las topologías en cascada y con ventilador de entrada y salida.

Primeros pasos

Implementa la solución de VMware para Azure

La "Solución Azure VMware" (AVS) es un servicio de cloud híbrido que proporciona SDDC de VMware totalmente funcionales dentro de un cloud público de Microsoft Azure. AVS es una solución de primera parte totalmente gestionada y compatible con Microsoft y verificada por VMware que utiliza infraestructura de Azure. Por lo tanto, los clientes obtienen VMware ESXi para virtualización informática, vSAN para almacenamiento hiperconvergente y NSX para redes y seguridad, y todo ello al tiempo que aprovechan la presencia global de Microsoft Azure, instalaciones de centros de datos líderes de su clase y la proximidad al rico ecosistema de servicios y soluciones nativos de Azure. Una combinación de un SDDC de la solución para Azure VMware y Azure NetApp Files proporciona el mejor rendimiento con una latencia de red mínima.

Para configurar una nube privada AVS en Azure, siga los pasos que se indican en este "enlace" Para la documentación de NetApp y en este "enlace" Para obtener documentación de Microsoft. Se puede utilizar un entorno piloto configurado con una configuración mínima para recuperaciones ante desastres. Esta configuración solo contiene componentes principales para admitir aplicaciones esenciales y puede escalar horizontalmente y generar más hosts para asumir la mayor carga si se produce una recuperación tras fallos.

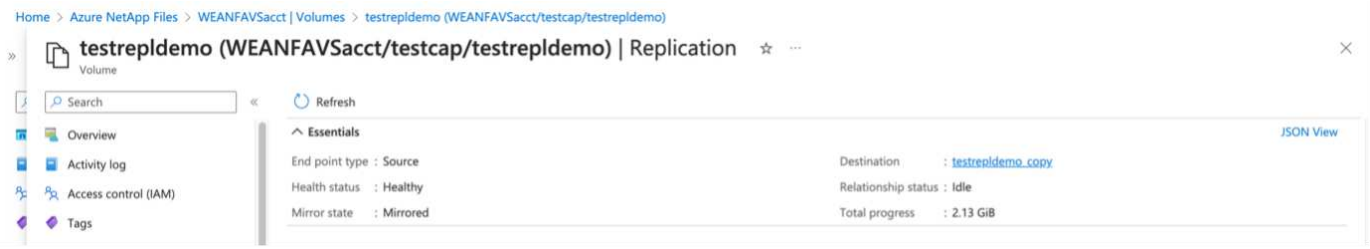
En la versión inicial, DRO admite un clúster SDDC AVS existente. La creación bajo demanda de SDDC estará disponible en una próxima versión.

Aprovisione y configure Azure NetApp Files

"Azure NetApp Files" es un servicio de almacenamiento de archivos de uso medido, de nivel empresarial y de alto rendimiento. Siga los pasos que se indican a continuación "enlace" Para aprovisionar y configurar Azure NetApp Files como almacén de datos NFS para optimizar las puestas en marcha de cloud privado de AVS.

Crear una replicación de volumen para volúmenes de almacenes de datos que funcionan con Azure NetApp Files

El primer paso es configurar la replicación entre regiones para los volúmenes de almacén de datos deseados desde el sitio primario AVS al sitio secundario AVS con las frecuencias y retenciones apropiadas.



Siga los pasos que se indican a continuación "enlace" para configurar la replicación entre regiones mediante la creación de pares de replicación. El nivel de servicio del pool de capacidad de destino puede coincidir con el del pool 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 desastre real o simulaciones de recuperación ante desastres.

Una relación de replicación entre regiones es un requisito previo y debe crearse de antemano.

Instalación DE DRO

Para comenzar con DRO, use el sistema operativo Ubuntu en la máquina virtual de Azure designada y asegúrese de cumplir con los requisitos previos. A continuación, instale el paquete.

Requisitos previos:

- Principal de servicio que puede acceder a los recursos.
- Asegúrese de que existe conectividad adecuada con las instancias de SDDC y Azure NetApp Files de origen y destino.
- La resolución DNS debe estar en su lugar si está utilizando nombres DNS. De lo contrario, use 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` para este nuevo permiso: `sudo chmod 666 /var/run/docker.sock`.

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

Los pasos son los siguientes:

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

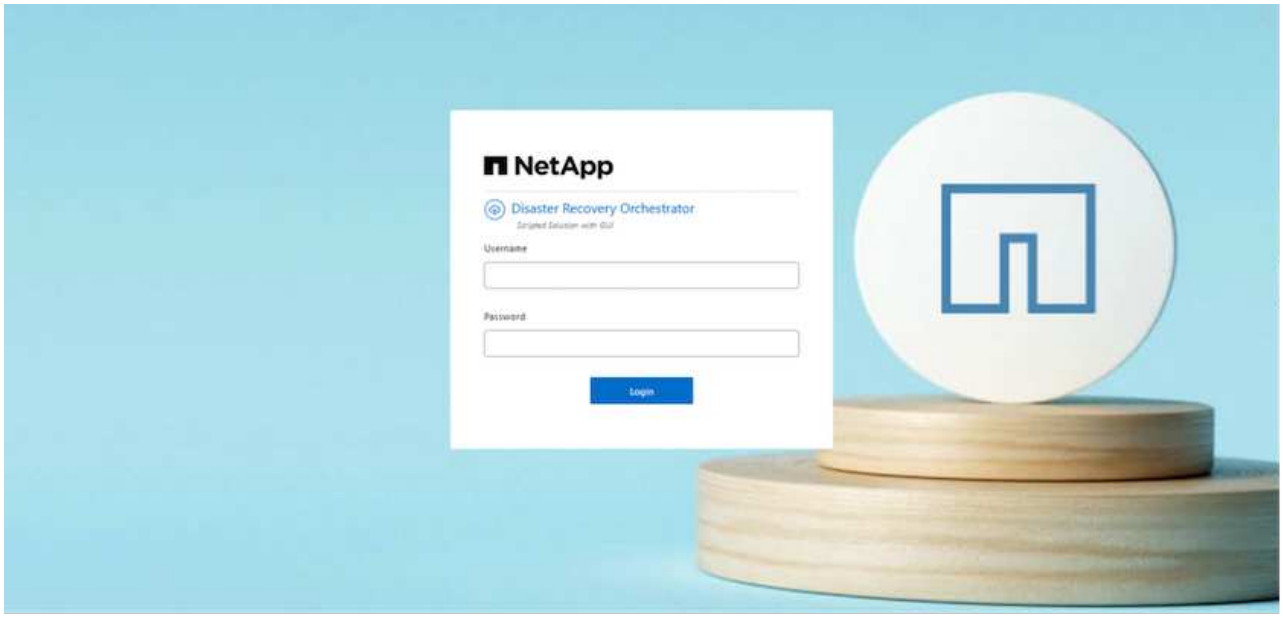
```
git clone https://github.com/NetApp/DRO-Azure.git
```

El agente debe instalarse en la región del sitio AVS secundario o en la región del sitio AVS principal en una zona de área de servicio independiente que el SDDC.

2. Descomprima el paquete, ejecute el script de despliegue e introduzca 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 con las siguientes credenciales:
    - Nombre de usuario: `admin`
    - Contraseña: `admin`



Configuración DE DRO

Después de 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 AVS principal al sitio AVS secundario. NetApp recomienda la puesta en marcha del agente DRO en el sitio AVS secundario y la configuración de la conexión de puerta de enlace ExpressRoute para que el agente DRO pueda comunicarse a través de la red con los componentes de AVS y Azure NetApp Files adecuados.

El primer paso es agregar credenciales. DRO requiere permiso para descubrir Azure NetApp Files y la solución Azure VMware. 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 enlazar el principal de servicio a su suscripción de Azure y asignarle un rol personalizado que tenga los permisos necesarios relevantes. Al agregar entornos de origen y destino, se le solicita que seleccione las credenciales asociadas al principal de servicio. Debe agregar estas credenciales a DRO antes de hacer clic en Agregar nuevo sitio.

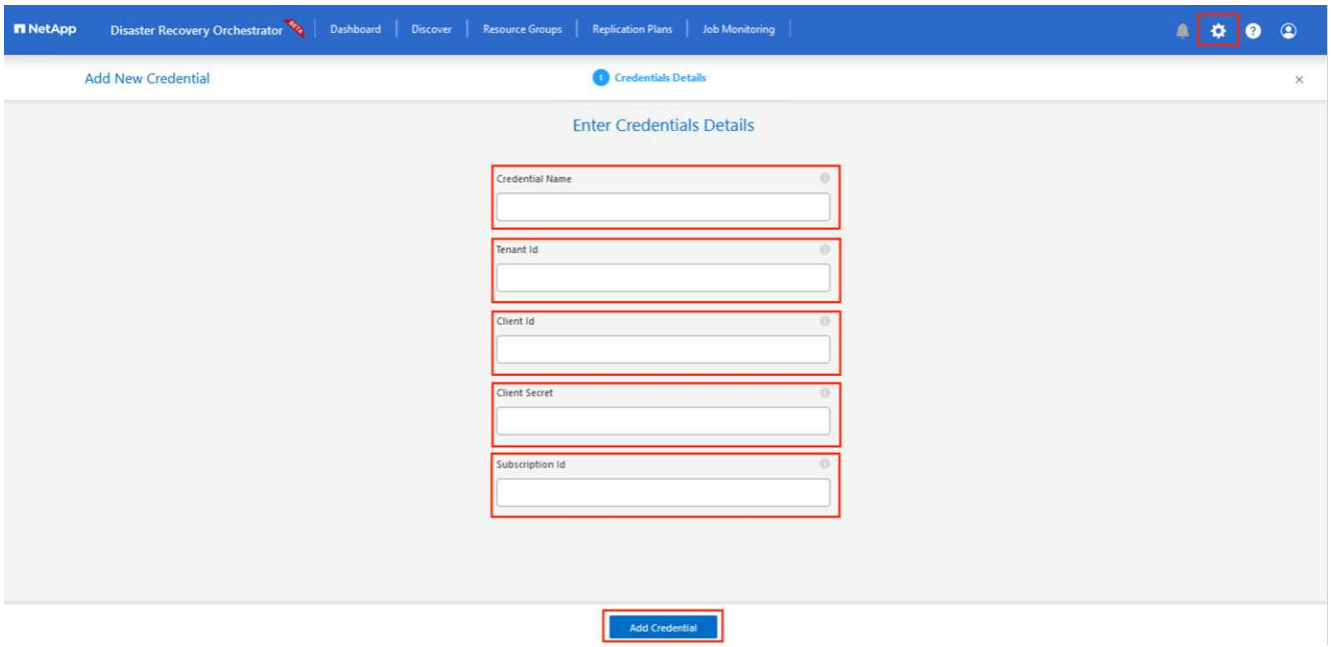
Para realizar esta operación, complete los siguientes pasos:

1. Abra DRO en un navegador compatible y utilice el nombre de usuario y la contraseña predeterminados (`/admin/admin`). La contraseña se puede restablecer después del primer inicio de sesión mediante la opción Cambiar contraseña.
2. En la parte superior derecha de la consola de DRO, haga clic en el icono **Configuración** y seleccione **Credenciales**.
3. Haga clic en Add New Credential y siga los pasos del asistente.
4. Para definir las credenciales, introduzca información sobre el principal de servicio de Azure Active Directory que otorga los permisos necesarios:
    - Nombre de credencial

- ID de inquilino
- ID del cliente
- Secreto de cliente
- ID de suscripción

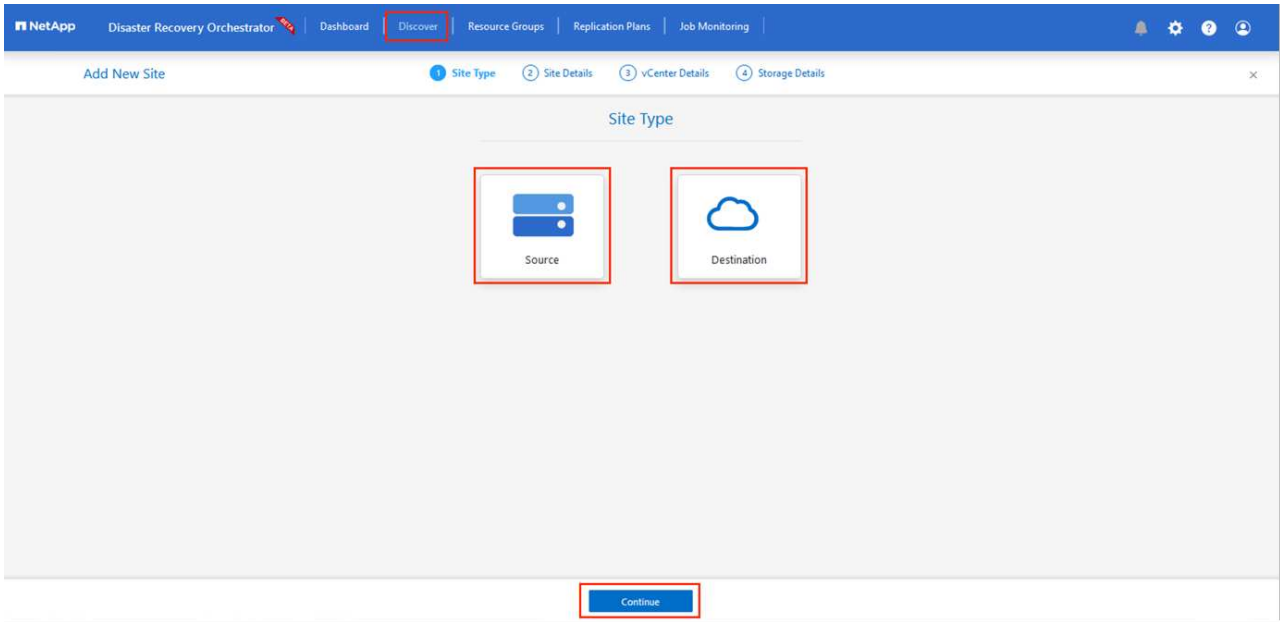
  Debe haber capturado esta información al crear la aplicación AD.

5. Confirme los detalles sobre las nuevas credenciales y haga clic en Add Credential.



Después de agregar las credenciales, es hora de detectar y agregar los sitios de AVS principales y secundarios (tanto vCenter como la cuenta de almacenamiento de Azure NetApp Files) a DRO. Para agregar el sitio de origen y destino, realice los siguientes pasos:

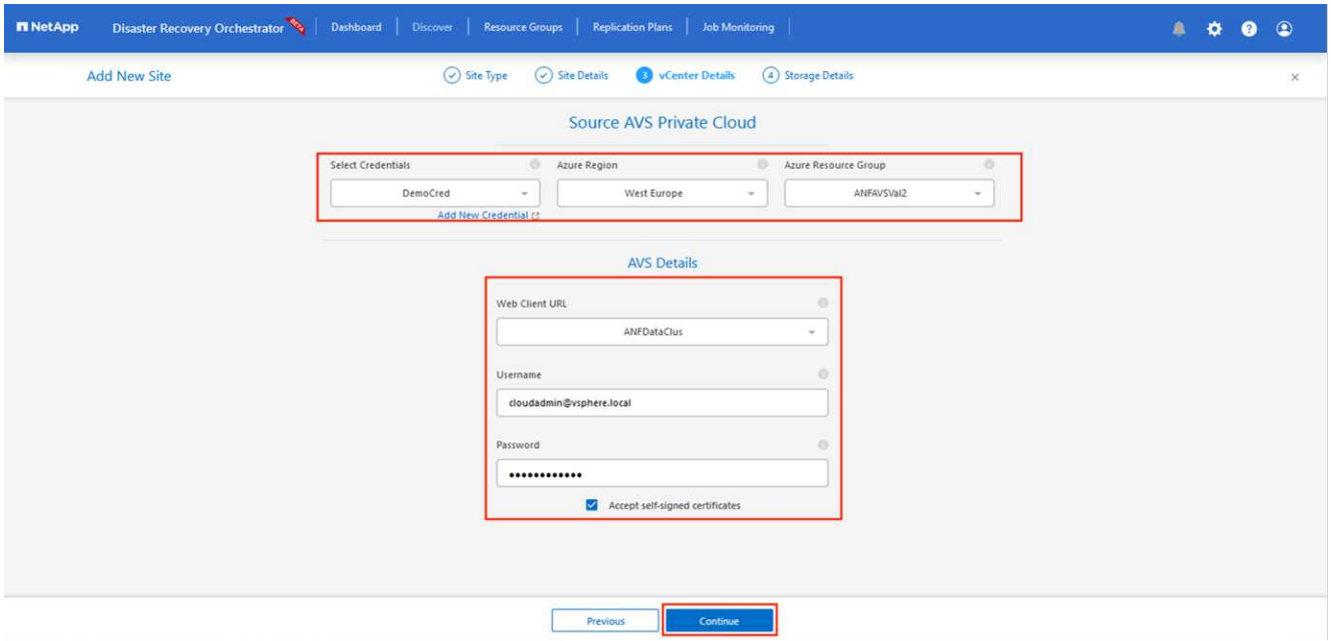
6. Vaya a la pestaña **Discover**.
7. Haga clic en **Agregar nuevo sitio**.
8. Agregue el siguiente sitio AVS principal (designado como **Source** en la consola).
   - SDDC vCenter
   - Cuenta de almacenamiento de Azure NetApp Files
9. Agregue el siguiente sitio AVS secundario (designado como **Destino** en la consola).
   - SDDC vCenter
   - Cuenta de almacenamiento de Azure NetApp Files



10. Agregue los detalles del sitio haciendo clic en **Fuente**, ingresando un nombre de sitio amigable, y seleccione el conector. A continuación, haga clic en **continuar**.

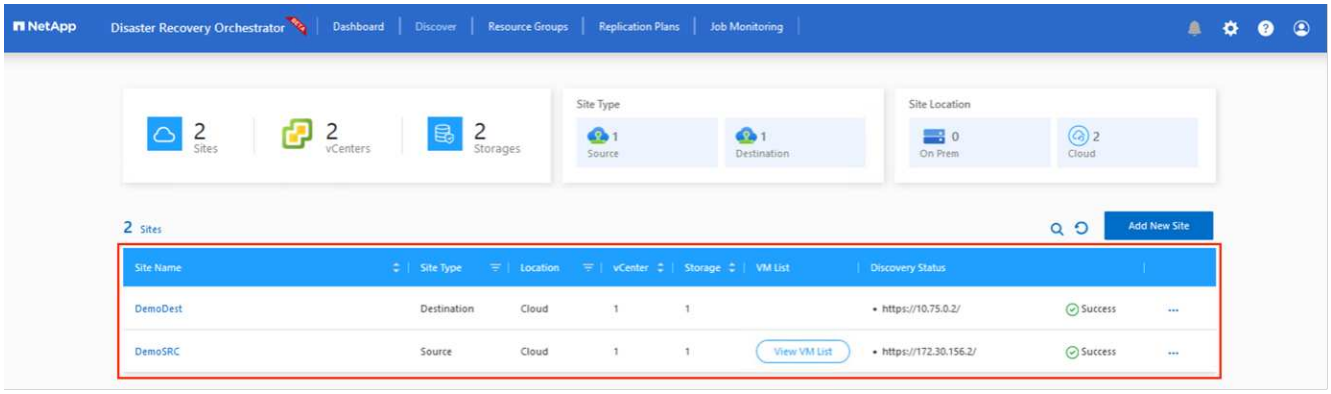
> A modo de demostración, en este documento se trata la adición de un sitio de origen.

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 AVS SDDC principal.
12. DRO muestra todos los SDDC disponibles dentro de la región. Seleccione la URL de cloud privado designada del menú desplegable.
13. Introduzca el `cloudadmin@vsphere.local` credenciales de usuario. A esto se puede acceder desde Azure Portal. Siga los pasos mencionados en este "enlace". Una vez hecho esto, haga clic en **Continuar**.

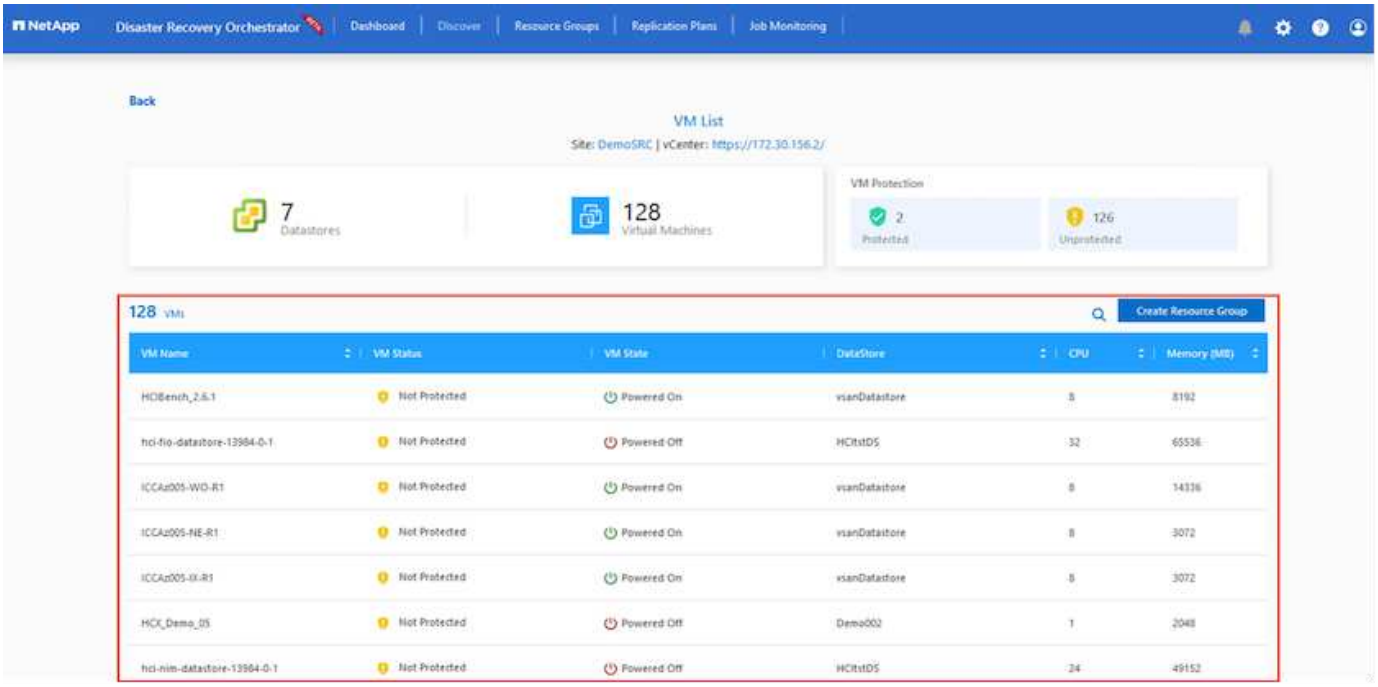


14. Seleccione los detalles de Source Storge (ANF) seleccionando el grupo de recursos de Azure y la cuenta de NetApp.

15. Haga clic en **Crear sitio**.



Una vez agregado, DRO realiza la detección automática y muestra las máquinas virtuales que tienen las réplicas entre regiones correspondientes desde el sitio de origen al sitio de destino. DRO detecta automáticamente las redes y los segmentos que utilizan las máquinas virtuales y los rellena.



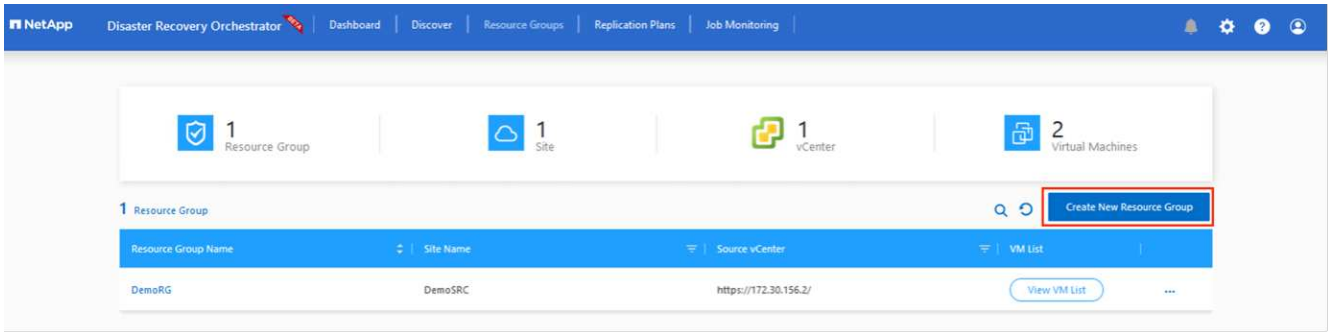
El siguiente paso es agrupar los equipos virtuales necesarios en sus grupos funcionales como grupos de recursos.

Agrupaciones de recursos

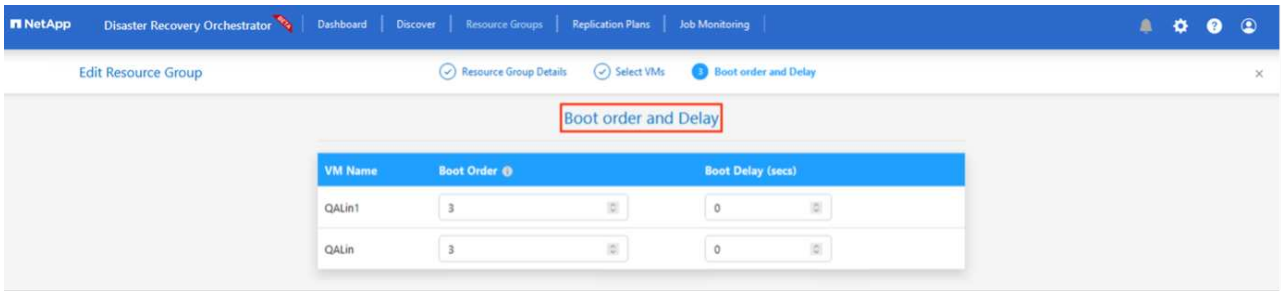
Una vez agregadas las plataformas, agrupe las máquinas virtuales que desee recuperar en grupos de recursos. LOS grupos de recursos DE DRO permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones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

Para comenzar a crear grupos de recursos, haga clic en el elemento de menú **Crear nuevo grupo de recursos**.

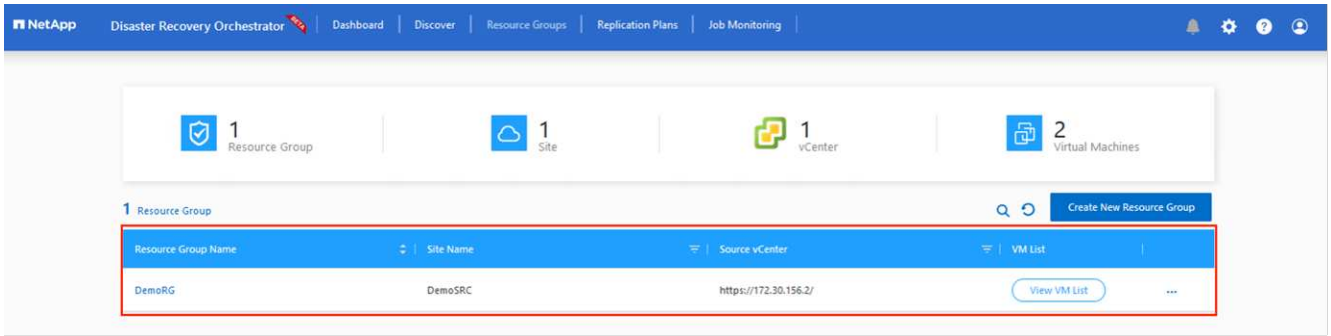
1. Acceda a **Resource Grou*ps y haga clic en *Crear nuevo grupo de recursos**.



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 apropiadas mediante la opción de búsqueda.
5. Seleccione el **Boot Order** y **Boot Delay** (segundos) para todas las VM seleccionadas. Establezca el orden de la secuencia de encendido seleccionando cada máquina virtual y configurando la prioridad para ella. El valor predeterminado para todas las máquinas virtuales es 3. Las opciones son las siguientes:
   - El primer equipo virtual que se enciende
   - Predeterminado
   - La última máquina virtual que se enciende



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

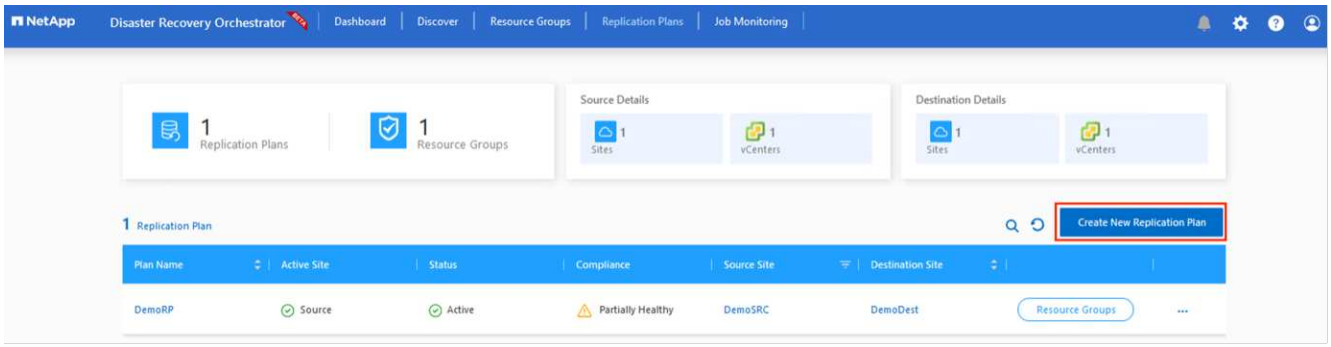


Planes de replicación

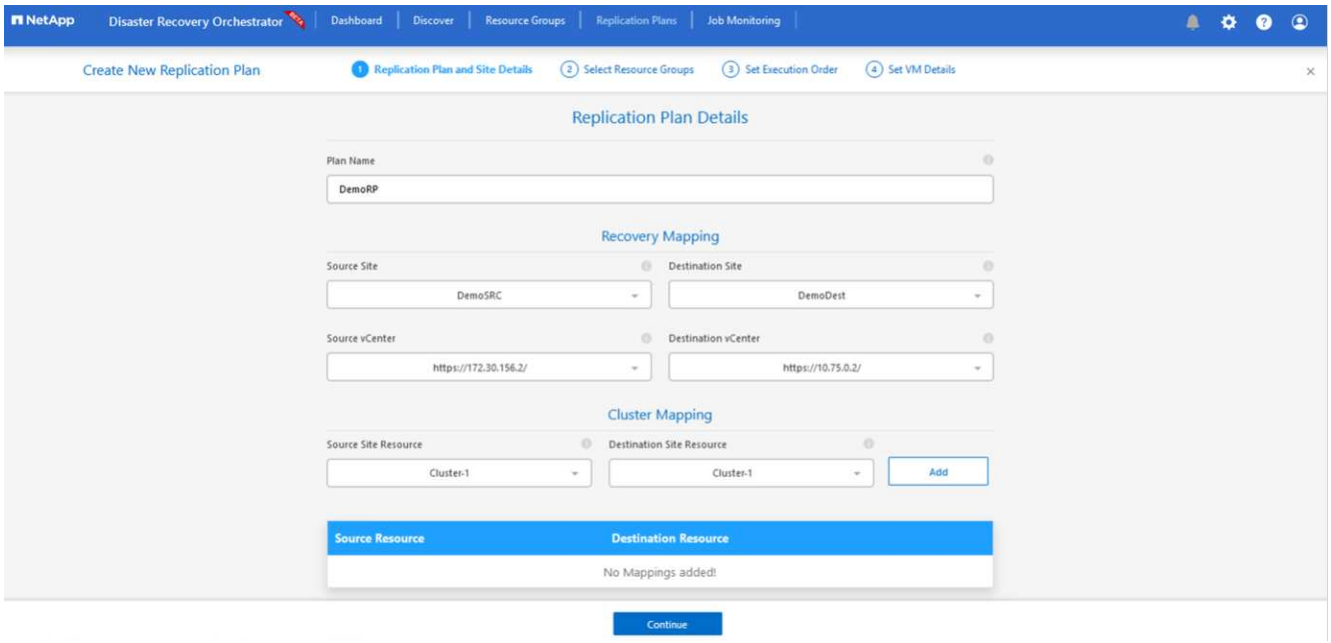
Es necesario tener un plan para la recuperación de aplicaciones en caso de desastre. Seleccione las plataformas vCenter de origen y destino en el menú desplegable, elija los grupos de recursos que se incluirán en este plan y también incluya la agrupación sobre cómo deben restaurarse y encenderse las aplicaciones (por ejemplo, controladores de dominio, nivel 1, nivel 2, etc.). A menudo, los planes también se denominan 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, lleve a cabo los siguientes pasos:

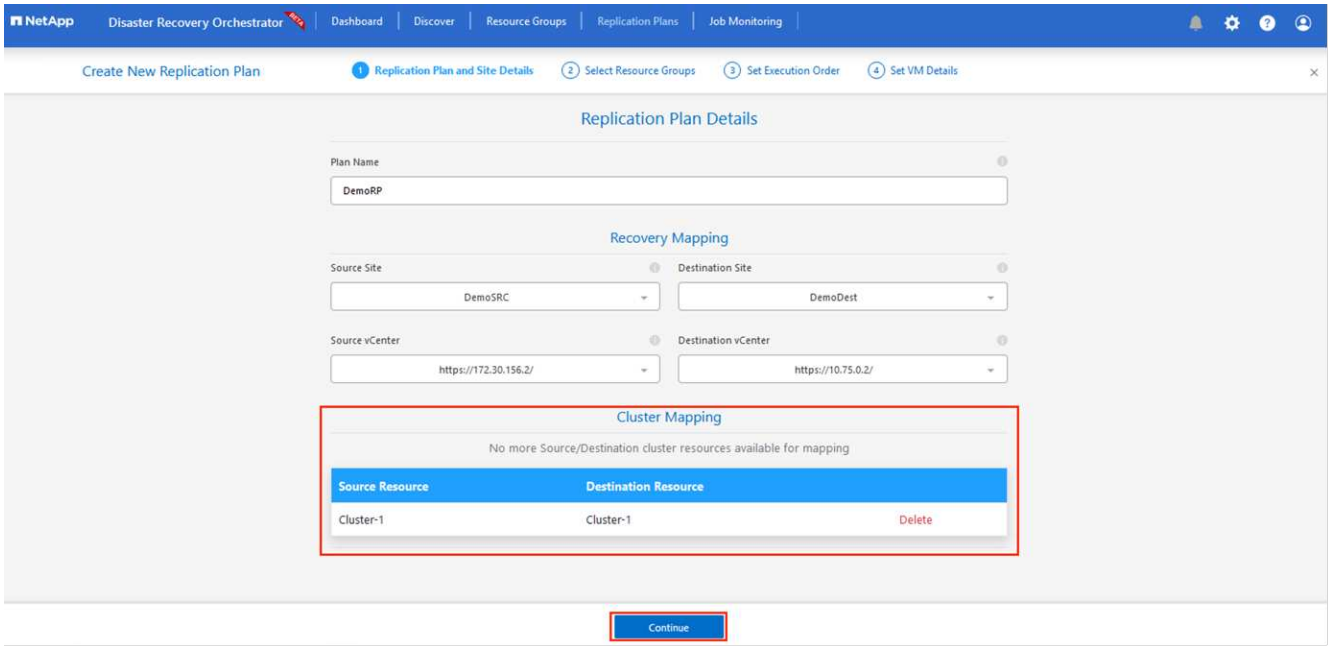
1. Vaya a **Planes de replicación** y haga clic en **Crear nuevo plan de replicación**.



2. En **New Replication Plan**, proporcione un nombre para el plan y agregue asignaciones de recuperación seleccionando el sitio de origen, vCenter asociado, el sitio de destino y vCenter asociado.

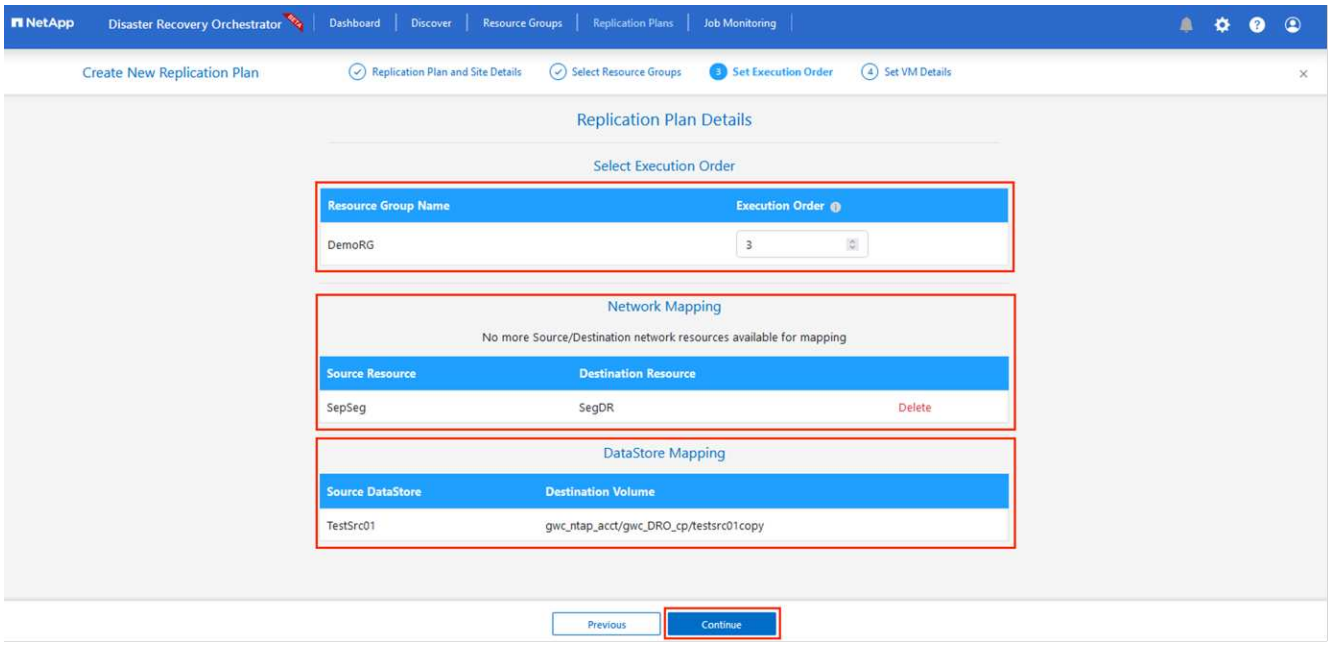


3. Después de completar el mapeo de recuperación, seleccione el **Cluster Mapping**.

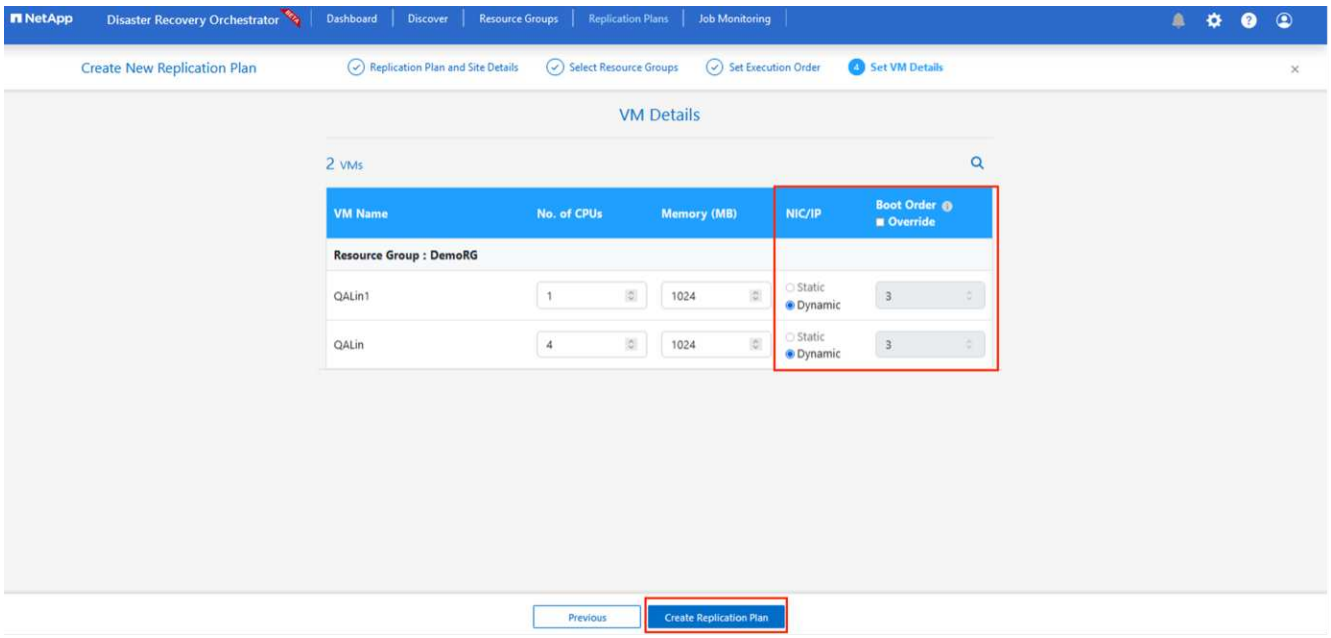


4. Seleccione **Detalles del grupo de recursos** y haga clic en **continuar**.
5. Establezca el orden de ejecución del grupo de recursos. Esta opción permite seleccionar la secuencia de operaciones cuando existen varios grupos de recursos.
6. Una vez hecho esto, defina la asignación de red en el segmento apropiado. Los segmentos ya se deben aprovisionar en el cluster AVS secundario y, para asignar las VM a ellas, seleccione el segmento apropiado.
7. Las asignaciones de almacenes de datos se seleccionan automáticamente según la selección de las máquinas virtuales.

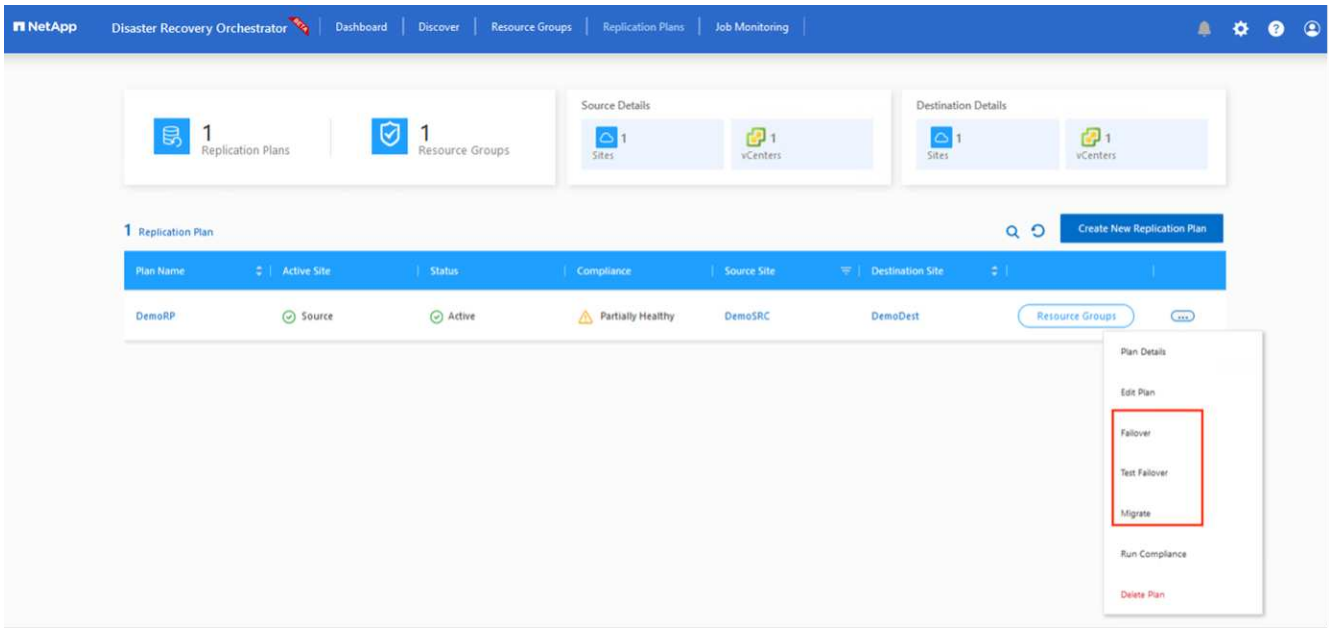
> La replicación entre regiones (CRR) se encuentra en el nivel del volumen. Por lo tanto, todas las máquinas virtuales que residen en el respectivo volumen se replican en el destino de CRR. Asegúrese de seleccionar todas las máquinas virtuales que forman parte del almacén de datos, ya que solo se procesan las máquinas virtuales que forman parte del plan de replicación.



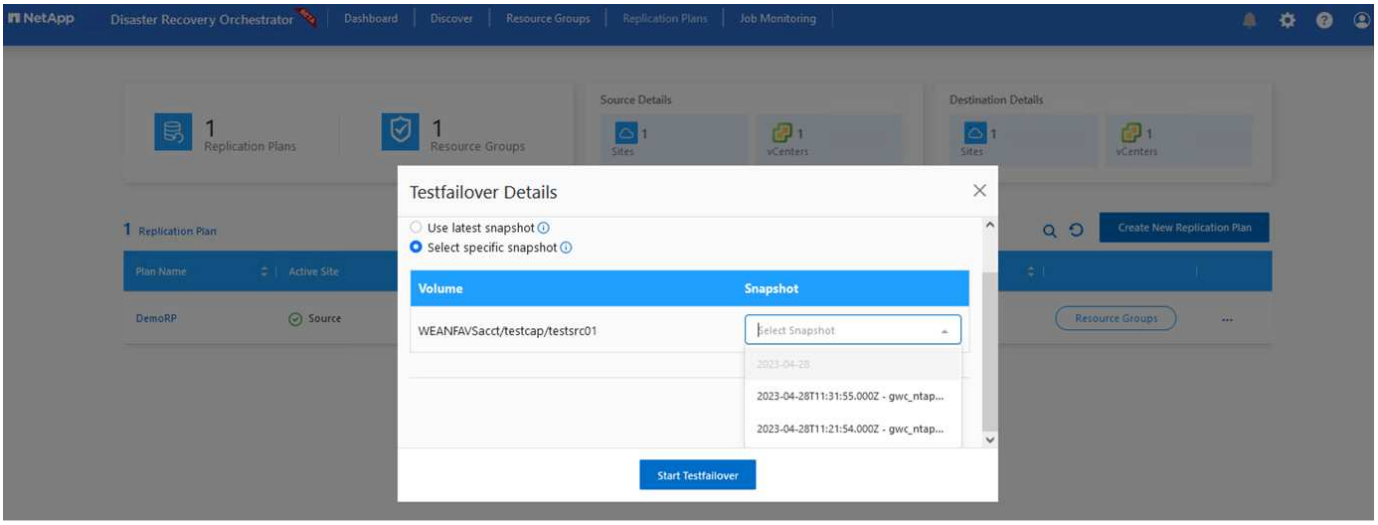
8. En Detalles de VM, opcionalmente puede cambiar el tamaño de los parámetros de CPU y RAM de VM. Esto puede ser muy útil cuando se recuperan entornos grandes en clústeres de destino de menor tamaño, o cuando se realizan pruebas de recuperación ante desastres sin tener que aprovisionar una infraestructura física de VMware uno a uno. Modifique además el orden de arranque y el retraso de inicio (segundos) para todas las máquinas virtuales seleccionadas en los grupos de recursos. Existe una opción adicional para modificar el orden de inicio si se requieren cambios en lo que seleccionó durante la selección de orden de inicio de grupo de recursos. De forma predeterminada, se utiliza el orden de inicio seleccionado durante la selección del grupo de recursos, sin embargo, se pueden realizar modificaciones en esta etapa.



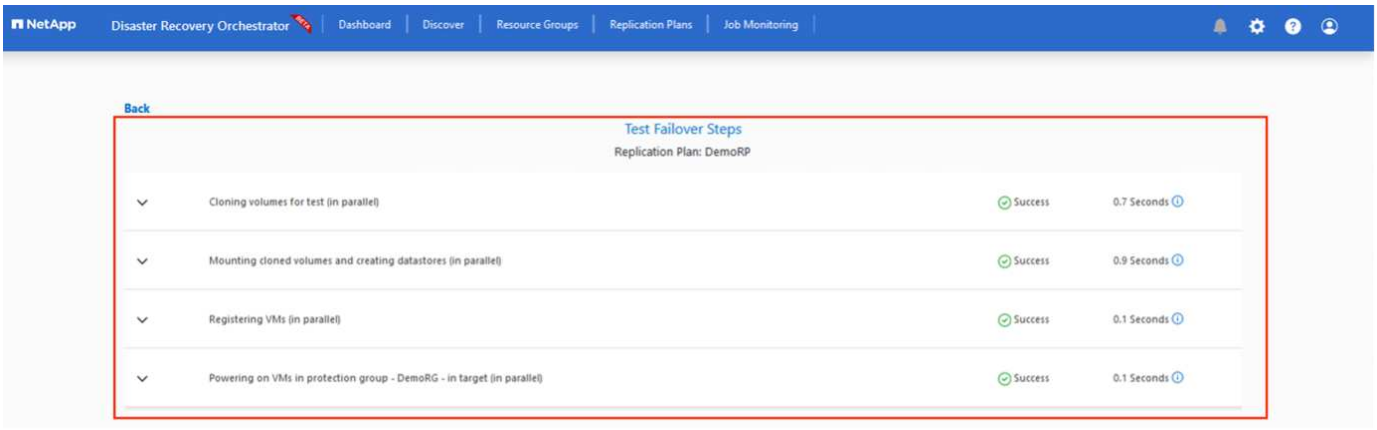
9. Haga clic en **Crear plan de replicación**.Después de crear el plan de replicación, puede ejercer las opciones de failover, failover de prueba o migración dependiendo de sus requisitos.



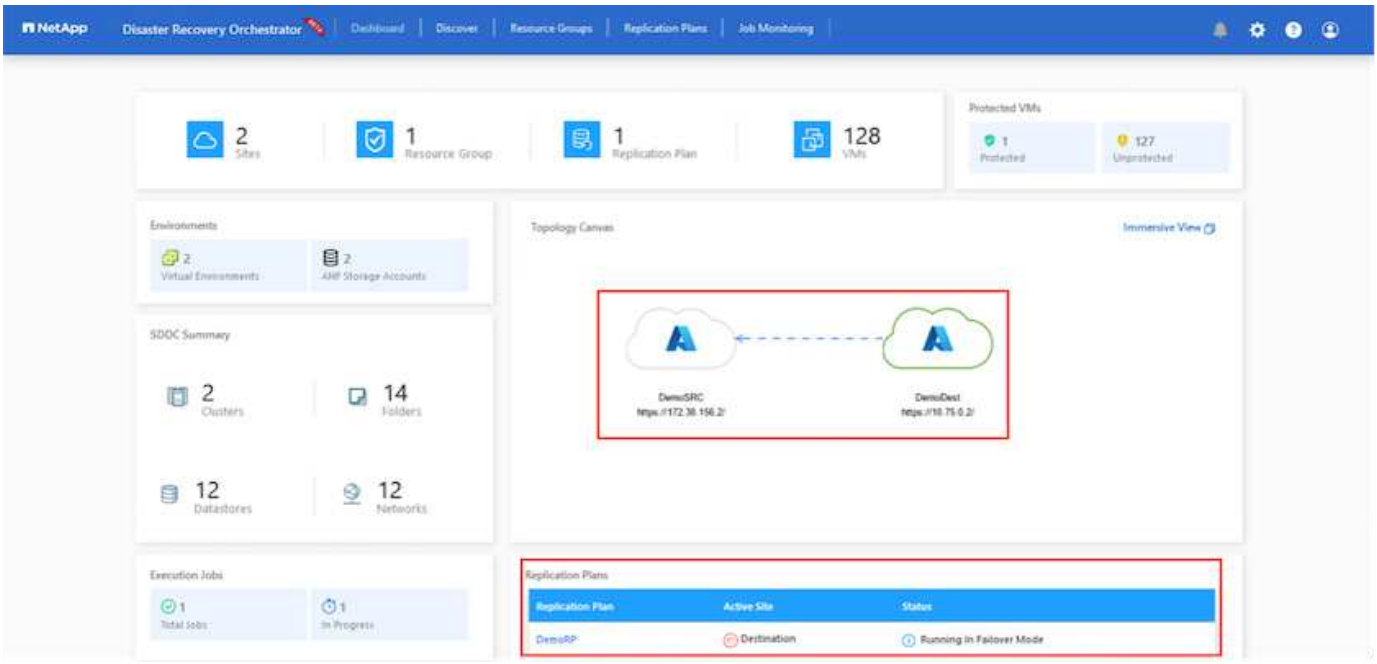
Durante las opciones de conmutación por error y conmutación por error de prueba, se utiliza la instantánea más reciente o se puede seleccionar una instantánea específica a partir de una instantánea puntual. La opción point-in-time puede ser muy beneficiosa si te enfrentas a un evento de corrupción como ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. DRO muestra todos los puntos de tiempo disponibles.



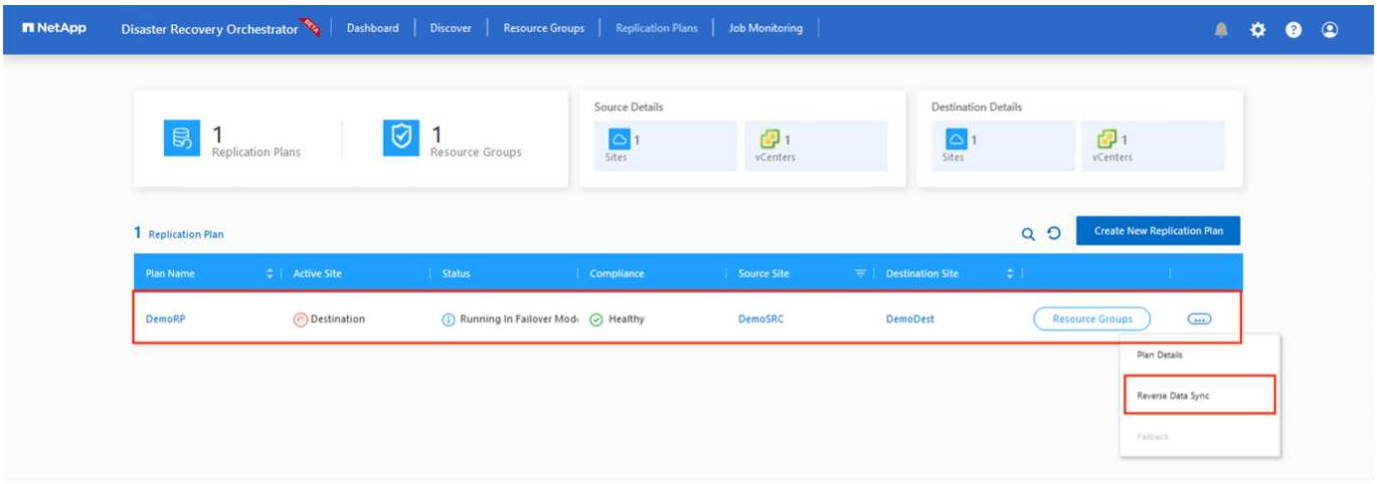
Para activar failover o failover de prueba con la configuración especificada en el plan de replicación, puede hacer clic en **Failover** o **Test Failover**. Puede supervisar el plan de replicación en el menú de tareas.



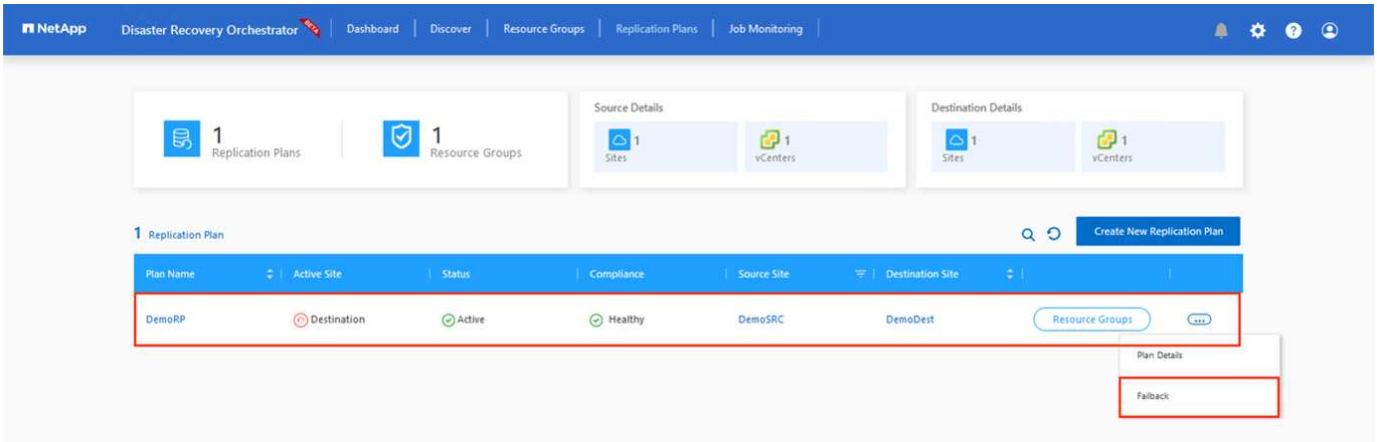
Una vez activada la conmutación al respaldo, los elementos recuperados pueden verse en el sitio secundario AVS SDDC vCenter (máquinas virtuales, redes y almacenes de datos). De forma predeterminada, las máquinas virtuales se recuperan en la carpeta Workload.

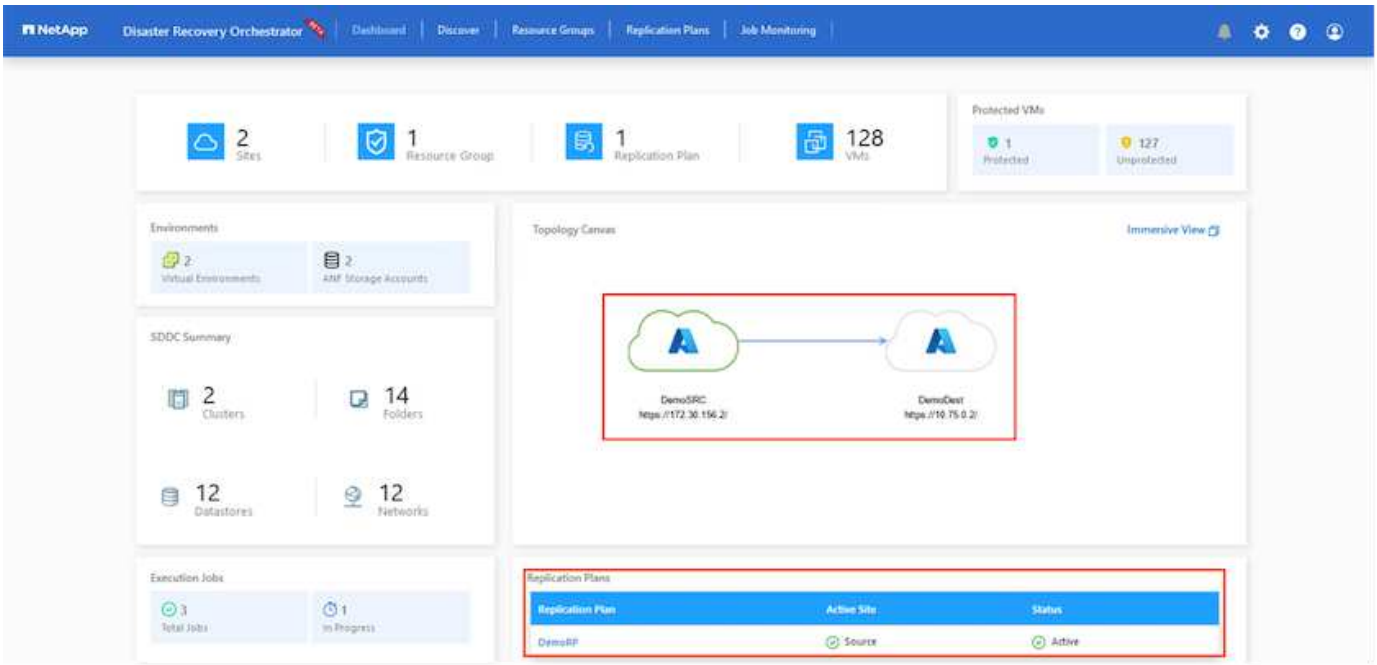


La conmutación tras recuperación se puede activar en el nivel del plan de replicación. En caso de conmutación por error de prueba, la opción de desmontaje puede utilizarse para revertir los cambios y eliminar el volumen recién creado. Los fallos relacionados con la conmutación al nodo de respaldo son un proceso de dos pasos. Seleccione el plan de replicación y seleccione **Reverse Data Sync**.



Una vez completado este paso, active la conmutación por recuperación para volver al sitio AVS principal.





Desde Azure Portal, podemos ver que el estado de la replicación se ha roto con los volúmenes apropiados que se asignaron al centro secundario AVS SDDC como volúmenes de lectura/escritura. Durante la conmutación al nodo de respaldo de prueba, DRO no asigna el volumen de destino o de réplica. En su lugar,

crea un nuevo volumen de la instantánea de replicación entre regiones necesaria y expone el volumen como almacén de datos, que consume capacidad física adicional del pool de capacidad y garantiza que el volumen de origen no se modifique. En particular, las tareas de replicación pueden continuar durante las pruebas de recuperación ante desastres o clasificar los flujos de trabajo. Además, este proceso garantiza que la recuperación se puede limpiar sin el riesgo de que la réplica se destruya en caso de que se produzcan errores o se recuperen datos dañados.

Recuperación de ransomware

Recuperarse del ransomware puede ser una tarea abrumadora. Concretamente, puede ser difícil para las ORGANIZACIONES DE TECNOLOGÍA identificar cuál es el punto de retorno seguro y, una vez determinado esto, cómo garantizar que las cargas de trabajo recuperadas se protejan de los ataques que se producen (por ejemplo, al dañar al dormir o a través de aplicaciones vulnerables).

DRO hace frente a estas preocupaciones permitiendo a las organizaciones recuperarse de cualquier momento específico disponible. A continuación, las cargas de trabajo se recuperan en redes funcionales y aisladas, de modo que las aplicaciones pueden funcionar y comunicarse entre sí, pero no están expuestas a ningún tráfico norte-sur. Este proceso proporciona a los equipos de seguridad un lugar seguro para realizar análisis forenses e identificar cualquier malware oculto o dormido.

Conclusión

La solución de recuperación ante desastres de Azure NetApp Files y Azure VMware le ofrece los siguientes beneficios:

- Aproveche la replicación entre regiones de Azure NetApp Files eficiente y resiliente.
- Recupere en cualquier momento específico disponible con retención de SnapVault.
- Automatizar por completo todos los pasos necesarios para recuperar cientos o miles de máquinas virtuales en los pasos de validación de almacenamiento, informática, red y aplicaciones.
- La recuperación de cargas de trabajo aprovecha el proceso «Crear volúmenes nuevos a partir de las instantáneas más recientes», que no manipula el volumen replicado.
- Evite el riesgo de que se dañen los datos en los volúmenes o las copias Snapshot.
- Evite las interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
- Aproveche los datos de recuperación ante desastres y los recursos tecnológicos en el cloud para flujos de trabajo más allá de la recuperación ante desastres, como desarrollo y pruebas, pruebas de seguridad, pruebas de revisiones y actualizaciones, y pruebas de correcciones.
- La optimización de CPU y RAM puede ayudar a reducir los costes de la nube al permitir la recuperación en clústeres de computación más pequeños.

Dónde encontrar información adicional

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

- Crear replicación de volúmenes para Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replicación entre regiones de los volúmenes de Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-

level-objectives"

- "Solución Azure VMware"

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

- Ponga en marcha y configure el entorno de virtualización en Azure

  "Configurar AVS en Azure"

- Pon en marcha y configura la solución Azure VMware

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Uso de la replicación de Veeam y el almacén de datos de Azure NetApp Files para recuperación ante desastres en la solución de Azure VMware

Autor: Niyaz Mohamed - Ingeniería de Soluciones NetApp

Descripción general

Los almacenes de datos de Azure NetApp Files (ANF) separan el almacenamiento de los nodos informáticos y libera la flexibilidad necesaria para que cualquier organización lleve sus cargas de trabajo al cloud. Proporciona a los clientes una infraestructura de almacenamiento flexible y de alto rendimiento que se escala independientemente de los recursos de computación. El almacén de datos de Azure NetApp Files simplifica y optimiza la implementación junto con la solución Azure VMware (AVS) como sitio de recuperación de desastres para entornos VMware en las instalaciones.

Los almacenes de datos NFS basados en volúmenes de Azure NetApp Files (ANF) pueden usarse para replicar datos desde las instalaciones con cualquier solución de terceros validada que proporcione la funcionalidad de replicación de VM. Al añadir almacenes de datos Azure NetApp Files, permitirá una puesta en marcha optimizada en costes frente a la creación de un SDDC para soluciones Azure VMware con una enorme cantidad de hosts ESXi para acomodar el almacenamiento. Este enfoque se llama un “Clúster de Luz Piloto”. Un clúster ligero piloto es una configuración de host AVS mínima (3 nodos AVS) junto con la capacidad del almacén de datos Azure NetApp Files.

El objetivo es mantener una infraestructura de bajo coste con todos los componentes principales para gestionar una recuperación tras fallos. Un clúster piloto ligero puede escalar horizontalmente y aprovisionar más hosts AVS si se produce una conmutación por error. Además, una vez finalizada la recuperación tras fallos y restablecida el funcionamiento normal, el clúster piloto puede volver a reducirse a un modo operativo de bajo coste.

Objetivos de este documento

Este artículo describe cómo usar el almacén de datos Azure NetApp Files con Veeam Backup y la replicación para configurar la recuperación de desastres para máquinas virtuales VMware (AVS) en las instalaciones usando la funcionalidad del software de replicación de Veeam VM.

Veeam Backup & Replication es una aplicación de backup y replicación para entornos virtuales. Cuando los equipos virtuales se replican, Veeam Backup & Replication se replica en AVS, el software creará una copia exacta de los equipos 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 máquina virtual original. La replicación proporciona el mejor objetivo de tiempo de recuperación (RTO) dado que hay una copia montada de un equipo virtual en el sitio de recuperación de desastres en estado listo para el inicio.

Este mecanismo de replicación garantiza que las cargas de trabajo puedan iniciarse rápidamente en un SDDC AVS en caso de desastre. El software Veeam Backup & Replication también optimiza la transmisión del tráfico para la replicación a través de WAN y conexiones lentas. Además, también filtra los bloques de datos duplicados, cero bloques de datos, archivos de intercambio y «archivos excluidos del SO invitado del equipo virtual». El software también comprimirá el tráfico de réplica. Para evitar que los trabajos de replicación consuman todo el ancho de banda de la red, se pueden utilizar aceleradores WAN y reglas de limitación de red.

El proceso de replicación en Veeam Backup & Replication está controlado por tareas, lo que significa que la replicación se realiza mediante la configuración de trabajos de replicación. En caso de desastre, se puede activar la conmutación al respaldo para recuperar las máquinas virtuales conmutando por error a su copia replicada. Cuando se realiza una conmutación por error, una máquina virtual replicada asume el rol de la máquina virtual original. La conmutación por error se puede realizar al estado más reciente de una réplica o a cualquiera de sus puntos de restauración conocidos. Esto permite la recuperación frente al ransomware o las pruebas aisladas según sea necesario. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.

[]

Puesta en marcha de la solución

Escalones de alto nivel

1. El software Veeam Backup and Replication se ejecuta en un entorno local con la conectividad de red adecuada.
2. "Pon en marcha la solución Azure VMware (AVS)" cloud privado y. "Adjunte almacenes de datos de Azure NetApp Files" A los hosts de la solución Azure VMware.

   Se puede utilizar un entorno piloto configurado con una configuración mínima para fines de recuperación ante desastres. Los equipos virtuales se conmutarán por error a este clúster en caso de que se produzca un incidente y se podrán agregar nodos adicionales).

3. Configure el trabajo de replicación para crear réplicas de máquinas virtuales con Veeam Backup and Replication.
4. Crear un plan de recuperación tras fallos y realizar una recuperación tras fallos.
5. Vuelva a los equipos virtuales de producción una vez que el evento de desastre haya finalizado y el sitio principal esté activo.

Requisitos previos para la replicación de Veeam VM en almacenes de datos AVS y ANF

1. Asegúrese de que la máquina virtual de backup de Veeam Backup & Replication está conectada al origen y a los clústeres de SDDC AVS de destino.
2. El servidor de copia de seguridad debe ser capaz de resolver nombres cortos y conectarse a vCenters de origen y destino.
3. El almacén de datos Azure NetApp Files de destino debe tener suficiente espacio libre para almacenar VMDK de máquinas virtuales replicadas.

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

Detalles de la implementación

Paso 1: Replicar máquinas virtuales

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

Para replicar equipos virtuales, siga los siguientes pasos:

1. Abra Veeam Backup & Replication Console.
2. En la vista Inicio. Haga clic con el botón derecho en el nodo JOBS y seleccione Replication Job > Virtual Machine.
3. Especifique un nombre de trabajo y seleccione la casilla de control avanzada adecuada. Haga clic en Siguiente.
   - Active la casilla de verificación Replica seeding si la conectividad entre las instalaciones y Azure tiene un ancho de banda restringido.
     *Seleccione la casilla de verificación Remapping de red (para sitios SDDC de AVS con diferentes redes) si los segmentos en SDDC de Azure VMware Solution 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 Réplica por IP (para sitios de DR con esquema de direccionamiento IP diferente).

     []
4. Seleccione las máquinas virtuales que se van a replicar en el almacén de datos Azure NetApp Files conectado a un SDDC de la solución VMware de Azure en el paso * Máquinas virtuales **. Las máquinas virtuales se pueden colocar en vSAN para llenar la capacidad de almacenes de datos vSAN disponible. En un clúster ligero piloto, la capacidad útil de un clúster de 3 nodos se verá limitada. El resto de los datos puede colocarse fácilmente en almacenes de datos Azure NetApp Files para que las máquinas virtuales se puedan recuperar. El clúster se puede expandir para cumplir los requisitos de CPU/mem. Haga clic en *Agregar**, luego en la ventana **Agregar Objeto** seleccione las VM o contenedores de VM necesarios y haga clic en **Agregar**. Haga clic en **Siguiente**.

   []
5. Después de eso, seleccione el destino como clúster/host SDDC de la solución VMware Azure y el conjunto de recursos apropiado, la carpeta de VM y el almacén de datos FSx para ONTAP para réplicas de VM. A continuación, 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 copia de seguridad que almacenará metadatos para réplicas de VM, política de retención, etc.
8. Actualice los servidores proxy **Source** y **Target** en el paso **Data Transfer** y deje la selección **Automatic** (predeterminada) y mantenga seleccionada la opción **Direct** y haga clic en **Next**.

9. En el paso **Guest Processing**, selecciona la opción **Enable application-aware processing** según sea necesario. Haga clic en **Siguiente**.

   []

10. Seleccione el programa de replicación para ejecutar el trabajo de replicación con regularidad.

    []

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

    []

Una vez que se inicia el trabajo de replicación, las máquinas virtuales con el sufijo especificado se rellenarán en el clúster/host AVS SDDC de destino.

[]

Si quiere más información sobre la replicación de Veeam, consulte "Funcionamiento de la replicación"

Paso 2: Crear un plan de failover

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

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

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

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

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

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

1. En la vista Inicio. Haga clic con el botón derecho en el nodo replicas y seleccione Failover Plans > Failover Plan > VMware vSphere.

   []

2. A continuación, proporcione un nombre y una descripción al plan. El script previo y posterior al failover se puede agregar según sea necesario. Por ejemplo, ejecute un script para cerrar los equipos virtuales antes de iniciar los equipos virtuales replicados.

   []

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

   []

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

Paso 3: Ejecute el plan de failover

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

Asegúrese de que la segmentación de la red está en su lugar para evitar conflictos de IP durante 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 con el botón derecho en su plan de conmutación por error. Selecciona ***Inicio**. Se conmutará al nodo de respaldo usando los puntos de restauración más recientes de réplicas de equipos virtuales. Para conmutar por error a puntos de restauración específicos de réplicas de VM, seleccione **Iniciar a**.

[]

[]

El estado de la réplica de VM cambia de Ready a Failover y VMs se iniciará en el clúster/host SDDC de Azure VMware Solution (AVS) de destino.

[]

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

[]

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

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

Paso 4: Conmutación por recuperación al sitio de producción

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

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

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

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

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

[]

[]

[]

[]

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

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

[]

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

[]

Conclusión

La funcionalidad de almacén de datos Azure NetApp Files permite a Veeam o cualquier herramienta de terceros validada proporcionar una solución de recuperación ante desastres de bajo coste mediante el uso de clústeres ligeros de Pilot en lugar de establecer un gran clúster solo para acomodar réplicas de máquinas virtuales. Esto proporciona una forma eficaz de manejar un plan de recuperación ante desastres

personalizado y personalizado, y de reutilizar productos de backup existentes internamente para recuperación ante desastres, lo que permite la recuperación ante desastres basada en el cloud mediante la salida de centros de datos de recuperación ante desastres en las instalaciones. Es posible conmutar al respaldo haciendo clic en un botón en caso de desastre o conmutando automáticamente al respaldo en caso de desastre.

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

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Migrar cargas de trabajo en Azure/AVS

TR-4940: Migre cargas de trabajo al almacén de datos de Azure NetApp Files mediante VMware HCX: Guía de inicio rápido

Autores: Ingeniería de soluciones de NetApp

Descripción general: Migrar máquinas virtuales con VMware HCX, almacenes de datos de Azure NetApp Files y solución VMware para Azure

Uno de los casos de uso más comunes de la solución para VMware Azure y el almacén de datos Azure NetApp Files es la migración de las cargas de trabajo de VMware. HCX de VMware es la opción preferida y ofrece diversos mecanismos de migración para mover máquinas virtuales (VM) locales y sus datos a almacenes de datos de Azure NetApp Files.

VMware HCX es principalmente una plataforma de migración diseñada para simplificar la migración de aplicaciones, el reequilibrado de las cargas de trabajo e incluso la continuidad de negocio entre clouds. 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.

Este documento proporciona guía paso a paso para aprovisionar almacenes de datos de Azure NetApp Files seguido de la descarga, la puesta en marcha y la configuración de VMware HCX, incluidos todos sus componentes principales en las instalaciones y en el lado de la solución VMware de Azure, incluida la interconexión, la extensión de red y la optimización WAN para habilitar diversos mecanismos de migración de máquinas virtuales.

> VMware HCX funciona con cualquier tipo de almacén de datos, ya que la migración se realiza a nivel de equipo virtual. Por lo tanto, este documento es aplicable a clientes existentes de NetApp y no de NetApp que tengan previsto poner en marcha Azure NetApp Files con la solución VMware de Azure para una puesta en marcha de cloud VMware rentable.

Escalones de alto nivel

Esta lista contiene los pasos de alto nivel necesarios para instalar y configurar HCX Cloud Manager en el cloud 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 VMware vCenter Server en las instalaciones.
3. Active HCX con la clave de licencia.
4. Empareje el conector VMware HCX en las instalaciones con la solución VMware de Azure HCX Cloud Manager.
5. Configure el perfil de red, el perfil de computación y la malla de servicio.
6. (Opcional) lleve a cabo la extensión de red para evitar la reIP durante las migraciones.
7. Valide el estado del dispositivo y asegúrese de que la migración sea posible.
8. Migrar las cargas de trabajo de la máquina virtual.

Requisitos previos

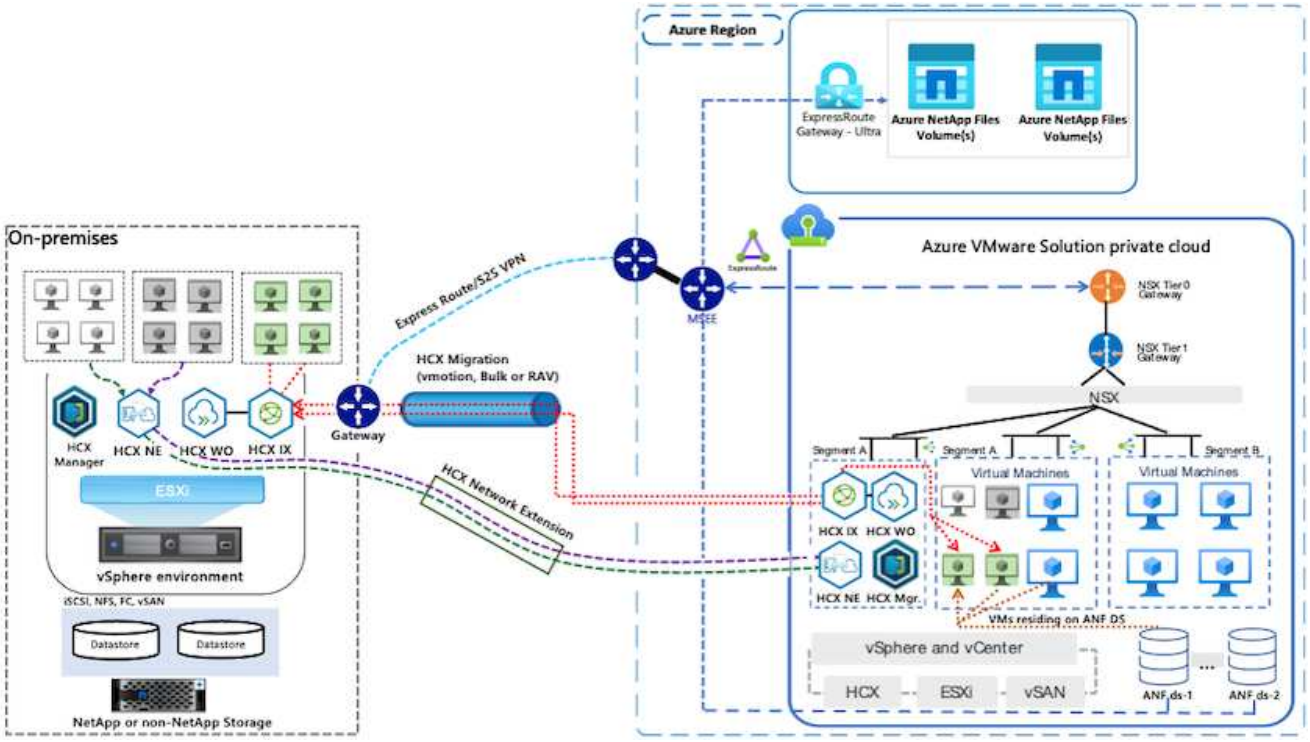
Antes de empezar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte este tema "enlace". Una vez que los requisitos previos, incluida la conectividad, estén vigentes, configure y active HCX generando la clave de licencia desde el portal de la solución VMware de Azure. 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 VMware HCX Enterprise Edition también está disponible a través de un ticket de soporte y se admite sin coste adicional.

- Utilice un centro de datos definido por software (SDDC) de la solución Azure VMware existente o cree un cloud privado utilizando este método "Enlace a NetApp" o esto "Vínculo de Microsoft".
- La migración de equipos virtuales y datos asociados desde el centro de datos integrado con VMware vSphere en las instalaciones requiere conectividad de red del centro de datos al entorno SDDC. Antes de migrar cargas de trabajo, "Configurar una conexión VPN de sitio a sitio o una conexión de acceso global de ruta Express" entre el entorno local y el cloud privado correspondiente.
- La ruta de red desde el entorno local de VMware vCenter Server hasta el cloud privado de la solución VMware para Azure debe admitir la migración de máquinas virtuales mediante vMotion.
- Asegúrese de que es necesario "reglas y puertos del firewall" Se permiten para el tráfico de vMotion entre la instancia local de vCenter Server y SDDC vCenter. En la nube privada, el enrutamiento de la red de vMotion está configurado de manera predeterminada.
- El volumen NFS de Azure NetApp Files debe montarse como almacén de datos en la solución VMware de Azure. Siga los pasos detallados en este documento "enlace" Para conectar almacenes de datos de Azure NetApp Files a los hosts de soluciones VMware de Azure.

Arquitectura de alto nivel

Para realizar las pruebas, el entorno de laboratorio de las instalaciones que se emplean para esta validación se conectó a través de una VPN sitio a sitio, lo que permite la conectividad en las instalaciones con la solución VMware para Azure.



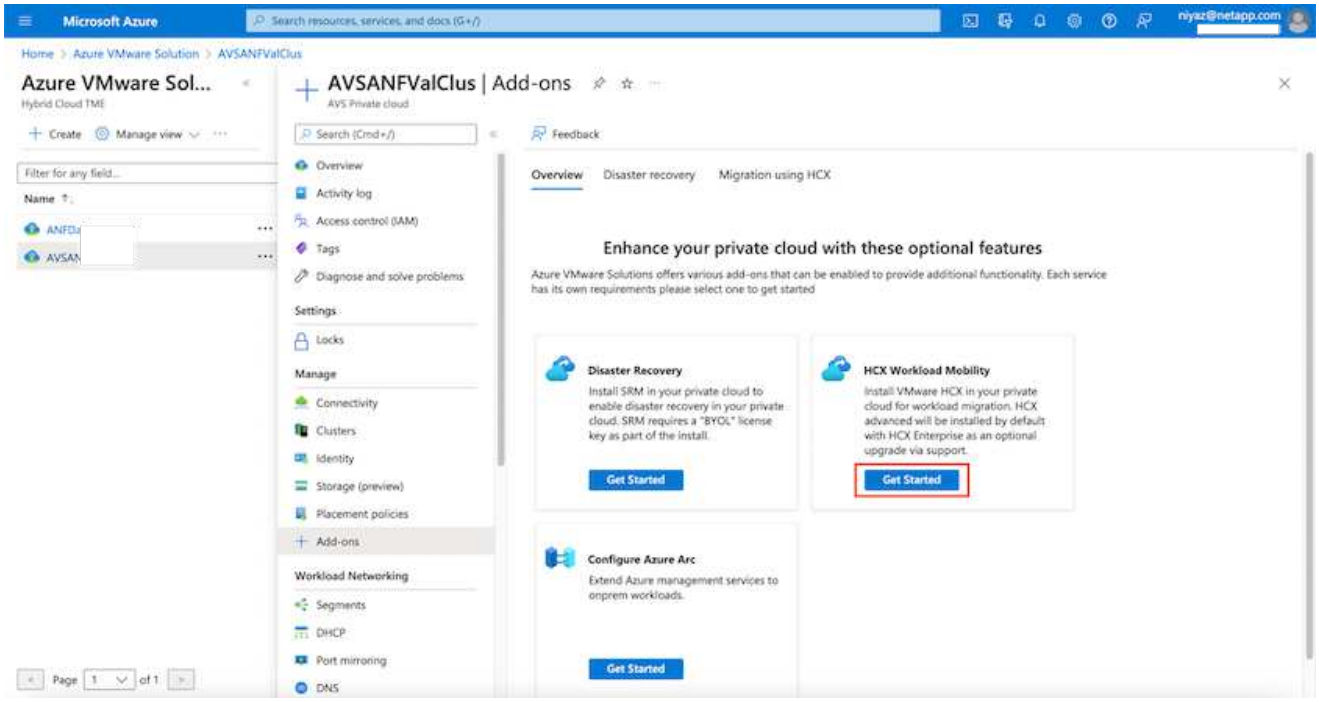
Puesta en marcha de la solución

Siga la serie de pasos para completar la implementación de esta solución:

Paso 1: Instale HCX a través de Azure Portal mediante la opción Add-ons

Para realizar la instalación, lleve a cabo los siguientes pasos:

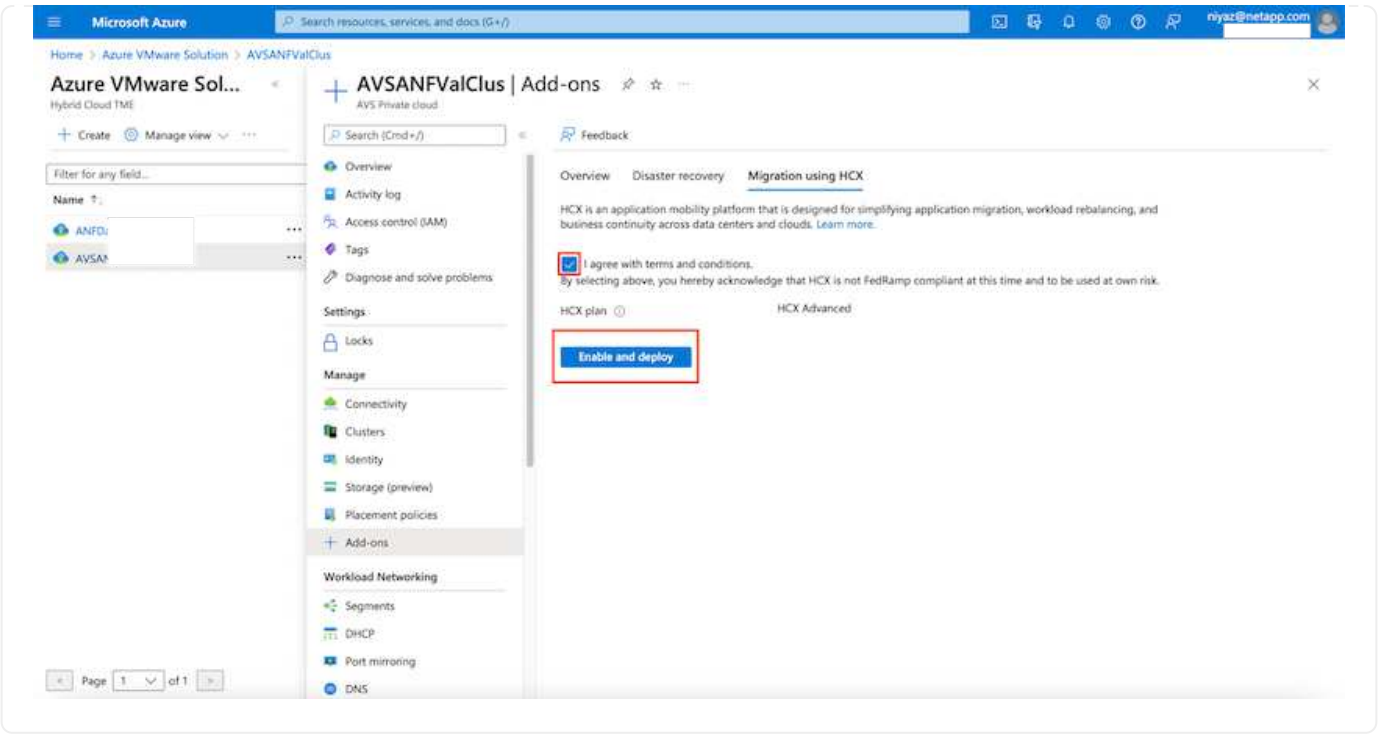
1. Inicie sesión en el portal de Azure y acceda al cloud privado de la solución VMware para Azure.
2. Seleccione el cloud privado adecuado y acceda a Add-ons. Esto se puede hacer navegando a **Administrar > Complementos**.
3. En la sección movilidad de carga de trabajo de HCX, haga clic en **comenzar**.



1. Seleccione la opción **Acepto los términos y condiciones** y haga clic en **Activar e implementar**.

> La implementación predeterminada es HCX Advanced. Abra una solicitud de soporte para activar la edición Enterprise.

> La puesta en marcha dura entre 25 y 30 minutos, aproximadamente.


Microsoft Azure
Search resources, services, and docs (G+/)
niyaz@netapp.com
Home > Azure VMware Solution > AVSANFValClus
Azure VMware Sol...
Hybrid Cloud TME
Create
Manage view
Filter for any field...
Name
ANFDu
AVSAN
Page 1 of 1
AVSANFValClus | Add-ons
AVS Private cloud
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Clusters
Identity
Storage (preview)
Placement policies
Add-ons
Workload Networking
Segments
DHCP
Port mirroring
DNS
Feedback
Overview
Disaster recovery
Migration using HCX
HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. Learn more.
I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.
HCX plan
HCX Advanced
Enable and deploy

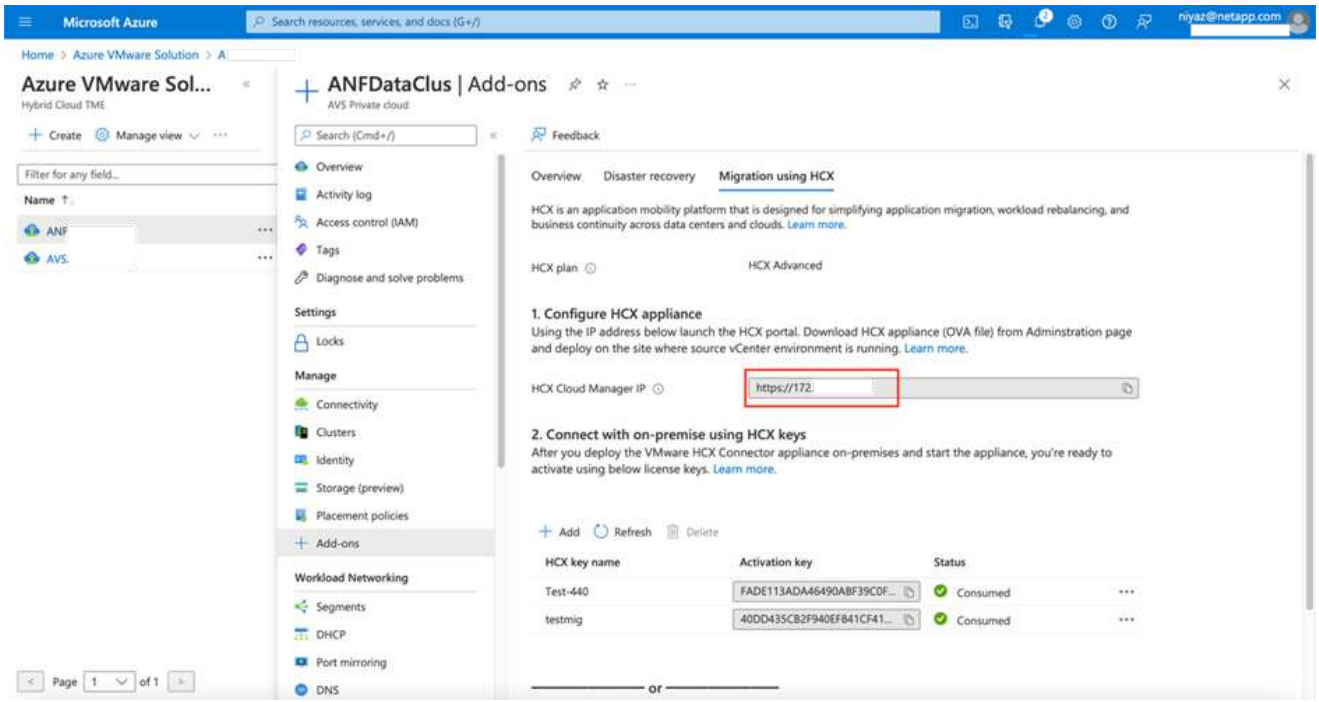
Paso 2: Ponga en marcha el OVA del instalador en la instancia local de vCenter Server

Para que el conector local se conecte al HCX Manager en la solución VMware de Azure, asegúrese de que los puertos de firewall adecuados están abiertos en el entorno local.

Para descargar e instalar el conector HCX en el vCenter Server local, complete los siguientes pasos:

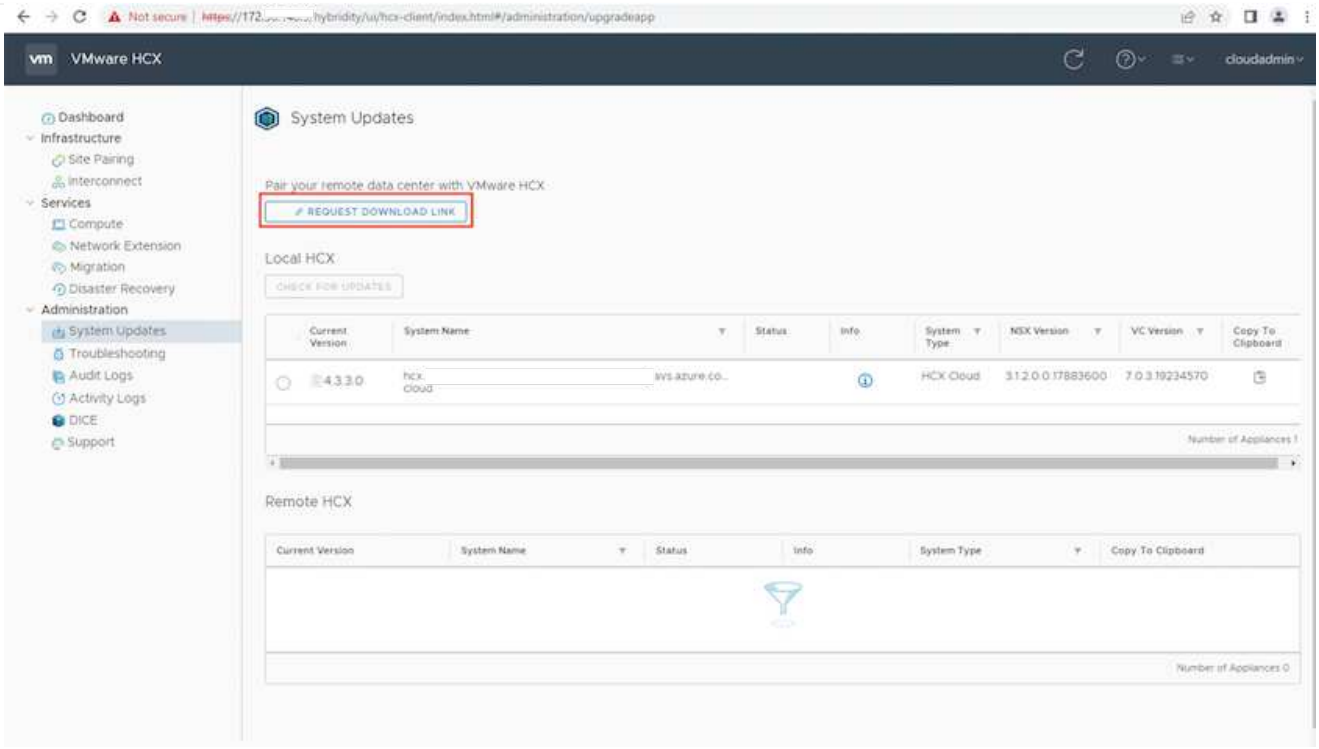
1. En el portal de Azure, vaya a la solución VMware para Azure, seleccione el cloud privado y seleccione **gestionar > Complementos > migración** mediante HCX y copie el portal HCX Cloud Manager para descargar el archivo OVA.

Utilice las credenciales de usuario predeterminadas de CloudAdmin para acceder al portal HCX.

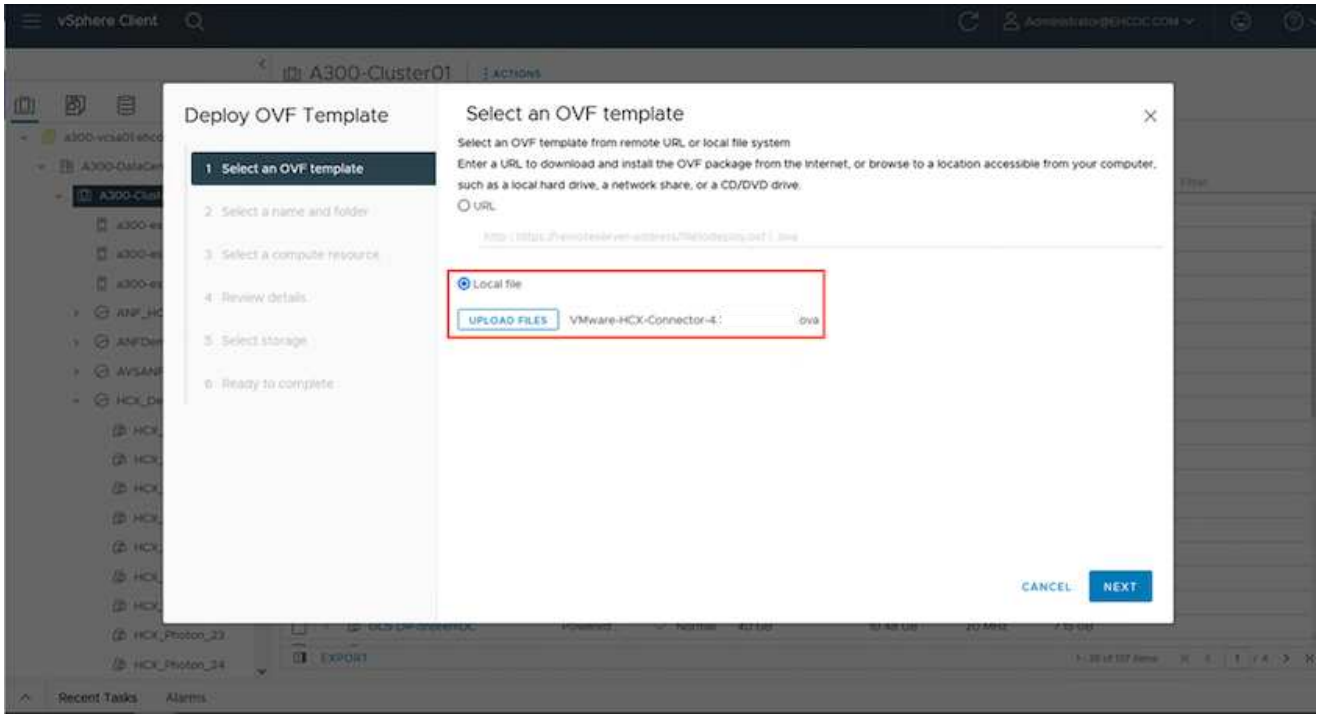


1. Después de acceder al portal HCX con cloudadmin@vsphere.loc/ usando el jumphost, navegue hasta **Administration > System Updates** y haga clic en **Request Download Link**.

Descargue o copie el enlace en el OVA y péguelo en un explorador para comenzar el proceso de descarga del archivo OVA de VMware HCX Connector que se implementará en la instancia local de vCenter Server.



1. Una vez descargado el OVA, póngalo en marcha en el entorno local de VMware vSphere mediante la opción **implementar plantilla OVF**.



1. Introduzca toda la información necesaria para la implementación de OVA, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar** para implementar el OVA del conector HCX de VMware.

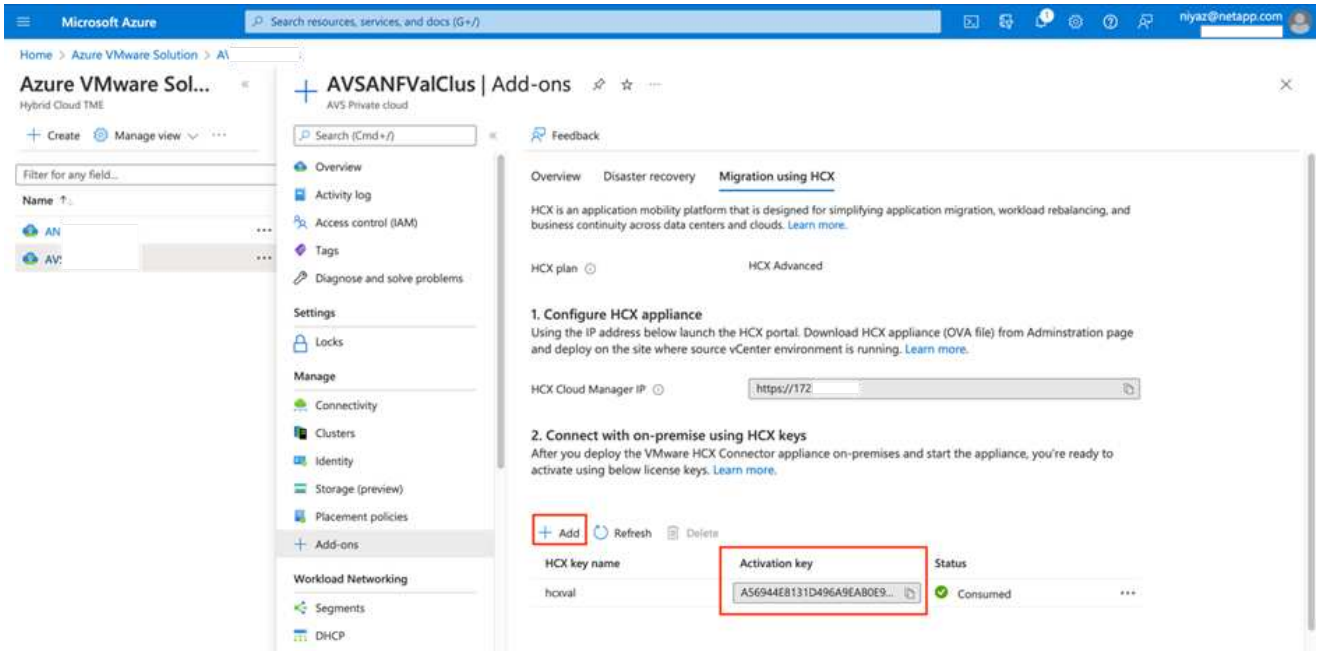
Encienda el dispositivo virtual manualmente.

Para obtener instrucciones paso a paso, consulte "Guía del usuario de VMware HCX".

Paso 3: Active el conector HCX con la clave de licencia

Después de implementar el OVA del conector HCX de VMware en las instalaciones e iniciar el dispositivo, lleve a cabo los siguientes pasos para activar el conector HCX. Genere la clave de licencia desde el portal de la solución VMware de Azure y actívela en el administrador HCX de VMware.

1. En el portal de Azure, vaya a la solución para VMware de Azure, seleccione el cloud privado y seleccione **gestionar > Complementos > migración mediante HCX**.
2. En **conectar con las instalaciones mediante las teclas HCX**, haga clic en **Agregar** y copie la clave de activación.



Se requiere una llave independiente para cada conector HCX local que esté desplegado.

1. Inicie sesión en el VMware HCX Manager local en "https://hcxmanagerIP:9443" uso de las credenciales de administrador.

Utilice la contraseña definida durante la implementación de OVA.

1. En la licencia, introduzca la clave copiada del paso 3 y haga clic en **Activar**.

El conector HCX de las instalaciones debe tener acceso a Internet.

1. En **Datacenter Location**, proporcione la ubicación más cercana para instalar el VMware HCX Manager en las instalaciones. Haga clic en **continuar**.
2. En **Nombre del sistema**, actualice el nombre y haga clic en **continuar**.
3. Haga clic en **Sí, continuar**.
4. En **Conecte 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**.

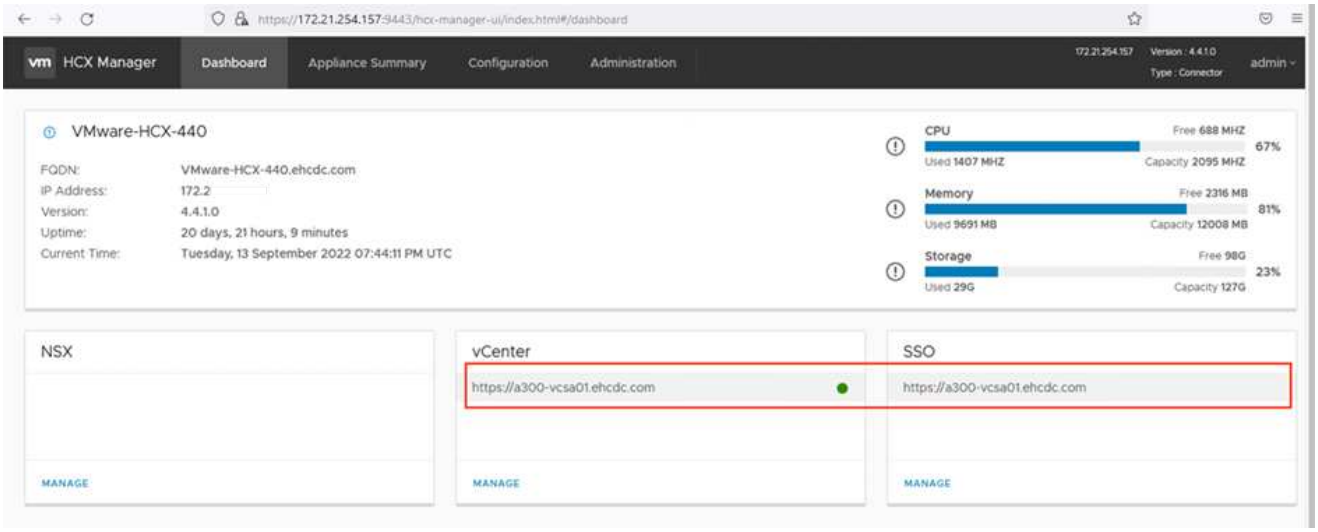
Utilice el FQDN para evitar problemas de conectividad más adelante.

1. En **Configurar SSO/PSC**, proporcione la dirección IP o FQDN del controlador de servicios de plataforma y haga clic en **continuar**.

Introduzca el nombre de dominio completo o la dirección IP de VMware vCenter Server.

1. Compruebe que la información introducida es correcta y haga clic en **Reiniciar**.
2. Después de reiniciar los servicios, vCenter Server se muestra como verde en la página que aparece. Tanto vCenter Server como SSO deben tener los parámetros de configuración adecuados, que deben ser los mismos que los de la página anterior.

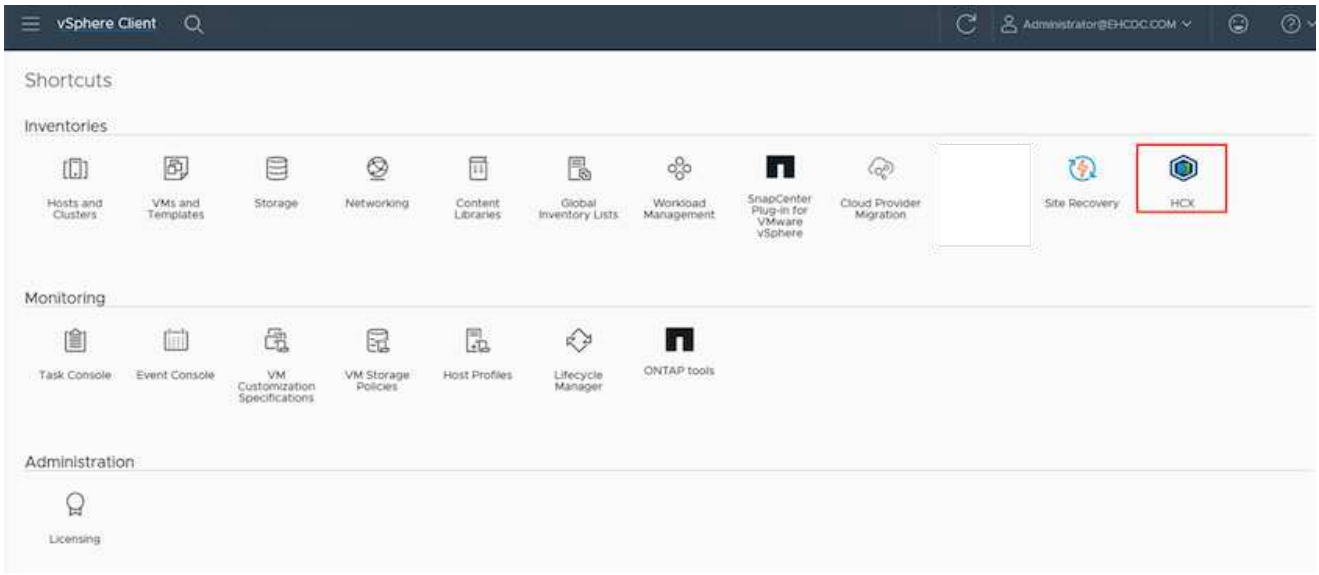
Este proceso debe tardar aproximadamente de 10 a 20 minutos y el plugin se añadirá a vCenter Server.



Paso 4: Emparejar el conector VMware HCX en las instalaciones con la solución de VMware Azure HCX Cloud Manager

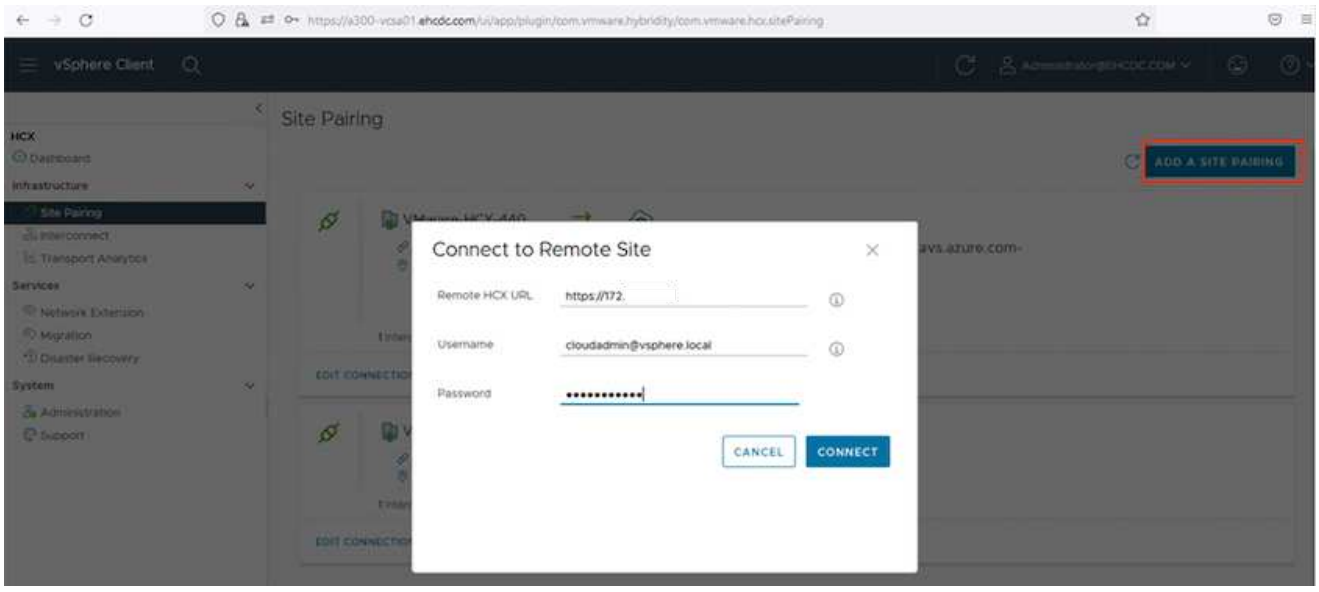
Después de instalar el conector HCX en la solución VMware de Azure y en las instalaciones, configure el cloud privado de VMware HCX Connector para la solución VMware de Azure agregando el emparejamiento. Para configurar el emparejamiento de sitios, lleve a cabo los siguientes pasos:

1. Para crear un par de sitios entre el entorno local de vCenter y el SDDC de la solución VMware para Azure, inicie sesión en la instancia local de vCenter Server y acceda al nuevo complemento HCX vSphere Web Client.



1. En Infraestructura, haga clic en **Agregar un emparejamiento de sitios**.

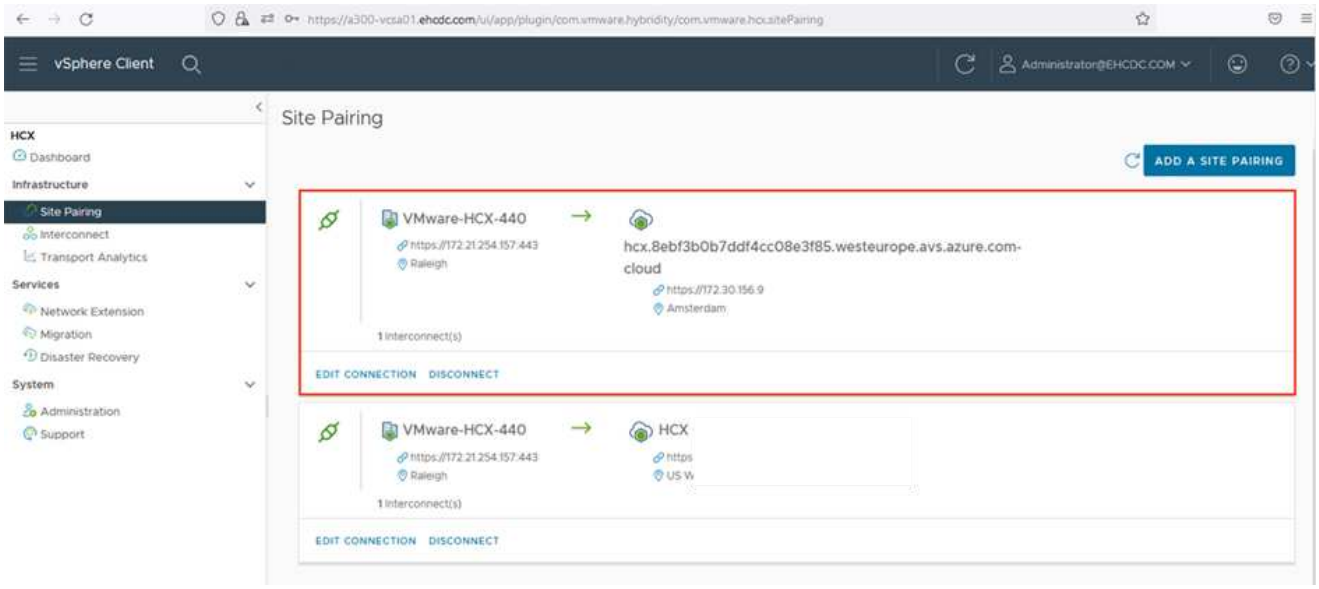
Introduzca la dirección URL o IP de HCX Cloud Manager de la solución Azure VMware y las credenciales del rol CloudAdmin para acceder a la nube privada.



1. Haga clic en **conectar**.

El conector HCX de VMware debe poder enrutar a HCX Cloud Manager IP a través del puerto 443.

1. Una vez creado el emparejamiento, el emparejamiento de sitios recién configurado está disponible en el panel de HCX.

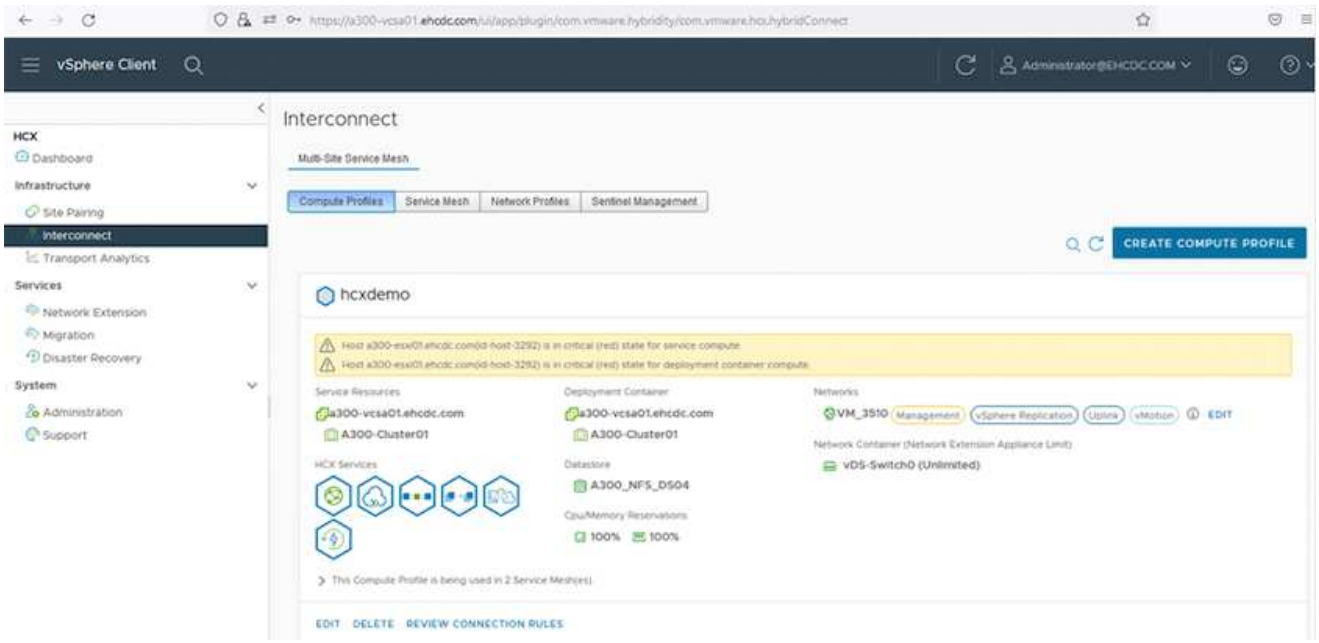


Paso 5: Configure el perfil de red, el perfil de computación y la malla de servicio

El dispositivo de servicio VMware HCX Interconnect proporciona funcionalidades de replicación y migración basada en vMotion a través de Internet y conexiones privadas al sitio de destino. La interconexión ofrece cifrado, ingeniería de tráfico y movilidad de máquinas virtuales. Para crear un dispositivo de servicio de interconexión, lleve a cabo los siguientes pasos:

1. En Infraestructura, seleccione **interconexión > malla de servicio multisitio > Perfiles de computación > Crear perfil de computación**.

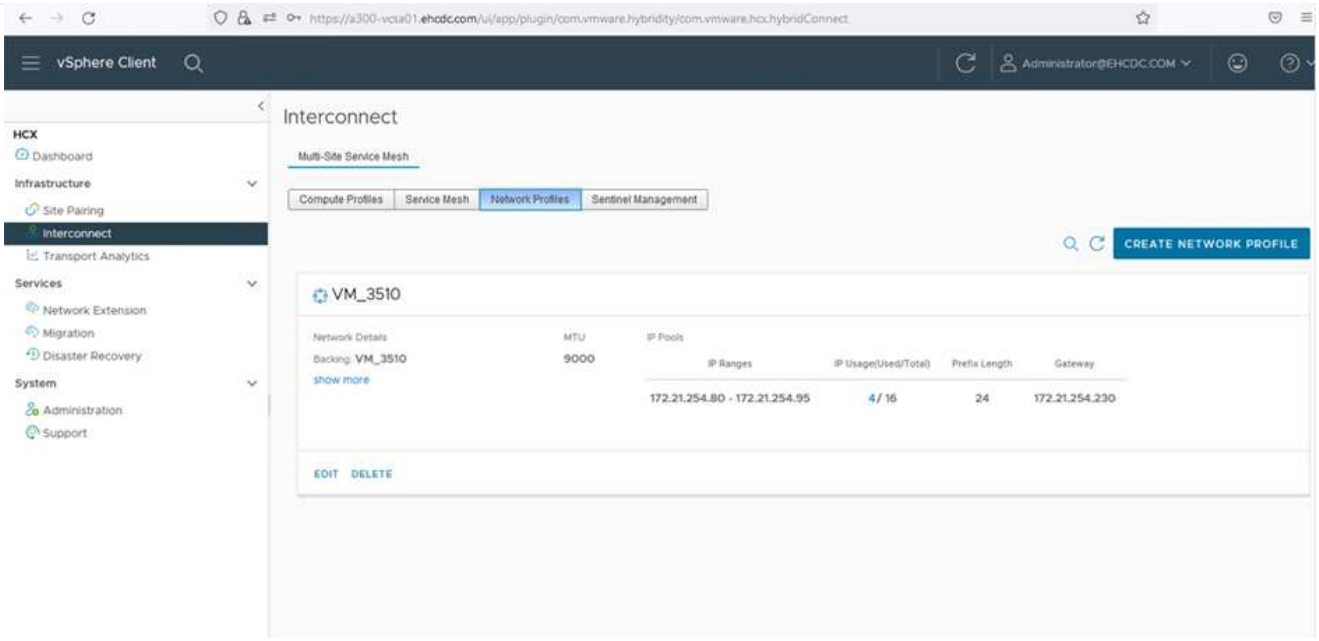
Los perfiles informáticos definen los parámetros de implementación, incluidos los dispositivos que se implementan y qué parte del centro de datos de VMware puede acceder al servicio HCX.



1. Después de crear el perfil de computación, cree los perfiles de red seleccionando **malla de servicio multisitio > Perfiles de red > Crear perfil de red**.

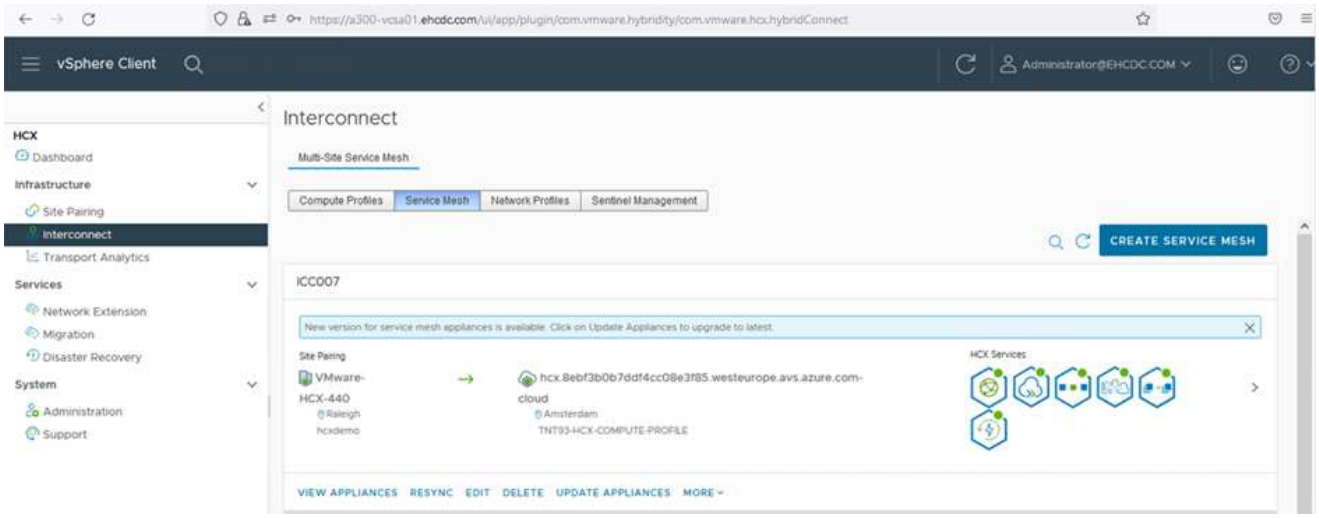
El perfil de red define un rango de direcciones IP y redes que utiliza HCX para sus dispositivos virtuales.

Este paso requiere dos o más direcciones IP. Estas direcciones IP se asignan desde la red de gestión a los dispositivos de interconexión.

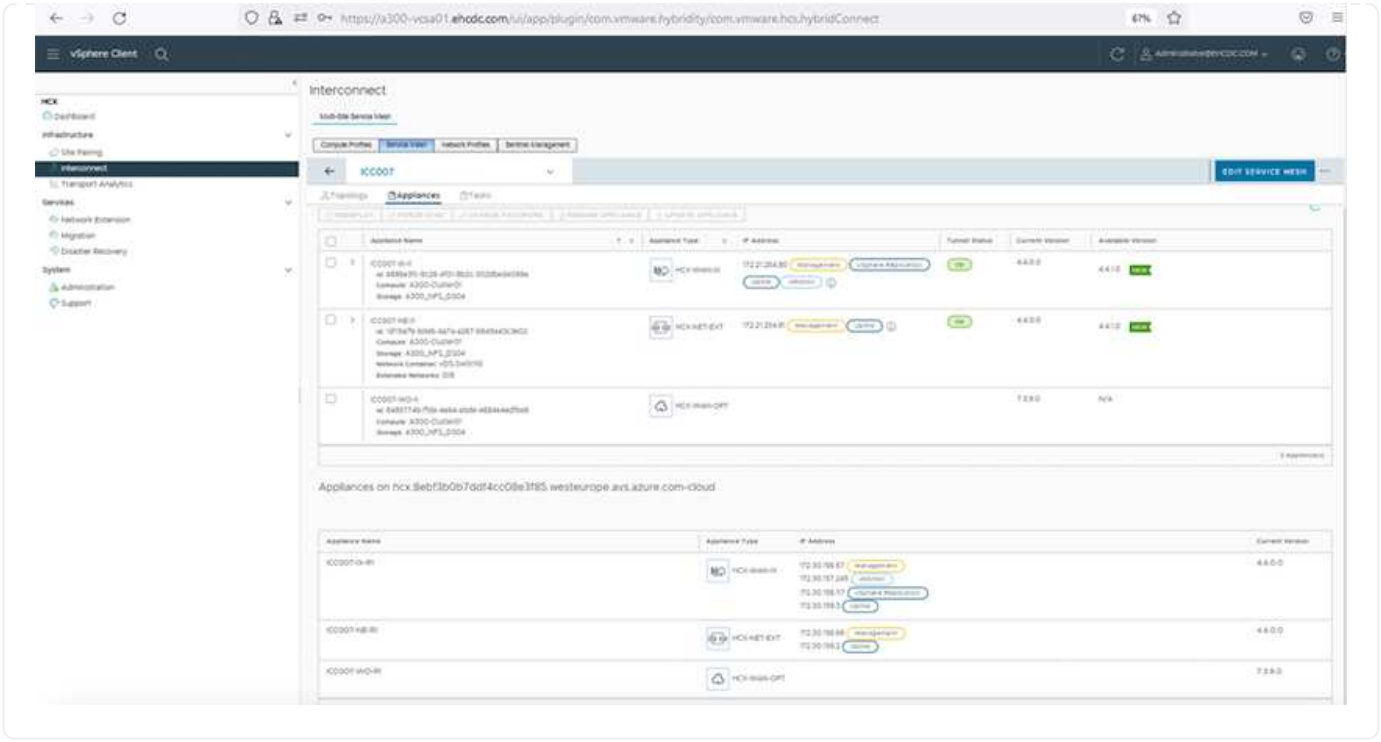


1. En este momento, se han creado correctamente los perfiles de computación y red.
2. Cree la malla de servicio seleccionando la pestaña **malla de servicio** en la opción **interconexión** y seleccione los sitios SDDC de las instalaciones y Azure.
3. La malla de servicio especifica una pareja de perfiles de red y de computación local y remota.

Como parte de este proceso, los dispositivos HCX se implementan y se configuran automáticamente tanto en los sitios de origen como en los de destino con el fin de crear una estructura de transporte segura.



1. Este es el paso final de la configuración. Esta operación debería tardar cerca de 30 minutos en completar la puesta en marcha. Una vez configurada la malla de servicio, el entorno está preparado con los túneles IPsec creados correctamente para migrar las VM de carga de trabajo.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

Paso 6: Migrar cargas de trabajo

Las cargas de trabajo se pueden migrar de manera bidireccional entre los centros de datos SDC de Azure y en las instalaciones mediante diversas tecnologías de migración HCX de VMware. Los equipos virtuales se pueden mover hacia y desde entidades activadas por HCX de VMware mediante varias tecnologías de migración, como la migración masiva de HCX, HCX vMotion, migración en frío de HCX, el asistente de replicación de HCX vMotion (disponible con la edición de HCX Enterprise) y la migración asistida por SO HCX (disponible con la edición de HCX Enterprise).

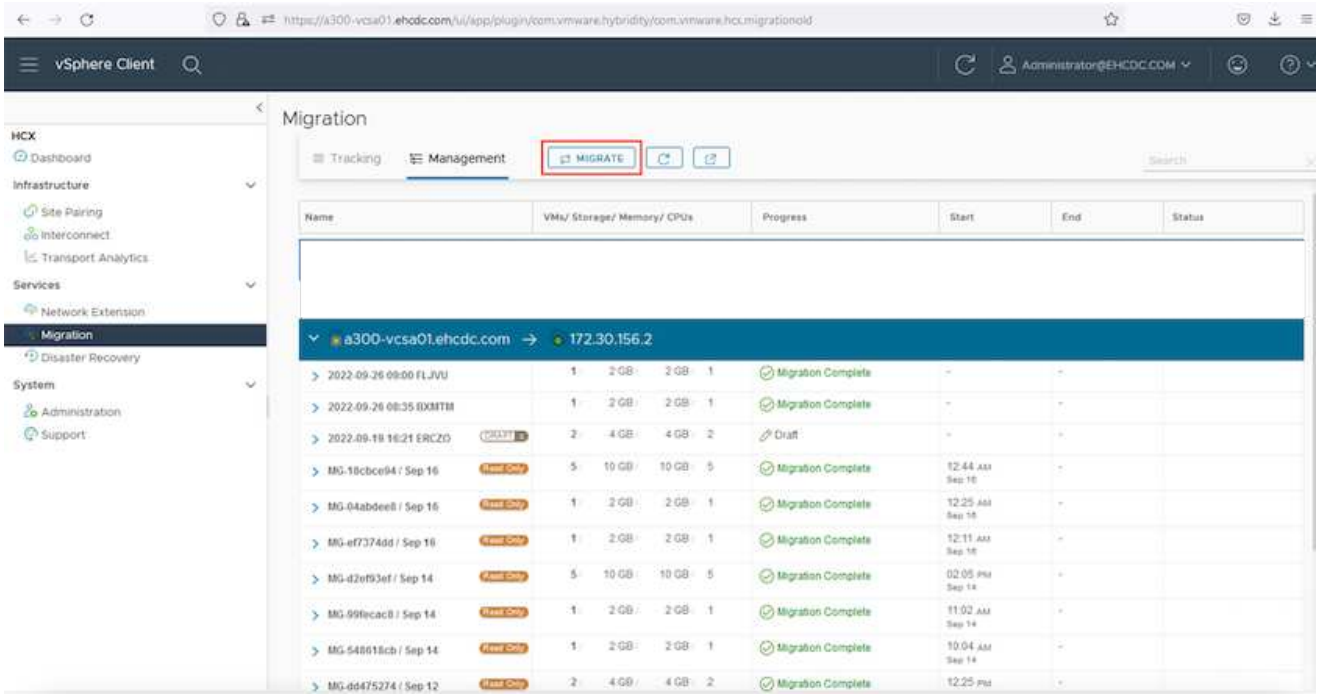
Para obtener más información sobre varios mecanismos de migración de HCX, consulte "Tipos de migración HCX de VMware".

Migración masiva

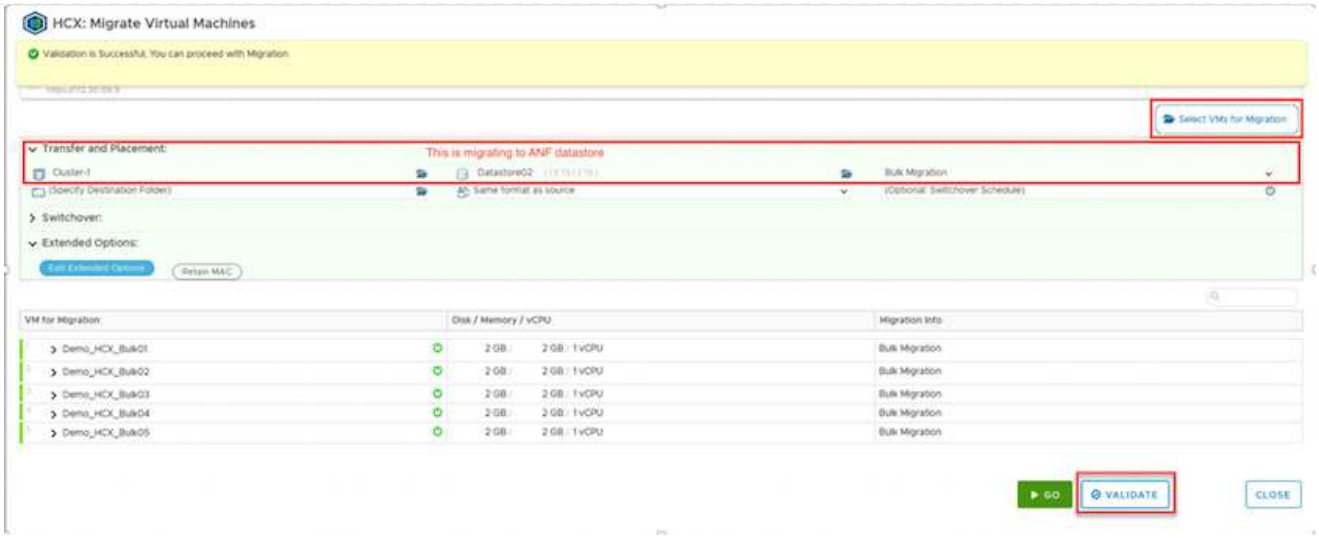
En esta sección se detalla el mecanismo de migración masiva. Durante una migración masiva, la funcionalidad de migración masiva de HCX utiliza la replicación de vSphere para migrar archivos de disco al mismo tiempo que vuelve a crear la máquina virtual en la instancia de vSphere HCX de destino.

Para iniciar migraciones masivas de máquinas virtuales, complete los siguientes pasos:

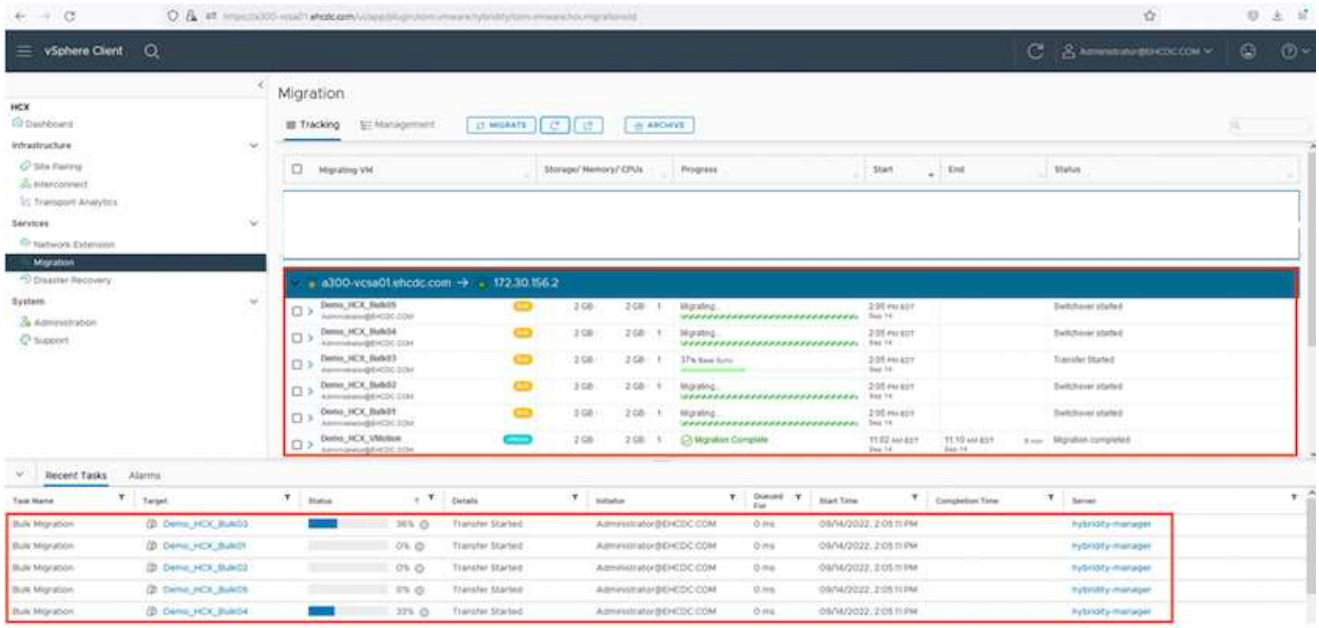
1. Acceda a la ficha **migración** en **Servicios > migración**.



1. En **Conexión a sitio remoto**, seleccione la conexión a sitio remoto y seleccione el origen y el destino. En este ejemplo, el destino es el extremo SDDC de la solución Azure para VMware.
2. Haga clic en **Seleccionar VM para migración**. Esto proporciona una lista de todas las máquinas virtuales en las instalaciones. Seleccione las VM basadas en la expresión match:Value y haga clic en **Add**.
3. En la sección **transferencia y colocación**, actualice los campos obligatorios (**Cluster**, **almacenamiento**, **destino** y **Red**), incluido el perfil de migración, y haga clic en **Validar**.

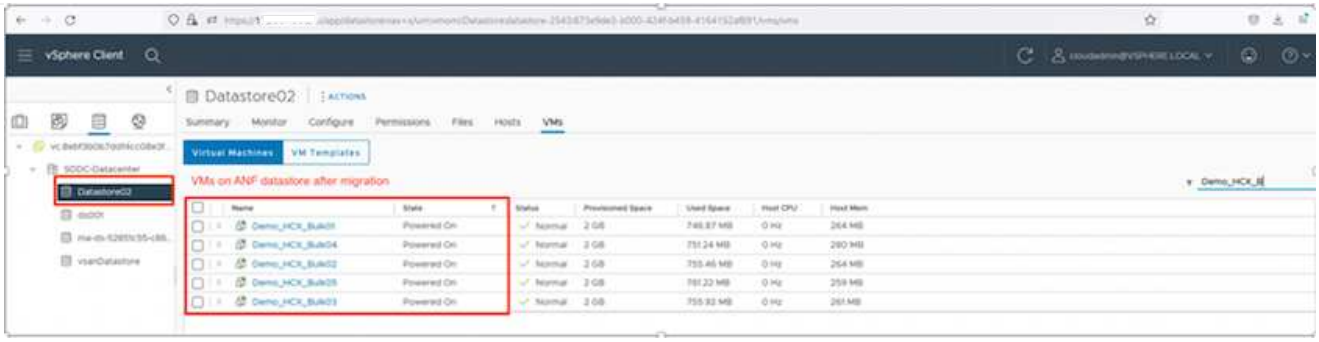


1. Una vez completadas las comprobaciones de validación, haga clic en **Ir** para iniciar la migración.



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 a los discos de marcador de posición. HBR se activa para realizar una sincronización completa en el destino y una vez que se completa la línea de base, se realiza una sincronización incremental en función del ciclo del objetivo de punto de recuperación (RPO). Una vez finalizada la sincronización completa/incremental, la conmutación se activa automáticamente a menos que se defina una programación específica.

1. Una vez finalizada la migración, valide lo mismo accediendo al centro de datos definido por software vCenter de destino.

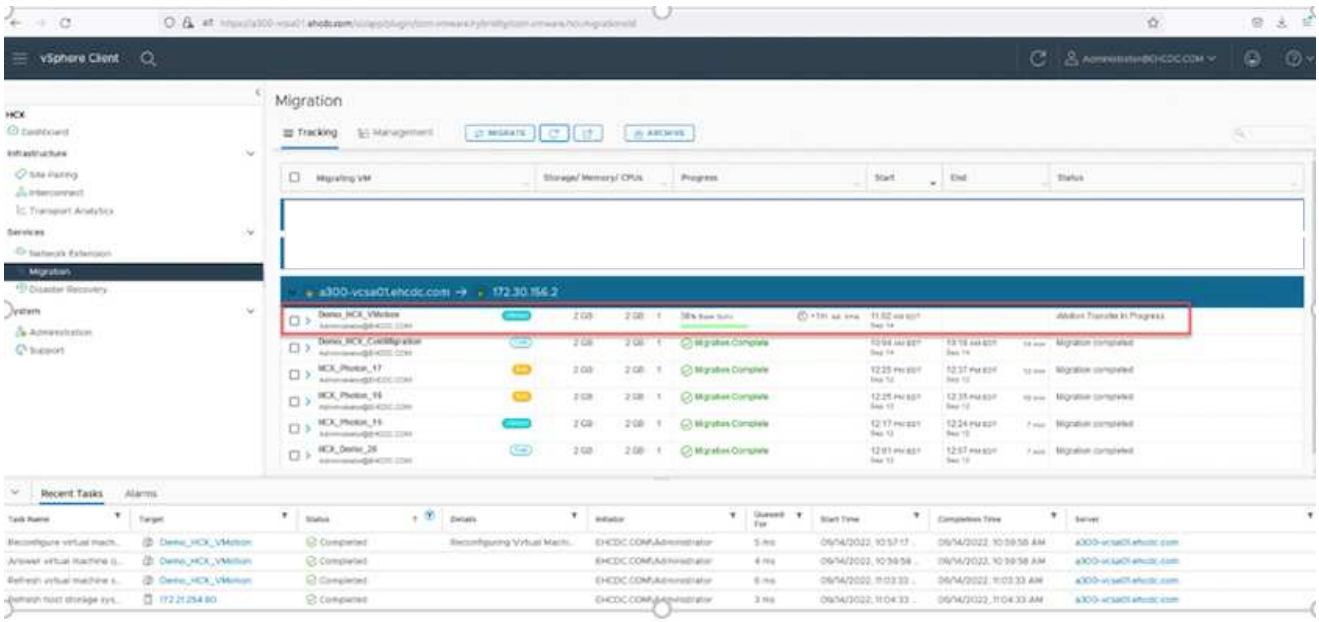


Si desea obtener información adicional y detallada sobre varias opciones de migración y sobre cómo migrar cargas de trabajo de las instalaciones a la solución VMware Azure mediante HCX, consulte "Guía del usuario de VMware HCX".

Para obtener más información sobre este proceso, no dude en ver el siguiente vídeo:

Migración de cargas de trabajo mediante HCX

Esta es una captura de pantalla de la opción HCX vMotion.



Para obtener más información sobre este proceso, no dude en ver el siguiente vídeo:

VMotion de HCX

Asegúrese de que hay suficiente ancho de banda disponible para gestionar la migración.

El almacén de datos ANF de destino debe tener suficiente espacio para gestionar la migración.

Conclusión

Tanto si su objetivo es el cloud híbrido como el cloud, y los datos residen en un almacenamiento de cualquier

tipo o proveedor en las instalaciones, Azure NetApp Files y HCX ofrecen excelentes opciones para poner en marcha y migrar las cargas de trabajo de la aplicación a la vez que reduce el TCO, ya que los requisitos de datos se adaptan sin problemas a la capa de la aplicación. Sea cual sea el caso práctico, elija la solución VMware de Azure junto con Azure NetApp Files para conocer rápidamente las ventajas del cloud, una infraestructura consistente y operaciones en las instalaciones y varios clouds, portabilidad bidireccional de cargas de trabajo, y capacidad y rendimiento de clase empresarial. Se trata del mismo proceso y procedimientos que ya conoce que se utiliza para conectar el almacenamiento y migrar máquinas virtuales mediante la replicación de VMware vSphere, VMware vMotion o incluso la copia de archivos de red (NFC).

Puntos

Los puntos clave de este documento son:

- Ahora puede utilizar Azure NetApp Files como almacén de datos en SDDC de la solución para VMware Azure.
- Puede migrar datos de manera sencilla desde las instalaciones a un almacén de datos de Azure NetApp Files.
- Es posible aumentar y reducir con facilidad el almacén de datos Azure NetApp Files para satisfacer los requisitos de capacidad y rendimiento durante la actividad de migración.

Dónde encontrar información adicional

Si quiere más información sobre la información descrita en este documento, consulte los siguientes enlaces a sitios web:

- Documentación de la solución VMware de Azure

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

- Documentación de Azure NetApp Files

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

- Guía del usuario de VMware HCX

"https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Region Availability – almacén de datos NFS suplementario para ANF

La disponibilidad de almacenes de datos NFS complementarios en Azure/AVS es definida por Microsoft. En primer lugar, es necesario determinar si tanto el AVS como el ANF están disponibles en una región específica. A continuación, debe determinar si el almacén de datos NFS suplementario ANF es compatible con esa región.

- Compruebe la disponibilidad de AVS y ANF "aquí".
- Compruebe la disponibilidad del almacén de datos NFS complementario ANF "aquí".

Funcionalidades de NetApp para Google Cloud Platform GCVE

Obtén más información sobre las funcionalidades que NetApp aporta a Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE), desde NetApp como dispositivo

de almacenamiento conectado invitado o un almacén de datos NFS complementario para migrar flujos de trabajo, extender/irrumpir a la nube, backup/restauración y recuperación ante desastres.

Para ir a la sección del contenido deseado, seleccione una de las siguientes opciones:

- "Configuración de GCVE en GCP"
- "Opciones de almacenamiento de NetApp para GCVE"
- "Soluciones cloud de NetApp/VMware"

Configuración de GCVE en GCP

Al igual que en las instalaciones, la planificación de un entorno de virtualización basado en cloud es crucial para tener un entorno preparado para la producción con éxito a la hora de crear equipos virtuales y migración.

En esta sección se describe cómo configurar y gestionar GCVE y cómo utilizarlo junto con las opciones disponibles para conectar el almacenamiento de NetApp.

El almacenamiento invitado es el único método compatible para conectar Cloud Volumes ONTAP y Cloud Volumes Services a GCVE.

El proceso de configuración puede dividirse en los siguientes pasos:

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

Vea el detalles "Pasos de configuración para GCVE".

Opciones de almacenamiento de NetApp para GCVE

El almacenamiento de NetApp se puede utilizar de varias maneras, ya sea como adivinar conectado o como un almacén de datos NFS complementario, en GCP GCVE.

Visite "Opciones de almacenamiento de NetApp admitidas" si quiere más información.

Google Cloud es compatible con almacenamiento de NetApp en las siguientes configuraciones:

- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado
- Cloud Volumes Service (CVS) como almacenamiento conectado como invitado
- Cloud Volumes Service (CVS) como almacén de datos NFS complementario

Vea el detalles "Opciones de almacenamiento de Guest Connect para GCVE".

Más información acerca de "Soporte de almacén de datos de Cloud Volumes Service de NetApp para Google Cloud VMware Engine (blog de NetApp)" o. "Cómo usar CVS de NetApp como almacenes de datos para Google Cloud VMware Engine (blog de Google)"

Casos de uso de soluciones

Con las soluciones cloud de NetApp y VMware, la puesta en marcha en Azure AVS resulta sencilla en muchos casos de uso. Los casos de ingenieros de sistemas se definen para cada una de las áreas cloud definidas de VMware:

- Protect (incluye recuperación ante desastres y backup/restauración)
- Extender
- Migración

"Consulte las soluciones de NetApp para Google Cloud GCVE"

Protección de cargas de trabajo en GCP / GCVE

Recuperación ante desastres coherente con las aplicaciones con NetApp SnapCenter y replicación de Veeam

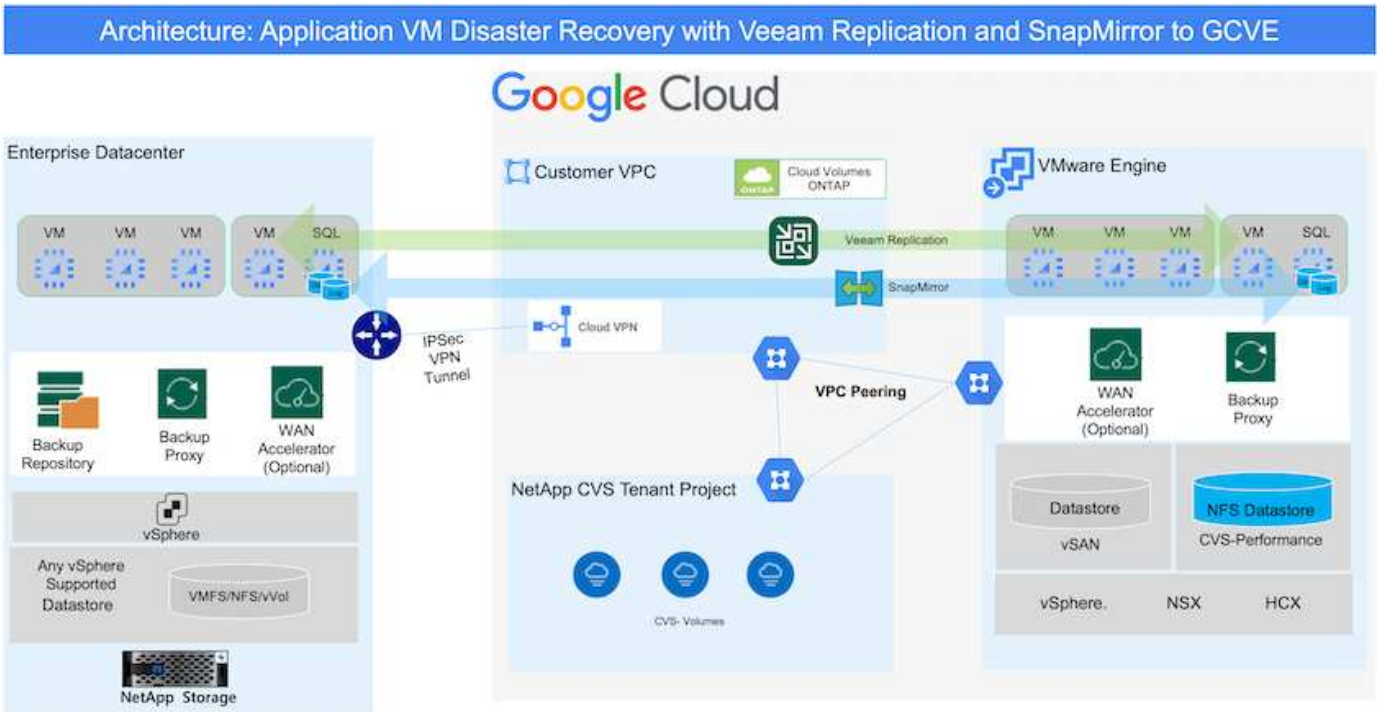
Autores: Suresh Thoppay, NetApp

Descripción general

Muchos clientes están buscando una solución de recuperación ante desastres eficaz para sus VM de aplicaciones alojadas en VMware vSphere. Muchos de ellos utilizan su solución de backup existente para realizar la recuperación durante el diaster.
Muchas veces esa solución aumenta el objetivo de tiempo de recuperación y no cumple con sus expectativas. Para reducir el objetivo de punto de recuperación y el objetivo de tiempo de recuperación, la replicación de Veeam VM se puede utilizar incluso desde on-premises a GCVE, siempre y cuando la conectividad de red y el entorno con los permisos adecuados estén disponibles.
NOTA: Veeam VM Replication no protege los dispositivos de almacenamiento conectados a invitados de VM como montajes iSCSI o NFS dentro de la VM invitada. Necesidad de protegerlos por separado.

Para la replicación consistente de las aplicaciones para SQL VM y para reducir el RTO, utilizamos SnapCenter para orquestar las operaciones de snapmirror de volúmenes de bases de datos y registros de SQL.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, Veeam y Google Cloud VMware Engine (GCVE) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con las aplicaciones.

> Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice las opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Google Cloud para conocer el método de conectividad apropiado de las instalaciones a Google.

Implementar la solución DR

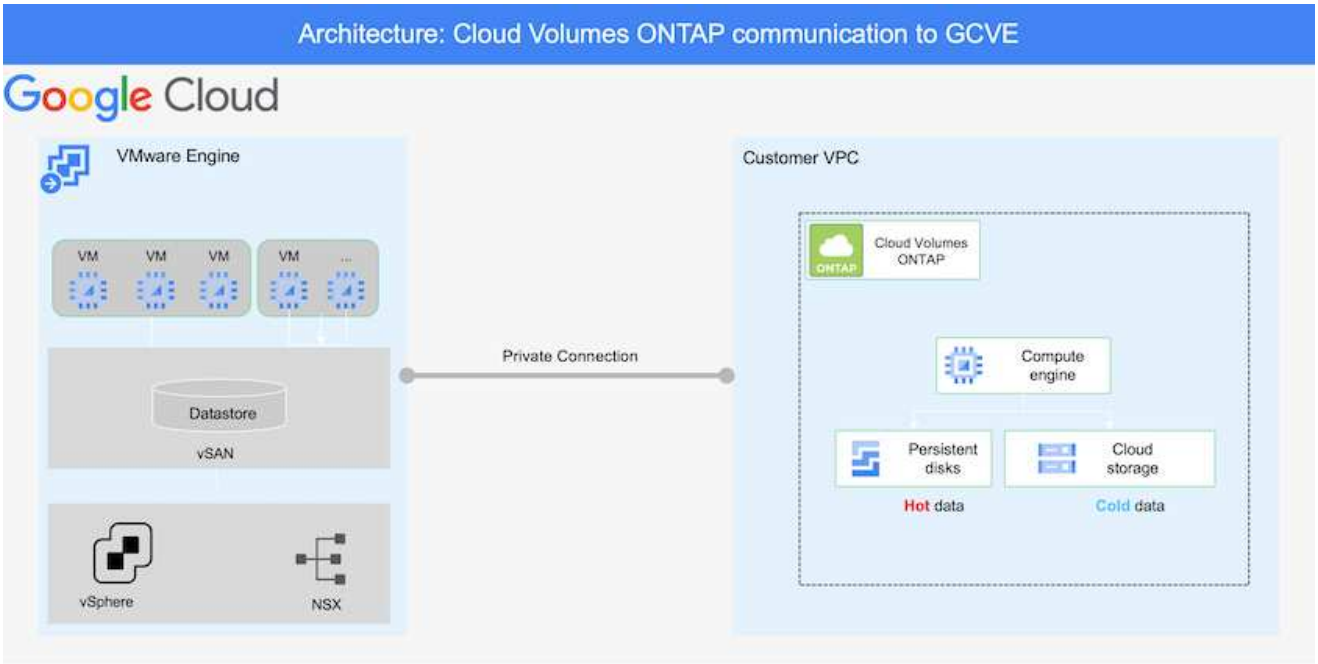
Descripción general de la puesta en marcha de soluciones

1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisiona Cloud Volumes ONTAP con el tamaño de instancia correcto mediante BlueXP en la suscripción y la red virtual adecuadas.
    a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.
    b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.
3. Instale el software Veeam y empiece a replicar máquinas virtuales a la instancia de Google Cloud VMware Engine.
4. Durante un desastre, interrumpa la relación de SnapMirror mediante BlueXP y activa la conmutación al nodo de respaldo de máquinas virtuales con Veeam.
    a. Vuelva a conectar las LUN ISCSI y los montajes NFS para los equipos virtuales de la aplicación.
    b. Ponga en marcha aplicaciones en línea.
5. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Google Cloud y replicar volúmenes a CVO

El primer paso es configurar Cloud Volumes ONTAP en Google Cloud ("cvo") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.



Para obtener instrucciones paso a paso de ejemplo sobre la configuración de SnapCenter y la replicación de datos, consulte "Configurar la replicación con SnapCenter"

Revisión de la protección de SQL VM con SnapCenter

Configurar los hosts GCVE y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar un SDDC son el tamaño del clúster SDDC en la solución GCVE y durante cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

El servicio Cloud Volume de NetApp para almacén de datos NFS y las bases de datos y el registro Cloud Volumes ONTAP para SQL pueden implementarse en cualquier VPC y GCVE deben tener conexión privada con ese VPC para montar almacén de datos NFS y tener conexión de máquinas virtuales a LUN de iSCSI.

Para configurar GCVE SDDC, consulte "Poner en marcha y configurar el entorno de virtualización en Google Cloud Platform (GCP)". Como requisito previo, compruebe que los equipos virtuales invitados que residen en los hosts GCVE pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de las cargas de trabajo en las instalaciones en GCVE (máquinas virtuales con VMDK de aplicación y máquinas virtuales con almacenamiento en invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de los volúmenes de aplicación en Cloud Volumes ONTAP.

Instale Veeam Components

Según el escenario de implementación, se debe poner en marcha el servidor de backup de Veeam, el repositorio de backup y el proxy de backup. En este caso de uso, no es necesario poner en marcha el almacén de objetos para Veeam y tampoco se requiere ningún repositorio de escalado horizontal.
"Consulte la documentación de Veeam para conocer el procedimiento de instalación"
Para obtener más información, consulte "Migración con Veeam Replication"

Configure la replicación de VM con Veeam

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam.
"Configure el trabajo de replicación de máquina virtual de vSphere" En el asistente Guest Processing, seleccione Desactivar el procesamiento de aplicaciones, ya que utilizará SnapCenter para los procesos de backup y recuperación con reconocimiento de aplicaciones.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Conmutación al nodo de respaldo de Microsoft SQL Server VM

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.

- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
  - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.
  - Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
  - Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.
- La replicación de Veeam permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

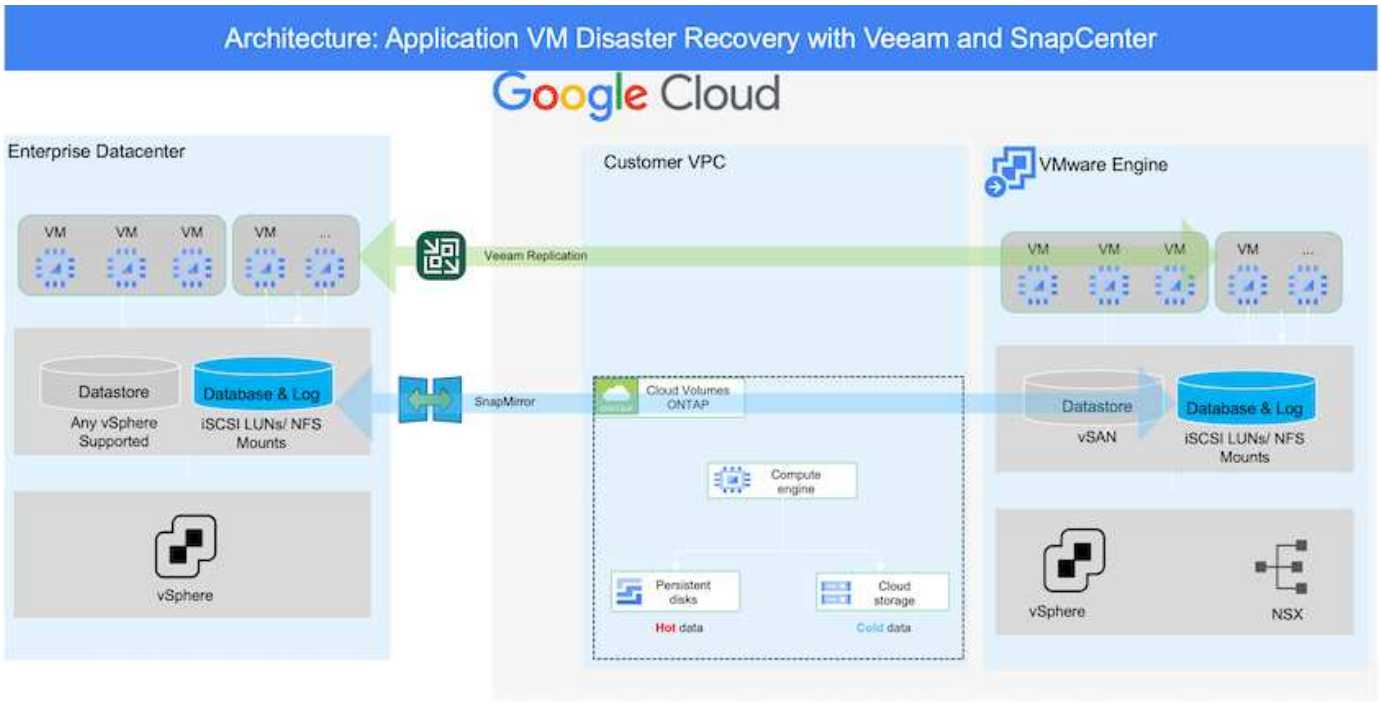
Recuperación ante desastres de aplicaciones con replicación de SnapCenter, Cloud Volumes ONTAP y Veeam

Autores: Suresh Thoppay, NetApp

Descripción general

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por datos como ransomware. Con SnapMirror de NetApp, las cargas de trabajo de VMware en las instalaciones que utilizan el almacenamiento conectado a invitado se pueden replicar a Cloud Volumes ONTAP de NetApp que se ejecuta en Google Cloud. Así se tratan los datos de aplicaciones; sin embargo, ¿qué ocurre con los equipos virtuales mismos? La recuperación ante desastres debería cubrir todos los componentes dependientes, incluidos equipos virtuales, VMDK, datos de aplicaciones, etc. Para ello, se puede utilizar SnapMirror y Veeam para recuperar sin problemas cargas de trabajo replicadas de las instalaciones a Cloud Volumes ONTAP a la vez que se utiliza almacenamiento VSAN para VMDK de máquinas virtuales.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, Veeam y Google Cloud VMware Engine (GCVE) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con las aplicaciones.

> Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice las opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Google Cloud para conocer el método de conectividad apropiado de las instalaciones a Google.

Implementar la solución DR

Descripción general de la puesta en marcha de soluciones

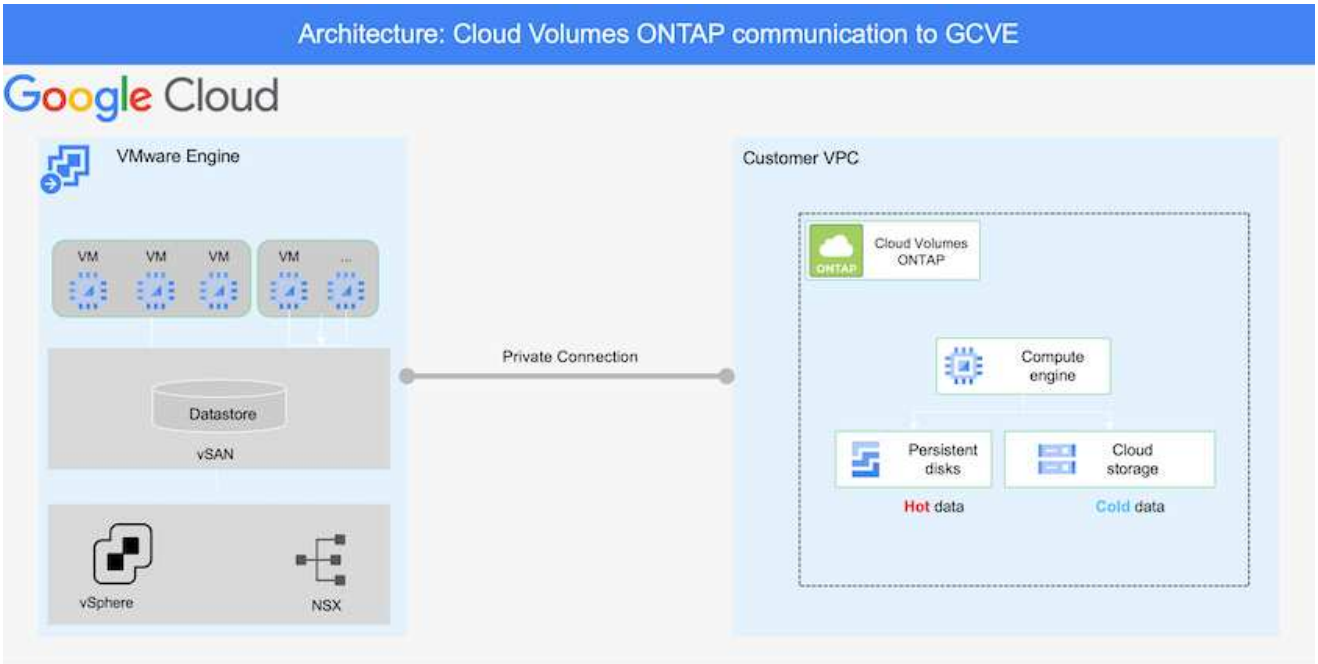
1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisione Cloud Volumes ONTAP con el tamaño de instancia correcto usando Cloud Manager dentro de la suscripción y la red virtual adecuadas.
   a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.
   b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.

3. Instale el software Veeam y empiece a replicar máquinas virtuales a la instancia de Google Cloud VMware Engine.
4. Durante un evento de desastre, rompa la relación de SnapMirror mediante Cloud Manager y active la conmutación al nodo de respaldo de máquinas virtuales con Veeam.
   a. Vuelva a conectar las LUN ISCSI y los montajes NFS para los equipos virtuales de la aplicación.
   b. Ponga en marcha aplicaciones en línea.
5. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Google Cloud y replicar volúmenes a CVO

El primer paso es configurar Cloud Volumes ONTAP en Google Cloud ("cvo") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.



Para obtener instrucciones paso a paso de ejemplo sobre la configuración de SnapCenter y la replicación de datos, consulte "Configurar la replicación con SnapCenter"

Configurar la replicación con SnapCenter

Configurar los hosts GCVE y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar un SDDC son el tamaño del clúster SDDC en la solución GCVE y durante cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

Cloud Volumes ONTAP se puede implementar en cualquier VPC y GCVE debe tener una conexión privada a ese VPC para que la máquina virtual se conecte a los LUN de iSCSI.

Para configurar GCVE SDDC, consulte "Poner en marcha y configurar el entorno de virtualización en Google Cloud Platform (GCP)". Como requisito previo, compruebe que los equipos virtuales invitados que residen en los hosts GCVE pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de las cargas de trabajo en las instalaciones en GCVE (máquinas virtuales con VMDK de aplicación y máquinas virtuales con almacenamiento en invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de los volúmenes de aplicación en Cloud Volumes ONTAP.

Instale Veeam Components

Según el escenario de implementación, se debe poner en marcha el servidor de backup de Veeam, el repositorio de backup y el proxy de backup. En este caso de uso, no es necesario poner en marcha el almacén de objetos para Veeam y tampoco se requiere ningún repositorio de escalado horizontal.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Consulte la documentación de Veeam para conocer el procedimiento de instalación"]

Configure la replicación de VM con Veeam

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam. "Configure el trabajo de replicación de máquina virtual de vSphere" En el asistente Guest Processing, seleccione Desactivar el procesamiento de aplicaciones, ya que utilizará SnapCenter para los procesos de backup y recuperación con reconocimiento de aplicaciones.

Configure el trabajo de replicación de máquina virtual de vSphere

Conmutación al nodo de respaldo de Microsoft SQL Server VM

Conmutación al nodo de respaldo de Microsoft SQL Server VM

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.
- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de

aplicaciones.

- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
  - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.
  - Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
  - Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.
- La replicación de Veeam permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

Migrar cargas de trabajo en GCP / GCVE

Migre cargas de trabajo al almacén de datos de Cloud Volume Service de NetApp en Google Cloud VMware Engine mediante la guía de inicio rápido de VMware HCX

Autores: Ingeniería de soluciones de NetApp

Descripción general: Migrar máquinas virtuales con VMware HCX, almacenes de datos de Cloud Volume Service de NetApp y Google Cloud VMware Engine (GCVE)

Uno de los casos de uso más comunes de los almacenes de datos de Google Cloud VMware Engine y Cloud Volume Service es la migración de las cargas de trabajo de VMware. HCX de VMware es la opción preferida y ofrece diversos mecanismos de migración para mover las máquinas virtuales (VM) locales y sus datos a los almacenes de datos NFS de Cloud Volume Service.

VMware HCX es principalmente una plataforma de migración diseñada para simplificar la migración de aplicaciones, el reequilibrado de las cargas de trabajo e incluso la continuidad de negocio entre clouds. Se incluye como parte de Google Cloud VMware Engine Private Cloud y ofrece muchas formas de migrar cargas de trabajo y se puede utilizar para operaciones de recuperación ante desastres.

Este documento proporciona orientación paso a paso para aprovisionar el almacén de datos de Cloud Volume Service seguido de la descarga, la puesta en marcha y la configuración de VMware HCX, incluidos todos sus componentes principales en las instalaciones y Google Cloud VMware Engine, que incluye interconexión, extensión de red y optimización de WAN para habilitar diversos mecanismos de migración de máquinas virtuales.

VMware HCX funciona con cualquier tipo de almacén de datos, ya que la migración se realiza a nivel de equipo virtual. Por lo tanto, este documento es aplicable a clientes existentes de NetApp y clientes que no son de NetApp que planeen poner en marcha Cloud Volume Service con Google Cloud VMware Engine para una puesta en marcha de cloud VMware rentable.

Escalones de alto nivel

Esta lista contiene 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 on-premises:

1. Prepare HCX a través del portal Google VMware Engine.
2. Descargue e implemente el instalador de HCX Connector Open Virtualization Appliance (OVA) en VMware vCenter Server en las instalaciones.
3. Active HCX con la clave de licencia.
4. Empareje el conector VMware HCX en las instalaciones con Google Cloud VMware Engine HCX Cloud Manager.
5. Configure el perfil de red, el perfil de computación y la malla de servicio.
6. (Opcional) lleve a cabo la extensión de red para evitar la reIP durante las migraciones.
7. Valide el estado del dispositivo y asegúrese de que la migración sea posible.
8. Migrar las cargas de trabajo de la máquina virtual.

Requisitos previos

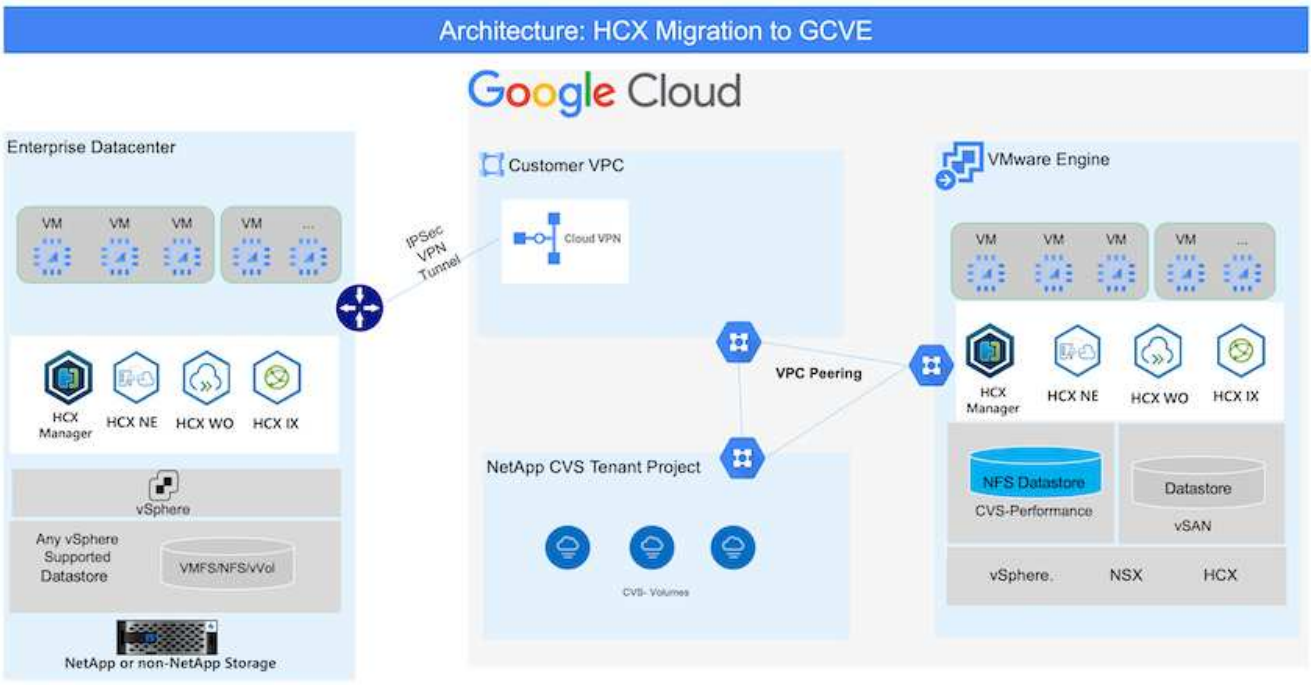
Antes de empezar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte este tema "enlace". Una vez que se hayan establecido los requisitos previos, incluida la conectividad, descargue la clave de licencia de HCX del portal Google Cloud VMware Engine. Después de descargar el instalador de OVA, continúe con el proceso de instalación como se describe a continuación.

> HCX Advanced es la opción predeterminada y VMware HCX Enterprise Edition también está disponible a través de un ticket de soporte y se admite sin coste adicional. Consulte "este enlace"

- Utilice un centro de datos definido por software (SDDC) de Google Cloud VMware Engine o cree un cloud privado utilizando este método "Enlace a NetApp" o esto "Vínculo de Google".
- La migración de equipos virtuales y datos asociados desde el centro de datos integrado con VMware vSphere en las instalaciones requiere conectividad de red del centro de datos al entorno SDDC. Antes de migrar cargas de trabajo, "Configure una conexión de Cloud VPN o de Cloud Interconnect" entre el entorno local y el cloud privado correspondiente.
- La ruta de red desde el entorno local de VMware vCenter Server al cloud privado de Google Cloud VMware Engine debe admitir la migración de las máquinas virtuales mediante vMotion.
- Asegúrese de que es necesario "reglas y puertos del firewall" Se permiten para el tráfico de vMotion entre la instancia local de vCenter Server y SDDC vCenter.
- El volumen de NFS de Cloud Volume Service debe montarse como un almacén de datos en Google Cloud VMware Engine. Siga los pasos detallados en este documento "enlace" Para conectar almacenes de datos de Cloud Volume Service a los hosts de Google Cloud VMware Engines.

Arquitectura de alto nivel

Para realizar las pruebas, el entorno de laboratorio de las instalaciones que se emplean para esta validación se conectó a través de una VPN de cloud que permite la conectividad local con Google Cloud VPC.



Para obtener un diagrama más detallado del HCX, consulte "Enlace de VMware"

Puesta en marcha de la solución

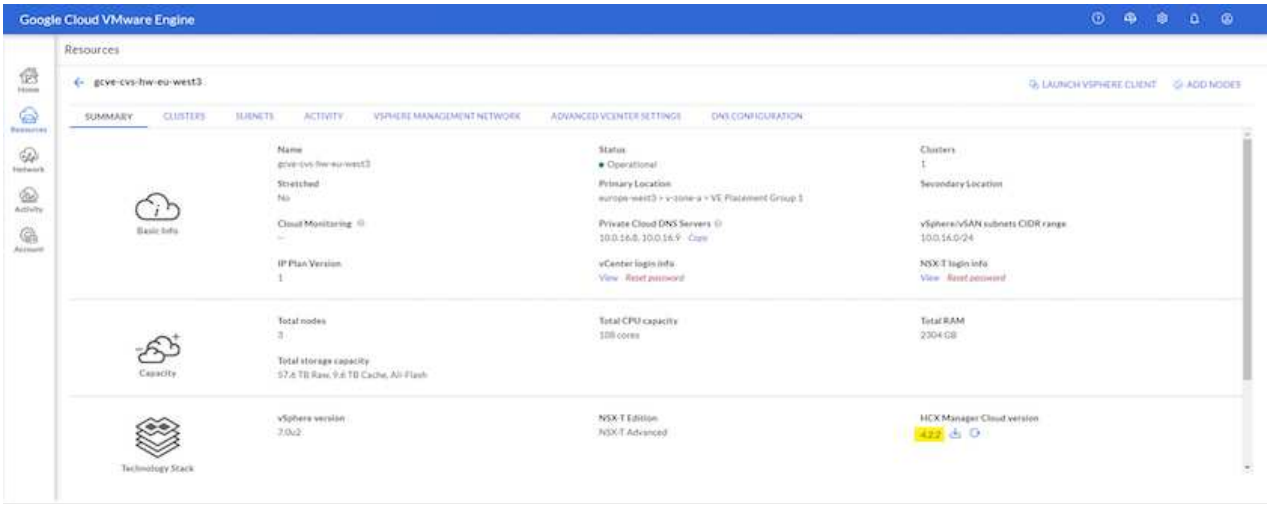
Siga la serie de pasos para completar la implementación de esta solución:

Paso 1: Preparación del HCX a través del portal Google VMware Engine

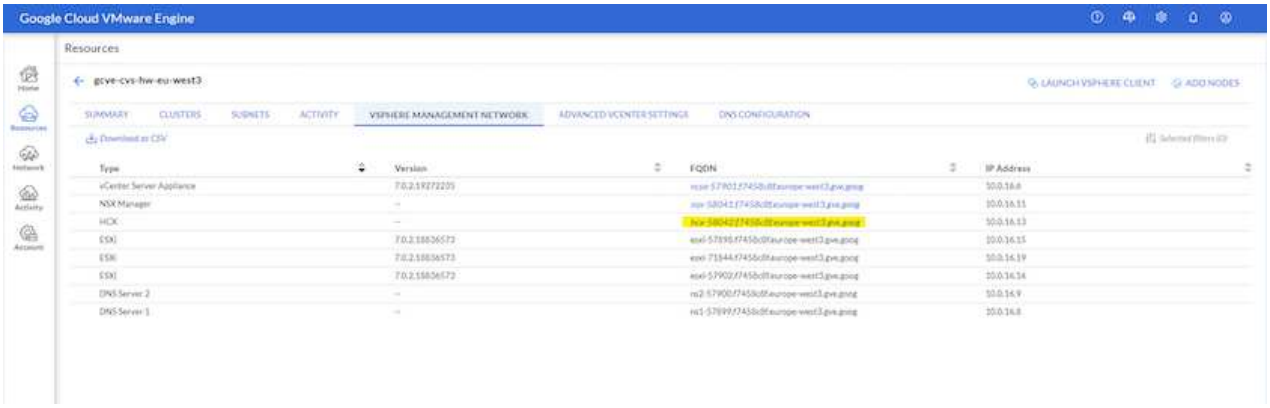
El componente DE HCX Cloud Manager se instala automáticamente a medida que aprovisiona el cloud privado con VMware Engine. Para preparar el emparejamiento de sitios, lleve a cabo los siguientes pasos:

1. Inicie sesión en el portal Google VMware Engine e inicie sesión en HCX Cloud Manager.

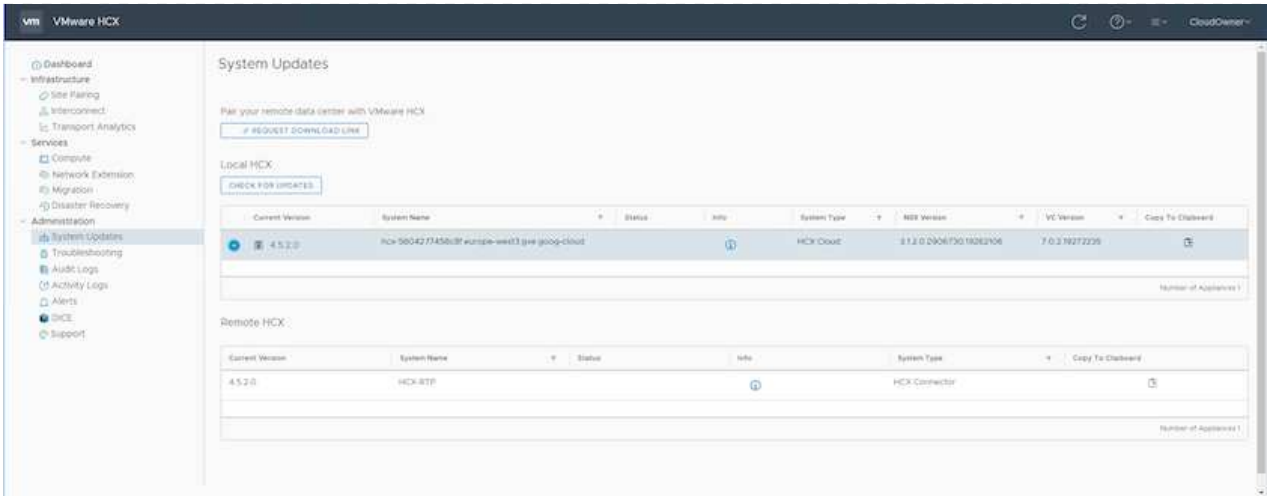
   Puede iniciar sesión en la consola HCX haciendo clic en el enlace de la versión HCX



   O bien, haga clic en HCX FQDN en la pestaña vSphere Management Network.



2. En HCX Cloud Manager, vaya a **Administración > actualizaciones del sistema**.
3. Haga clic en **solicitar enlace de descarga** y descargue el archivo OVA.



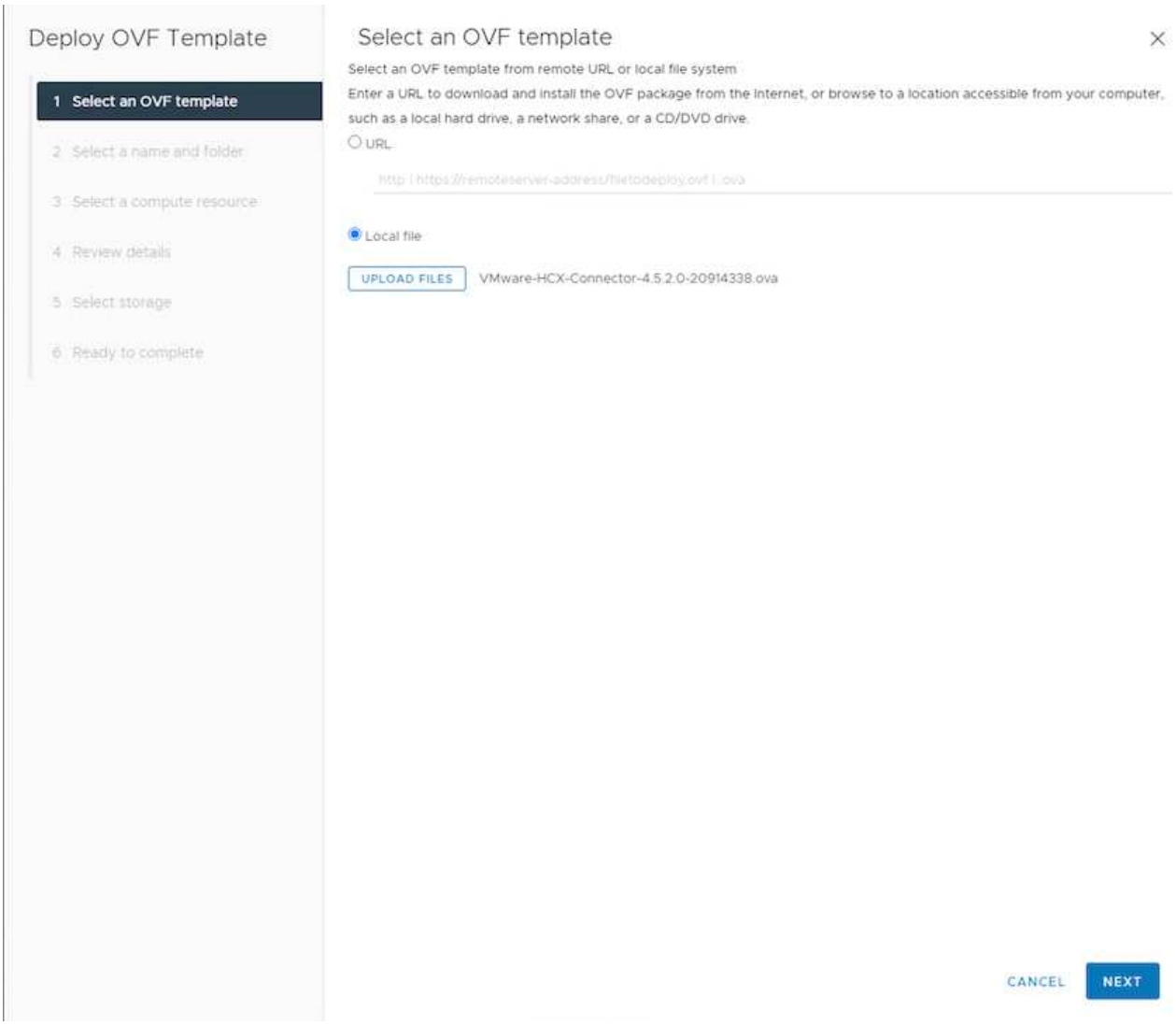
4. Actualice HCX Cloud Manager a la última versión disponible desde la interfaz de usuario de HCX Cloud Manager.

Paso 2: Ponga en marcha el OVA del instalador en la instancia local de vCenter Server

Para que el conector local se conecte al HCX Manager en Google Cloud VMware Engine, asegúrese de que los puertos de firewall adecuados están abiertos en el entorno local.

Para descargar e instalar el conector HCX en el vCenter Server local, complete los siguientes pasos:

1. Haga que la ova se descargue de la consola HCX en Google Cloud VMware Engine como se indica en el paso anterior.
2. Una vez descargado el OVA, póngalo en marcha en el entorno local de VMware vSphere mediante la opción **implementar plantilla OVF**.



3. Introduzca toda la información necesaria para la implementación de OVA, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar** para implementar el OVA del conector HCX de VMware.

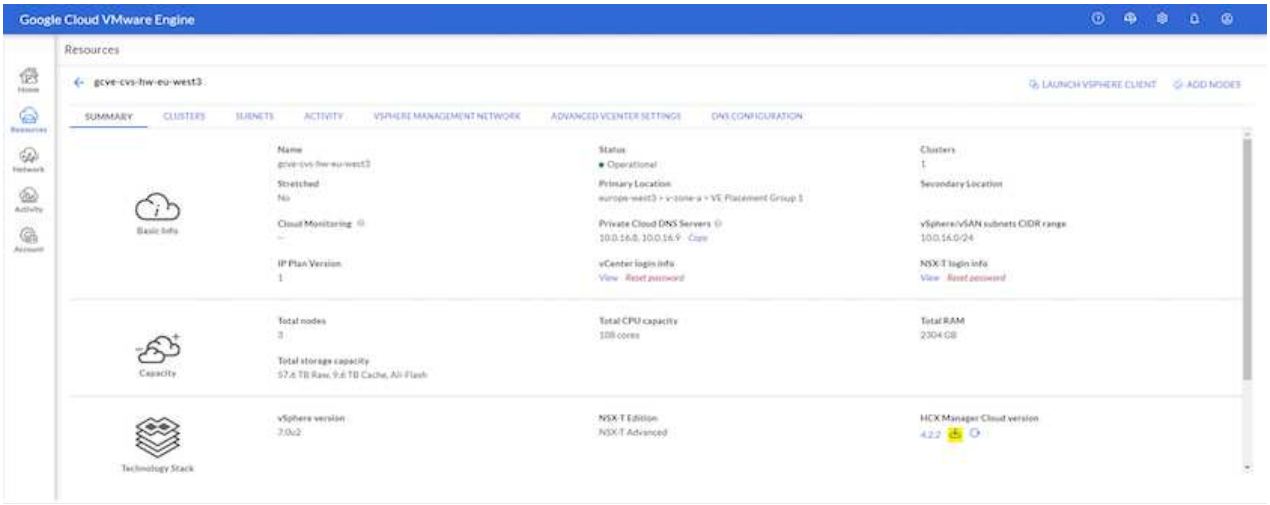
Encienda el dispositivo virtual manualmente.

Para obtener instrucciones paso a paso, consulte "Guía del usuario de VMware HCX".

Paso 3: Active el conector HCX con la clave de licencia

Después de implementar el OVA del conector HCX de VMware en las instalaciones e iniciar el dispositivo, lleve a cabo los siguientes pasos para activar el conector HCX. Genere la clave de licencia desde el portal Google Cloud VMware Engine y actívela en VMware HCX Manager.

1. En el portal VMware Engine, haga clic en Resources, seleccione la nube privada y **haga clic en el icono de descarga en HCX Manager Cloud Version**
.



Abra el archivo descargado y copie la cadena de claves de licencia.

2. Inicie sesión en el VMware HCX Manager local en "https://hcxmanagerIP:9443" uso de las credenciales de administrador.

> Utilice hcxmanagerIP y la contraseña definidos durante la implementación de OVA.

3. En la licencia, introduzca la clave copiada del paso 3 y haga clic en **Activar**.

> El conector HCX de las instalaciones debe tener acceso a Internet.

4. En **Datacenter Location**, proporcione la ubicación más cercana para instalar el 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 **Conecte 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.

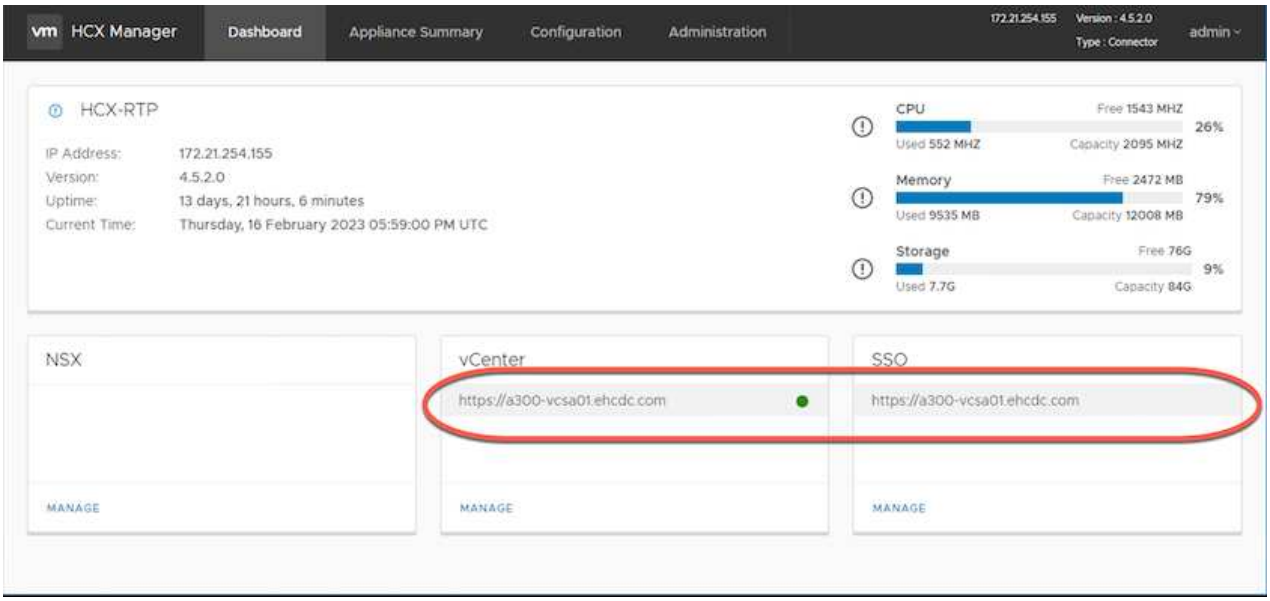
8. En **Configurar SSO/PSC**, proporcione el FQDN o la dirección IP del controlador de servicios de plataforma (PSC) y haga clic en **continuar**.

> Para el PSC integrado, introduzca el FQDN de VMware vCenter Server o la dirección IP.

9. Compruebe que la información introducida es correcta y haga clic en **Reiniciar**.

10. Después de reiniciar los servicios, vCenter Server se muestra como verde en la página que aparece. Tanto vCenter Server como SSO deben tener los parámetros de configuración adecuados, que deben ser los mismos que los de la página anterior.

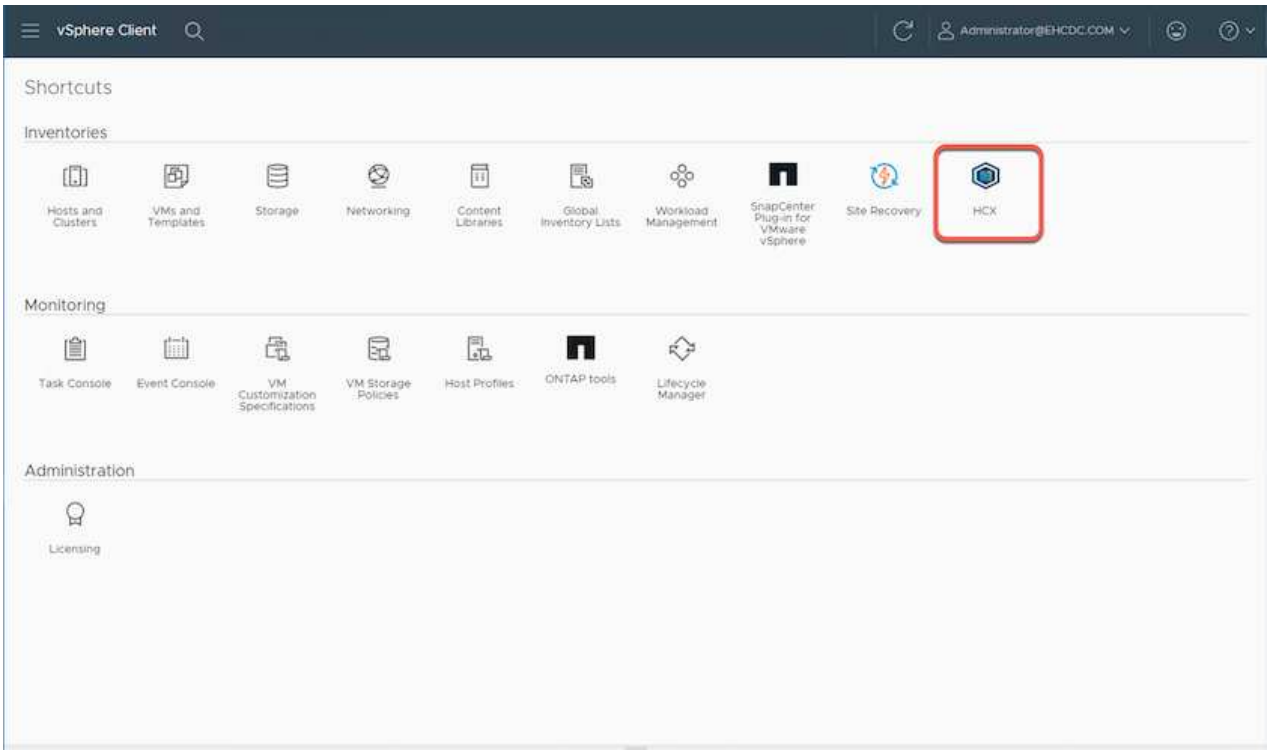
> Este proceso debe tardar aproximadamente de 10 a 20 minutos y el plugin se añadirá a vCenter Server.



Paso 4: Emparejar el conector VMware HCX en las instalaciones con Google Cloud VMware Engine HCX Cloud Manager

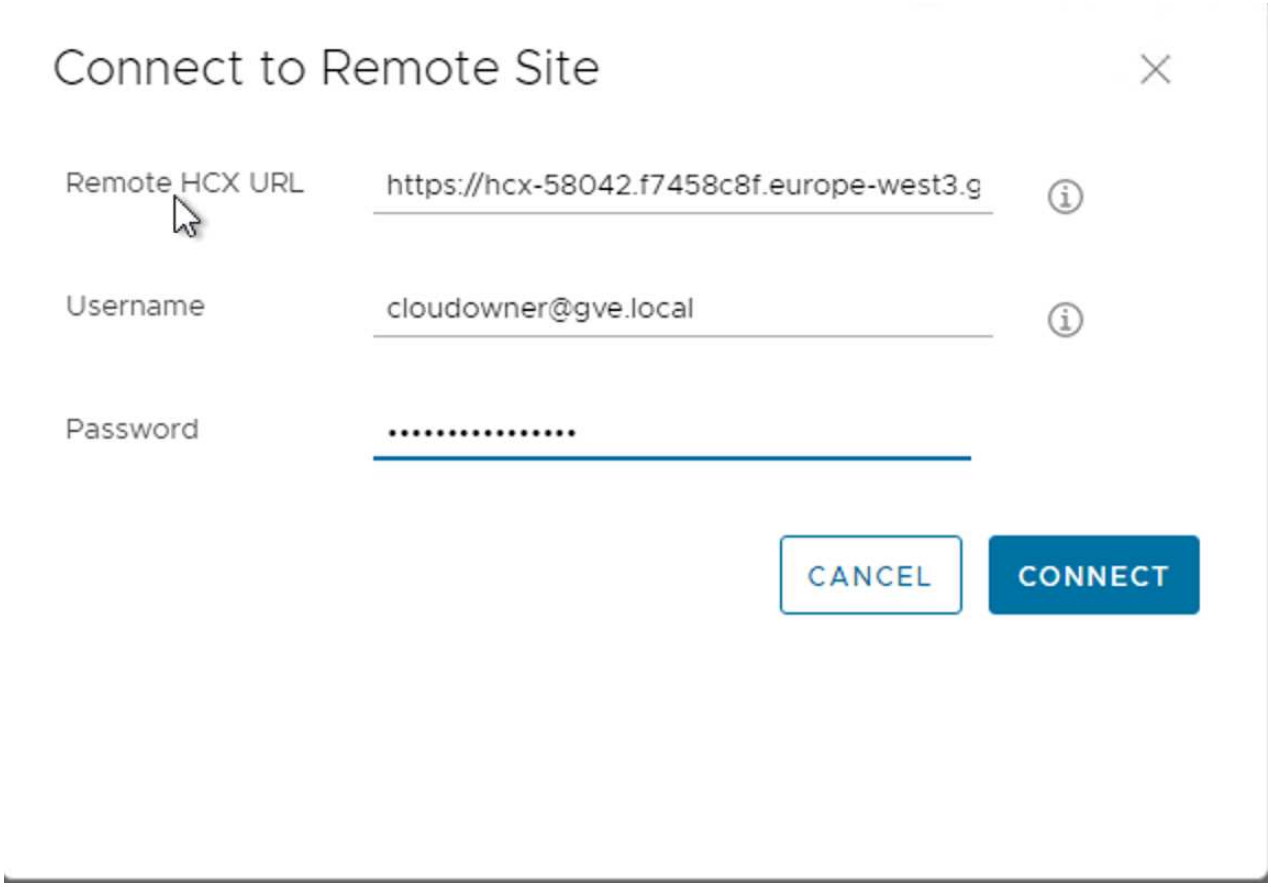
Después de implementar y configurar el conector HCX en el vCenter local, establezca la conexión con Cloud Manager añadiendo el emparejamiento. Para configurar el emparejamiento de sitios, lleve a cabo los siguientes pasos:

1. Para crear una pareja de sitios entre el entorno local de vCenter y el motor SDDC de Google Cloud VMware, inicie sesión en la instancia local de vCenter Server y acceda al nuevo complemento HCX vSphere Web Client.



2. En Infraestructura, haga clic en **Agregar un emparejamiento de sitios**.

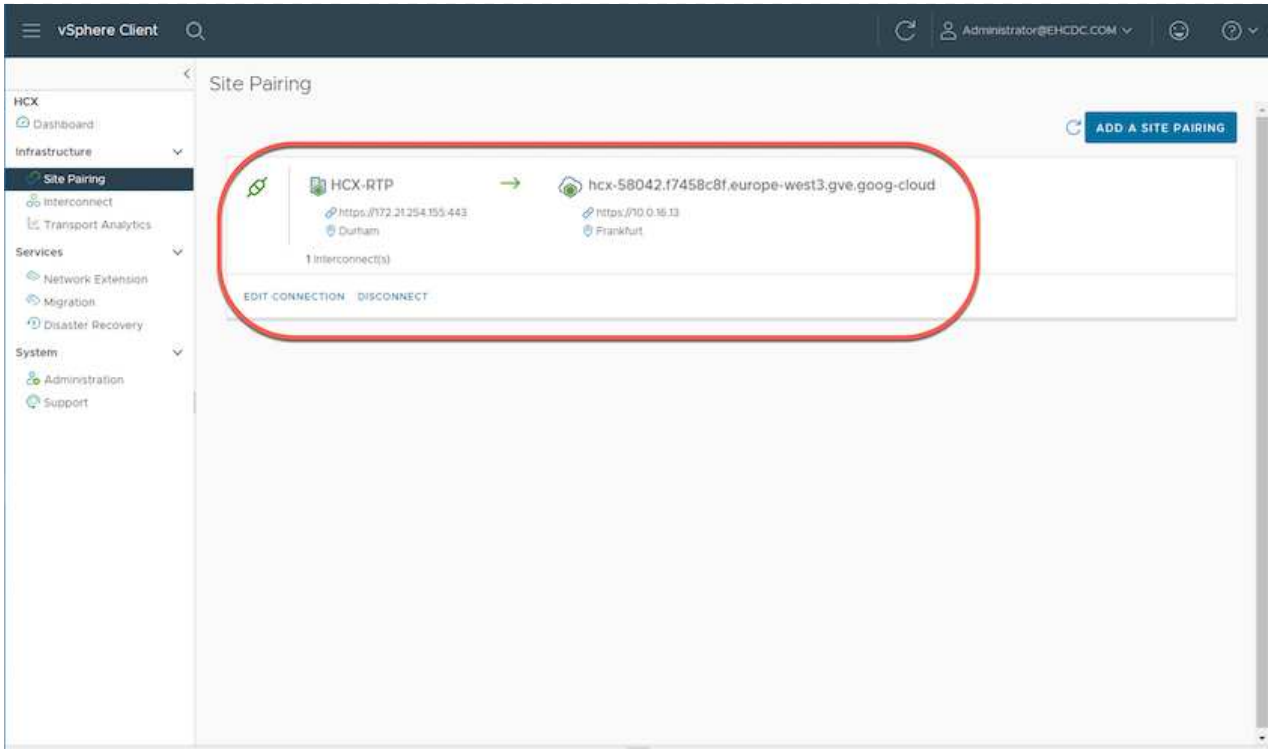
Introduzca la dirección URL o dirección IP de HCX Cloud Manager de Google Cloud Engine y las credenciales para el usuario con privilegios de rol de propietario de cloud para acceder al cloud privado.



3. Haga clic en **conectar**.

> El conector HCX de VMware debe poder enrutar a HCX Cloud Manager IP a través del puerto 443.

4. Una vez creado el emparejamiento, el emparejamiento de sitios recién configurado está disponible en el panel de HCX.

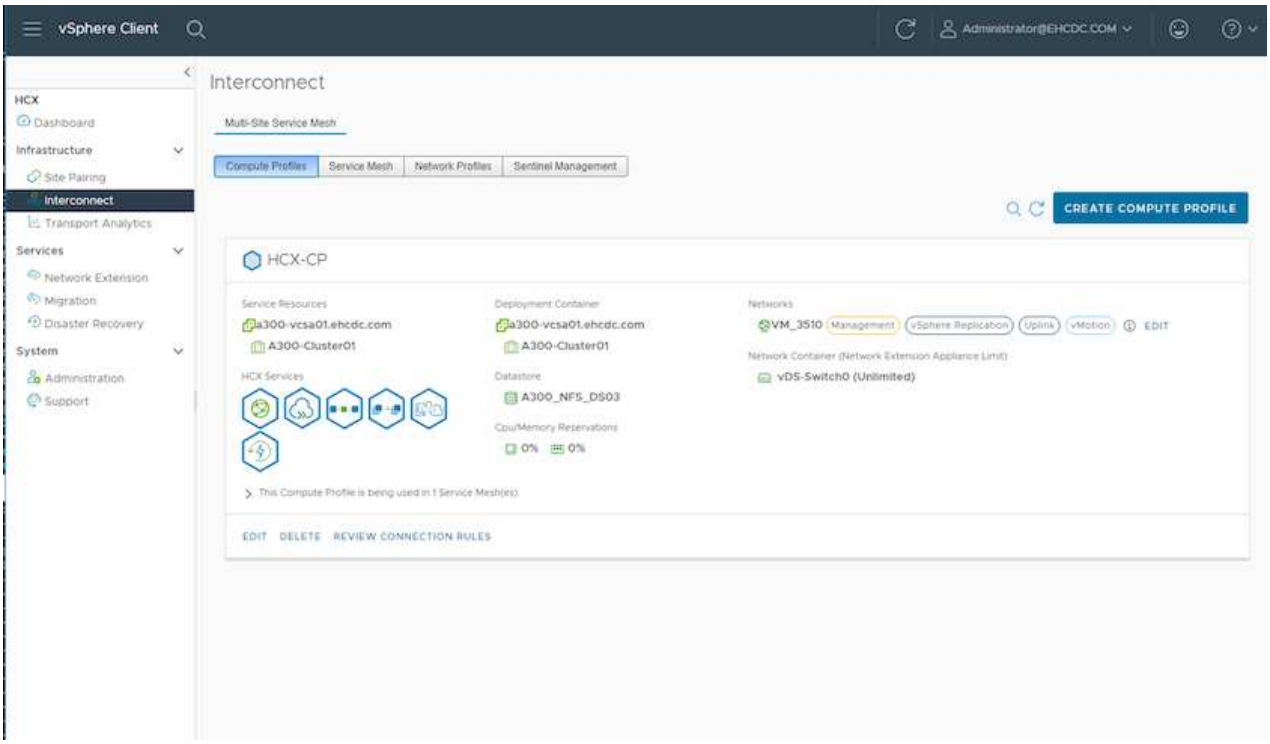

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

Paso 5: Configure el perfil de red, el perfil de computación y la malla de servicio

El dispositivo de servicio VMware HCX Interconnect proporciona funcionalidades de replicación y migración basada en vMotion a través de Internet y conexiones privadas al sitio de destino. La interconexión ofrece cifrado, ingeniería de tráfico y movilidad de máquinas virtuales. Para crear un dispositivo de servicio de interconexión, lleve a cabo los siguientes pasos:

1. En Infraestructura, seleccione **interconexión > malla de servicio multisitio > Perfiles de computación > Crear perfil de computación**.

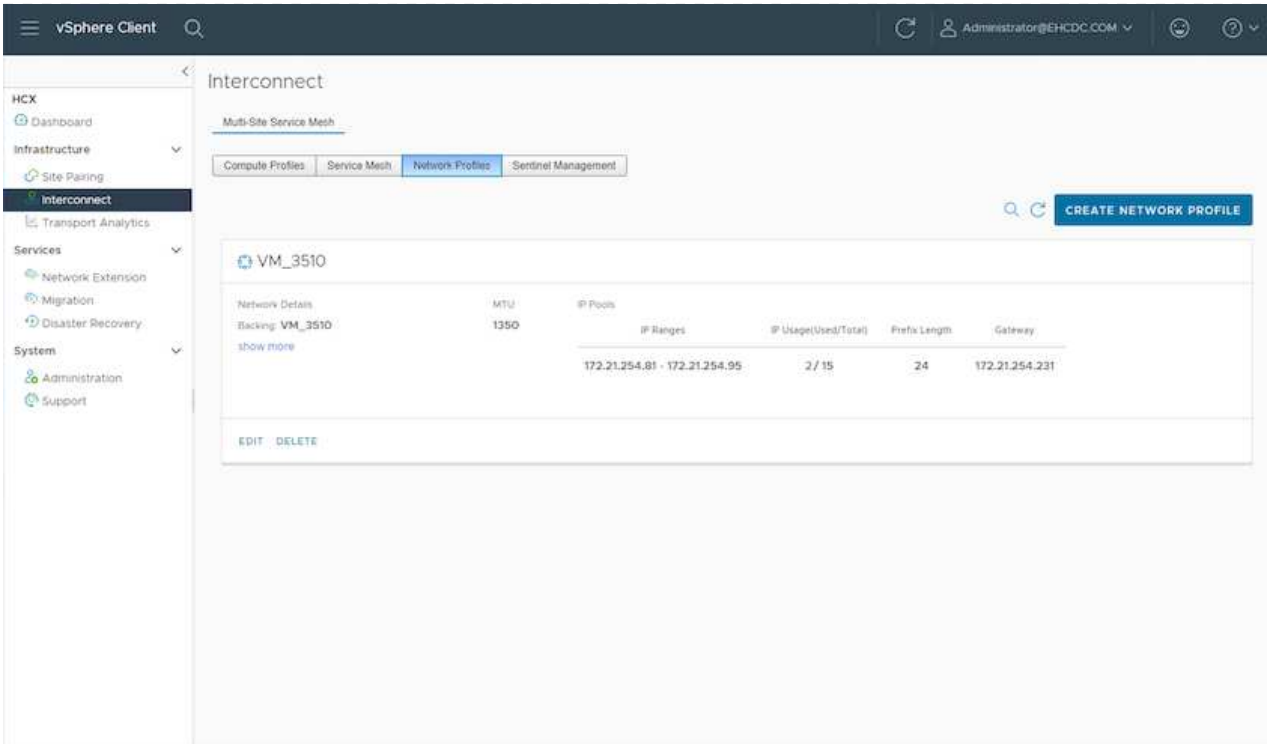
   Los perfiles informáticos definen los parámetros de implementación, incluidos los dispositivos que se implementan y qué parte del centro de datos de VMware puede acceder al servicio HCX.



2. Después de crear el perfil de computación, cree los perfiles de red seleccionando **malla de servicio multisitio > Perfiles de red > Crear perfil de red**.

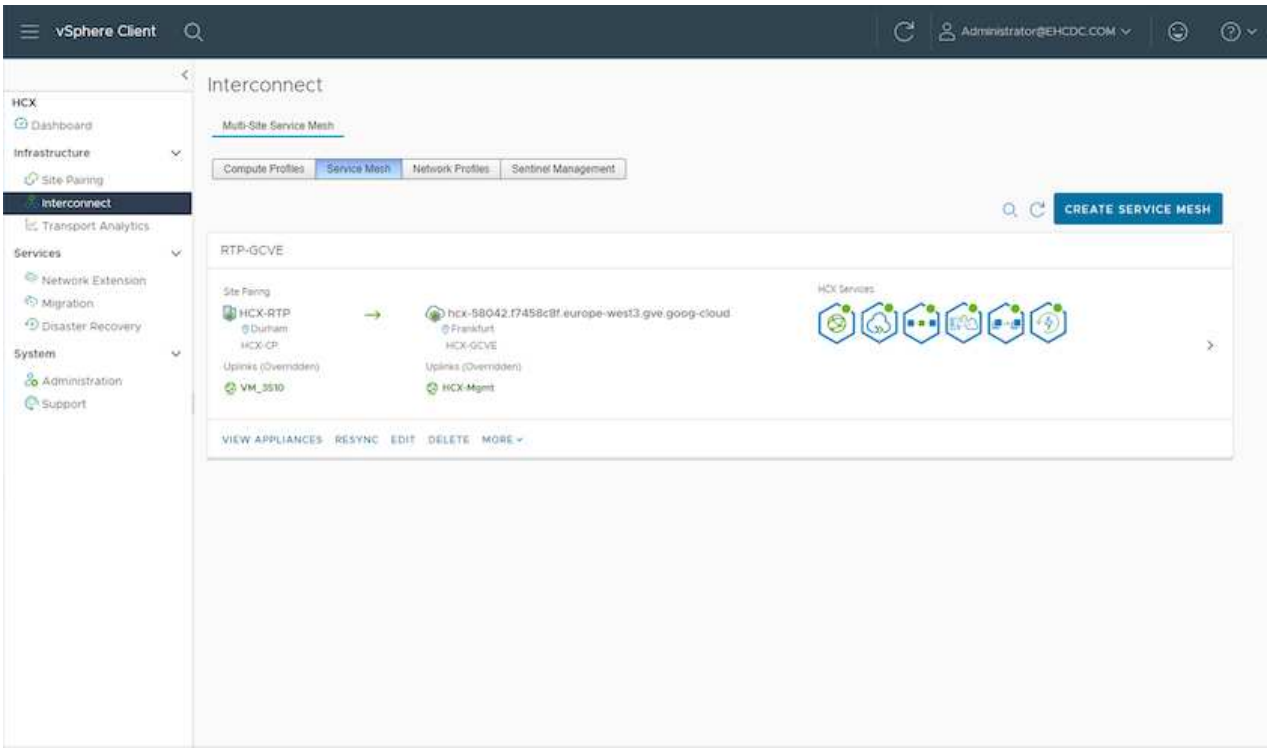
   El perfil de red define un rango de direcciones IP y redes que utiliza HCX para sus dispositivos virtuales.

   Este paso requiere dos o más direcciones IP. Estas direcciones IP se asignan desde la red de gestión a los dispositivos de interconexión.

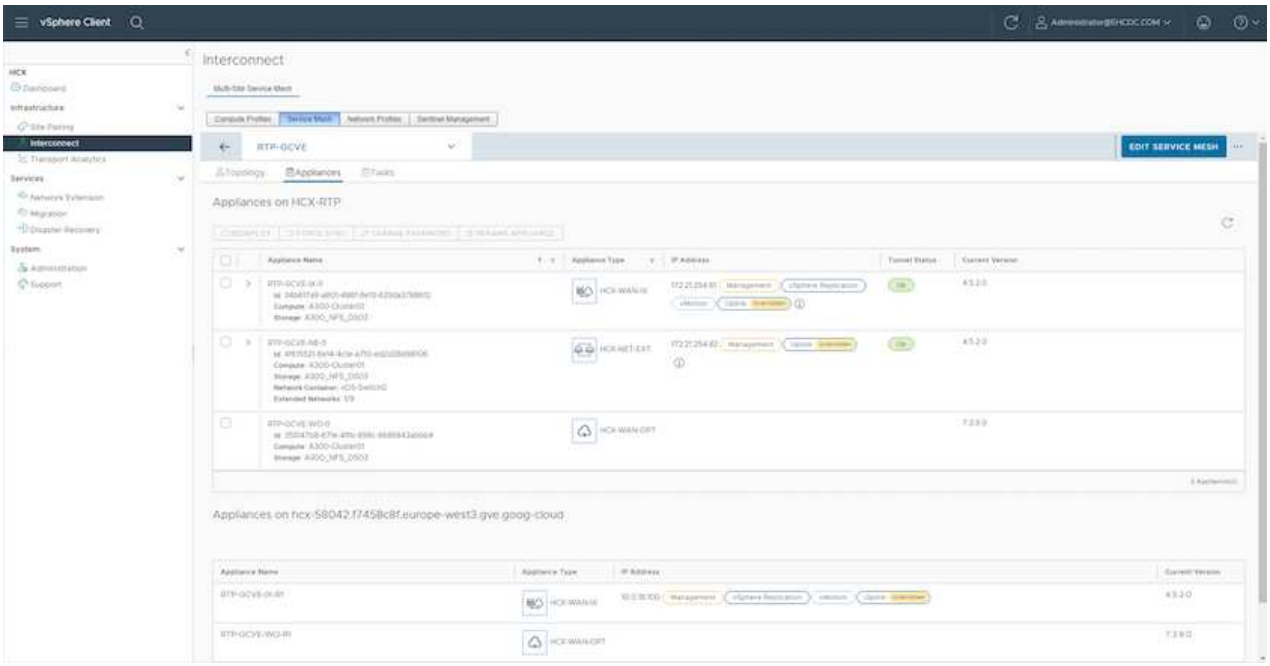


3. En este momento, se han creado correctamente los perfiles de computación y red.
4. Cree la malla de servicio seleccionando la pestaña **malla de servicio** en la opción **interconexión** y seleccione los sitios SDDC en las instalaciones y GCVE.
5. La malla de servicio especifica una pareja de perfiles de red y de computación local y remota.

Como parte de este proceso, los dispositivos HCX se implementan y se configuran automáticamente tanto en los sitios de origen como en los de destino con el fin de crear una estructura de transporte segura.



6. Este es el paso final de la configuración. Esta operación debería tardar cerca de 30 minutos en completar la puesta en marcha. Una vez configurada la malla de servicio, el entorno está preparado con los túneles IPsec creados correctamente para migrar las VM de carga de trabajo.



Paso 6: Migrar cargas de trabajo

Las cargas de trabajo se pueden migrar de manera bidireccional entre los centros de datos de GCVE y sus instalaciones mediante diversas tecnologías de migración de VMware HCX. Los equipos virtuales se pueden mover hacia y desde entidades activadas por HCX de VMware mediante varias tecnologías de migración, como la migración masiva de HCX, HCX vMotion, migración en frío de HCX, el asistente de replicación de HCX vMotion (disponible con la edición de HCX Enterprise) y la migración asistida por SO HCX (disponible con la edición de HCX Enterprise).

Para obtener más información sobre varios mecanismos de migración de HCX, consulte "Tipos de migración HCX de VMware".

El dispositivo HCX-IX utiliza el servicio de agente de movilidad para realizar migraciones vMotion, de frío y de replicación asistida (RAV).

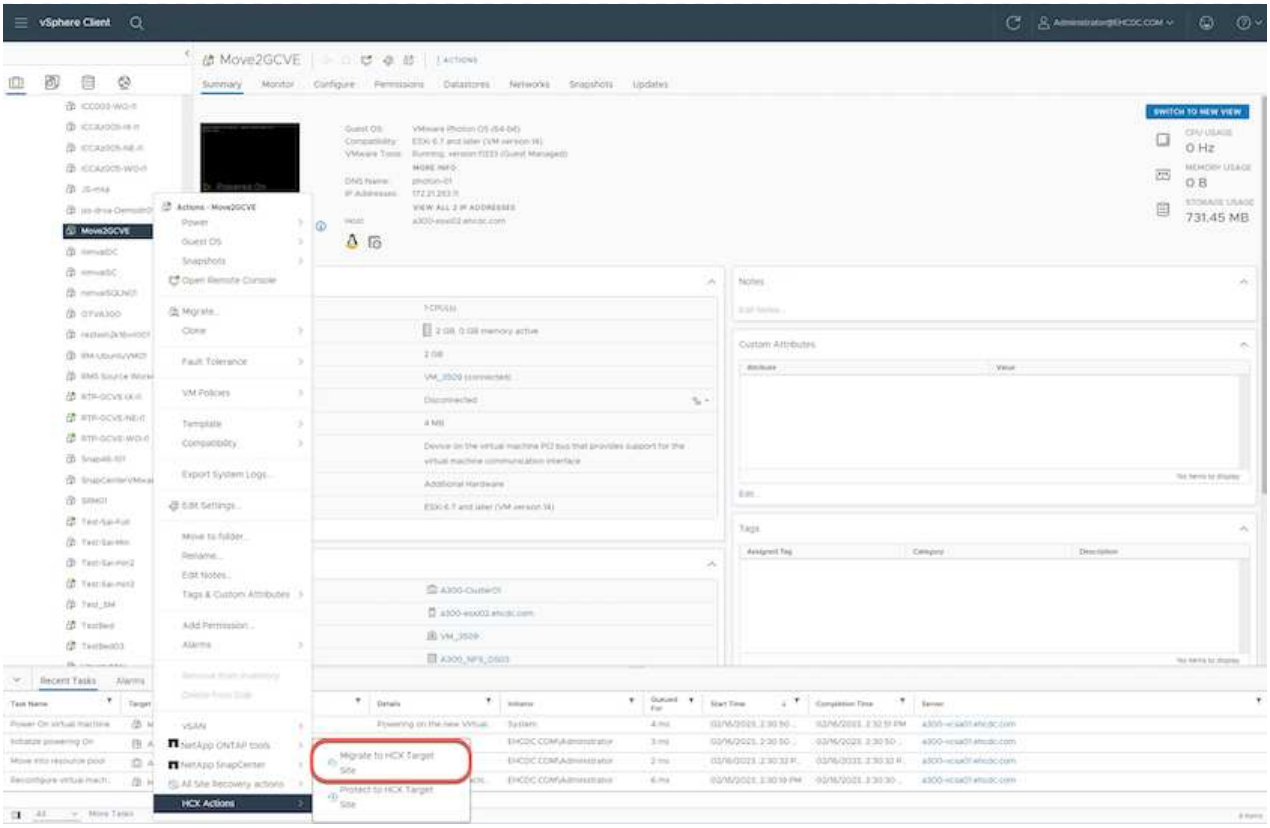
> El dispositivo HCX-IX agrega el servicio Mobility Agent como un objeto host en vCenter Server. El procesador, la memoria, los recursos de almacenamiento y redes que se muestran en este objeto no representan el consumo real en el hipervisor físico que aloja el dispositivo IX.

HCX vMotion

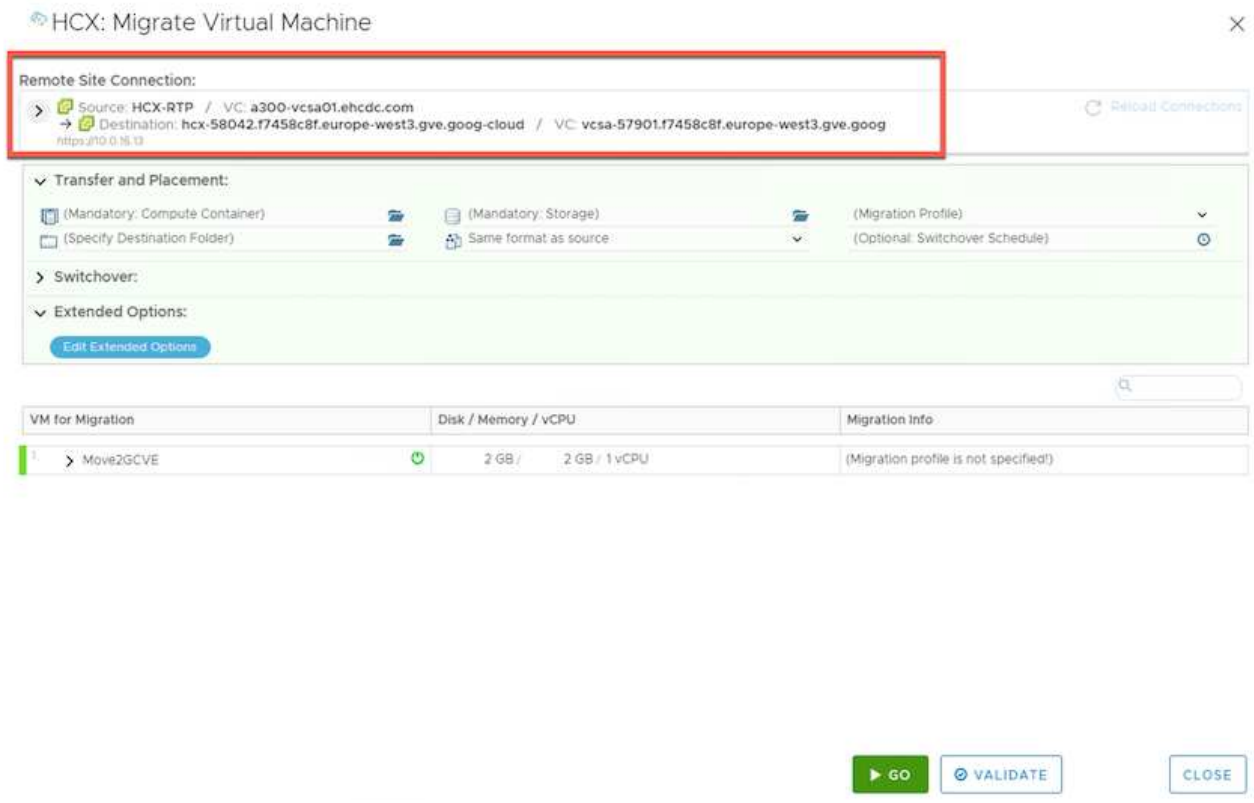
En esta sección se describe el mecanismo HCX vMotion. Esta tecnología de migración utiliza el protocolo VMware vMotion para migrar un equipo virtual a GCVE. La opción de migración de vMotion se utiliza para migrar el estado de las máquinas virtuales de una única máquina virtual a la vez. No se produce ninguna 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 máquina virtual) para migrar la máquina virtual sin necesidad de modificar la dirección IP.

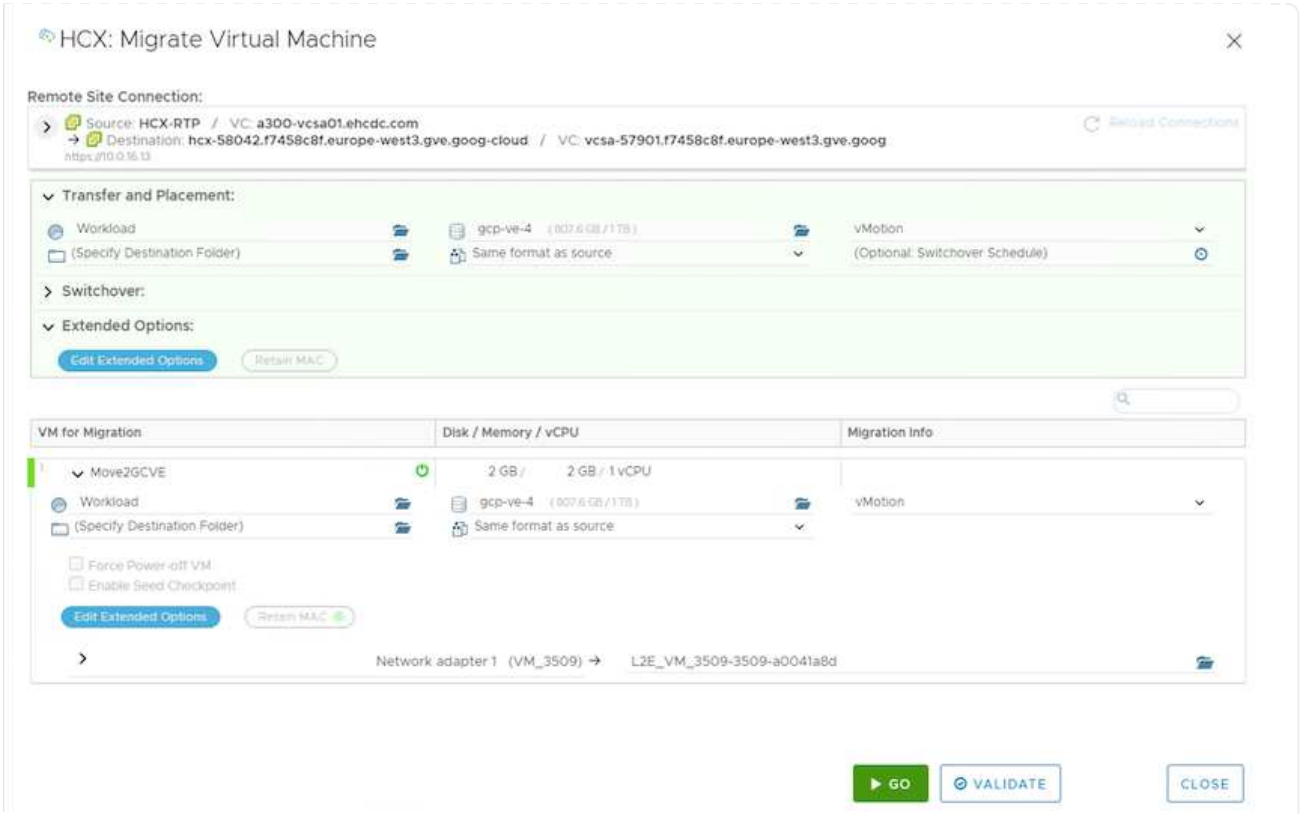
1. Desde el cliente vSphere local, vaya a Inventory, haga clic con el botón derecho en la máquina virtual que se va a migrar y seleccione HCX Actions > Migrate to HCX Target Site.



2. En el asistente Migrate Virtual Machine, seleccione Remote Site Connection (GCVE de destino).



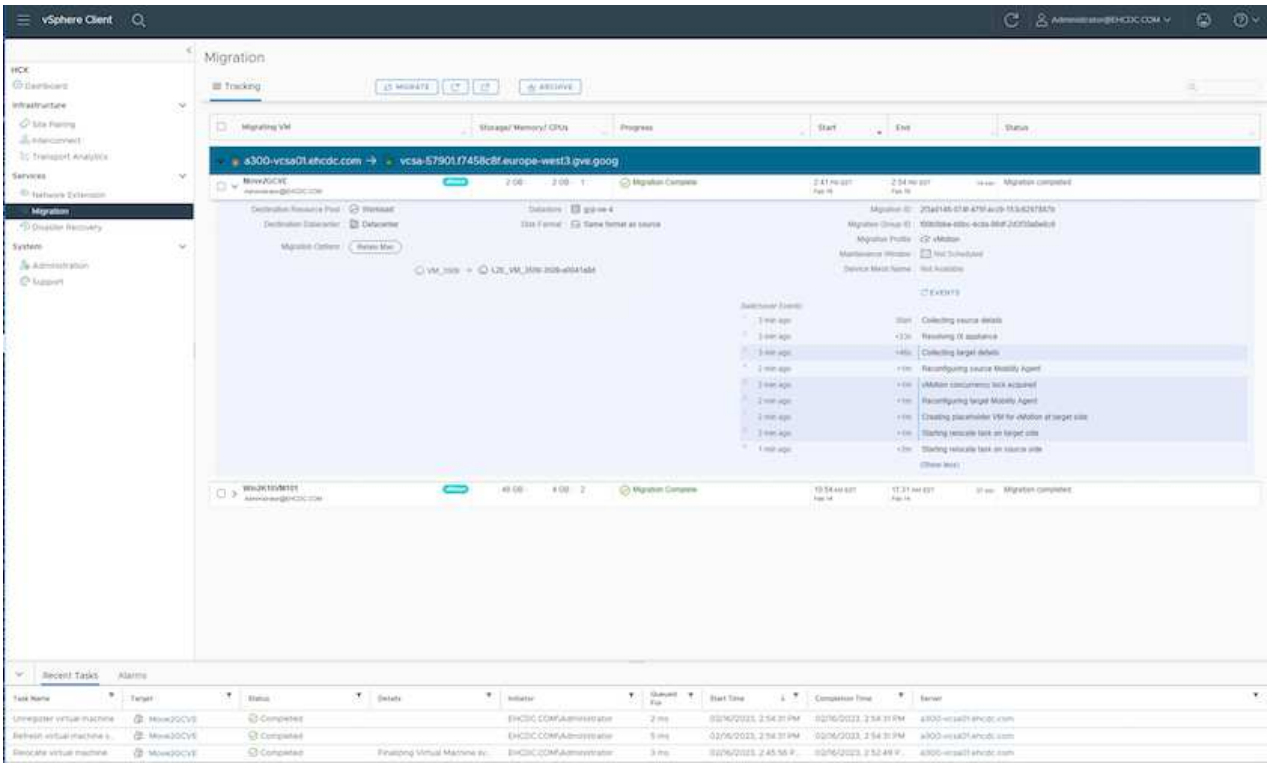
3. Actualice los campos obligatorios (clúster, almacenamiento y red de destino), haga clic en Validate.



4. Una vez finalizadas las comprobaciones de validación, haga clic en Ir para iniciar la migración.

> La transferencia de vMotion captura la memoria activa de la máquina virtual, su estado de ejecución, su dirección IP y su dirección MAC. Para obtener más información sobre los requisitos y las limitaciones de HCX vMotion, consulte "Comprender vMotion y la migración de datos fríos de VMware HCX".

5. Es posible supervisar el progreso y la finalización de vMotion desde el panel HCX > Migration.



El almacén de datos CVS NFS de destino debe tener espacio suficiente para manejar la migración.

Conclusión

Tanto si su objetivo es el cloud híbrido como el cloud, y los datos residen en un almacenamiento de cualquier tipo o proveedor en las instalaciones, Cloud Volume Service y HCX proporcionan opciones excelentes para poner en marcha y migrar las cargas de trabajo de las aplicaciones, a la vez que reduce el TCO porque los requisitos de datos se adaptan perfectamente a la capa de la aplicación. Sea cual sea el caso práctico, elija Google Cloud VMware Engine junto con Cloud Volume Service para obtener rápidamente las ventajas del cloud, una infraestructura consistente y operaciones en las instalaciones y en varios clouds, portabilidad bidireccional de cargas de trabajo, y capacidad y rendimiento de clase empresarial. Se trata del mismo proceso y procedimientos que ya conoce que se utiliza para conectar el almacenamiento y migrar máquinas virtuales mediante la replicación de VMware vSphere, VMware vMotion o incluso la copia de archivos de red (NFC).

Puntos

Los puntos clave de este documento son:

- Ahora puede usar Cloud Volume Service como almacén de datos en Google Cloud VMware Engine SDDC.
- Puede migrar datos fácilmente desde las instalaciones a un 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

- "Despliegue el conector HCX con GCVE"
- "Configure HCX ServiceMesh con GCVE"
- "Migrar VM con HCX a GCVE"

De VMware

- "Despliegue del conector HCX para GCVE"
- "Configuración DE ServiceMesh DE HCX para GCVE"
- "Migración de carga de trabajo HCX a GCVE"

Dónde encontrar información adicional

Si quiere más información sobre la información descrita en este documento, consulte los siguientes enlaces a sitios web:

- Documentación de Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Documentación de Cloud Volume Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- Guía del usuario de VMware HCX

  "https://docs.vmware.com/en/VMware-HCX/index.html"

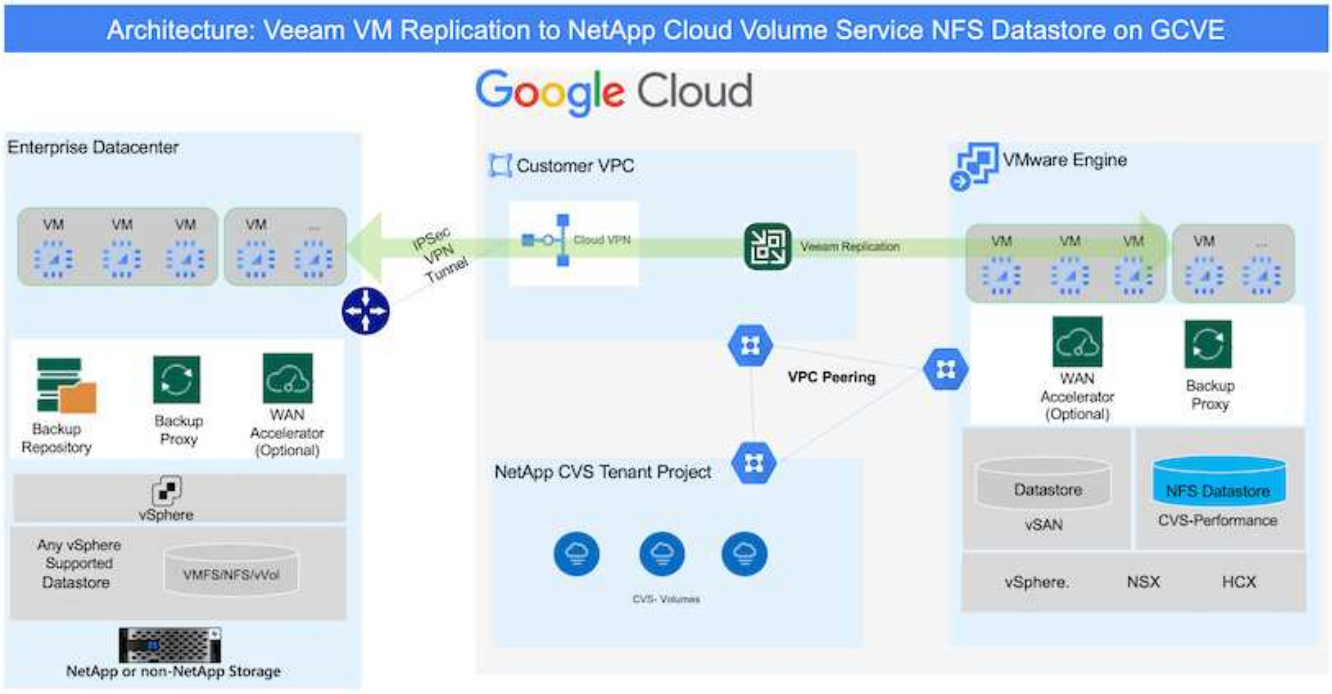
Migración de máquinas virtuales a NetApp Cloud Volume Service NFS Datastore en Google Cloud VMware Engine mediante la función de replicación de Veeam

Descripción general

Autores: Suresh Thoppay, NetApp

Las cargas de trabajo de máquinas virtuales 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 VM que utiliza el servicio Cloud Volume de NetApp, Veeam y el motor de VMware de Google Cloud (GCVE).



Supuestos

En este documento se asume que tiene Google Cloud VPN o Cloud Interconnect u otra opción de red para establecer la conectividad de red desde los servidores vSphere existentes a Google Cloud VMware Engine.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la "Documentación de Google Cloud" Para el método de conectividad de on-premises a Google adecuado.

Puesta en marcha de la solución de migración

Descripción general de la puesta en marcha de soluciones

1. Asegúrese de que el almacén de datos NFS del servicio NetApp Cloud Volume esté montado en GCVE vCenter.
2. Compruebe que Veeam Backup Recovery se implementa en el entorno de VMware vSphere existente
3. Crear trabajo de replicación para iniciar la replicación de máquinas virtuales en la instancia de Google Cloud VMware Engine.
4. Realizar failover del trabajo de replicación de Veeam.
5. Realice failover permanente en Veeam.

Detalles de la implementación

Asegúrese de que el almacén de datos NFS del servicio NetApp Cloud Volume esté montado en GCVE vCenter

Inicie sesión en GCVE vCenter y asegúrese de que el almacén de datos NFS tenga espacio suficiente disponible.
Si no es así, consulte "Monte NetApp CVS como almacén de datos NFS en GCVE"

Compruebe que Veeam Backup Recovery se implementa en el entorno de VMware vSphere existente

Consulte "Componentes de replicación de Veeam" documentación para instalar los componentes requeridos.

Crear trabajo de replicación para iniciar la replicación de máquinas virtuales en la instancia de Google Cloud VMware Engine.

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam. "Configure el trabajo de replicación de máquina virtual de vSphere"
Aquí hay un video que explica cómo hacerlo
"Configurar trabajo de replicación".

> La VM de réplica puede tener una IP diferente a la VM de origen y también puede conectarse a un grupo de puertos diferente. Para obtener más detalles, consulte el vídeo de arriba.

Realizar failover del trabajo de replicación de Veeam

Para migrar máquinas virtuales, ejecute el "Realice el failover"

Realice failover permanente en Veeam.

Para tratar a GCVE como su nuevo entorno de origen, realice "Recuperación tras fallos permanente"

Ventajas de esta solución

- La infraestructura existente de backup de Veeam puede utilizarse para la migración.
- Veeam Replication permite cambiar las direcciones IP de VM en el sitio de destino.
- Tiene la capacidad de reasignar los datos existentes replicados fuera de Veeam (como los datos replicados de BlueXP)
- Tiene capacidad para especificar diferentes grupos de puertos de red en el sitio de destino.
- Puede especificar el orden de encendido de las máquinas virtuales.
- Utiliza VMware Change Block Tracking para minimizar la cantidad de datos que se deben enviar a través de la WAN.
- Capacidad para ejecutar scripts previos y posteriores para la replicación.
- Capacidad para ejecutar scripts previos y posteriores para instantáneas.

Disponibilidad de región – almacén de datos NFS complementario para Google Cloud Platform (GCP)

El almacén de datos NFS complementario para GCVE es compatible con el servicio de volúmenes de cloud de NetApp.

> Solo se pueden usar volúmenes de CVS-Performance para el almacén de datos NFS de GCVE. Para conocer la ubicación disponible, consulte "Mapa de región global"

Google Cloud VMware Engine está disponible en las siguientes ubicaciones

Para minimizar la latencia, NetApp CVS Volume y GCVE, donde se intenta montar el volumen, deben estar en la misma zona de disponibilidad.

Trabaja con Google y NetApp Solution Architects para obtener optimizaciones de TCO y disponibilidad.

Descripción general de la seguridad: Cloud Volumes Service de NetApp (CVS) en Google Cloud

TR-4918: Descripción general de la seguridad: Cloud Volumes Service de NetApp en Google Cloud

Oliver Krause, Justin Parisi, NetApp

Alcance del documento

La seguridad, especialmente en el cloud, donde la infraestructura se encuentra fuera del control de los administradores de almacenamiento, es primordial para confiar en sus datos para ofrecer servicios ofrecidos por los proveedores de cloud. Este documento ofrece una visión general de las ofertas de seguridad de NetApp "Cloud Volumes Service proporciona en Google Cloud".

Audiencia de destino

La audiencia de destino de este documento incluye, entre otros, los siguientes roles:

- Proveedores de cloud
- Administradores de almacenamiento
- Arquitectos de almacenamiento
- Recursos sobre el terreno
- Responsables de la toma de decisiones empresariales

Si tiene alguna pregunta sobre el contenido de este informe técnico, consulte la sección "“Contacto”."

Abreviatura	Definición
CVS-SW	Cloud Volumes Service, tipo de servicio CVS
CVS-Performance	Cloud Volume Service, tipo de servicio CVS-Performance
SAL	

Cómo Cloud Volumes Service en Google Cloud protege sus datos

Cloud Volumes Service en Google Cloud ofrece múltiples formas de proteger sus datos de forma nativa.

Arquitectura segura y modelo de multi-tenancy

Cloud Volumes Service proporciona una arquitectura segura en Google Cloud al segmentar la gestión de servicios (plano de control) y el acceso a los datos (plano de datos) en diferentes extremos, de modo que ninguno de ellos puede afectar al otro (consulte la sección "“Arquitectura Cloud Volumes Service”"). Utiliza Google's. "acceso a servicios privados" (PSA) marco para prestar el servicio. Este marco distingue entre el productor de servicios, que ofrece NetApp y está gestionado por este, y el consumidor de servicios, que es un cloud privado virtual (VPC) en un proyecto de cliente, alojando los clientes que deseen acceder a recursos compartidos de archivos de Cloud Volumes Service.

En esta arquitectura, los clientes (consulte la sección "“Modelo de soporte”") Se definen como proyectos de Google Cloud que están completamente aislados entre sí a menos que el usuario lo conecte explícitamente. Los clientes permiten el aislamiento completo de volúmenes de datos, servicios de nombres externos y otras piezas esenciales de la solución de otros clientes con la plataforma de volúmenes de Cloud Volumes Service.

Dado que la plataforma Cloud Volumes Service se conecta a través de la agrupación VPC, ese aislamiento también se aplica a ella. Para habilitar el uso compartido de volúmenes de Cloud Volumes Service entre varios proyectos, utilice un VPC compartido (consulte la sección ""“VPC compartidos”""). Puede aplicar controles de acceso a recursos compartidos de SMB y exportaciones de NFS para limitar quién o qué puede ver o modificar conjuntos de datos.

Gestión de identidades sólida para el plano de control

En el plano de control en el que se lleva a cabo la configuración de Cloud Volumes Service, la gestión de identidades se gestiona mediante "Gestión de acceso a identidades (IAM)". IAM es un servicio estándar que permite controlar la autenticación (inicios de sesión) y la autorización (permisos) de las instancias de proyectos de Google Cloud. Toda la configuración se realiza con las API de Cloud Volumes Service mediante un transporte HTTPS seguro con 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 Cloud Volumes Service convierte las entradas del usuario en llamadas a la API de Cloud Volumes Service.

Seguridad reforzada: Limitar las superficies de ataque

Parte de la seguridad efectiva está limitando el número de superficies de ataque disponibles en un servicio. Las superficies de ataque pueden incluir diversas cosas, como datos en reposo, transferencias en tránsito, inicios de sesión y los propios conjuntos de datos.

Un servicio gestionado elimina algunas de las superficies de ataque de forma inherente en su diseño. Gestión de infraestructuras, como se describe en la sección ""“Funcionamiento de servicio”," es manejado por un equipo específico y es automatizado para reducir el número de veces que un ser humano realmente toca configuraciones, lo que ayuda a reducir el número de errores intencionales y no intencionales. La conexión de red está cerrada de modo que solo los servicios necesarios puedan acceder los unos a los otros. El cifrado se lleva a cabo en el almacenamiento de datos, y solo el plano de datos necesita atención de seguridad de los administradores de Cloud Volumes Service. Al ocultar la mayor parte de la gestión de una interfaz API, la seguridad se logra 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 basándose únicamente en mecanismos externos (como firewalls y sistemas de detección de intrusiones) para mitigar las amenazas. Sin embargo, los ataques y las infracciones evolucionaron para evitar la verificación en entornos mediante el phishing, la ingeniería social, las amenazas internas y otros métodos que proporcionan la verificación para entrar en redes y causar estragos.

Zero Trust se ha convertido en una nueva metodología en seguridad, con el mantra actual “confiar en nada mientras sigue verificando todo”. Por lo tanto, no se permite el acceso predeterminado a nada. Este mantra se aplica de diversas maneras, incluidos los cortafuegos estándar y los sistemas de detección de intrusiones (IDS) y también con los siguientes métodos:

- Métodos de autenticación sólidos (como Kerberos con cifrado AES o tokens JWT)
- Fuentes sólidas de identidades únicas (como Windows Active Directory, Lightweight Directory Access Protocol (LDAP) y Google IAM)
- Segmentación de red y multi-tenancy seguro (solo se permite el acceso de forma predeterminada a los inquilinos)
- Controles de acceso granular con políticas de acceso con privilegios mínimos
- Listas exclusivas pequeñas de administradores dedicados y de confianza con auditorías digitales y pistas en papel

La ejecución de Cloud Volumes Service en Google Cloud cumple con el modelo Zero Trust, al implementar la postura "no confiar en nada, verificar todo".

Cifrado

Cifrar datos en reposo (consulte la sección ""Cifrado de datos en reposo"") Mediante el uso de cifrados XTS-AES-256 con el cifrado de volúmenes de NetApp (NVE) y en tránsito con ""Cifrado SMB"" O soporte para NFS Kerberos 5p. Las transferencias de replicación entre regiones con REST sencilla están protegidas con cifrado TLS 1.2 (consulte la sección ""Replicación entre regiones""). Además, Google Networking 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 backups

La seguridad no se trata sólo de la prevención de ataques. También se trata de cómo recuperamos los ataques cuando se producen. Esta estrategia incluye protección de datos y backups. Cloud Volumes Service proporciona métodos para replicar en otras regiones en caso de interrupciones del servicio (consulte la sección ""Replicación entre regiones"") o si un conjunto de datos se ve afectado por un ataque de ransomware. También puede realizar backups asíncronos de datos en ubicaciones externas a la instancia de Cloud Volumes Service mediante el uso de "Backup de Cloud Volumes Service". Con los backups periódicos, la mitigación de los eventos de seguridad puede llevar menos tiempo y ahorrar dinero y angustia para los administradores.

Mitigación de ransomware rápida con copias Snapshot líderes en el sector

Además de la protección de datos y los backups, Cloud Volumes Service ofrece compatibilidad con copias Snapshot inalterables (consulte la sección ""Copias Snapshot inmutables"") de volúmenes que permiten la recuperación de ataques de ransomware (consulte la sección ""Funcionamiento de servicio"") en cuestión de segundos de descubrir el problema y con una interrupción mínima. El tiempo y los efectos de la recuperación dependen de la programación de la copia Snapshot, pero puede crear copias de SnapVault que proporcionen deltas de solo una hora en ataques de ransomware. Las copias Snapshot afectan al rendimiento y al uso de la capacidad y son un enfoque de bajo riesgo y gran recompensa para proteger sus conjuntos de datos.

Consideraciones de seguridad y superficies de ataque

El primer paso para comprender cómo proteger los datos es identificar los riesgos y las posibles superficies de ataque.

Estos incluyen (pero no se limitan a) lo siguiente:

- Administración y inicios de sesión
- Datos en reposo
- Datos en movimiento
- Red y firewalls
- Ransomware, malware y virus

Comprender las superficies de ataque puede ayudarle a proteger mejor sus entornos. Cloud Volumes Service 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 esenciales de su infraestructura, es fundamental asegurarse de que solo los usuarios aprobados puedan iniciar sesión y gestionar sus entornos. Si los agentes erróneos infringen sus credenciales administrativas, tienen las claves para el castillo y pueden hacer lo que quieran: Cambiar configuraciones, eliminar volúmenes y backups, crear puertas traseras o deshabilitar las programaciones de Snapshot.

Cloud Volumes Service para Google Cloud proporciona protección contra accesos administrativos no autorizados a través de la confusión del almacenamiento como servicio (StaaS). Cloud Volumes Service está completamente mantenido por el proveedor de cloud sin disponibilidad para iniciar sesión externamente. Todas las operaciones de configuración y configuración se automatizan por completo, por lo que un administrador humano nunca tiene que interactuar con los sistemas excepto en circunstancias muy raras.

Si se requiere inicio de sesión, Cloud Volumes Service en Google Cloud asegura los inicios de sesión manteniendo una lista muy corta de administradores de confianza que tienen acceso para iniciar sesión en los sistemas. Este método de gatekeeping ayuda a reducir el número de posibles malos actores con acceso. Además, la red de Google Cloud oculta los sistemas tras capas de seguridad de la red y sólo expone lo que se necesita al mundo exterior. Si quiere más información sobre la arquitectura de Google Cloud y Cloud Volumes Service, consulte la sección ""Arquitectura de Cloud Volumes Service"."

Administración de clústeres y actualizaciones

Dos áreas con riesgos potenciales de seguridad incluyen la administración de clústeres (lo que ocurre si un actor defectuoso tiene acceso de administrador) y las actualizaciones (lo que ocurre si una imagen de software está comprometida).

Protección en la administración del almacenamiento

El almacenamiento proporcionado como servicio elimina el riesgo añadido de exposición a los administradores al eliminar ese acceso a los usuarios finales fuera del centro de datos de cloud. En su lugar, la única configuración que se realiza es para el plano de acceso a los datos por parte de los clientes. Cada inquilino gestiona sus propios volúmenes y ningún inquilino puede llegar a otras instancias de Cloud Volumes Service. El servicio se gestiona mediante automatización, con una pequeña lista de administradores de confianza a los que se les da acceso a los sistemas a través de los procesos que se tratan en la sección ""Funcionamiento de servicio"."

El tipo de servicio CVS-Performance ofrece replicación entre regiones como una opción para proporcionar protección de datos a otra región en caso de un fallo en una región. En esos casos, Cloud Volumes Service puede realizar una conmutación por error a la región no afectada para mantener el acceso a los datos.

Actualizaciones de servicios

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 que las actualizaciones verifiquen que las imágenes oficiales se utilizan y que las actualizaciones no se ven comprometidas por actores defectuosos.

Con Cloud Volumes Service, los equipos del proveedor de cloud se encargan de gestionar las actualizaciones, lo que elimina la exposición al riesgo para los equipos de administrador, al proporcionar a los expertos conocedor de la configuración y las actualizaciones, que han automatizado y probado totalmente el proceso. Las actualizaciones no son disruptivas, y Cloud Volumes Service mantiene las últimas actualizaciones para obtener los mejores resultados generales.

Para obtener información acerca del equipo de administrador que realiza estas actualizaciones de servicio, consulte la sección ""Funcionamiento de servicio"."

Protección de datos en reposo

El cifrado de datos en reposo es importante para proteger los datos confidenciales en caso de robo, devolución o reasignación de un disco. Los datos de Cloud Volumes Service se protegen en reposo mediante el cifrado basado en software.

- Las claves generadas por Google se utilizan para CVS-SW.
- Para CVS-Performance, las claves por volumen se almacenan en un gestor de claves incorporado en Cloud Volumes Service, que usa CryptoMod de ONTAP de NetApp para generar claves de cifrado AES-256. CryptoMod aparece en la lista CMVP de módulos validados FIPS 140-2-2. Consulte "FIPS 140-2 certificado n.o 4144".

A partir de noviembre de 2021, se empezó a disponer de la funcionalidad de cifrado gestionado por el cliente (CMEK) para CVS-Performance. Esta funcionalidad le permite cifrar las claves por volumen con claves maestras por proyecto y región alojadas en Google Key Management Service (KMS). KMS le permite asociar gestores de claves externos.

Para obtener detalles sobre cómo configurar KMS para CVS-Performance, "Consulte la documentación de Cloud Volumes Service".

Para obtener más información acerca de la arquitectura, consulte la sección ""Arquitectura de Cloud Volumes Service"."

Protección de datos en tránsito

Además de proteger los datos en reposo, también debe ser capaz de proteger los datos cuando están en tránsito entre la instancia de Cloud Volumes Service y un destino de cliente o replicación. Cloud Volumes Service proporciona cifrado para los datos en tránsito en protocolos NAS mediante métodos de cifrado como el cifrado SMB mediante Kerberos, la firma/sellado de paquetes y NFS Kerberos 5p para el cifrado integral de transferencias de datos.

La replicación de volúmenes de Cloud Volumes Service utiliza TLS 1.2, que aprovecha los métodos de cifrado AES-GCM.

Los protocolos en vuelo más inseguros, como telnet, NDMP, etc., están desactivados de forma predeterminada. Sin embargo, DNS no está encriptado por Cloud Volumes Service (no admite segundos DNS) y debe ser encriptada usando cifrado de red externa cuando sea posible. Consulte la sección ""Cifrado de datos en tránsito"" para obtener más información sobre cómo proteger los datos en movimiento.

Para obtener información acerca del cifrado del protocolo NAS, consulte la sección ""Protocolos NAS"."

Usuarios y grupos para permisos NAS

Parte de la protección de datos en el cloud implica una autenticación de usuarios y grupos adecuada, en la que se comprueban los usuarios que acceden a los datos como usuarios reales del entorno y los grupos contienen usuarios válidos. Estos usuarios y grupos proporcionan acceso inicial al recurso compartido y a la exportación, así como validación de permisos para archivos y carpetas en el sistema de almacenamiento.

Cloud Volumes Service utiliza la autenticación estándar de grupos y usuarios de Windows basada en Active Directory para recursos compartidos de SMB y permisos de estilo Windows. El servicio también puede aprovechar proveedores de identidad UNIX, como LDAP para usuarios y grupos de UNIX para exportaciones NFS, validación de ID de NFSv4, autenticación Kerberos y ACL de NFSv4.

Actualmente sólo el LDAP de Active Directory es compatible con Cloud Volumes Service para la funcionalidad LDAP.

Detección, prevención y mitigación de ransomware, malware y virus

El ransomware, el malware y los virus representan una amenaza persistente para los administradores, y la detección, prevención y mitigación de esas amenazas son siempre una prioridad para las organizaciones empresariales. Un solo evento de ransomware en un conjunto de datos crucial puede costar potencialmente millones de dólares, por lo que es beneficioso hacer lo que puede minimizar el riesgo.

Aunque Cloud Volumes Service no incluye actualmente medidas de detección o prevención nativas, como la protección antivirus o "detección automática de ransomware", Hay formas de recuperarse rápidamente de un evento de ransomware mediante la habilitación de horarios habituales de copias Snapshot. Las copias Snapshot no modificables y de solo lectura hacen referencia a los bloques modificados del sistema de ficheros, son casi instantáneas, tienen un impacto mínimo en el rendimiento y solo utilizan espacio cuando se modifican o eliminan datos. Puede configurar programaciones para copias Snapshot de acuerdo con el objetivo de punto de recuperación (RPO)/objetivo de tiempo de recuperación (RTO) que desee y puede conservar hasta 1,024 copias Snapshot por volumen.

El soporte de copias Snapshot se incluye sin coste adicional (además de los cargos en el almacenamiento de datos correspondientes a los bloques/datos modificados que conservan las copias Snapshot) con Cloud Volumes Service y, en el caso de un ataque de ransomware, se puede usar para revertir a una copia Snapshot antes de que se produjera el ataque. Las restauraciones Snapshot se realizan en cuestión de segundos y, a continuación, puede volver a servir datos de forma normal. Para obtener más información, consulte "La solución de NetApp para ransomware".

Para evitar que el ransomware afecte a su negocio es necesario un enfoque multicapa que incluya una o varias de las siguientes opciones:

- Protección de terminales
- Protección contra amenazas externas a través de firewalls de red
- Detección de anomalías de datos
- Múltiples backups (in situ y fuera de ellas) de conjuntos de datos cruciales
- Pruebas de restauración de backups periódicas
- Copias Snapshot de NetApp de solo lectura inalterables
- Autenticación multifactor para la infraestructura crucial
- Auditorías de seguridad de inicios de sesión del sistema

Esta lista dista mucho de ser exhaustiva, pero es un buen proyecto a seguir cuando se trata del potencial de ataques de ransomware. Cloud Volumes Service en Google Cloud proporciona varias formas de protegerse contra eventos de ransomware y reducir sus efectos.

Copias Snapshot modificables

De forma nativa, Cloud Volumes Service proporciona copias Snapshot inmutables de solo lectura que se utilizan en una programación personalizable para una recuperación rápida de un momento específico en caso de eliminación de datos o si un volumen completo ha sido victimizado por un ataque de ransomware. Las restauraciones de Snapshot a copias Snapshot en buenas condiciones anteriores son rápidas y minimizan la pérdida de datos en función del período de retención de sus programaciones de Snapshot, y de objetivos de tiempo y de punto de recuperación. El efecto que tiene la tecnología Snapshot en el rendimiento es mínimo.

Como las copias snapshot de Cloud Volumes Service son de solo lectura, no pueden infectarse con el ransomware a menos que el ransomware haya proliferado en el conjunto de datos inadvertido y las copias snapshot se han tomado de los datos infectados por el ransomware. Por este motivo, también debe considerar la detección de ransomware basada en anomalías de los datos. Cloud Volumes Service no ofrece actualmente una detección de forma nativa, pero puede utilizar un software de supervisión externo.

Backups y restauraciones

Cloud Volumes Service proporciona funcionalidades de backup de clientes NAS estándar (como backups a través de NFS o SMB).

- CVS-Performance ofrece replicación de volúmenes entre regiones a otros volúmenes CVS-Performance. Para obtener más información, consulte "replicación de volúmenes" En la documentación de Cloud Volumes Service.
- CVS-SW ofrece funcionalidades de backup y restauración de volúmenes nativas del servicio. Para obtener más información, consulte "backup en el cloud" En la documentación de Cloud Volumes Service.

La replicación de volúmenes proporciona una copia exacta del volumen de origen para una conmutación por error rápida en caso de un desastre, incluidos los eventos de ransomware.

Replicación entre regiones

CVS-Performance le permite replicar de forma segura volúmenes en las regiones de Google Cloud para la protección de datos y casos de uso de archivado mediante el cifrado TLS1.2 AES 256 GCM en una red de servicios de back-end controlada por NetApp mediante interfaces específicas que se utilizan para la replicación que se ejecuta en la red de Google. Un volumen primario (origen) contiene los datos de producción activos y se replica en un volumen secundario (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 cambiados de un volumen primario. Por ejemplo, si una base de datos de 1 TB que reside en un volumen primario se replica en el volumen secundario, se transfiere 1 TB de espacio en la replicación inicial. Si esa base de datos tiene unos pocos cientos de filas (hipotéticamente, unos pocos MB) que cambian entre la inicialización y la siguiente actualización, sólo los bloques con las filas modificadas se replican al secundario (unos pocos MB). Esto ayuda a garantizar que los tiempos de transferencia siguen siendo bajos y que los costes de replicación siguen bajos.

Todos los permisos de los archivos y carpetas se replican en el volumen secundario, pero los permisos de acceso al recurso compartido (como políticas y reglas de exportación o recursos compartidos de SMB y ACL 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 las conexiones de dominio de Active Directory para proporcionar un manejo coherente de identidades y permisos de usuarios y grupos. Puede usar un volumen secundario como destino de conmutación por error en caso de un desastre si se rompe la relación de replicación, que convierte el volumen secundario en lectura/escritura.

Las réplicas de volúmenes son de solo lectura, lo que proporciona una copia inalterable de datos fuera de las instalaciones para una recuperación rápida de los datos en instancias donde un virus ha infectado los datos o ransomware ha cifrado el conjunto de datos principal. Los datos de solo lectura no se cifrarán, pero, si el volumen primario se ve afectado y se produce la replicación, los bloques infectados también se replican. Puede utilizar copias Snapshot antiguas no afectadas para la recuperación, pero es posible que los acuerdos de nivel de servicio no estén dentro del rango de objetivo de tiempo de recuperación/objetivo de punto de recuperación prometido en función de la rapidez con la que se detecte un ataque.

Además, puede evitar acciones administrativas maliciosas, como eliminaciones de volúmenes, eliminaciones

de copias Snapshot o cambios de programación de Snapshot, con gestión de replicación entre regiones (CRR) en Google Cloud. Para ello, se crean funciones personalizadas que separan a los administradores de volúmenes, que pueden eliminar volúmenes de origen, pero no interrumpir las operaciones y, por lo tanto, no se pueden eliminar los volúmenes de destino, de los administradores de CRR, que no pueden realizar ninguna operación de volumen. Consulte "Consideraciones de seguridad" En la documentación de Cloud Volumes Service para los permisos que permite cada grupo de administradores.

Backup de Cloud Volumes Service

Aunque Cloud Volumes Service proporciona una gran durabilidad de los datos, los eventos externos pueden causar la pérdida de datos. En caso de producirse un evento de seguridad, como un virus o ransomware, los backups y las restauraciones se convierten en algo crucial para reanudar el acceso a los datos de forma puntual. Un administrador puede eliminar accidentalmente un volumen de Cloud Volumes Service. O los usuarios simplemente quieren conservar las versiones de backup de sus datos durante muchos meses y mantener el espacio adicional de copia Snapshot dentro del volumen supone un reto de costes. A pesar de que las copias Snapshot deberían ser la forma preferida de conservar las versiones de backup durante las últimas semanas para restaurar los datos perdidos de ellas, se encuentran dentro del volumen y se pierden si este desaparece.

Por todas estas razones, NetApp Cloud Volumes Service ofrece servicios de backup a través de "Backup de Cloud Volumes Service".

El backup de Cloud Volumes Service genera una copia del volumen en Google Cloud Storage (GCS). Solo realiza un backup de los datos reales almacenados en el volumen, no del espacio libre. Funciona como siempre incremental, lo que significa que transfiere el contenido del volumen una vez y desde allí sólo se realiza el backup de los datos modificados. En comparación con los conceptos clásicos de backup con varios backups completos, ahorrará una gran cantidad de almacenamiento de backup al reducir costes. Puesto que el precio mensual del espacio de backup es más bajo en comparación con un volumen, es el lugar ideal para mantener las versiones de backup por más tiempo.

Los usuarios pueden utilizar una copia de seguridad de Cloud Volumes Service para restaurar cualquier versión de copia de seguridad en el mismo volumen o en otro dentro de la misma región. Si el volumen de origen se elimina, se conservan los datos de backup y se debe gestionar (por ejemplo, se eliminan) de forma independiente.

Cloud Volumes Service backup está integrado en Cloud Volumes Service as Option. Los usuarios pueden decidir qué volúmenes proteger activando el backup de Cloud Volumes Service por volumen. Consulte "Documentación de backup de Cloud Volumes Service" para obtener información sobre los backups, el "número máximo de versiones de backup admitidas", programación, y. "precios".

Todos los datos de backup de un proyecto se almacenan en un bloque de GCS que gestiona el servicio y que el usuario no puede ver. Cada proyecto utiliza un bloque diferente. Actualmente, los bloques se encuentran en la misma región que los volúmenes Cloud Volumes Service, pero se están debatiendo más opciones. Consulte la documentación para obtener la información más reciente.

El transporte de datos desde un bloque de Cloud Volumes Service a GCS utiliza redes de Google internas en servicio con HTTPS y TLS1.2. Los datos se cifran en reposo con claves gestionadas por Google.

Para gestionar el backup de Cloud Volumes Service (crear, eliminar y restaurar backups), un usuario debe tener el "roles/netappcloudvolumes.admin" función.

Arquitectura

Descripción general

Parte de confiar en una solución cloud es comprender la arquitectura y el modo en el que se protege. En esta sección se presentan distintos aspectos de la arquitectura de Cloud Volumes Service en Google para ayudar a solucionar los posibles problemas relacionados con la seguridad de los datos, así como llamadas a áreas en las que se puedan necesitar pasos de configuración adicionales para obtener la puesta en marcha más segura.

La arquitectura general de Cloud Volumes Service se puede dividir en dos componentes principales: El plano de control y el plano de datos.

Plano de control

El plano de control en Cloud Volumes Service es la infraestructura de back-end gestionada por los administradores de Cloud Volumes Service 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 ofrecer valor a una solución residente en cloud como Cloud Volumes Service.

Plano de datos

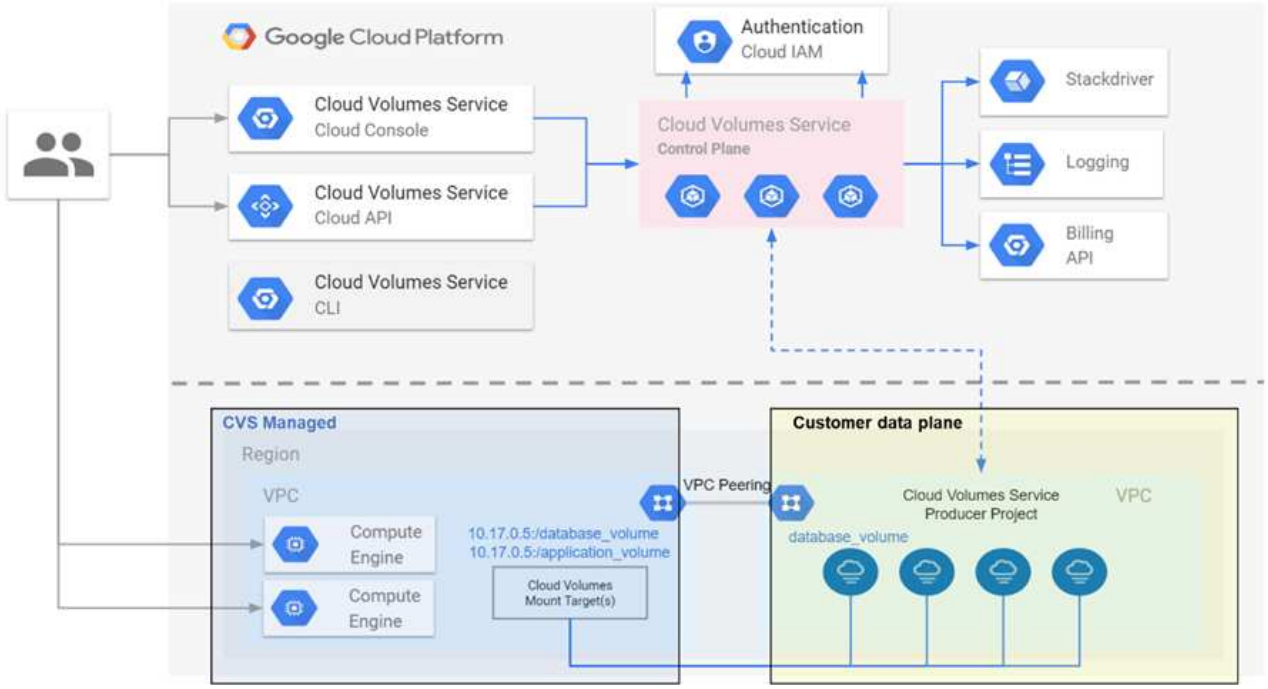
El plano de datos en Cloud Volumes Service incluye los volúmenes de datos reales y la configuración de Cloud Volumes Service general (como el control de acceso, la autenticación de Kerberos, etc.). El plano de datos está totalmente bajo el control de los usuarios finales y de los consumidores de la plataforma Cloud Volumes Service.

Existen diferencias distintas en cómo se asegura y gestiona cada plano. En las siguientes secciones se tratan estas diferencias, empezando por la descripción general de la arquitectura de Cloud Volumes Service.

Arquitectura Cloud Volumes Service

De forma similar a otros servicios nativos de Google Cloud como CloudSQL, Google Cloud VMware Engine (GCVE) y filestore, utiliza Cloud Volumes Service "Google PSA" para prestar el servicio. En PSA, los servicios se construyen dentro de un proyecto de productor de servicios, que utiliza "Agrupación de redes VPC" para conectarse con el consumidor de servicios. El productor de servicios lo proporciona y controla NetApp, y el consumidor de servicios es un VPC en un proyecto de cliente, que aloja a los clientes que desean acceder a recursos compartidos de archivos de Cloud Volumes Service.

La siguiente figura, a la que se hace referencia desde "sección de arquitectura" De la documentación de Cloud Volumes Service, muestra una vista de alto nivel.



La pieza situada encima de la línea de puntos muestra el plano de control del servicio, que controla el ciclo de vida del volumen. La pieza debajo de la línea de puntos muestra el plano de datos. El cuadro azul izquierdo muestra el VPC (consumidor de servicios) del usuario, el cuadro azul derecho es el productor de servicios que proporciona NetApp. Ambos se conectan mediante la agrupación de VPC.

Modelo de tenancy

En Cloud Volumes Service, los proyectos individuales se consideran inquilinos únicos. Esto significa que la manipulación de volúmenes, copias Snapshot, etc. se realiza por proyecto. En otras palabras, todos los volúmenes son propiedad del proyecto en el que se crearon y solo ese proyecto puede gestionar y acceder a los datos de su interior de forma predeterminada. Se considera la vista del plano de control del servicio.

VPC compartidos

En la vista del plano de datos, Cloud Volumes Service puede conectarse a un VPC compartido. Se pueden crear volúmenes en el proyecto de host o en uno de los proyectos de servicio conectados al VPC compartido. Todos los proyectos (host o servicio) conectados al VPC compartido pueden llegar a los volúmenes de la capa de red (TCP/IP). Debido a que todos los clientes con conectividad de red en el VPC compartido pueden acceder potencialmente a los datos mediante los protocolos NAS, se debe utilizar el control de acceso en el volumen individual (como las listas de control de acceso de usuarios/grupos (ACL) y los nombres de host/direcciones IP para las exportaciones de NFS para controlar quién puede acceder a los datos.

Puede conectar Cloud Volumes Service hasta a cinco VPC por proyecto de cliente. En el plano de control, el proyecto le permite gestionar todos los volúmenes creados, independientemente del VPC al que estén conectados. En el plano de datos, las PC están aisladas entre sí y cada volumen solo se puede conectar a un VPC.

El acceso a los volúmenes individuales está controlado por mecanismos de control de acceso específicos de los protocolos (NFS/SMB).

En otras palabras, en la capa de red, todos los proyectos conectados al VPC compartido pueden ver el volumen, mientras que, por el lado de la gestión, el plano de control solo permite que el proyecto del

propietario vea el volumen.

Controles de servicio VPC

Los controles de servicio 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 identidades de usuario, pero no pueden restringir desde qué solicitudes de ubicación de red se originan. Los controles de servicio VPC cierran esa brecha introduciendo las funcionalidades para restringir el acceso a las redes definidas.

El plano de datos Cloud Volumes Service no está conectado a Internet externo sino a ordenadores virtuales privados con límites de red bien definidos (perímetros). Dentro de esa red, cada volumen utiliza un control de acceso específico del protocolo. Los administradores de proyectos de Google Cloud crean explícitamente cualquier conectividad de red externa. Sin embargo, el plano de control no proporciona las mismas protecciones que el plano de datos y puede ser accesible por cualquier persona desde cualquier lugar con credenciales válidas ("Fichas JWT").

En resumen, el plano de datos Cloud Volumes Service proporciona la funcionalidad de control de acceso a la red, sin el requisito de admitir controles de servicio VPC y no utiliza de forma explícita los controles de servicio VPC.

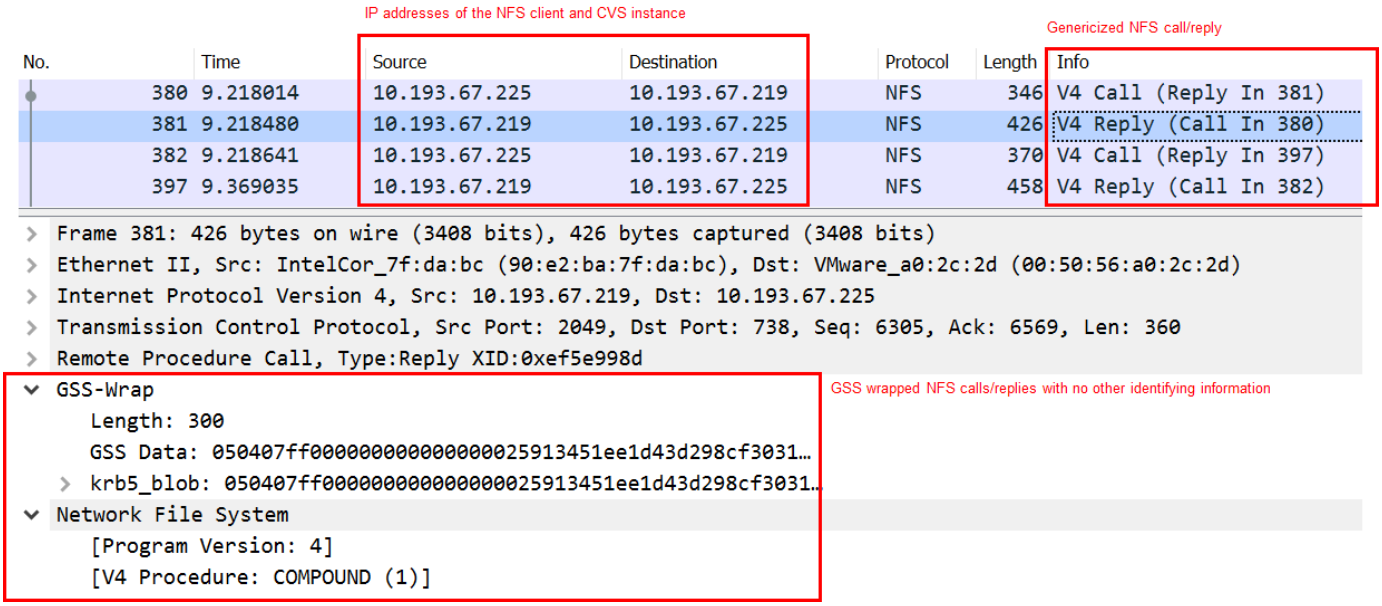
Consideraciones sobre rastreo y rastreo de paquetes

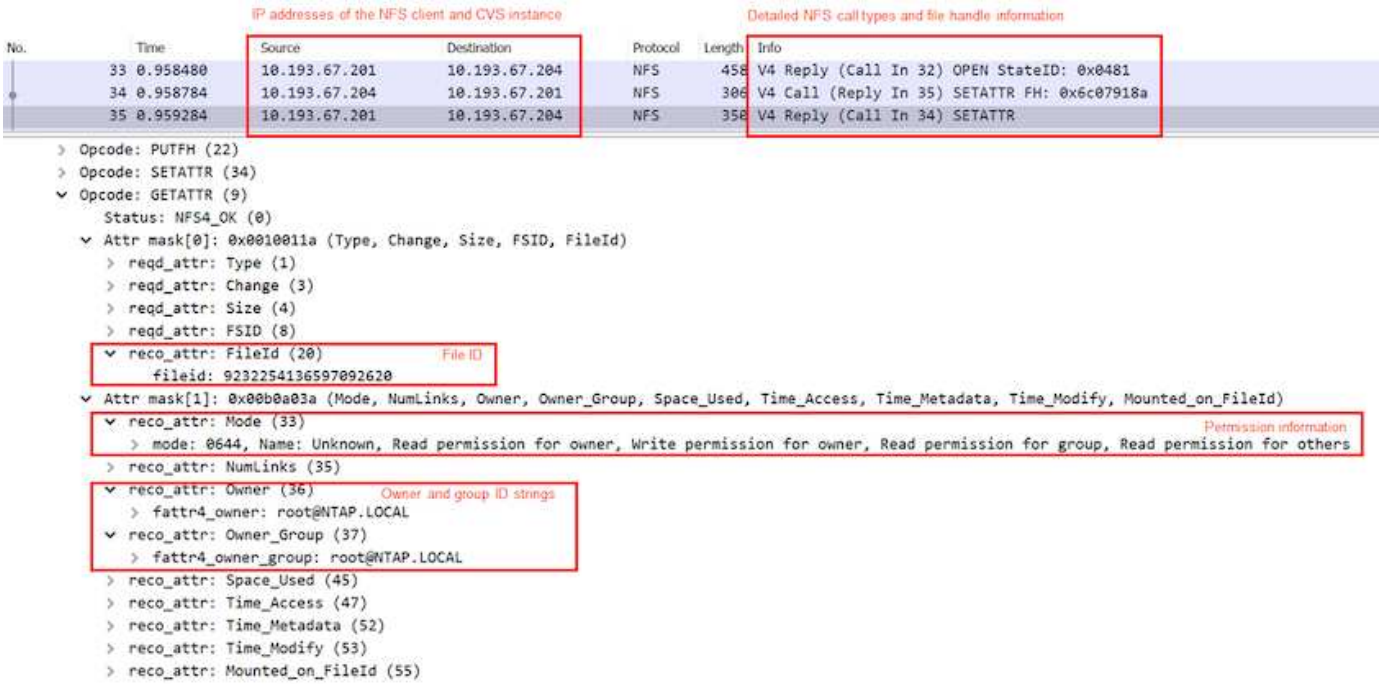
Las capturas de paquetes pueden ser útiles para solucionar problemas de red u otros problemas (como permisos NAS, conectividad LDAP, etc.), pero también se pueden usar de forma malintencionada para obtener información sobre direcciones IP de red, direcciones MAC, nombres de usuarios y grupos, y sobre qué nivel de seguridad se está utilizando en los extremos. Debido a la forma en que se configuran las reglas de red, VPC y firewall de Google Cloud, el acceso no deseado a los paquetes de red debería ser difícil de obtener sin credenciales de inicio de sesión del usuario o "Fichas JWT" a las instancias de cloud. Las capturas de paquetes solo son posibles en extremos (como máquinas virtuales (VM)) y solo en extremos internos en el VPC, a menos que se utilice un VPC compartido o un reenvío de túnel/IP de red externo para permitir de forma explícita el tráfico externo a los extremos. No hay forma de sniff el tráfico fuera de los clientes.

Cuando se utilizan VPC compartidos, cifrado en tránsito con NFS Kerberos y/o. "Cifrado SMB" puede enmascarar gran parte de la información obtenida de las trazas. Sin embargo, cierto tráfico se sigue enviando en texto sin texto, como "DNS" y.. "Consultas LDAP". En la siguiente figura se muestra una captura de paquetes de una consulta LDAP de texto sin formato originada en Cloud Volumes Service y la información de identificación potencial que se expone. Las consultas LDAP en Cloud Volumes Service actualmente no admiten cifrado ni LDAP sobre SSL. CVS-Performance admite la firma LDAP, si es solicitada por Active Directory. CVS-SW no admite la firma LDAP.

UnixUserPassword es consultada por LDAP y no se envía en texto sin formato sino en un hash salado. De forma predeterminada, LDAP de Windows no rellena los campos unixUserPassword. Este campo sólo es necesario si necesita aprovechar LDAP de Windows para inicios de sesión interactivos a través de LDAP a clientes. Cloud Volumes Service no admite inicios de sesión LDAP interactivos en las instancias.

En la siguiente figura se muestra una captura de paquetes desde una conversación Kerberos de NFS junto a una captura de NFS sobre AUTH_SYS. Tenga en cuenta que la información disponible en una traza difiere entre ambas y cómo habilitar el cifrado en tránsito ofrece una mayor seguridad general para el tráfico NAS.





Interfaces de red de equipos virtuales

Un truco que los atacantes podrían intentar es agregar una nueva tarjeta de interfaz de red (NIC) a una VM en "modo promiscuo" (Duplicación de puertos) o habilite el modo promiscuo en una NIC existente para sniff todo el tráfico. En Google Cloud, agregar una nueva NIC requiere que una máquina virtual se cierre por completo, lo que crea alertas, por lo que los atacantes no pueden pasar por alto.

Además, las NIC no se pueden establecer en modo promiscuo y activarán alertas en Google Cloud.

Arquitectura del plano de control

Todas las acciones de gestión a Cloud Volumes Service se realizan mediante API. La gestión de Cloud Volumes Service integrada en la consola cloud de GCP también utiliza la API de Cloud Volumes Service.

Gestión de acceso e identidad

Gestión de acceso e identidad ("IAM") Es un servicio estándar que le permite controlar la autenticación (inicios de sesión) y la autorización (permisos) a las instancias de proyecto de Google Cloud. Google IAM proporciona un registro de auditoría completo de la autorización y eliminación de permisos. Actualmente, Cloud Volumes Service no proporciona auditoría del plano de control.

Información general sobre autorización/permisos

IAM ofrece permisos granulares integrados para Cloud Volumes Service. Puede encontrar un "complete aquí la lista de permisos granulares".

IAM también ofrece dos roles predefinidos llamados `netappcloudvolumes.admin` y.. `netappcloudvolumes.viewer`. Estos roles pueden asignarse a usuarios o cuentas de servicio específicos.

Asigne roles y permisos adecuados para permitir que los usuarios de IAM gestionen Cloud Volumes Service.

Algunos ejemplos para el uso de permisos granulares son los siguientes:

- Cree una función personalizada con sólo permisos get/list/create/update para que los usuarios no puedan eliminar volúmenes.
- Use un rol personalizado con solo `snapshot.*` Permisos para crear una cuenta de servicio que se utilice para crear una integración de Snapshot coherente con las aplicaciones.
- Cree un rol personalizado para delegar `volumereplication.*` para usuarios específicos.

Cuentas de servicio

Para realizar llamadas a la API de Cloud Volumes Service a través de scripts o. "Terraform", debe crear una cuenta de servicio con `roles/netappcloudvolumes.admin` función. Puede utilizar esta cuenta de servicio para generar los tokens JWT necesarios para autenticar las solicitudes de API de Cloud Volumes Service de dos maneras diferentes:

- Genere una clave JSON y utilice las API de Google para obtener un token de JWT de él. Este es el método más sencillo, pero implica la gestión de secretos manuales (la clave JSON).
- Uso "Suplantación de cuentas de servicio" con `roles/iam.serviceAccountTokenCreator`. El código (script, Terraform, etc.) se ejecuta con "Credenciales predeterminadas de la aplicación" e representa a la cuenta de servicio para obtener sus permisos. Este enfoque refleja las mejores prácticas de seguridad de Google.

Consulte "Creación de la cuenta de servicio y la clave privada" Para obtener más información, consulte la documentación de cloud de Google.

API de Cloud Volumes Service

La API de Cloud Volumes Service utiliza una API basada en REST usando HTTPS (TLSv1.2) como transporte de red subyacente. Puede encontrar la definición de API más reciente "aquí" E información acerca de cómo utilizar la API en "API de Cloud Volumes en la documentación de Google Cloud".

NetApp utiliza y protege el extremo de la API mediante la funcionalidad estándar HTTPS (TLSv1.2).

Fichas JWT

La autenticación a la API se realiza con tokens JWT portadores ("RFC-7519"). Se deben obtener tokens JWT válidos mediante la autenticación de Google Cloud IAM. Para ello, debe obtener un token del IAM mediante la obtención de una clave JSON de la cuenta de servicio.

Registro de auditoría

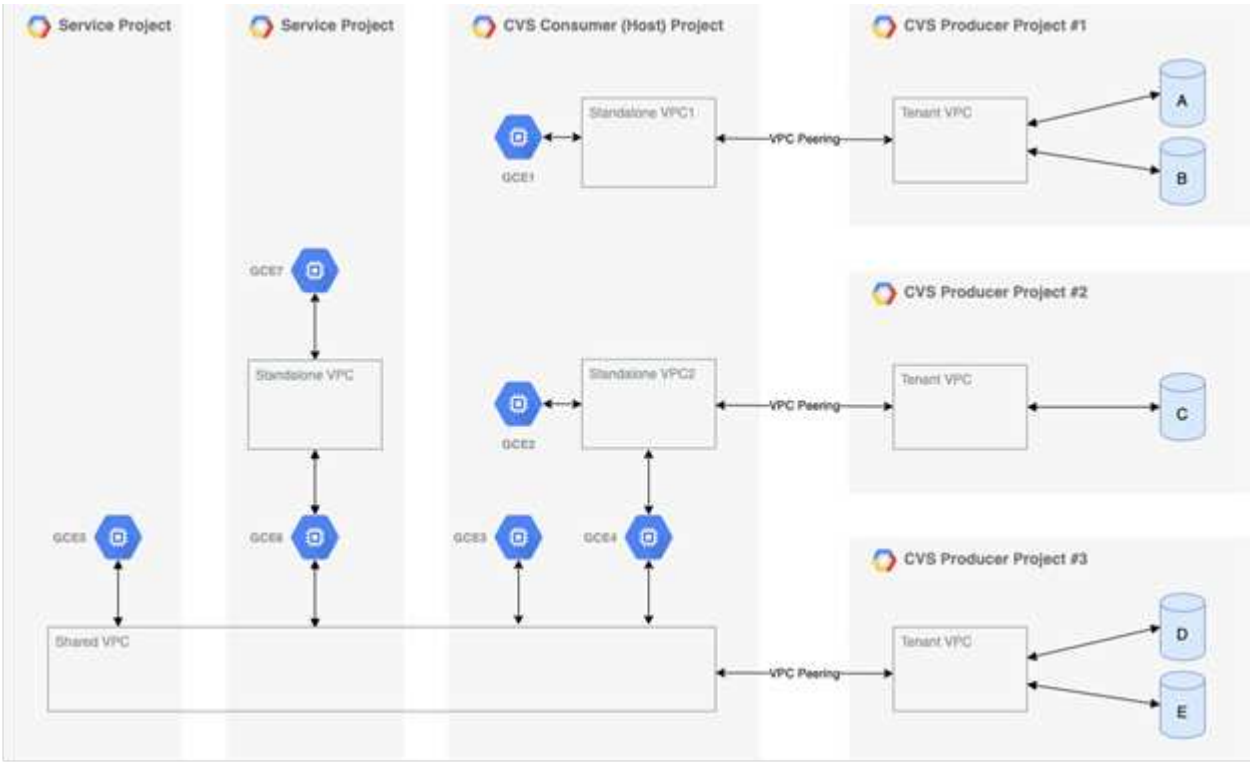
Actualmente, no hay registros de auditoría del plano de control a los que el usuario pueda acceder.

Arquitectura de plano de datos

Cloud Volumes Service para Google Cloud aprovecha Google Cloud "acceso a servicios privados" marco. En este marco, los usuarios pueden conectarse a Cloud Volumes Service. Este marco usa construcciones de paridad de Service Networking y VPC, al igual que otros servicios de Google Cloud, para garantizar un aislamiento completo entre clientes.

Para obtener información general sobre la arquitectura de Cloud Volumes Service para Google Cloud, consulte "Para Cloud Volumes Service".

Las VPC de usuario (independientes o compartidas) tienen una relación entre sí y las VPC dentro de los proyectos de arrendatarios administrados de Cloud Volumes Service, que alojan los volúmenes.



La figura anterior muestra un proyecto (el proyecto para consumidores CVS en el medio) con tres redes VPC conectadas a Cloud Volumes Service y a varios equipos virtuales de Compute Engine (GCE1-7) compartiendo volúmenes:

- VPC1 permite a GCE1 acceder a los volúmenes A y B.
- VPC2 permite a GCE2 y GCE4 acceder al volumen C.
- La tercera red VPC es un VPC compartido, compartido con dos proyectos de servicio. Permite a GCE3, GCE4, GCE5 y GCE6 acceder a los volúmenes D y E. Las redes VPC compartidas solo se admiten para volúmenes del tipo de servicio CVS-Performance.

GCE7 no puede acceder a ningún volumen.

Los datos se pueden cifrar tanto en tránsito (mediante Kerberos y/o cifrado SMB) como en reposo en Cloud Volumes Service.

Cifrado de datos en tránsito

Los datos en tránsito pueden cifrarse en la capa de protocolo NAS, y la propia red de Google Cloud está cifrada, tal y como se describe en las siguientes secciones.

Red de Google Cloud

Google Cloud cifra el tráfico en el nivel de la red, tal y como se describe en "Cifrado en tránsito" En la documentación de Google. Como se mencionó en la sección "Arquitectura de Cloud Volumes Services", Cloud Volumes Service se ofrece desde un proyecto de productor de PSA controlado por NetApp.

En caso de CVS-SW, el inquilino productor ejecuta las VM de Google para ofrecer el servicio. Google cifra

automáticamente el tráfico entre los equipos virtuales del usuario y los equipos virtuales de Cloud Volumes Service.

Aunque la ruta de datos para CVS-Performance no está completamente cifrada en la capa de red, NetApp y Google usan una combinación de ambos "De cifrado IEEE 802.1AE (MACSec)", "encapsulación" (Cifrado de datos) y redes con limitaciones físicas para proteger los datos en tránsito entre el tipo de servicio CVS-Performance de Cloud Volumes Service y Google Cloud.

Protocolos NAS

Los protocolos NFS y SMB NAS proporcionan un cifrado de transporte opcional en la capa del protocolo.

Cifrado SMB

"Cifrado SMB" Proporciona cifrado integral de datos SMB y protege los datos de espionaje en redes que no son de confianza. Puede habilitar el cifrado tanto para la conexión de datos de cliente/servidor (solo disponible para clientes compatibles con SMB3.x) como para la autenticación de la controladora de servidor/dominio.

Cuando el cifrado SMB está habilitado, los clientes que no admiten el cifrado no pueden acceder al recurso compartido.

Cloud Volumes Service admite cifrados de seguridad RC4-HMAC, AES-128-CTS-HMAC-SHA1 y AES-256-CTS-HMAC-SHA1 para el cifrado SMB. SMB negocia con el tipo de cifrado más alto admitido por el servidor.

NFSv4.1 Kerberos

Para NFSv4.1, CVS-Performance ofrece autenticación de Kerberos, tal como se describe en "RFC7530". Puede activar Kerberos por volumen.

El tipo de cifrado disponible más actual para Kerberos es AES-256-CTS-HMAC-SHA1. Cloud Volumes Service de NetApp es compatible con AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 y DES para NFS. También admite ARCFOUR-HMAC (RC4) para el tráfico CIFS/SMB, pero no para NFS.

Kerberos proporciona tres niveles de seguridad distintos para montajes NFS que ofrecen opciones para la solidez de la seguridad de Kerberos.

Según RedHat's "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 mayor sea el nivel de seguridad de Kerberos, peor será el rendimiento, puesto que el cliente y el servidor pasan tiempo cifrando y descifrando las operaciones de NFS para cada paquete enviado. Muchos clientes y servidores NFS ofrecen 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 integral) es significativamente mayor que el impacto de Kerberos 5 (autenticación de usuario).

En la siguiente tabla se muestran las diferencias en el rendimiento y la seguridad de cada nivel.

Nivel de seguridad	Seguridad	Rendimiento
NFSv3: System	• Menos seguro; texto sin formato con ID de usuario/ID de grupo numéricos • Capaz de ver UID, GID, direcciones IP de cliente, rutas de exportación, nombres de archivos, permisos en capturas de paquetes	• Lo mejor para la mayoría de los casos
NFSv4.x: Sys	• Más seguro que NFSv3 (identificadores de cliente, coincidencia de cadena de nombre/cadena de dominio) pero texto sin formato • Se puede ver UID, GID, direcciones IP de cliente, cadenas de nombre, identificadores de dominio, rutas de exportación, nombres de archivo y permisos en capturas de paquetes	• Bueno para cargas de trabajo secuenciales (como equipos virtuales, bases de datos, archivos de gran tamaño) • Malo con un número elevado de archivos/metadatos altos (un 30-50% peor)
NFS: Krb5	• El 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 el acceso al montaje necesita un ticket Kerberos válido (ya sea mediante el nombre de usuario/contraseña o el cambio de tabulación manual); el ticket caduca después de un período de tiempo especificado y el usuario debe volver a autenticarse para el acceso • No existe cifrado para operaciones de NFS ni para protocolos auxiliares como Mount/portmapper/nlm (puede ver rutas de exportación, direcciones IP, identificadores 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	Rendimiento
NFS: Krb5i	• El 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 el acceso al montaje necesita un ticket Kerberos válido (ya sea mediante el nombre de usuario/contraseña o el cambio de tabulación manual); el ticket caduca después de un período de tiempo especificado y el usuario debe volver a autenticarse para el acceso • No existe cifrado para operaciones de NFS ni para protocolos auxiliares como Mount/portmapper/nlm (puede ver rutas de exportación, direcciones IP, identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes) • La suma de comprobación de Kerberos GSS se agrega a cada paquete para garantizar que nada intercepta los paquetes. Si coinciden sumas de comprobación, se permite la conversación.	• Mejor que krb5p porque la carga útil NFS no está cifrada; solo la sobrecarga añadida en comparación con krb5 es la suma de comprobación de integridad. El rendimiento del krb5i no será mucho peor que el krb5, pero sí que se verá algo de degradación.

Nivel de seguridad	Seguridad	Rendimiento
NFS: Krb5p	• El 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 cambio manual de keytab); el ticket caduca después del período de tiempo especificado y el usuario debe volver a autenticarse para acceder • Todas las cargas de paquetes NFS se cifran con el contenedor GSS (no se pueden ver los identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes). • Incluye comprobación de integridad. • El tipo de operación NFS es visible (FSINFO, ACCESS, GETATTR, etc.). • Los protocolos auxiliares (Mount, portmap, nlm, etc.) no están cifrados (puede ver rutas de exportación, direcciones IP)	• El peor rendimiento de los niveles de seguridad; krb5p debe cifrar/descifrar más. • Mejor rendimiento que krb5p con NFSv4.x para cargas de trabajo con un gran número de archivos.

En Cloud Volumes Service, un servidor de Active Directory configurado se utiliza como servidor Kerberos y servidor LDAP (para buscar identidades de usuario desde un esquema compatible con RFC2307). No se admiten otros servidores Kerberos o LDAP. NetApp recomienda encarecidamente utilizar LDAP para la gestión de identidades en Cloud Volumes Service. Para obtener más información acerca de cómo se muestra NFS Kerberos en capturas de paquetes, consulte la sección ""Consideraciones sobre rastreo y rastreo de paquetes"."

Cifrado de datos en reposo

Todos los volúmenes de Cloud Volumes Service se cifran en reposo mediante el cifrado AES-256, lo que significa que todos los datos de usuario escritos en medios se cifran y solo se pueden descifrar con una clave por volumen.

- Para CVS-SW, se usan claves generadas por Google.
- Para CVS-Performance, las claves por volumen se almacenan en un gestor de claves incorporado en Cloud Volumes Service.

A partir de noviembre de 2021, ya estaba disponible la funcionalidad de obtener una vista previa de las claves de cifrado gestionadas por el cliente (CMEK). Esto permite cifrar las claves por volumen con una clave maestra por proyecto y por región alojada en "Servicio de administración de claves (KMS) de Google." KMS le permite asociar gestores de claves externos.

Para obtener información acerca de la configuración de KMS para CVS-Performance, consulte "Configurar las claves de cifrado gestionadas por el cliente".

Servidor de seguridad

Cloud Volumes Service expone varios puertos TCP para que sirvan a los recursos compartidos NFS y SMB:

- "Puertos necesarios para el acceso NFS"
- "Puertos necesarios para el acceso a SMB"

Además, SMB, NFS con LDAP incluido Kerberos y configuraciones de protocolo dual requieren acceso a un dominio de Windows Active Directory. Deben estar las conexiones de Active Directory "configurado" por región. Los controladores de dominio de Active Directory (DC) se identifican mediante el uso "Descubrimiento de DC basado en DNS" Utilizando los servidores DNS especificados. Se utiliza cualquiera de los DC devueltos. La lista de centros de datos elegibles se puede limitar especificando un sitio de Active Directory.

Cloud Volumes Service se dirige a través de direcciones IP del rango CIDR asignado con el `gcloud compute address` command mientras "Integración de Cloud Volumes Service". Puede utilizar este CIDR como direcciones de origen para configurar firewalls entrantes en los controladores de dominio de Active Directory.

Los controladores de dominio de Active Directory deben "Exponer los puertos a los CIDR de Cloud Volumes Service como se menciona aquí".

Protocolos NAS

Información general sobre los protocolos NAS

Los protocolos NAS incluyen NFS (v3 y v4.1) y SMB/CIFS (2.x y 3.x). Estos protocolos son cómo CVS permite el acceso compartido a los datos entre varios clientes NAS. Además, Cloud Volumes Service puede proporcionar acceso a clientes NFS y SMB/CIFS simultáneamente (doble protocolo) a la vez que se respetan toda la configuración de identidades y permisos de los archivos y carpetas de los recursos compartidos NAS. Para mantener la seguridad de transferencia de datos más alta posible, Cloud Volumes Service admite el cifrado de protocolos en transferencia usando cifrado SMB y NFS Kerberos 5p.

El protocolo dual solo está disponible con CVS-Performance.

Conceptos básicos de los protocolos NAS

Los protocolos NAS representan formas en las que varios clientes de una red pueden acceder a los mismos datos en un sistema de almacenamiento, como Cloud Volumes Service en GCP. NFS y SMB son los protocolos NAS definidos y funcionan

cliente/servidor donde Cloud Volumes Service actúa como servidor. Los clientes envían solicitudes de acceso, lectura y escritura al servidor y éste es responsable de coordinar los mecanismos de bloqueo de archivos, de almacenar permisos y de 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, y así sucesivamente); el servidor responde con la información si el cliente y el usuario solicitante tienen los permisos necesarios en la carpeta principal.
2. Si los permisos del directorio permiten el acceso, el cliente le preguntará al servidor si el nombre de archivo que se está creando ya existe en el sistema de archivos. Si el nombre del archivo ya está en uso, se produce un error en la creación. Si el nombre del archivo no existe, el servidor hace saber al cliente que puede continuar.
3. El cliente realiza una llamada al servidor para crear el archivo con el identificador de directorio y el nombre de archivo y establece el acceso y las horas modificadas. El servidor emite un ID de archivo único al archivo para asegurarse de que no se crean otros archivos con el mismo ID de archivo.
4. El cliente envía una llamada para comprobar los atributos del archivo antes de la operación DE ESCRITURA. Si los permisos lo permiten, el cliente escribe el nuevo archivo. Si el protocolo/aplicación utiliza el bloqueo, el cliente solicita al servidor un bloqueo para evitar que otros clientes accedan al archivo mientras está bloqueado para evitar que se dañen los datos.

NFS

NFS es un protocolo de sistema de archivos distribuido que es un estándar abierto IETF definido en solicitud de comentarios (RFC) que permite a cualquiera implementar el protocolo.

Los volúmenes de Cloud Volumes Service se comparten a los clientes NFS exportando una ruta a la que pueden acceder un cliente o un conjunto de clientes. Los permisos para montar estas exportaciones se definen mediante políticas y reglas de exportación, que los administradores de Cloud Volumes Service pueden configurar.

La implantación de NFS de NetApp se considera un estándar oro para el protocolo y se utiliza en innumerables entornos NAS empresariales. En las siguientes secciones se tratan el NFS y las características de seguridad específicas disponibles en Cloud Volumes Service y cómo se implementan.

Usuarios y grupos UNIX locales predeterminados

Cloud Volumes Service contiene varios usuarios y grupos UNIX predeterminados para varias funcionalidades básicas. Estos usuarios y grupos no se pueden modificar ni eliminar actualmente. No es posible agregar nuevos usuarios y grupos locales a Cloud Volumes Service en este momento. Los usuarios y grupos de UNIX fuera de los usuarios y grupos predeterminados deben ser proporcionados por un servicio de nombres LDAP externo.

En la siguiente tabla se muestran los usuarios y grupos predeterminados y sus correspondientes ID numéricos. NetApp recomienda no crear nuevos usuarios o grupos en LDAP o en los clientes locales que vuelvan a usar estos ID numéricos.

Usuarios predeterminados: ID numéricos	Grupos predeterminados: ID numéricos
• raíz:0 • pcuser:65534 • nadie:65535	• raíz:0 • daemon:1 • pcuser:65534 • nadie:65535

Cuando se utiliza NFSv4.1, el usuario raíz podría mostrarse como nadie cuando se ejecutan comandos de lista de directorios en clientes NFS. Esto se debe a la configuración de asignación de dominio de ID del cliente. Consulte la sección llamada NFSv4.1 y el usuario/grupo nadie para obtener detalles sobre esta edición y cómo resolverla.

El usuario raíz

En Linux, la cuenta raíz tiene acceso a todos los comandos, archivos y carpetas de un sistema de archivos basado en Linux. Debido a la eficacia de esta cuenta, las prácticas recomendadas de seguridad a menudo requieren que el usuario raíz se desactive o se restrinja de alguna manera. En las exportaciones NFS, la potencia que tienen los usuarios raíz sobre los archivos y carpetas se puede controlar en Cloud Volumes Service mediante las normas y políticas de exportación, y un concepto denominado squash raíz.

La función de ocupación de raíz garantiza que el usuario root que accede a un montaje NFS esté almacenado en la base del usuario numérico anónimo 65534 (consulte la sección “El usuario anónimo”) y actualmente sólo está disponible cuando se utiliza CVS-Performance seleccionando Off para acceso raíz durante la creación de reglas de política de exportación. Si el usuario root está almacenado en el nombre del usuario anónimo, ya no tiene acceso a ejecutar chown o. "comandos setuid/setgid (el bit de pegado)" En los archivos o carpetas del montaje NFS, y los archivos o carpetas creados por el usuario raíz muestran el UID anon como el propietario/grupo. Además, el usuario raíz no puede modificar las ACL de NFSv4. Sin embargo, el usuario raíz todavía tiene acceso a chmod y 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 la posibilidad de usar un volumen con ACL NTFS, creando un usuario de Windows con el nombre `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 solicitudes de cliente que llegan sin credenciales de NFS válidas. Esto puede incluir al usuario root cuando se utiliza la función root squashing. El usuario anon en Cloud Volumes Service es 65534.

Este UID normalmente está asociado con el nombre de usuario `nobody` o. `nfsnobody` En entornos Linux. Cloud Volumes Service utiliza también 65534 como usuario local de UNIX' pcuser» (véase la sección “Usuarios y grupos UNIX locales predeterminados”), que también es el usuario de respaldo predeterminado para las asignaciones de nombres de Windows a UNIX cuando no se encuentra ningún usuario de UNIX válido coincidente en LDAP.

Debido a las diferencias en los nombres de usuario en Linux y Cloud Volumes Service para UID 65534, es posible que la cadena de nombre de los usuarios asignados a 65534 no coincida cuando se utiliza NFSv4.1. Como resultado, puede que vea `nobody` como usuario en algunos archivos y carpetas. Consulte la sección “NFSv4.1 y el usuario/grupo nadie” para obtener información sobre este problema y cómo resolverlo.

Control de accesos/exportaciones

El acceso inicial a las exportaciones y recursos compartidos para montajes NFS se controla mediante reglas de la política de exportación basadas en host contenidas en una política de exportación. Se define una IP de host, nombre de host, subred, netgroup o dominio para permitir el acceso al montaje del recurso compartido de NFS y el nivel de acceso permitido al host. Las opciones de configuración de las reglas de política de exportación dependen del nivel de Cloud Volumes Service.

Para CVS-SW, hay disponibles las siguientes opciones para la configuración de la política de exportación:

- **Coincidencia de cliente.** Lista de direcciones IP separadas por comas, lista separada por comas de nombres de host, subredes, grupos de red, nombres de dominio.
- **Reglas de acceso RO/RW.** Seleccione sólo lectura/escritura o lectura para controlar el nivel de acceso a la exportación.CVS-Performance ofrece las siguientes opciones:
- **Coincidencia de cliente.** Lista de direcciones IP separadas por comas, lista separada por comas de nombres de host, subredes, grupos de red, nombres de dominio.
- **Reglas de acceso RO/RW.** Seleccione sólo lectura/escritura o lectura para controlar el nivel de acceso a la exportación.
- **Acceso raíz (on/OFF).** configura el squash raíz (consulte la sección “El usuario raíz" para obtener más información).
- **Tipo de protocolo.** esto limita el acceso al montaje NFS a una versión específica del protocolo. Cuando se especifican NFSv3 y NFSv4.1 para el volumen, deje las dos casillas en blanco o marque ambas.
- **Nivel de seguridad de Kerberos (cuando se selecciona Enable Kerberos).** proporciona las opciones de krb5, krb5i y/o krb5p para acceso de solo lectura o de lectura/escritura.

Cambiar la propiedad (chown) y cambiar el grupo (chgrp)

NFS en Cloud Volumes Service sólo permite al usuario raíz ejecutar chown/chgrp en archivos y carpetas. Otros usuarios ven a. `Operation not permitted` error: incluso en los archivos que poseen. Si utiliza la raíz de squash (como se describe en la sección “El usuario raíz”), la raíz está ocupada para un usuario que no es raíz y no se permite el acceso a chown y chgrp. Actualmente no hay soluciones alternativas en Cloud Volumes Service para permitir chown y chgrp para usuarios no raíz. Si se requieren cambios de propiedad, considere usar volúmenes de protocolo dual y establezca el estilo de seguridad en NTFS para controlar los permisos del lado de Windows.

Gestión de permisos

Cloud Volumes Service admite ambos bits de modo (como 644, 777, etc. para rwx) y ACL de NFSv4.1 para controlar los permisos de los clientes NFS de los volúmenes que utilicen el estilo de seguridad UNIX. La gestión de permisos estándar se utiliza para estos (como chmod, chown o nfs4_setfacl) y funciona con cualquier cliente Linux que los admita.

Además, cuando se usan volúmenes de protocolo dual establecidos en NTFS, los clientes NFS pueden aprovechar la asignación de nombres Cloud Volumes Service a usuarios de Windows, que se utilizan para resolver los permisos NTFS. Esto requiere una conexión LDAP a Cloud Volumes Service para proporcionar traducciones de ID-a-nombre de usuario numérico porque Cloud Volumes Service requiere un nombre de usuario UNIX válido para asignar correctamente a un nombre de usuario de Windows.

Proporcionar ACL granulares para NFSv3

Los permisos de bit de modo solo cubren al propietario, al grupo y a todos los demás en la semántica, lo que significa que no hay controles de acceso de usuario granulares disponibles para NFSv3 básico. Cloud

Volumes Service no admite ACL de POSIX, ni atributos extendidos (como chattr), de modo que las listas de control de acceso granulares solo son posibles en los siguientes escenarios con NFSv3:

- Volúmenes de estilo de seguridad NTFS (servidor CIFS necesario) con asignaciones de usuarios de UNIX a Windows válidas.
- Las ACL de NFSv4.1 se aplican mediante el montaje de NFSv4.1 en un cliente de administrador para aplicar ACL.

Ambos métodos requieren una conexión LDAP para la administración de identidades de UNIX y una información de grupo y usuario de UNIX válida rellenada (consulte la sección ""LDAP"") Y sólo están disponibles con las instancias CVS-Performance. Para utilizar volúmenes de estilo de seguridad NTFS con NFS, debe utilizar el protocolo dual (SMB y NFSv3) o el protocolo doble (SMB y NFSv4.1), incluso si no se realiza ninguna conexión SMB. Para utilizar las ACL de NFSv4.1 con montajes NFSv3, debe seleccionar `Both (NFSv3/NFSv4.1)` como tipo de protocolo.

Los bits del modo UNIX normal no proporcionan el mismo nivel de granularidad en permisos que proporcionan las ACL de NTFS o NFSv4.x. En la siguiente tabla, se compara la granularidad de permisos entre bits del modo NFSv3 y ACL de NFSv4.1. Para obtener más información sobre las ACL de NFSv4.1, consulte "Nfs4_acl - Listas de control de acceso de NFSv4".

Bits del modo NFSv3	ACL de NFSv4.1
• Defina el ID de usuario en la ejecución • Establezca el ID de grupo en la ejecución • Guardar texto intercambiado (no definido en POSIX) • Permiso de lectura para el propietario • Permiso de escritura para el propietario • Ejecutar permiso para el propietario en un archivo; o buscar (buscar) permiso para el propietario en el directorio • Permiso de lectura para grupo • Permiso de escritura para grupo • Ejecutar permiso para grupo en un archivo o buscar (buscar) permiso para grupo en el directorio • Permiso de lectura para otros • Permiso de escritura para otros • Ejecutar permiso para otros usuarios en un archivo; o buscar (buscar) permiso para otros en el directorio	Tipos de entrada de control de acceso (ACE) (permitir/Denegar/Auditoría) * indicadores de herencia * directorio-heredar * archivo-heredar * no-propagar-heredar * heredar-sólo Permisos * datos de lectura (archivos) / directorio de lista (directorios) * escribir-datos (archivos) / crear-archivo (directorios) * anexar-datos (archivos) / subdirectorio de creación (directorios) * ejecutar (archivos) / cambiar-directorio (directorios) * eliminar * eliminar-hijo * atributos de lectura-escritura * escribir-atributos * atributos-ACL de lectura-escritura * Sincronizar-escritura-escritura-propietario * ACL

Por último, la pertenencia a grupos de 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 a través de ACL granulares de usuarios y grupos (hasta 1024 entradas por ACE).

Además, Cloud Volumes Service ofrece compatibilidad ampliada con grupos para ampliar el número máximo

de grupos admitidos hasta 32. Esto requiere una conexión LDAP a un servidor LDAP que contenga identidades de grupo y de usuario UNIX válidas. Para obtener más información acerca de cómo configurar esto, consulte "Crear y gestionar volúmenes de NFS" En la documentación de Google.

ID de usuario y grupo de NFSv3

Los ID de usuario y de grupo de NFSv3 se encuentran en el cable como identificadores numéricos en lugar de como nombres. Cloud Volumes Service no soluciona el nombre de usuario de estos ID numéricos con NFSv3, con los volúmenes de estilo de seguridad de UNIX que utilizan únicamente bits del modo. Cuando hay ACL de NFSv4.1, es necesario realizar una búsqueda de ID numéricos y/o una búsqueda de cadenas de nombre para resolver la ACL correctamente, incluso cuando se utiliza NFSv3. Con volúmenes de estilo de seguridad NTFS, Cloud Volumes Service debe resolver un ID numérico a un usuario UNIX válido y, a continuación, asignar a un usuario de Windows válido para negociar derechos de acceso.

Limitaciones de seguridad de los ID de usuario y de grupo de NFSv3

Con NFSv3, el cliente y el servidor nunca tienen que confirmar que el usuario que intenta leer o escribir con un ID numérico es un usuario válido; sólo es de confianza implícita. Esto abre el sistema de archivos hasta posibles infracciones simplemente falsificar cualquier ID numérico. Para evitar agujeros de seguridad como este, hay algunas opciones disponibles para Cloud Volumes Service.

- La implementación de Kerberos para NFS obliga a los usuarios a autenticarse con un nombre de usuario y contraseña o un archivo keytab a obtener un vale Kerberos para permitir el acceso a un montaje. Kerberos solo está disponible con las instancias CVS-Performance y con NFSv4.1.
- Limitar la lista de hosts de las reglas de la política de exportación los límites que los clientes NFSv3 tienen acceso al volumen de Cloud Volumes Service.
- El uso de volúmenes de protocolo doble y la aplicación de ACL NTFS a los volúmenes obliga a los clientes NFSv3 a resolver los ID numéricos a nombres de usuario de UNIX válidos para autenticar correctamente el acceso a los montajes. Esto requiere habilitar LDAP y configurar las identidades de usuarios y grupos de UNIX.
- Al SQUID el usuario raíz limita el daño que un usuario raíz puede hacer a un montaje NFS, pero no elimina por completo el riesgo. Para obtener más información, consulte la sección “El usuario raíz.”

En última instancia, la seguridad de NFS se limita a qué versión del protocolo utiliza que ofrece. NFSv3, aunque tiene un rendimiento general superior al de NFSv4.1, no proporciona el mismo nivel de seguridad.

NFSv4.1

NFSv4.1 proporciona una mayor seguridad y fiabilidad en comparación con NFSv3, por los siguientes motivos:

- Bloqueo integrado mediante un mecanismo basado en arrendamiento
- Sesiones con estado
- Todas las funciones de NFS en un único puerto (2049)
- Solo TCP
- Asignación de dominio de ID
- Integración de Kerberos (NFSv3 puede utilizar Kerberos, pero solo para NFS, no para protocolos auxiliares como NLM)

Dependencias de NFSv4.1

Debido a las funciones de seguridad adicionales de NFSv4.1, existen algunas dependencias externas

implicadas que no fueron necesarias para utilizar NFSv3 (de forma similar a cómo requiere SMB dependencias como Active Directory).

ACL de NFSv4.1

Cloud Volumes Service ofrece compatibilidad con las ACL de NFSv4.x, las cuales proporcionan ventajas distintivas con respecto a los permisos de estilo POSIX normales, como las siguientes:

- Control granular del acceso de los usuarios a los archivos y directorios
- Mejor seguridad NFS
- Interoperabilidad mejorada con CIFS/SMB
- Eliminación de la limitación NFS de 16 grupos por usuario con seguridad AUTH_SYS
- Los ACL omiten la necesidad de resolución del identificador de grupo (GID), que elimina en realidad las ACL de GID limititNFSv4.1 se controlan desde clientes NFS, no desde Cloud Volumes Service. Para utilizar las ACL de NFSv4.1, asegúrese de que la versión de software de su cliente las admite y de que están instaladas las utilidades NFS adecuadas.

Compatibilidad entre las ACL de NFSv4.1 y los clientes de SMB

Las ACL de NFSv4 son distintas de las de ACL de nivel de archivo de Windows (ACL de NTFS), pero llevan funciones similares. Sin embargo, en los entornos NAS multiprotocolo, si hay ACL de NFSv4.1 y utiliza acceso de doble protocolo (NFS y SMB en los mismos conjuntos de datos), los clientes que utilicen SMB2.0 y versiones posteriores no podrán ver ni gestionar ACL desde 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).** Entrada de permiso en la lista.

Cuando un cliente establece una ACL de NFSv4.1 en un archivo durante una operación SETATTR, Cloud Volumes Service establece esa ACL en el objeto, por lo que se sustituye cualquier ACL existente. Si no hay ACL en un archivo, los permisos de modo en el archivo se calculan a partir de OWNER@, GROUP@ y EVERYONE@. Si hay algún bit SUID/SGID/STICKY existente en el archivo, no se verán afectados.

Cuando un cliente obtiene una ACL de NFSv4.1 en un archivo durante UNA operación GETATTR, Cloud Volumes Service lee la ACL de NFSv4.1 asociada con el objeto, construye una lista de ACE y devuelve la lista al cliente. Si el archivo tiene una ACL de NT o bits de modo, se crea una ACL a partir de bits de modo y se devuelve al cliente.

Se deniega el acceso si EXISTE UNA ACE DENEGADA en la ACL; el acceso se concede si existe una ACE DE PERMISO. Sin embargo, también se deniega el acceso si ninguno de los ACE está presente en el ACL.

Un descriptor de seguridad consiste en una ACL de seguridad (SACL) y una ACL discrecional (DACL). Cuando NFSv4.1 interactúa con CIFS/SMB, el DACL se asigna de uno a uno con NFSv4 y CIFS. El DACL consta de LOS ACs PERMITIR Y DENEGAR.

Si es un básico `chmod` Se ejecuta en un archivo o carpeta con conjuntos de ACL de NFSv4.1, se conservan las ACL de usuario y grupo existentes, pero se modifican las ACL de PROPIETARIO@, GRUPO@ y TODOS@ predeterminadas.

Un cliente que utilice las ACL de NFSv4.1 puede definir y ver ACL de archivos y directorios en el sistema.

Cuando se crea un archivo o subdirectorio nuevo en un directorio que tiene una ACL, ese objeto hereda todos los ACE de la ACL que se han etiquetado con el correspondiente "indicadores de herencia".

Si un archivo o directorio tiene una ACL de NFSv4.1, esa ACL se utiliza para controlar el acceso, independientemente de qué protocolo se utilice para acceder al archivo o directorio.

Los archivos y directorios heredan los ACE de las ACL de NFSv4 en directorios principales (posiblemente con las modificaciones adecuadas) siempre que se hayan etiquetado los ACE con las marcas de herencia correctas.

Cuando se crea un archivo o directorio como resultado de una solicitud de NFSv4, la ACL del archivo o directorio resultante depende de si la solicitud de creación de archivos incluye una ACL o solo permisos de acceso estándar a archivos UNIX. La ACL también depende de si el directorio primario tiene una ACL.

- Si la solicitud incluye una ACL, se utiliza esa ACL.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio principal no tiene una ACL, el modo de archivo de cliente se utiliza para establecer permisos de acceso estándar a archivos UNIX.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio primario 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 sólo permisos de acceso estándar a archivos UNIX pero el directorio principal tiene una ACL, el archivo o directorio nuevos heredan los ACE de la ACL del directorio principal siempre que se hayan etiquetado los ACE con los indicadores de herencia correspondientes.

Permisos 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 acerca de estos valores de letra, consulte "CÓMO: Utilizar NFSv4 ACL".

Comportamiento de ACL de NFSv4.1 con herencia umask y ACL

"Las ACL de NFSv4 proporcionan la capacidad de ofrecer herencia de ACL". La herencia de ACL significa que los archivos o carpetas creados debajo de los objetos con conjuntos de ACL de NFSv4.1 pueden heredar las ACL según la configuración de "Indicador de herencia de ACL".

"Umask" se utiliza para controlar el nivel de permisos en el que se crean archivos y carpetas en un directorio sin interacción del administrador. De forma predeterminada, Cloud Volumes Service permite a umask reemplazar las ACL heredadas, que es el comportamiento esperado según "RFC 5661".

Formato de ACL

Las ACL de NFSv4.1 tienen formato específico. El ejemplo siguiente es un conjunto ACE en un archivo:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

El ejemplo anterior sigue las directrices de formato ACL de:

```
type:flags:principal:permissions
```

Tipo de `A` significa “permitir”. Los indicadores heredar no se establecen en este caso, porque el principal no es un grupo y no incluye la herencia. Además, como ACE no es una entrada DE AUDITORÍA, no es necesario establecer 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 se establece correctamente (o el cliente y el servidor no pueden resolver una cadena de nombre), es posible que la ACL no se comporte como se espera o que el cambio de ACL no se pueda aplicar y generar un error.

Los errores de muestra son los siguientes:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

RECHAZO explícito

Los permisos de NFSv4.1 pueden incluir atributos DE DENEGACIÓN explícitos para EL PROPIETARIO, EL GRUPO Y TODOS. Esto se debe a que las ACL de NFSv4.1 son denegadas por defecto, lo que significa que si un ACE no concede explícitamente una ACL, se deniega. Los atributos DE DENEGACIÓN explícita anulan cualquier ACE de ACCESO, explícita o no.

DENEGAR ACE se establece con una etiqueta de atributo de `D`.

En el siguiente ejemplo, SE permite a GROUP@ todos los permisos de lectura y ejecución, pero se le deniega todo el 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
```

DENEGAR ACs debe evitarse siempre que sea posible porque pueden ser confusos y complicados; PERMITIR que las ACL que no están definidas explícitamente se deniegan implícitamente. Cuando SE establecen LAS ACE DENEGADAS, es posible que se deniegue el acceso a los usuarios cuando esperan que se les conceda el acceso.

El conjunto anterior de ACE es equivalente a 755 bits de modo, lo que significa:

- El propietario tiene derechos completos.
- Los grupos tienen sólo lectura.
- Otros sólo han leído.

Sin embargo, incluso si los permisos se ajustan al equivalente de 775, se puede denegar el acceso debido a LA DENEGACIÓN explícita establecida en TODOS.

Dependencias de asignación de dominio de ID de NFSv4.1

NFSv4.1 aprovecha la lógica de asignación de dominio de ID como capa de seguridad para ayudar a verificar que un usuario que intenta acceder a un montaje de NFSv4.1 es realmente lo que afirman que es. En estos casos, el nombre de usuario y el nombre del grupo que provienen del cliente NFSv4.1 anexa una cadena de nombres y la envía a la instancia de Cloud Volumes Service. Si esa combinación de nombre de usuario/grupo y cadena de ID no coincide, el usuario y/o grupo se utiliza en la función no se define ningún usuario por defecto en la `/etc/idmapd.conf` archivo en el cliente.

Esta cadena de ID es un requisito para la observancia correcta de los permisos, especialmente cuando se utilizan las ACL de NFSv4.1 y/o Kerberos. Como resultado, las dependencias del servidor del servicio de nombres, como los servidores LDAP, son necesarias para garantizar la coherencia entre los clientes y la Cloud Volumes Service con el fin de resolver correctamente la identidad de nombres de usuario y grupo.

Cloud Volumes Service utiliza un valor de nombre de dominio de ID predeterminado estático de `defaultv4iddomain.com`. Los clientes NFS utilizan de forma predeterminada el nombre de dominio DNS para la configuración de nombre de dominio ID, pero puede ajustar manualmente el nombre de dominio ID en `/etc/idmapd.conf`.

Si LDAP está habilitado en Cloud Volumes Service, Cloud Volumes Service automatiza el dominio de identificador de NFS para cambiar a lo que está configurado para el dominio de búsqueda en DNS y los clientes no tendrán que modificarse a menos que utilicen nombres de búsqueda de dominio DNS diferentes.

Cuando Cloud Volumes Service puede resolver un nombre de usuario o de grupo en archivos locales o LDAP, se utiliza la cadena de dominio y los ID de dominio no coincidentes no se pueden squash a nadie. Si Cloud Volumes Service no puede encontrar un nombre de usuario o nombre de grupo en los archivos locales o LDAP, se utiliza el valor de ID numérico y el cliente NFS resuelve el nombre correctamente (esto es similar al comportamiento de NFSv3).

Sin cambiar el dominio de Id. De NFSv4.1 del cliente para que coincida con el uso del volumen de Cloud Volumes Service, verá el siguiente comportamiento:

- Los usuarios y grupos UNIX con entradas locales en Cloud Volumes Service (como root, tal como se define en los usuarios y grupos locales de UNIX) se utilizan en el valor nobody.
- Los usuarios y grupos de UNIX con entradas en LDAP (si Cloud Volumes Service está configurado para usar LDAP) no se conectan a nadie si los dominios DNS son diferentes entre los clientes NFS y Cloud Volumes Service.
- Los usuarios y grupos de UNIX que no tienen entradas locales ni entradas LDAP utilizan el valor de ID numérico y resuelven el nombre especificado en el cliente NFS. Si no existe ningún nombre en el cliente, sólo se muestra el ID numérico.

A continuación se muestran los resultados de la situación 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 ID de cliente y servidor coinciden, así es como el mismo aspecto del 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 acerca de este problema y cómo resolverlo, consulte la sección "NFSv4.1 y el usuario/grupo nadie."

Dependencias de Kerberos

Si va a utilizar Kerberos con NFS, debe tener lo siguiente con Cloud Volumes Service:

- Dominio de Active Directory para 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 Cloud Volumes Service requiere un SPN de usuario a la asignación de usuarios UNIX para una funcionalidad adecuada).
- LDAP habilitado en la instancia de Cloud Volumes Service
- Dominio de Active Directory para servicios DNS

NFSv4.1 y el usuario/grupo nadie

Uno de los problemas más comunes que se ven con una configuración de NFSv4.1 es cuando se muestra un archivo o una carpeta en un listado mediante `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, es posible que el archivo muestre el propietario correcto pero `nobody` como grupo.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

¿Quién no es nadie?

La `nobody` El usuario de NFSv4.1 es diferente del `nfsnobody` usuario. Puede ver cómo un cliente NFS ve cada usuario ejecutando el `id` comando:

```
# 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` user es el usuario predeterminado definido por `idmapd.conf` file y puede definirse como cualquier usuario que desee utilizar.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

¿Por qué sucede esto?

Puesto que la seguridad mediante la asignación de cadenas de nombres es un conjunto de claves de las operaciones de NFSv4.1, el comportamiento predeterminado cuando una cadena de nombres no coincide correctamente es squash a ese usuario con uno que normalmente no tendrá acceso a los archivos y carpetas que pertenecen a usuarios y grupos.

Cuando vea `nobody` Para el usuario o el grupo de los listados de archivos, esto generalmente significa que hay algo configurado para NFSv4.1. Aquí puede entrar en juego la sensibilidad del caso.

Por ejemplo, si usuario1@CVSDEMO.LOLARL (uid 1234, gid 1234) está accediendo a una exportación, entonces Cloud Volumes Service debe ser capaz de encontrar usuario1@CVSDEMO.LOLARL (uid 1234, gid 1234). Si el usuario en Cloud Volumes Service es USER1@CVSDEMO.LLOLex, entonces no coincidiría (USUARIO1 en mayúscula frente al usuario en minúscula 1). 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 afirma que es, por lo que debe comprobar lo siguiente para asegurarse de que el usuario que ve el cliente tiene la misma información que el usuario que ve Cloud Volumes Service.

- **Dominio de ID NFSv4.x.** Cliente: `idmapd.conf` Archivo; utiliza Cloud Volumes Service `defaultv4iddomain.com` y no se puede cambiar manualmente. Si se utiliza LDAP con NFSv4.1, Cloud Volumes Service cambia el dominio de ID por lo que utiliza el dominio de búsqueda DNS, que es el mismo que el dominio de AD.
- **Nombre de usuario e ID numéricos.** esto determina dónde busca el cliente los nombres de usuario y aprovecha la configuración del conmutador de servicio de nombres—cliente: `nsswitch.conf` Y/o archivos locales passwd y group; Cloud Volumes Service no permite modificaciones a esto pero agrega automáticamente LDAP a la configuración cuando está habilitado.
- **Nombre del grupo e ID numéricos.** esto determina dónde está buscando el cliente los nombres de grupo y aprovecha la configuración del conmutador de servicio de nombres—cliente: `nsswitch.conf` Y/o archivos locales passwd y group; Cloud Volumes Service no permite modificaciones a esto pero agrega automáticamente LDAP a la configuración cuando está habilitado.

En casi todos los casos, si ve `nobody` En las listas de usuarios y grupos de clientes, el problema es la traducción de ID de dominio de nombre de usuario o grupo entre Cloud Volumes Service y el cliente NFS. Para evitar esta situación, use LDAP para resolver la información de usuario y grupo entre los clientes y Cloud Volumes Service.

Ver cadenas de ID de nombres para NFSv4.1 en clientes

Si utiliza NFSv4.1, hay una asignación de cadena de nombre que se realiza durante las operaciones de NFS, como se ha descrito anteriormente.

Además de utilizar `/var/log/messages` Para encontrar un problema con los ID de NFSv4, puede utilizar la "nfsidmap -l" Comando en el cliente NFS para ver los nombres de usuario que se han asignado correctamente al dominio de NFSv4.

Por ejemplo, se trata del resultado del comando después de que un usuario que puede encontrar el cliente y Cloud Volumes Service 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 que no se asigna correctamente al dominio de ID de NFSv4.1 (en este caso, `netapp-user`) intenta acceder al mismo montaje y toca un archivo, están asignados `nobody:nobody`, según lo esperado.

```
# 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
```

La `nfsidmap -l` salida muestra al usuario `pcuser` en la pantalla pero no `netapp-user`; éste 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 uso compartido de archivos de red desarrollado por Microsoft que proporciona autenticación centralizada de usuarios/grupos, permisos, bloqueo y uso compartido de archivos a varios 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 recursos compartidos y ofrecen control de acceso mediante permisos de nivel de recursos compartidos. SMB puede presentarse a cualquier cliente que ofrezca compatibilidad con el protocolo, incluidos clientes de Windows, Apple y Linux.

Cloud Volumes Service es compatible con las versiones SMB 2.1 y 3.x del protocolo.

Control de acceso/recursos compartidos de SMB

- Cuando un nombre de usuario de Windows solicita acceso al volumen Cloud Volumes Service, Cloud Volumes Service busca un nombre de usuario UNIX utilizando los métodos configurados por los administradores de Cloud Volumes Service.
- Si se configura un proveedor de identidad UNIX externo (LDAP) y los nombres de usuario de

Windows/UNIX son idénticos, entonces los nombres de usuario de Windows asignarán 1:1 a nombres de usuario de UNIX sin necesidad de ninguna configuración adicional. Cuando LDAP está habilitado, Active Directory se utiliza para alojar esos atributos UNIX para objetos de grupo y usuario.

- Si los nombres de Windows y UNIX no coinciden de la misma manera, se debe configurar LDAP para permitir que Cloud Volumes Service utilice la configuración de asignación de nombres LDAP (consulte la sección ""Utilizar LDAP para asignar nombres asimétricos"").
- Si LDAP no está en uso, los usuarios SMB de Windows se asignan a un usuario UNIX local predeterminado denominado `pcuser` En Cloud Volumes Service. Esto significa que los usuarios que se asignan a los archivos escritos en Windows `pcuser` Mostrar propiedad de UNIX como `pcuser` En entornos NAS multiprotocolo. `pcuser` aquí está efectivamente la `nobody` Usuario en entornos Linux (UID 65534).

En implementaciones con solo SMB, el `pcuser` La asignación se sigue produciendo, pero no importa, porque la propiedad de usuarios y grupos de Windows se muestra correctamente y no se permite el acceso NFS al volumen sólo para SMB. Además, los volúmenes solo para SMB no admiten la conversión a volúmenes de protocolo doble o NFS después de crearse.

Windows utiliza Kerberos para la autenticación de nombre de usuario con los controladores de dominio de Active Directory, que requiere un intercambio de nombre de usuario/contraseña con los DC de AD, que es externo a la instancia de Cloud Volumes Service. La autenticación Kerberos se utiliza cuando el `\\SERVERNAME` Los clientes SMB utilizan la ruta UNC que es la siguiente:

- Existe una entrada DNS A/AAAA para SERVERNAME
- Existe un SPN válido para el acceso SMB/CIFS para SERVERNAME

Cuando se crea un volumen SMB de Cloud Volumes Service, se crea el nombre de la cuenta de la máquina, tal como se define en la sección ""Cómo aparece Cloud Volumes Service en Active Directory."" Ese nombre de cuenta de equipo también se convierte en la ruta de acceso a recursos compartidos SMB porque Cloud Volumes Service aprovecha DNS dinámico (DDNS) para crear las entradas A/AAAA y PTR necesarias en DNS y las entradas SPN necesarias en el principal de cuenta de máquina.

> Para crear entradas PTR, la zona de búsqueda inversa para la dirección IP de la instancia Cloud Volumes Service debe existir en el servidor DNS.

Por ejemplo, este volumen Cloud Volumes Service utiliza la siguiente ruta de uso compartido UNC: `\\cvs-east- 433d.cvsdemo.local`.

En Active Directory, estas son las entradas de SPN generadas por el servicio Cloud 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 búsqueda directa/inversa de DNS:

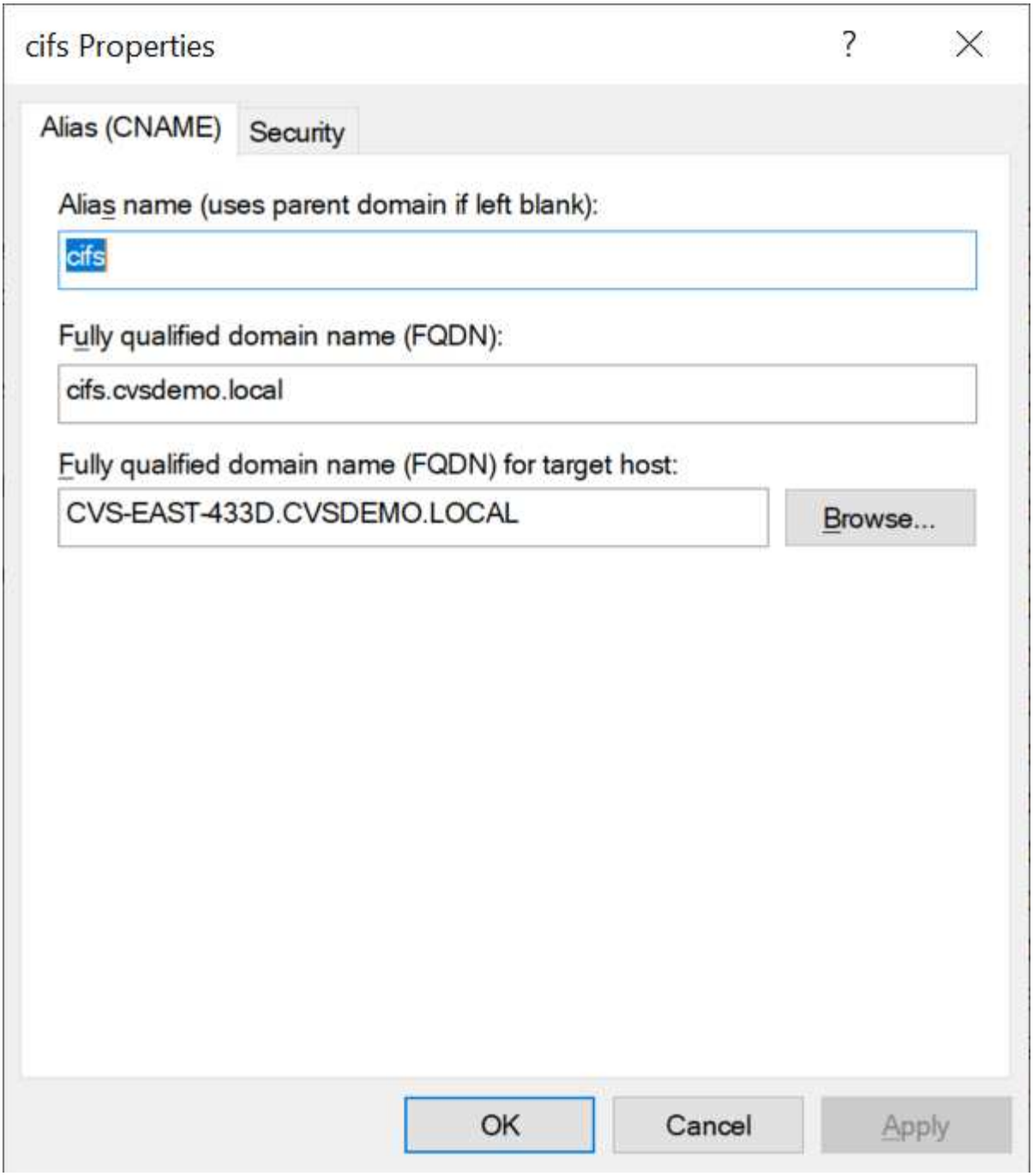
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

De manera opcional, se puede aplicar un mayor control de acceso al habilitar o requerir el cifrado SMB para recursos compartidos SMB en Cloud Volumes Service. Si uno de los extremos no admite el cifrado SMB, no se permite el acceso.

Usar alias de nombre de SMB

En algunos casos, podría ser una preocupación de seguridad para los usuarios finales saber el nombre de la cuenta de equipo que se está utilizando para Cloud Volumes Service. En otros casos, es posible que simplemente desee proporcionar una ruta de acceso más sencilla a sus usuarios finales. En esos casos, puede crear alias SMB.

Si desea crear alias para la ruta de acceso compartida SMB, puede aprovechar lo que se conoce como registro CNAME en DNS. Por ejemplo, si desea usar el nombre `\\CIFS` para acceder a los recursos compartidos en lugar de `\\cvs-east- 433d.cvsdemo.local`, Pero todavía desea utilizar la autenticación Kerberos, un CNAME en DNS que señala al registro A/AAAA existente y un SPN adicional agregado a la cuenta de equipo existente proporciona acceso Kerberos.



Este es el resultado de 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:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Esta es la consulta SPN resultante tras agregar nuevos números de dominio:

```
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 paquete, podemos ver la solicitud de configuración de sesión mediante 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

Cloud Volumes Service admite lo siguiente "dialectos" Para la autenticación SMB:

- LM
- NTLM
- NTLMv2
- Kerberos

La autenticación Kerberos para 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.

Cloud Volumes Service también admite compatibilidad con versiones anteriores de la autenticación LM y NTLM. Cuando Kerberos está mal configurado (como al crear alias SMB), el acceso al recurso compartido vuelve a los métodos de autenticación más débiles (como NTLMv2). Debido a que estos mecanismos son menos seguros, se desactivan en algunos entornos de Active Directory. Si los métodos de autenticación más débiles están desactivados y Kerberos no está configurado correctamente, el acceso al recurso compartido falla porque no hay ningún método de autenticación válido al que recurrir.

Para obtener información acerca de cómo configurar o ver los niveles de autenticación compatibles en Active Directory, consulte "Seguridad de red: Nivel de autenticación de LAN Manager".

Modelos de permisos

Permisos NTFS/Archivo

Los permisos NTFS son los permisos aplicados a archivos y carpetas en sistemas de archivos que cumplen la lógica NTFS. Puede aplicar permisos NTFS en `Basic` o. `Advanced` y se puede establecer en `Allow` o. `Deny` para control de acceso.

Los permisos básicos incluyen los siguientes:

- Control total
- Modificar
- Lectura y ejecución
- Lea
- Escritura

Cuando establece permisos para un usuario o grupo, denominado ACE, reside en una ACL. Los permisos NTFS utilizan los mismos conceptos básicos de lectura/escritura/ejecución que los bits de modo UNIX, pero también pueden extenderse a controles de acceso más granulares y extendidos (también conocidos como permisos especiales), como tomar posesión, Crear carpetas/datos anexados, escribir atributos, etc.

Los bits de modo UNIX estándar no proporcionan el mismo nivel de granularidad que los permisos NTFS (como ser capaz de establecer permisos para objetos de usuario y grupo individuales 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 de uso compartido y se pueden utilizar junto con los permisos de uso compartido. Con las estructuras de permisos NTFS, se aplica el más restrictivo. Como tal, las denegaciones explícitas a un usuario o grupo anulan incluso Control total al definir los derechos de acceso.

Los permisos NTFS se controlan desde clientes SMB de Windows.

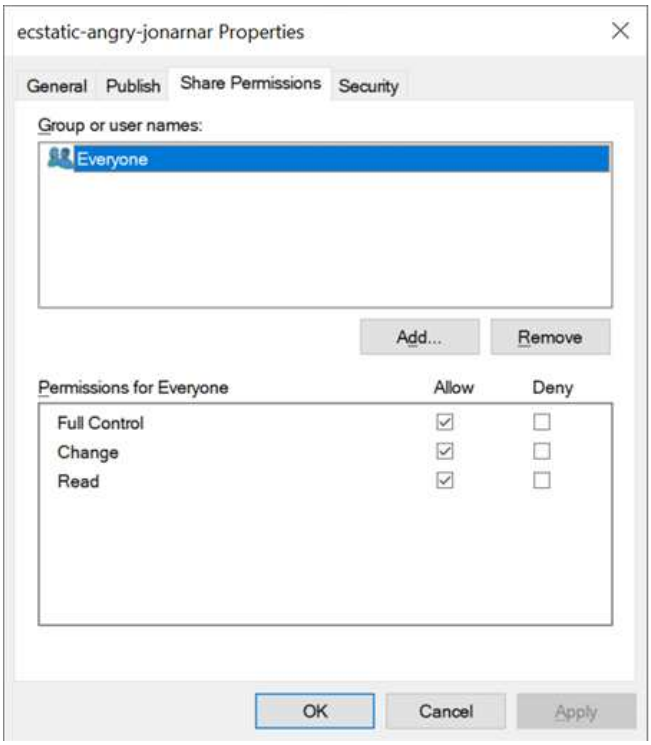
Comparta los permisos

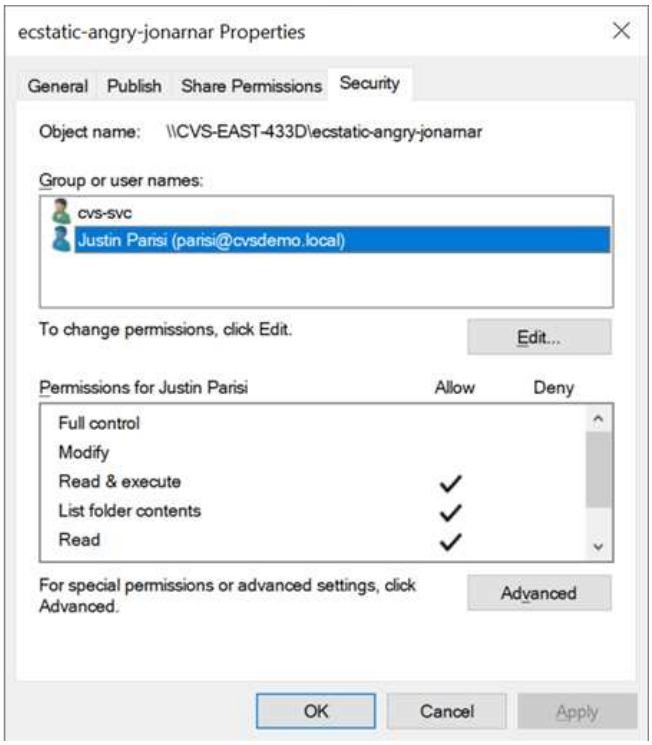
Los permisos de recursos compartidos son más generales que los permisos NTFS (sólo lectura/cambio/control total) y controlan la entrada inicial en un recurso compartido SMB, de forma similar a cómo funcionan las reglas de política de exportación NFS.

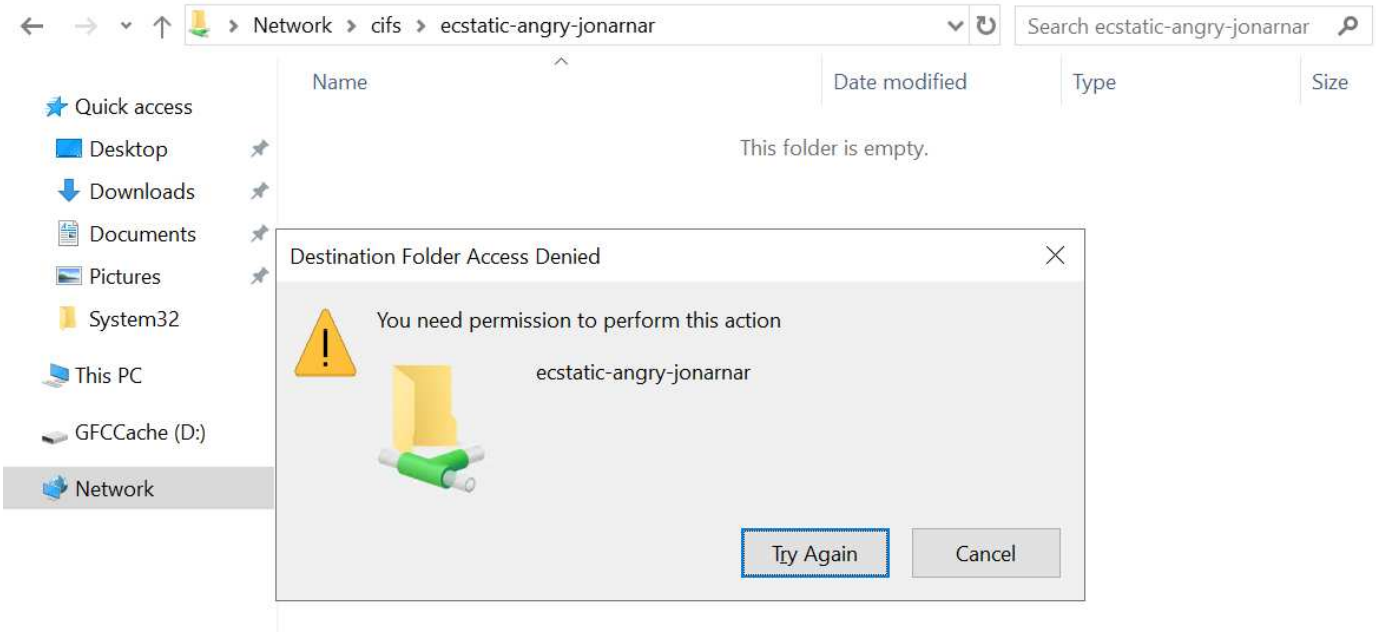
Si bien las reglas de política de exportación de NFS controlan el acceso mediante información basada en hosts, como direcciones IP o nombres de hosts, los permisos de uso compartido de SMB pueden controlar el acceso mediante ACE de usuario y de grupo en una ACL compartida. Puede configurar las ACL para compartir desde el cliente de Windows o desde la IU de gestión de Cloud Volumes Service.

De forma predeterminada, las ACL compartidas y las ACL de volumen inicial incluyen a todos los usuarios con control total. Las ACL de archivo se deben cambiar pero los permisos de uso compartido están anulados por los permisos de archivo de los objetos del recurso compartido.

Por ejemplo, si a un usuario solo se le permite acceso de lectura a la ACL del archivo de volumen Cloud Volumes Service, se les deniega el acceso para crear archivos y carpetas aunque la ACL de uso compartido esté establecida en todos los usuarios con control completo, como se muestra en la siguiente figura.







Para obtener los mejores resultados de seguridad, haga lo siguiente:

- Elimine a todos los usuarios de las ACL de uso compartido y de archivo y, en su lugar, establezca el acceso compartido para usuarios o grupos.
- Utilice grupos para controlar el acceso en lugar de usuarios individuales con el fin de facilitar la gestión y agilizar la incorporación/eliminación de usuarios para compartir ACL a través de la gestión de grupos.
- Permita un acceso compartido menos restrictivo y más general a los ACE en los permisos de uso compartido y bloquee el acceso a los usuarios y grupos con permisos de archivos para obtener un control de acceso más granular.
- Evite el uso general de ACL de denegación explícita, ya que anulan permitir ACL. Limitar el uso de ACL de denegación explícita para usuarios o grupos que deben restringirse rápidamente del acceso a un sistema

de archivos.

- Asegúrese de prestar atención al "Herencia de ACL" configuración al modificar los permisos; establecer el indicador de herencia en el nivel superior de un directorio o volumen con altos recuentos de archivos significa que cada archivo debajo de ese directorio o volumen ha heredado permisos que se le han agregado, que puede crear comportamientos no deseados como acceso no intencionado/denegación y pérdida prolongada de modificación de permisos a medida que se ajusta cada archivo.

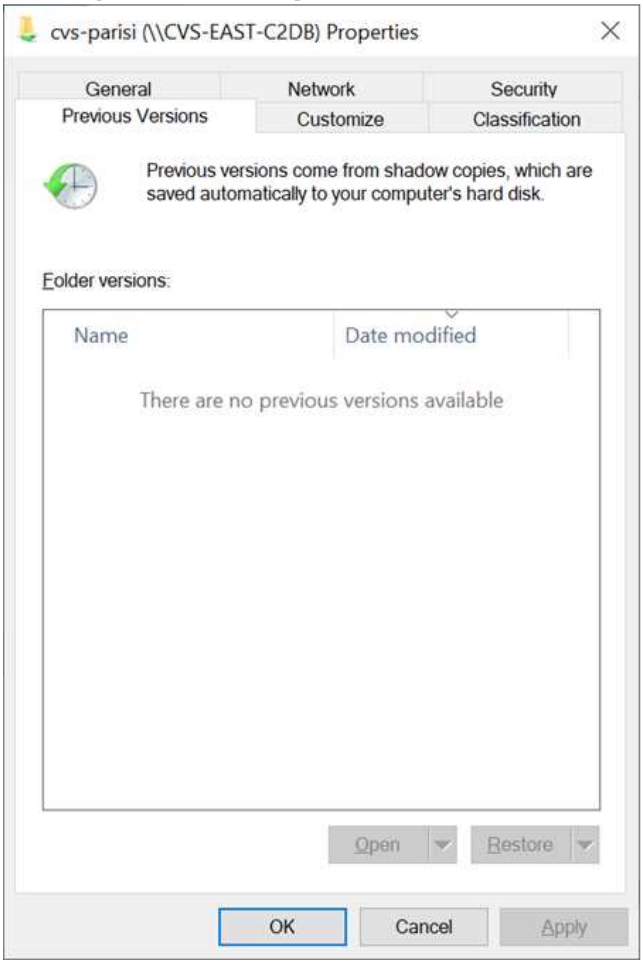
Funciones de seguridad para recursos compartidos de SMB

Cuando se crea por primera vez un volumen con acceso de SMB en Cloud Volumes Service, se presenta una serie de opciones para proteger ese volumen.

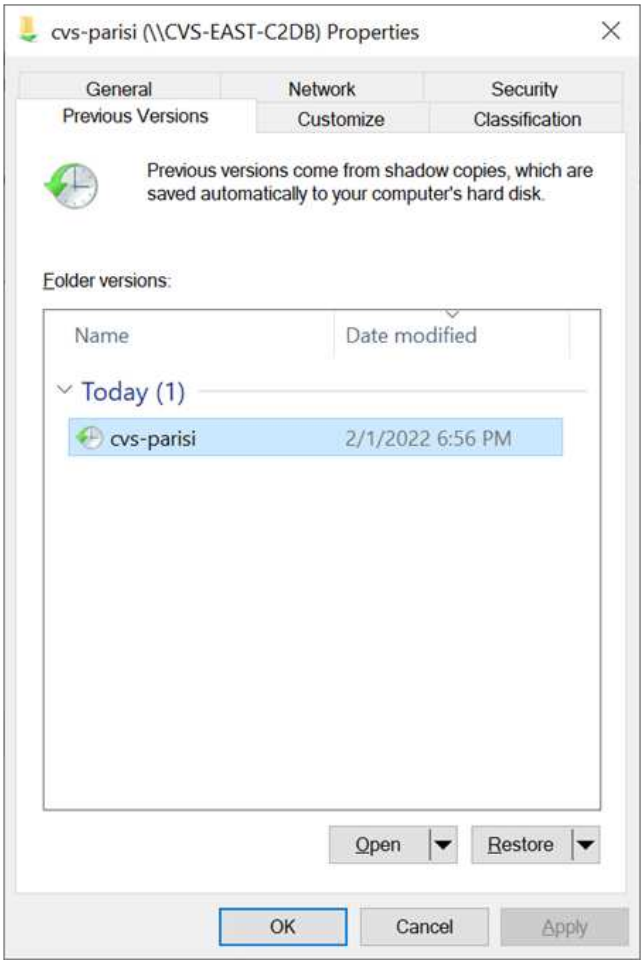
Algunas de estas opciones dependen del nivel de Cloud Volumes Service (rendimiento o software) y las opciones disponibles son:

- **Hacer visible el directorio de la instantánea (disponible tanto para CVS-Performance como para CVS-SW).** esta opción controla si los clientes de SMB pueden acceder al directorio de la instantánea en un recurso compartido de SMB (`\\server\share\~snapshot` Y/o la ficha versiones anteriores). La configuración predeterminada no está activada, lo que significa que el volumen se oculta y se despermite el acceso a la `~snapshot` y no aparecen copias Snapshot en la pestaña versiones anteriores del volumen.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Ocultar copias Snapshot de usuarios finales puede ser conveniente por motivos de seguridad, por motivos de rendimiento (ocultar estas carpetas de los análisis AV) o por preferencias. Las instantáneas Cloud Volumes

Service son de sólo lectura, por lo que aunque estas Snapshots estén visibles, los usuarios finales no pueden eliminar ni modificar archivos en el directorio Snapshot. Se aplican permisos de archivo en los archivos o carpetas en el momento en que se realizó la copia snapshot. Si los permisos de un archivo o carpeta cambian entre copias Snapshot, los cambios también se aplican a los archivos o carpetas del directorio Snapshot. Los usuarios y grupos pueden obtener acceso a estos archivos o carpetas en función de los permisos. Aunque no es posible eliminar o modificar archivos del directorio Snapshot, es posible copiar archivos o carpetas fuera del directorio Snapshot.

- **Activar cifrado SMB (disponible tanto para CVS-Performance como para CVS-SW).** el cifrado SMB está desactivado en el recurso compartido SMB de forma predeterminada (sin seleccionar). Al activar la casilla se habilita el cifrado SMB, lo que significa que el tráfico entre el cliente SMB y el servidor se cifra en tránsito con los niveles de cifrado más altos admitidos negociados. Cloud Volumes Service admite hasta el cifrado AES-256 para SMB. La habilitación del cifrado SMB supone un detrimento del rendimiento que puede o no ser perceptible para sus clientes de SMB, aproximadamente en el rango de 10-20 %. NetApp recomienda encarecidamente realizar pruebas para ver si esa penalización en el rendimiento es aceptable.
- **Ocultar recurso compartido SMB (disponible tanto para CVS-Performance como para CVS-SW).** al establecer esta opción se oculta la ruta de acceso compartido SMB de la navegación normal. Esto significa que los clientes que no conocen la ruta de acceso al recurso compartido no pueden ver los recursos compartidos al acceder a la ruta UNC predeterminada (por ejemplo `\\CVS-SMB`). Cuando se selecciona la casilla de verificación, solo los clientes que conozcan explícitamente la ruta de acceso compartido SMB o que tengan la ruta de acceso de recurso compartido definida por un objeto de directiva de grupo pueden tener acceso a ella (seguridad mediante ocultación).
- **Activar enumeración basada en acceso (ABE) (sólo CVS-SW).** esto es similar a ocultar el recurso compartido SMB, excepto que los recursos compartidos o archivos sólo están ocultos de 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 acceso de lectura a través de los permisos, entonces el usuario de Windows `joe` No se pueden ver los archivos o recursos compartidos de SMB en absoluto. Esta opción está deshabilitada de forma predeterminada y puede habilitarla mediante la selección de 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)?"
- **Activar soporte compartido de disponibilidad continua (CA) (CVS-Performance solamente).** "Recursos compartidos de SMB disponibles de forma continua" Proporcionar una forma de minimizar las interrupciones de aplicaciones durante eventos de conmutación por error mediante la replicación de estados de bloqueo entre nodos del sistema de entorno de administración de Cloud Volumes Service. Esta no es una función de seguridad, pero sí ofrece una mejor resiliencia general. Actualmente, sólo se admiten las aplicaciones SQL Server y FSLogix para esta funcionalidad.

Recursos compartidos ocultos predeterminados

Cuando se crea un servidor SMB en Cloud Volumes Service, existen "recursos compartidos administrativos ocultos" (Usa la convención de nomenclatura de $) que se crean además del recurso compartido de SMB del volumen de datos. Entre ellas se incluyen C$ (acceso al espacio de nombres) e IPC$ (uso compartido de canalizaciones con nombre para la comunicación entre programas, como las llamadas a procedimiento remoto (RPC) utilizadas para el acceso a Microsoft Management Console (MMC)).

El recurso compartido IPC$ no contiene ACL compartidos y no se puede modificar; se utiliza estrictamente para las llamadas RPC y. "Windows no permite el acceso anónimo a estos recursos compartidos de forma predeterminada".

El recurso compartido C$ permite el acceso BUILTIN/Administrators de forma predeterminada, pero la automatización Cloud Volumes Service elimina la ACL compartida 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

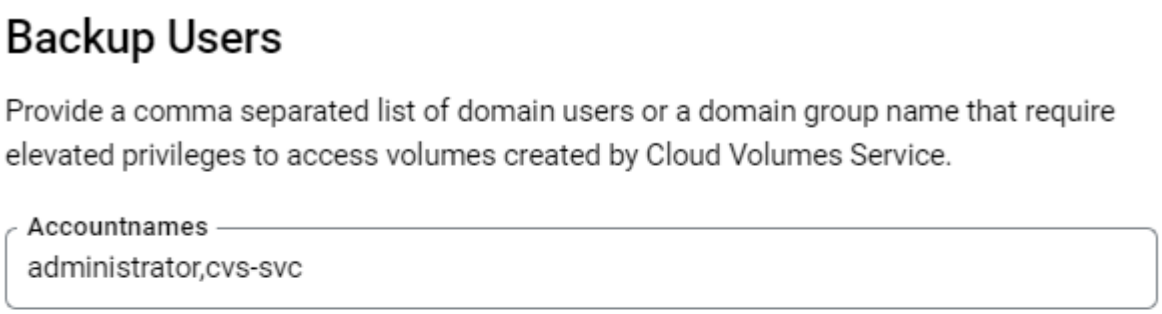
archivos Cloud Volumes Service. Como resultado, intenta navegar a. `\\SERVER\C$` error.

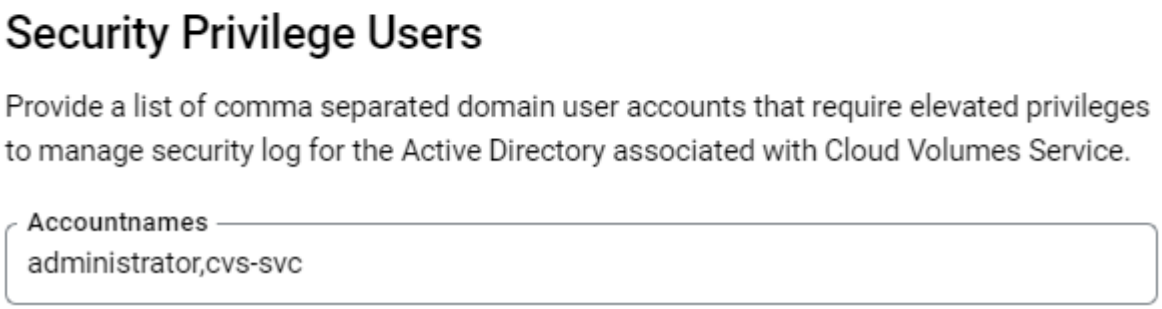
Cuentas con derechos de administrador/copia de seguridad local/BUILTIN

Los servidores SMB de Cloud Volumes Service mantienen una funcionalidad similar a los servidores SMB de Windows regulares en el sentido de que hay grupos locales (como BUILTIN\Administrators) que aplican derechos de acceso a determinados usuarios y grupos de dominio.

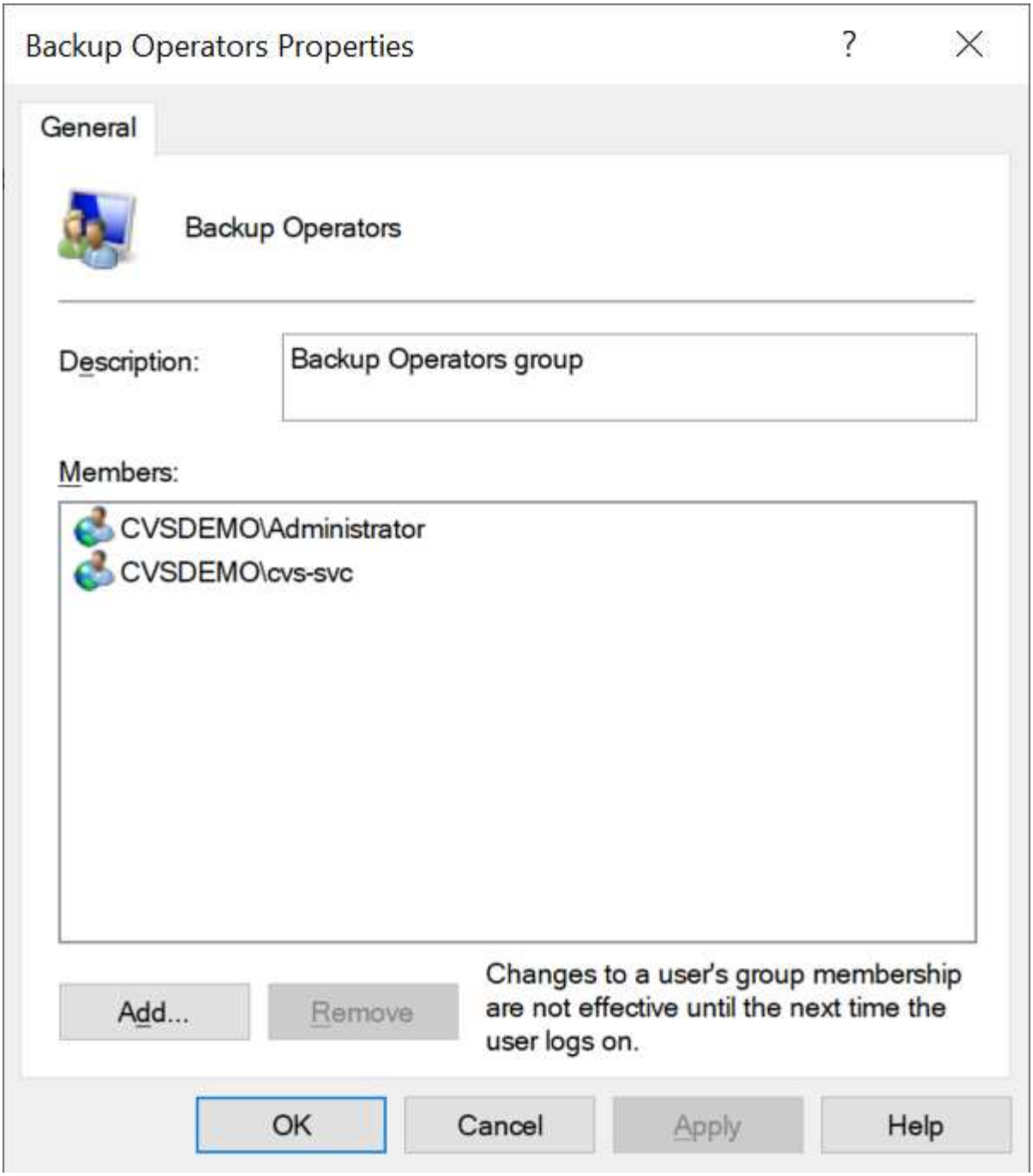
Cuando se especifica un usuario que se va a agregar a los usuarios de copia de seguridad, el usuario se agrega al grupo BUILTIN\operadores de copia de seguridad en la instancia de Cloud Volumes Service que utiliza esa conexión de Active Directory, que a continuación obtiene la "SeBackupPrivilege y SeRestorePrivilege".

Cuando agrega un usuario a usuarios de privilegios de seguridad, se le da al usuario SeSecurityPrivilege, que es útil en algunos casos de uso de aplicaciones, como "SQL Server en recursos compartidos de SMB".





Puede ver las pertenencias a grupos locales de Cloud Volumes Service a través de MMC con los privilegios adecuados. La siguiente figura muestra los usuarios que se han agregado mediante la consola de Cloud Volumes Service.

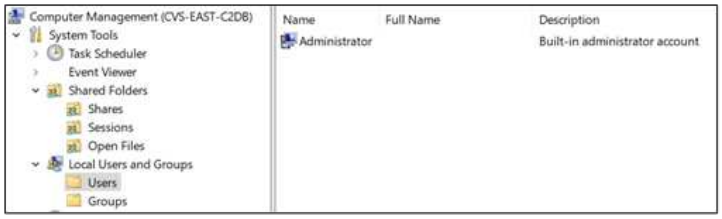


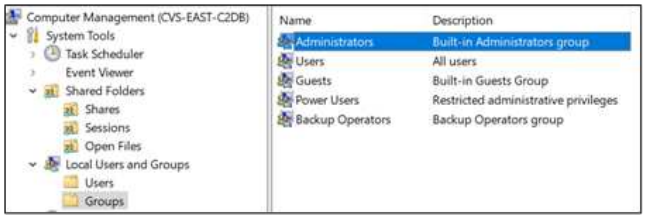
La siguiente tabla muestra la lista de grupos BUILTIN predeterminados y qué usuarios/grupos se agregan de forma predeterminada.

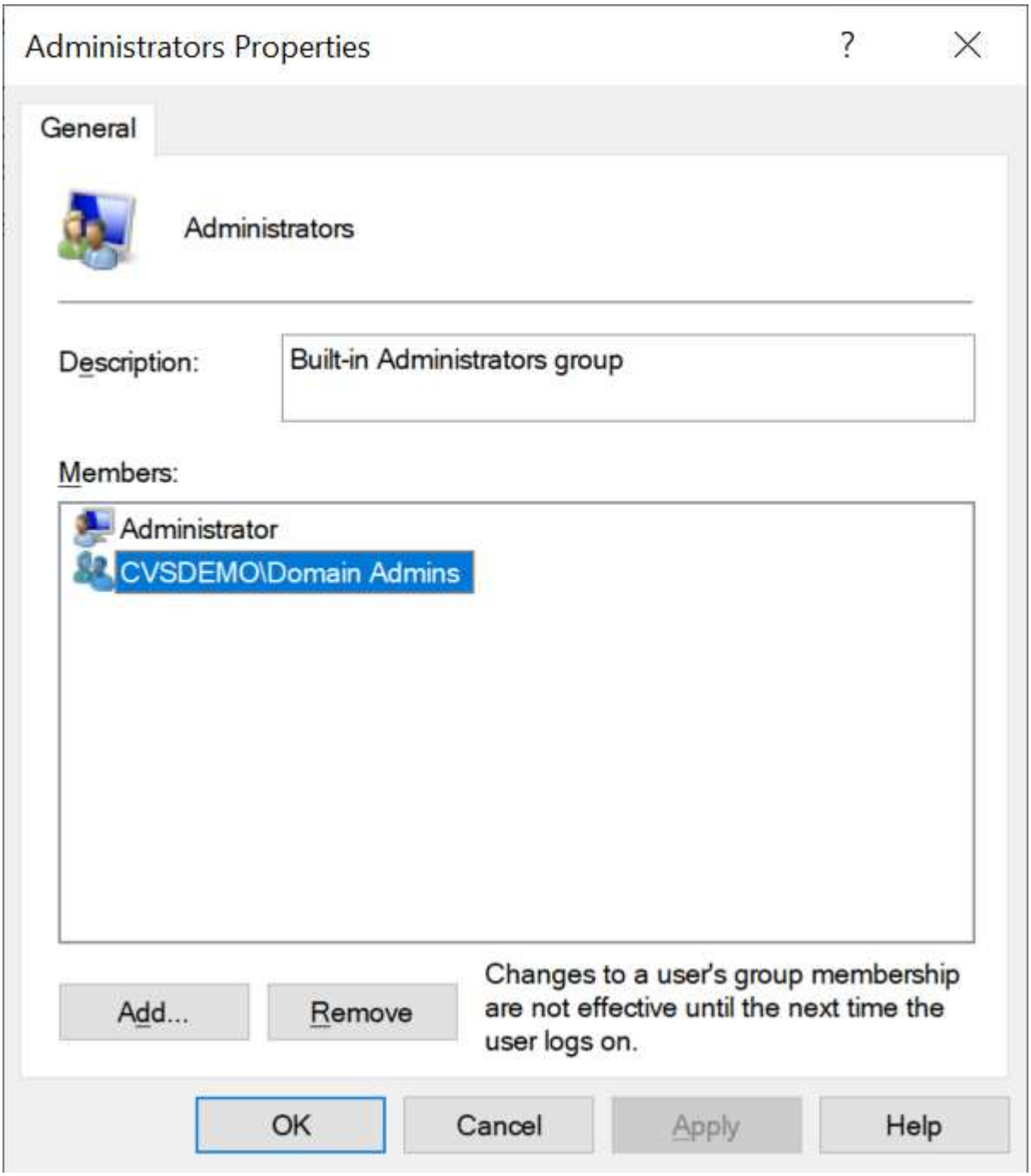
Grupo local/BUILTIN	Miembros predeterminados
BUILTIN\Administrators*	Dominio\Administradores de dominio
Operadores DE COPIAS DE seguridad/BUILTIN*	Ninguno
EDIFICIO\huéspedes	Dominio\invitados de dominio
Usuarios AVANZADOS\BUILTIN	Ninguno
USUARIOS DE BUILTIN\Domain	USUARIOS de DOMINIO/dominio

*Pertenencia a grupos controlada en la configuración de conexión de Cloud Volumes Service Active Directory.

Puede ver los usuarios y grupos locales (y los miembros del grupo) en la ventana MMC, pero no puede agregar ni eliminar objetos ni cambiar las pertenencias a grupos desde esta consola. De forma predeterminada, sólo el grupo Administradores de dominio y Administrador se agregan al grupo BUILTIN\Administradores de Cloud Volumes Service. Actualmente, no puede modificarlo.







Acceso a MMC/Computer Management

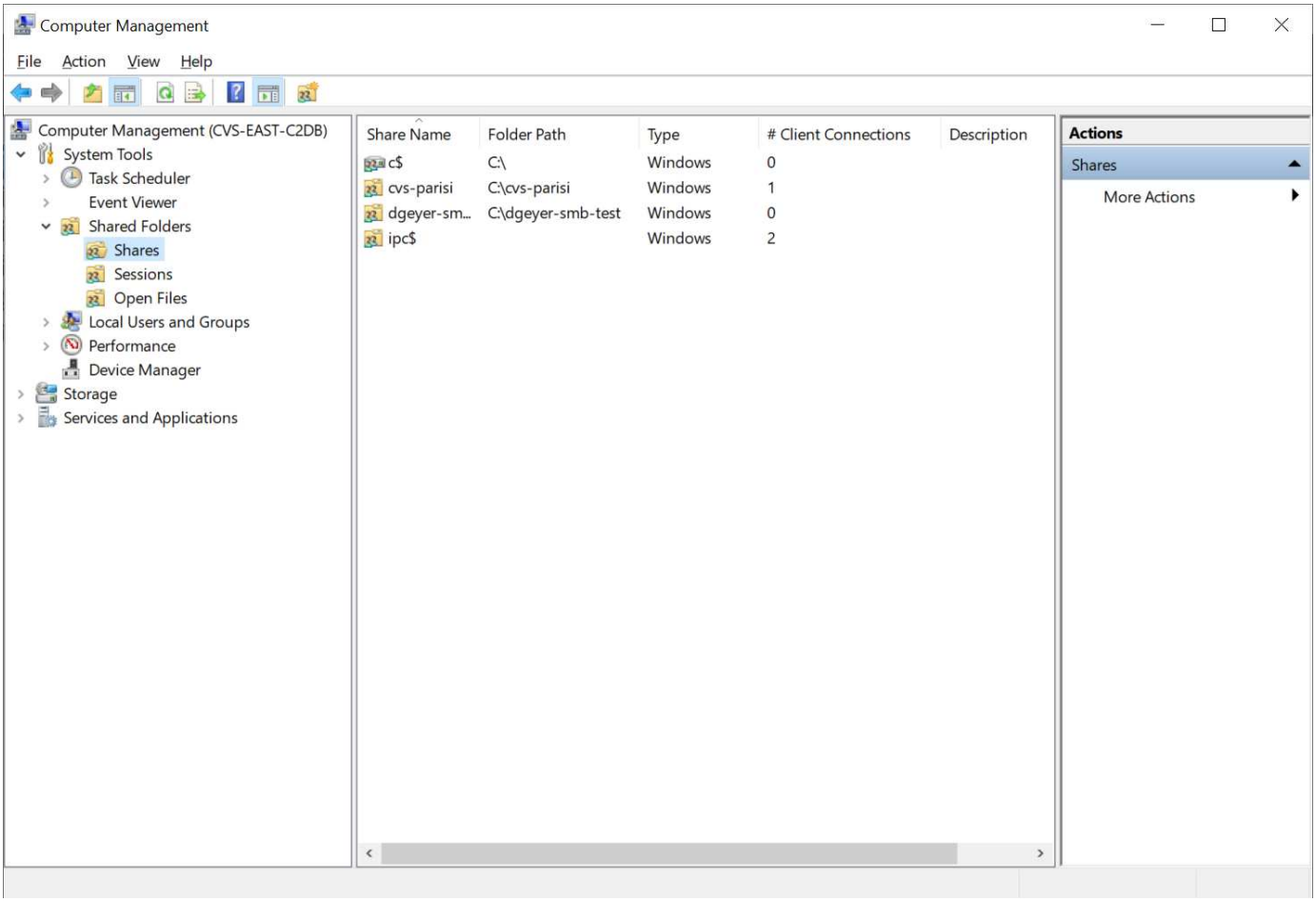
El acceso de SMB en Cloud Volumes Service proporciona conectividad a la MMC de gestión de equipos, que permite ver recursos compartidos, gestionar ACL de uso compartido, ver/gestionar sesiones de SMB y archivos abiertos.

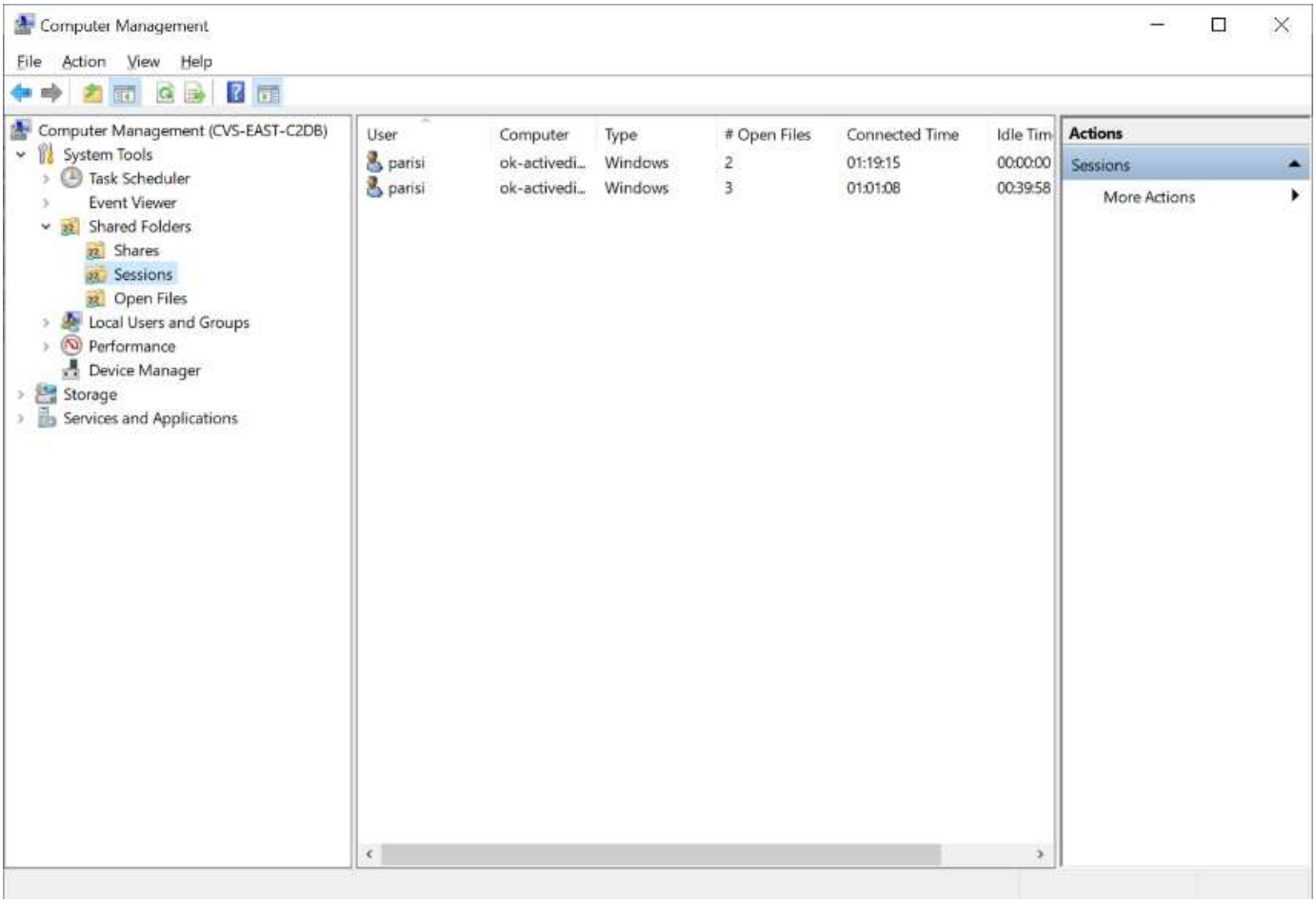
Para utilizar MMC para ver los recursos compartidos y las sesiones de SMB en Cloud Volumes Service, el usuario que ha iniciado sesión debe ser un administrador de dominio. A otros usuarios se les permite el acceso para ver o administrar el servidor SMB desde MMC y recibir un cuadro de diálogo no tiene permisos al intentar ver recursos compartidos o sesiones en la instancia del SMB de Cloud Volumes Service.

Para conectarse al servidor SMB, abra Administración de equipos, haga clic con el botón derecho en Administración de equipos y, a continuación, seleccione conectar a otro equipo. Con esto se abre el cuadro de diálogo Seleccionar equipo, donde puede introducir el nombre del servidor SMB (que se encuentra en la información del volumen Cloud Volumes Service).

Cuando se ven los recursos compartidos de SMB con los permisos adecuados, se ven todos los recursos compartidos disponibles en la instancia de Cloud Volumes Service 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 Cloud Volumes Service.

Recuerde que sólo se permite una conexión de Active Directory por región.





En la siguiente tabla se muestra una lista de las funciones compatibles/no admitidas para MMC.

Funciones admitidas	Funciones no admitidas
• Ver recursos compartidos • Ver sesiones SMB activas • Ver archivos abiertos • Ver usuarios y grupos locales • Ver las membresías de grupo local • Enumera la lista de sesiones, archivos y conexiones de árbol del sistema • Cierre los archivos abiertos en el sistema • Cierre las sesiones abiertas • Cree/gestione recursos compartidos	• Creación de nuevos usuarios/grupos locales • Gestión/visualización de usuarios/grupos locales existentes • Ver eventos o registros de rendimiento • Gestionar el almacenamiento • Gestión de servicios y aplicaciones

Información de seguridad del servidor SMB

El servidor SMB en Cloud Volumes Service utiliza una serie de opciones que definen políticas de seguridad para las conexiones SMB, incluidos factores como la desviación del reloj de Kerberos, la antigüedad de los tickets, el cifrado, etc.

La siguiente tabla contiene una lista de esas opciones, qué hacen, las configuraciones predeterminadas y si

se pueden modificar con Cloud Volumes Service. Algunas opciones no se aplican a Cloud Volumes Service.

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Sesgo de reloj Kerberos máximo (minutos)	Desfase de tiempo máximo entre Cloud Volumes Service y controladoras de dominio. Si la desviación de tiempo supera los 5 minutos, la autenticación de Kerberos fallará. Se establece en el valor predeterminado de Active Directory.	5	No
Duración de la entrada de Kerberos (horas)	Tiempo máximo que un ticket de Kerberos permanece válido antes de requerir una renovación. Si no se produce ninguna renovación antes de las 10 horas, debe obtener un boleto nuevo. Cloud Volumes Service realiza estas renovaciones automáticamente. 10 horas es el valor predeterminado de Active Directory.	10	No
Renovación máxima de entradas Kerberos (días)	Número máximo de días que se puede renovar un billete Kerberos antes de que se necesite una nueva solicitud de autorización. Cloud Volumes Service renueva automáticamente los boletos para las conexiones SMB. Seven Days es el valor predeterminado de Active Directory.	7	No
Tiempo de espera de conexión Kerberos KDC (segundos)	Número de segundos antes de que se agote el tiempo de espera de una conexión KDC.	3	No

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Es necesario firmar para tráfico entrante del bloque de mensajes del servidor	Configuración para requerir la firma para el tráfico SMB. Si se establece en true, los clientes que no admiten la conectividad de firma fallan.	Falso	
Requerir complejidad de contraseña para cuentas de usuario locales	Se usa para las contraseñas en usuarios SMB locales. Cloud Volumes Service no admite la creación de usuarios locales, por lo que esta opción no se aplica a Cloud Volumes Service.	Verdadero	No
Utilice START_tls para conexiones LDAP de Active Directory	Se utiliza para habilitar conexiones TLS de inicio para LDAP de Active Directory. Cloud Volumes Service no admite habilitar esto actualmente.	Falso	No
Es el cifrado AES-128 y AES-256 para Kerberos habilitado	Esto controla si el cifrado AES se utiliza para conexiones de Active Directory y se controla con la opción Activar cifrado AES para autenticación de Active Directory al crear o modificar la conexión de Active Directory.	Falso	Sí
Nivel de compatibilidad LM	Nivel de dialectos de autenticación compatibles para conexiones de Active Directory. Consulte la sección “Dialectos de autenticación SMB” para más información.	ntlmv2-krb	No
Se requiere cifrado SMB para el tráfico CIFS entrante	Requiere cifrado SMB para todos los recursos compartidos. Cloud Volumes Service no lo utiliza; en su lugar, establezca el cifrado por volumen (consulte la sección “Funciones de seguridad para recursos compartidos de SMB”).	Falso	No

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Seguridad de sesión de cliente	Establece la firma y/o el sellado para la comunicación LDAP. Esto no está establecido actualmente en Cloud Volumes Service, pero podría ser necesario en futuras versiones para abordar . La solución de problemas de autenticación LDAP debidos a la revisión de Windows se trata en la sección ""Enlace del canal LDAP"."".	Ninguno	No
Activación de SMB2 para conexiones de CC	Utiliza SMB2 para conexiones de CC. Activado de forma predeterminada.	Valor predeterminado del sistema	No
Especificación de referencia LDAP	Al usar varios servidores LDAP, la búsqueda de referencias permite al cliente consultar otros servidores LDAP de la lista cuando no se encuentra una entrada en el primer servidor. Actualmente, Cloud Volumes Service no admite esta operación.	Falso	No
Utilice LDAPS para conexiones seguras de Active Directory	Permite el uso de LDAP sobre SSL. Actualmente no es compatible con Cloud Volumes Service.	Falso	No
Se requiere cifrado para la conexión de CC	Requiere cifrado para conexiones DC correctas. Deshabilitado de forma predeterminada en Cloud Volumes Service.	Falso	No

Protocolo doble/multiprotocolo

Cloud Volumes Service permite compartir los mismos conjuntos de datos tanto con clientes SMB como NFS, a la vez que mantiene los permisos de acceso adecuados ("protocolo dual"). Esto se realiza coordinando la asignación de identidades entre protocolos y utilizando un servidor LDAP de backend centralizado para proporcionar las identidades de UNIX a Cloud Volumes Service. Puede utilizar Windows Active Directory para proporcionar facilidad de uso a los usuarios de Windows y UNIX.

Control de acceso

- **Controles de acceso compartido.** determine qué clientes y/o usuarios y grupos pueden acceder a un recurso compartido NAS. Para NFS, las reglas y políticas de exportación controlan el acceso del cliente a las exportaciones. Las exportaciones NFS se gestionan desde la instancia de Cloud Volumes Service. SMB utiliza recursos compartidos de CIFS/SMB y ACL de uso compartido para proporcionar un control más granular a nivel de usuarios y grupos. Solo puede configurar las ACL a nivel de uso compartido desde clientes de SMB mediante "Administración de MMC/Computer" Con una cuenta que tiene derechos de administrador en la instancia de Cloud Volumes Service (consulte la sección ""Cuentas con derechos de administrador/copia de seguridad local/BUILTIN."").
- **Controles de acceso a archivos.** Controle los permisos 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 de NFSv4. Los clientes de SMB aprovechan los permisos NTFS.

El control de acceso de 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 permisos."

Asignación de usuarios

Cuando un cliente accede a un volumen, Cloud Volumes Service intenta asignar el usuario entrante a un usuario válido en la dirección opuesta. Esto es necesario para que se determine el acceso adecuado a través de los protocolos y para garantizar que el usuario que solicita acceso sea realmente lo que afirma ser.

Por ejemplo, si un usuario de Windows llamado `joe` Intenta acceder a un volumen con permisos UNIX a través del bloque de mensajes del servidor y, a continuación, Cloud Volumes Service realiza una búsqueda para encontrar el usuario UNIX correspondiente llamado `joe`. Si existe, los archivos que se escriben en un recurso compartido SMB como usuario de Windows `joe` Aparece como usuario UNIX `joe` De clientes NFS.

Como alternativa, si un usuario de UNIX llamado `joe` Intenta acceder al volumen Cloud Volumes Service con permisos de Windows y el usuario UNIX debe poder asignarlo a un usuario de Windows válido. De lo contrario, se deniega el acceso al volumen.

Actualmente, sólo se admite Active Directory para la gestión de identidades de UNIX externas con LDAP. Para obtener más información acerca de cómo configurar el acceso a este servicio, consulte "Creación de una conexión AD".

Modelo de permisos

Cuando se utilizan configuraciones de protocolo dual, Cloud Volumes Service utiliza estilos de seguridad para volúmenes para determinar el tipo de ACL. Estos estilos de seguridad se establecen en función de la especificación del protocolo NAS, o en el caso del protocolo dual, es la opción elegida en el momento de la creación del volumen de Cloud Volumes Service.

- Si solo utiliza NFS, los volúmenes de Cloud Volumes Service utilizan permisos de UNIX.
- Si solo utiliza SMB, los volúmenes de Cloud Volumes Service utilizan permisos NTFS.

Si se crea un volumen de protocolo doble, se puede elegir el estilo de ACL al crear un volumen. Esta decisión debe tomarse en función de la administración de permisos deseada. Si los usuarios gestionan permisos desde clientes de Windows/SMB, seleccione NTFS. Si sus usuarios prefieren usar clientes NFS y chmod/chown, utilice los estilos de seguridad de UNIX.

Consideraciones para crear conexiones de Active Directory

Cloud Volumes Service permite conectar la instancia de Cloud Volumes Service a un servidor de Active Directory externo para la gestión de identidades tanto para usuarios de SMB como UNIX. Se requiere crear una conexión de Active Directory para utilizar SMB en Cloud Volumes Service.

La configuración para esto ofrece varias opciones que requieren cierta consideración para la seguridad. El servidor de Active Directory externo puede ser una instancia de las instalaciones o una nativa del cloud. Si utiliza un servidor de Active Directory en las instalaciones, no exponga el dominio a la red externa (como con una DMZ o una dirección IP externa). En su lugar, utilice túneles privados seguros o VPN, fideicomisos forestales de un solo sentido o conexiones de red dedicadas a las redes locales con "Acceso privado a Google". Consulte la documentación de Google Cloud para obtener más información acerca de "Prácticas recomendadas con Active Directory en Google Cloud".

> CVS-SW requiere que los servidores de Active Directory se encuentren en la misma región. Si se intenta una conexión de CC en CVS-SW a otra región, el intento falla. Cuando utilice CVS-SW, asegúrese de crear sitios de Active Directory que incluyan los DC de Active Directory y, a continuación, especifique los sitios en Cloud Volumes Service para evitar intentos de conexión de DC entre regiones.

Credenciales de Active Directory

Cuando se habilita SMB o LDAP para NFS, Cloud Volumes Service interactúa con los controladores de Active Directory para crear un objeto de cuenta de máquina que se usará para la autenticación. Esto no difiere del modo en que un cliente SMB de Windows se une a un dominio y requiere los mismos derechos de acceso a las unidades organizativas (OU) de Active Directory.

En muchos casos, los grupos de seguridad no permiten el uso de una cuenta de administrador de Windows en servidores externos como Cloud Volumes Service. En algunos casos, el usuario Administrador de Windows está completamente deshabilitado como una práctica recomendada de seguridad.

Permisos necesarios para crear cuentas de máquina SMB

Para agregar objetos de máquina Cloud Volumes Service a un Active Directory, una cuenta que tenga derechos administrativos en el dominio o tiene "permisos delegados para crear y modificar objetos de cuenta de equipo" A una unidad organizativa especificada es necesaria. Puede hacerlo con el Asistente para delegación de control de Active Directory creando una tarea personalizada que proporcione a un usuario acceso a la creación o eliminación de objetos del equipo con los siguientes permisos de acceso proporcionados:

- Lectura/Escritura
- Crear/eliminar todos los objetos secundarios
- Todas las propiedades de lectura y escritura
- Cambiar/restablecer contraseña

Al hacerlo, se agrega automáticamente una ACL de seguridad para el usuario definido a la unidad organizativa de Active Directory y se minimiza el acceso al entorno de Active Directory. Una vez delegado un usuario, ese nombre de usuario y la 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 del objeto de cuenta de equipo y la creación para mayor seguridad.

Detalles de conexión de Active Directory

La "Detalles de conexión de Active Directory" Proporcione campos para que los administradores proporcionen información específica del esquema de Active Directory para la colocación de la cuenta de la máquina, como los siguientes:

- **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 Cloud Volumes Service o CVS-Performance. Si se establece de forma incorrecta en una conexión existente, es posible que no funcione correctamente cuando se utilice o edite.
- **Dominio.** el nombre de dominio de Active Directory.
- **Sitio.** limita los servidores de Active Directory a un sitio específico para seguridad y rendimiento "consideraciones". Esto es necesario cuando varios servidores de Active Directory abarcan regiones porque Cloud Volumes Service no admite actualmente la activación de solicitudes de autenticación de Active Directory a servidores de Active Directory en una región diferente a la instancia de Cloud Volumes Service. (Por ejemplo, el controlador de dominio de Active Directory se encuentra en una región que sólo soporta CVS-Performance pero desea un recurso compartido SMB en una instancia CVS-SW.)
- **Servidores DNS.** servidores DNS para utilizar en búsquedas de nombre.
- **Nombre NetBIOS (opcional).** Si lo desea, el nombre NetBIOS del servidor. Esto se utiliza cuando se crean cuentas de equipo nuevas mediante la conexión de Active Directory. Por ejemplo, si el nombre NetBIOS se establece en CVS-EAST, los nombres de la cuenta de la máquina serán CVS-EAST-{1234}. Consulte la sección "Cómo se muestra Cloud Volumes Service en Active Directory" si quiere más información.
- **Unidad organizativa (OU).** la unidad organizativa específica para crear la cuenta de equipo. Esto resulta útil si va a delegar el control a un usuario para las cuentas de equipo a una unidad organizativa específica.
- **Cifrado AES.** también puede activar o desactivar la casilla de verificación Activar cifrado AES para autenticación AD. Habilitar el cifrado AES para la autenticación de Active Directory proporciona seguridad adicional para la comunicación de Cloud Volumes Service a Active Directory durante las búsquedas de usuarios y grupos. Antes de habilitar esta opción, consulte con el 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 desactivan los cifrados más débiles (COMO DES o RC4-HMAC), pero si decide deshabilitar los cifrados más débiles, confirme que la conexión a Active Directory de Cloud Volumes Service se ha configurado para habilitar AES. De lo contrario, se producen fallos de autenticación. Al habilitar el cifrado AES, no se deshabilitan las cifrados, sino que se añade compatibilidad con AES a la cuenta de equipo SMB de Cloud Volumes Service.

Detalles del dominio de Kerberos

Esta opción no se aplica a los servidores SMB. En su lugar, se utiliza al configurar NFS Kerberos para el sistema Cloud Volumes Service. Cuando se rellenan estos detalles, el Reino de Kerberos de NFS se configura (similar al archivo krb5.conf en Linux) y se utiliza cuando se especifica NFS Kerberos en la creación de volúmenes de Cloud Volumes Service, ya que la conexión de Active Directory actúa como el Centro de distribución de Kerberos de NFS (KDC).

Actualmente no se admiten los KDC que no son de Windows para su uso con Cloud Volumes Service.

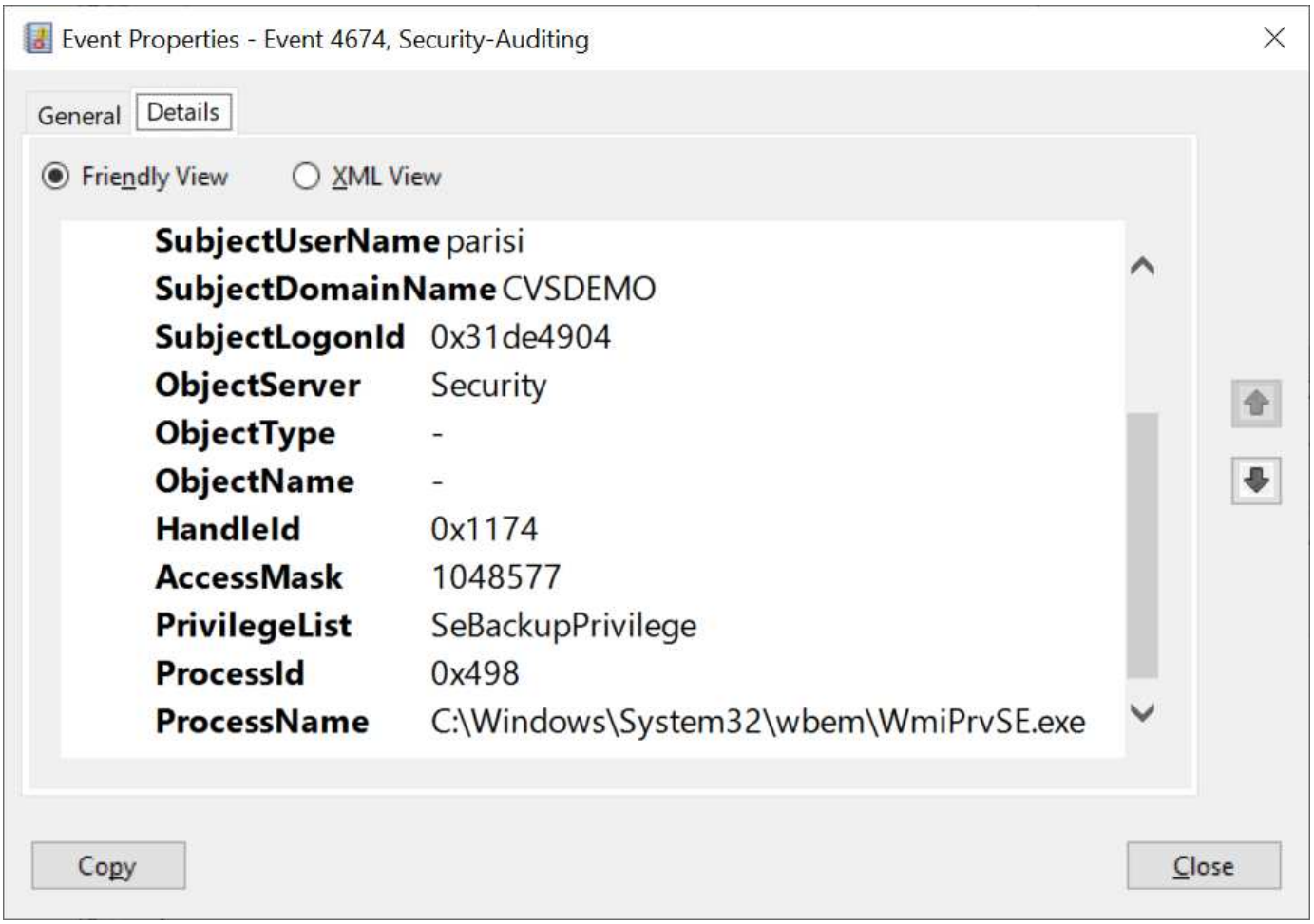
Región

Una región le permite especificar la ubicación donde reside la conexión de Active Directory. Esta región debe ser la misma región que el volumen Cloud Volumes Service.

- **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 la compatibilidad con la pertenencia a grupos de usuarios 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 desea utilizar usuarios UNIX locales (como root), seleccione esta opción.

Usuarios de backup

Esta opción permite especificar usuarios de Windows que tienen permisos de backup en el volumen de Cloud Volumes Service. Los privilegios de backup (SeBackupPrivilege) son necesarios para que algunas aplicaciones puedan realizar backups y restaurar correctamente los datos en los volúmenes NAS. Este usuario tiene un alto nivel de acceso a los datos del volumen, por lo que debe tenerse en cuenta "habilitar la auditoría del acceso de ese usuario". Una vez habilitado, los eventos de auditoría aparecen en el Visor de sucesos > registros de Windows > Seguridad.



Usuarios con privilegios de seguridad

Esta opción permite especificar usuarios de Windows que tienen permisos de modificación de seguridad en el volumen de Cloud Volumes Service. Los privilegios de seguridad (SeSecurityPrivilege) son necesarios para algunas aplicaciones ("Como SQL Server") para establecer correctamente los permisos durante la instalación. Este privilegio se necesita para gestionar el registro de seguridad. Aunque este privilegio no es tan potente 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 se muestra Cloud Volumes Service en Active Directory

Cloud Volumes Service aparece en Active Directory como un objeto de cuenta de equipo normal. Las convenciones de nomenclatura son las siguientes.

- CIFS/SMB y NFS Kerberos crean objetos de cuentas de equipo independientes.
- NFS con LDAP habilitado crea una cuenta de máquina en Active Directory para vínculos LDAP de Kerberos.
- Los volúmenes dobles de protocolo con LDAP comparten la cuenta de máquina CIFS/SMB para LDAP y SMB.
- Las cuentas de máquina de CIFS/SMB utilizan una convención de nomenclatura del NOMBRE-1234 (ID de cuatro dígitos aleatorio con un guión anexado al nombre de <10 caracteres) para la cuenta de la máquina. Puede definir EL NOMBRE mediante el valor de nombre NetBIOS en la conexión de Active Directory (consulte la sección “Detalles de 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-TRUNCADO-NAME-1234.
- Las instancias de CVS-Performance de NFS solo con LDAP habilitado crean una cuenta de máquina SMB para enlazar al servidor LDAP con la misma convención de nomenclatura que las instancias de CIFS/SMB.
- Cuando se crea una cuenta de máquina SMB, los recursos compartidos admin ocultos predeterminados (consulte la sección ""Recursos compartidos ocultos predeterminados"") También se crean (c$, admin$, ipc$), pero esos recursos compartidos no tienen ACL asignados y son inaccesibles.
- Los objetos de cuenta de equipo se colocan de forma predeterminada en CN=Computers, pero a puede especificar una unidad organizativa diferente cuando sea necesario. Consulte la sección “Permisos necesarios para crear cuentas de máquina SMB” Para obtener información sobre los derechos de acceso necesarios para agregar/eliminar objetos de cuenta de máquina para Cloud Volumes Service.

Cuando Cloud Volumes Service agrega la cuenta de la máquina SMB a Active Directory, se rellenan 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 permite EL intercambio DE la cuenta DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_HMAC_96 con la cuenta SMB)
- Nombre (con el nombre del servidor SMB)
- SAMAccountName (con smbServer$)

- ServicePrincipalName (con host/smbserver.domain.com y host/smbServer SPN para Kerberos)

Si desea deshabilitar los tipos de cifrado Kerberos más débiles (enctype) en la cuenta de la máquina, puede cambiar el valor MSDS-SupportedEncryptionTypes de la cuenta de la máquina a uno de los valores de la tabla siguiente para permitir sólo AES.

MSDS-SupportedEncryptionTypes de valor	Enctype activado
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 cuentas de equipo SMB, haga clic en Activar cifrado AES para autenticación AD al crear la conexión de Active Directory.

Para habilitar el cifrado AES para Kerberos de NFS, "Consulte la documentación de Cloud Volumes Service".

Otras dependencias de servicios de infraestructura NAS (KDC, LDAP y DNS)

Cuando se utiliza Cloud Volumes Service para recursos compartidos NAS, es posible que sea necesario tener dependencias externas para disponer de una funcionalidad adecuada. Estas dependencias están en juego en circunstancias específicas. En la siguiente tabla se muestran diversas opciones de configuración y qué dependencias, si las hay, son necesarias.

Configuración	Dependencias necesarias
Solo NFSv3	Ninguno
Solo Kerberos para NFSv3	Active Directory de Windows: * KDC * DNS * LDAP
Solo NFSv4.1	Configuración de asignación de ID de cliente (/etc/idmap.conf)
Solo NFSv4.1 Kerberos	• Configuración de asignación de ID de cliente (/etc/idmap.conf) • Active Directory de Windows: LDAP de DNS de KDC
Solo SMB	Active Directory: * KDC * DNS

Configuración	Dependencias necesarias
NAS multiprotocolo (NFS y SMB)	• Configuración de asignación de ID de cliente (solo NFSv4.1; /etc/idmap.conf) • Active Directory de Windows: LDAP de DNS de KDC

Kerberos keytab rotation/password restablecerse para objetos de cuenta de equipo

Con las cuentas de máquina SMB, Cloud Volumes Service programa reinicios periódicos de contraseñas para la cuenta de la máquina SMB. Estos restablecimientos de contraseña se producen utilizando el cifrado Kerberos y funcionan según una programación de cada cuarto domingo a una hora aleatoria entre LAS 11:00 y LAS 01:00. Estos restablecimientos de contraseña cambian las versiones de clave Kerberos, giran las pestañas clave almacenadas en el sistema Cloud Volumes Service y ayudan a mantener un mayor nivel de seguridad para los servidores SMB que se ejecutan en Cloud Volumes Service. Las contraseñas de las cuentas de equipo son aleatorias y no son conocidas por los administradores.

Para las cuentas de máquina NFS Kerberos, los restablecimientos de contraseña sólo tienen lugar cuando se crea o se intercambia una nueva keytab con el KDC. Actualmente, no es posible hacerlo en Cloud Volumes Service.

Puertos de red para su uso con LDAP y Kerberos

Cuando se utilizan LDAP y Kerberos, debe determinar los puertos de red que utilizan estos servicios. En el, puede encontrar una lista completa de los puertos que utiliza Cloud Volumes Service "Documentación de Cloud Volumes Service sobre consideraciones de seguridad".

LDAP

Cloud Volumes Service actúa como un cliente LDAP y utiliza consultas de búsqueda LDAP estándar para búsquedas de usuarios y grupos de identidades de UNIX. LDAP es necesario si tiene la intención de utilizar usuarios y grupos fuera de los usuarios predeterminados estándar proporcionados por Cloud Volumes Service. LDAP también es necesario si tiene previsto utilizar NFS Kerberos con directores de usuario (como user1@domain.com). Actualmente, sólo LDAP con Microsoft Active Directory es compatible.

Para utilizar Active Directory como servidor LDAP de UNIX, debe rellenar los atributos UNIX necesarios en los usuarios y grupos que desee utilizar para las identidades de UNIX. Cloud Volumes Service utiliza una plantilla de esquema LDAP predeterminada en la que consulta atributos basados "RFC-2307-bis". Como resultado, en la siguiente tabla se muestran los atributos de Active Directory mínimos necesarios que se deben rellenar para los usuarios y grupos y para qué se utiliza cada atributo.

Para obtener más información acerca de la configuración de atributos LDAP en Active Directory, consulte "Gestión del acceso de doble protocolo."

Atributo	Qué hace
uid*	Especifica el nombre de usuario UNIX
UidNumber*	Especifica el ID numérico del usuario UNIX
GidNumber*	Especifica el identificador numérico del grupo principal del usuario UNIX

Atributo	Qué hace
ObjectClass*	Especifica qué tipo de objeto se está utilizando; Cloud Volumes Service requiere que “user” se incluya en la lista de clases de objeto (se incluye de forma predeterminada en la mayoría de implementaciones de Active Directory).
nombre	Información general sobre la cuenta (nombre real, número de teléfono, etc., también conocido como gecos)
UnixUserPassword	No es necesario configurar esto; no se utiliza en las búsquedas de identidad de UNIX para la autenticación NAS. Al establecer esta opción, el valor de unixUserPassword configurado se coloca en texto sin formato.
UnixHomeDirectory	Define la ruta a los directorios iniciales de UNIX cuando un usuario autentica con LDAP desde un cliente Linux. Establezca esta opción si desea utilizar la funcionalidad de directorio raíz de LDAP para UNIX.
LoginShell	Define la ruta al shell bash/profile para clientes Linux cuando un usuario autentica de acuerdo con LDAP.

*Denota atributo es necesario para una funcionalidad adecuada con Cloud Volumes Service. Los atributos restantes son para uso exclusivo del cliente.

Atributo	Qué hace
cn*	Especifica el nombre del grupo UNIX. Cuando se utiliza Active Directory para LDAP, se establece 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 denominado user1 pertenece a un grupo denominado user1 en su cliente Linux, Windows no permite dos objetos con el mismo atributo cn. Para evitar esto, cambie el nombre del usuario de Windows por un nombre único (como user1-UNIX); LDAP en Cloud Volumes Service utiliza el atributo uid para los nombres de usuario de UNIX.
GidNumber*	Especifica el identificador numérico del grupo UNIX.
ObjectClass*	Especifica qué tipo de objeto se está utilizando; Cloud Volumes Service requiere que se incluya un grupo en la lista de clases de objeto (este atributo se incluye de forma predeterminada en la mayoría de las implementaciones de Active Directory).

Atributo	Qué hace
MemberUid	Especifica qué usuarios UNIX son miembros del grupo UNIX. Con LDAP de Active Directory en Cloud Volumes Service, este campo no es necesario. El esquema LDAP de Cloud Volumes Service utiliza el campo Miembro para las pertenencias a grupos.
Miembro*	Necesario para grupos de miembros/grupos UNIX secundarios. Para rellenar este campo, agregue usuarios de Windows a grupos de Windows. Sin embargo, si los grupos de Windows no tienen atributos UNIX rellenados, no se incluyen en las listas de miembros de grupo del usuario UNIX. Todos los grupos que tengan que estar disponibles en NFS deben rellenar los atributos de grupo UNIX necesarios que aparecen en esta tabla.

*Denota atributo es necesario para una funcionalidad adecuada con Cloud Volumes Service. Los atributos restantes son para uso exclusivo del cliente.

Información de enlace LDAP

Para consultar a los usuarios en LDAP, Cloud Volumes Service debe enlazar (iniciar sesión) con el servicio LDAP. Este inicio de sesión tiene permisos de sólo lectura y se utiliza para consultar atributos UNIX LDAP para búsquedas de directorios. Actualmente, los vínculos LDAP sólo son posibles mediante una cuenta de máquina SMB.

Solo puede habilitar LDAP para `CVS-Performance` Y utilícelo para NFSv3, NFSv4.1 o volúmenes de protocolo doble. Debe establecerse una conexión de Active Directory en la misma región que el volumen de Cloud Volumes Service para implementar correctamente el volumen habilitado para LDAP.

Cuando LDAP está habilitado, lo siguiente se produce en situaciones específicas.

- Si solo se utilizan NFSv3 o NFSv4.1 para el proyecto de Cloud Volumes Service, se crea una nueva cuenta de máquina en la controladora de dominio de Active Directory y el cliente LDAP de Cloud Volumes Service se enlaza a Active Directory mediante las credenciales de la cuenta del equipo. No se crean recursos compartidos de SMB para el volumen NFS ni los recursos compartidos administrativos ocultos predeterminados (consulte la sección ""Recursos compartidos ocultos predeterminados"") Se han eliminado las ACL compartidas.
- Si se utilizan volúmenes de protocolo doble para el proyecto Cloud Volumes Service, solo se utiliza la cuenta de máquina única creada para el acceso SMB para vincular el cliente LDAP en Cloud Volumes Service a Active Directory. No se crean cuentas de equipo adicionales.
- Si los volúmenes SMB dedicados se crean por separado (antes o después de que se habilitaron los volúmenes NFS con LDAP), la cuenta de máquina para los vínculos LDAP se comparte con la cuenta de la máquina SMB.
- Si también está habilitado NFS Kerberos, se crean dos cuentas de máquina: Una para recursos compartidos SMB y/o enlaces LDAP y una para autenticación Kerberos NFS.

Consultas LDAP

Aunque los vínculos LDAP están cifrados, las consultas LDAP se pasan por el cable en texto sin formato utilizando el puerto LDAP 389 común. Este puerto conocido no se puede cambiar actualmente en Cloud

Volumes Service. Como resultado, alguien con acceso al rastreo de paquetes en la red puede ver nombres de usuarios y grupos, identificadores numéricos y pertenencias a grupos.

Sin embargo, las máquinas virtuales de Google Cloud no pueden snifar el tráfico unicast de otras máquinas virtuales. Solo las máquinas virtuales que participan activamente en el tráfico LDAP (es decir, que se pueden enlazar) pueden ver tráfico del servidor LDAP. Para obtener más información sobre el rastreo de paquetes en Cloud Volumes Service, consulte la sección "“Consideraciones sobre rastreo y rastreo de paquetes”."

Valores predeterminados de la configuración del cliente LDAP

Cuando se habilita LDAP en una instancia de Cloud Volumes Service, se crea una configuración de cliente LDAP con detalles de configuración específicos de forma predeterminada. En algunos casos, las opciones no se aplican a Cloud Volumes Service (no se admiten) o no son configurables.

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Lista de servidores LDAP	Establece los nombres de servidor LDAP o las direcciones IP que se utilizarán para las consultas. Esto no se utiliza para Cloud Volumes Service. En su lugar, el dominio de Active Directory se utiliza para definir servidores LDAP.	No configurado	No
Dominio de Active Directory	Establece el dominio de Active Directory que se utilizará para consultas LDAP. Cloud Volumes Service aprovecha los registros SRV para LDAP en DNS para buscar 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 que se utilizarán para LDAP. Que Cloud Volumes Service no admite. En su lugar, utilice los sitios de Active Directory para controlar la selección del servidor LDAP.	No configurado.	No
Enlazar mediante credenciales de SMB Server	Enlaza a LDAP mediante la cuenta de máquina SMB. Actualmente, el único método de enlace LDAP admitido en Cloud Volumes Service.	Verdadero	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
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. Cloud Volumes Service utiliza actualmente sólo el puerto LDAP estándar 389. LDAPS/el puerto 636 actualmente no es compatible.	389	No
LDAPS habilitado	Controla si se utiliza LDAP sobre Secure Sockets Layer (SSL) para consultas y vínculos. Actualmente no es compatible con Cloud Volumes Service.	Falso	No
Tiempo de espera de consulta (s)	Tiempo de espera para consultas. Si las consultas tardan más tiempo que el valor especificado, las consultas no se pueden realizar.	3	No
Nivel de autenticación de enlace mínimo	El nivel de enlace mínimo admitido. Dado que Cloud Volumes Service utiliza cuentas de equipo para los vínculos LDAP y Active Directory no admite enlaces anónimos de forma predeterminada, esta opción no entra en juego para la seguridad.	Anónimo	No
Enlazar DN	El nombre de usuario/distintivo (DN) utilizado para los vínculos cuando se utiliza el enlace simple. Cloud Volumes Service utiliza cuentas de equipo para enlaces LDAP y actualmente no admite autenticación de enlace simple.	No configurado	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
DN base	El DN base que se utiliza para las búsquedas LDAP.	El dominio de Windows se utiliza para la conexión de Active Directory, en formato DN (es decir, DC=dominio, DC=local).	No
Ámbito de búsqueda base	El ámbito de búsqueda para las búsquedas de DN base. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service sólo admite búsquedas en subárboles.	Subárbol	No
DN de usuario	Define el DN en el que se inician las búsquedas del usuario para las consultas LDAP. Actualmente no es compatible con Cloud Volumes Service, por lo que todas las búsquedas de usuarios comienzan en el DN base.	No configurado	No
Ámbito de búsqueda de usuarios	El ámbito de búsqueda para las búsquedas de DN de usuario. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service no admite la configuración del ámbito de búsqueda de usuarios.	Subárbol	No
DN de grupo	Define el DN donde comienzan las búsquedas de grupo para consultas LDAP. Actualmente no es compatible con Cloud Volumes Service, por lo que todas las búsquedas de grupo comienzan en el DN base.	No configurado	No
Ámbito de búsqueda de grupos	El ámbito de búsqueda para las búsquedas de DN de grupo. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service no admite la configuración del ámbito de búsqueda de grupos.	Subárbol	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
DN de grupo de red	Define el DN donde comienzan las búsquedas de netgroup para las consultas LDAP. Actualmente no es compatible con Cloud Volumes Service, por lo que todas las búsquedas de netgroup comienzan en el DN base.	No configurado	No
Ámbito de búsqueda de grupos de red	El ámbito de búsqueda para las búsquedas de DN de grupo de red. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service no admite la configuración del ámbito de búsqueda de netgroup.	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 Cloud Volumes Service.	Falso	No
Habilite la búsqueda de netgroup-by-host	Habilita búsquedas de netgroup por nombre de host en lugar de expandir grupos de red para enumerar todos los miembros. Actualmente no es compatible con Cloud Volumes Service.	Falso	No
DN de netgroup por host	Define el DN donde comienzan las búsquedas netgroup-by-host para las consultas LDAP. Actualmente, netgroup-by-host no es compatible con Cloud Volumes Service.	No configurado	No
Ámbito de búsqueda netgroup-by-host	El ámbito de búsqueda para las búsquedas DN de netgroup-by-host. Los valores pueden incluir base, onelevel o subárbol. Actualmente, netgroup-by-host no es compatible con Cloud Volumes Service.	Subárbol	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Seguridad de sesión de cliente	Define qué nivel de seguridad de sesión utiliza LDAP (firma, sello o ninguno). La firma LDAP es compatible con CVS-Performance, si es solicitada por Active Directory. CVS-SW no admite la firma LDAP. En ambos tipos de servicio, el sellado no es compatible actualmente.	Ninguno	No
Búsqueda de referencias LDAP	Al usar varios servidores LDAP, la búsqueda de referencias permite al cliente consultar otros servidores LDAP de la lista cuando no se encuentra una entrada en el primer servidor. Actualmente, Cloud Volumes Service no admite esta operación.	Falso	No
Filtro de pertenencia a grupos	Proporciona un filtro de búsqueda LDAP personalizado que se utilizará al buscar miembros de grupo desde un servidor LDAP. Actualmente no es compatible con Cloud Volumes Service.	No configurado	No

Se utiliza LDAP para la asignación de nombres asimétricos

Cloud Volumes Service, de forma predeterminada, asigna usuarios de Windows y usuarios UNIX con nombres de usuario idénticos de manera bidireccional sin configuración especial. Siempre que Cloud Volumes Service pueda encontrar un usuario UNIX válido (con LDAP), se producirá una asignación de nombre 1:1. Por ejemplo, si el usuario de Windows `johnsmith` Se utiliza, entonces, si Cloud Volumes Service puede encontrar un usuario UNIX llamado `johnsmith` En LDAP, la asignación de nombres se realiza correctamente para ese usuario, todos los archivos/carpetas creados por `johnsmith` Mostrar la propiedad de usuario correcta y todas las ACL que afectan `johnsmith` Sean honrados independientemente del protocolo NAS que se utilice. Esto se conoce como asignación simétrica de nombres.

La asignación de nombres asimétricos se produce cuando la identidad del usuario de Windows y de UNIX no coinciden. Por ejemplo, si el usuario de Windows `johnsmith` Tiene una identidad UNIX de `jsmith`, Cloud Volumes Service necesita una manera de ser contada acerca de la variación. Puesto que Cloud Volumes Service no admite actualmente la creación de reglas estáticas de asignación de nombres, se debe utilizar LDAP para buscar la identidad de los usuarios tanto para las identidades de Windows como UNIX para garantizar la propiedad correcta de los archivos y carpetas y los permisos esperados.

De forma predeterminada, Cloud Volumes Service incluye `LDAP` En el switch ns de la instancia de la base de datos de asignación de nombres, de modo que para proporcionar la funcionalidad de asignación de nombres mediante el uso de LDAP para nombres asimétricos, sólo es necesario modificar algunos de los atributos de usuario/grupo para reflejar lo que busca Cloud Volumes Service.

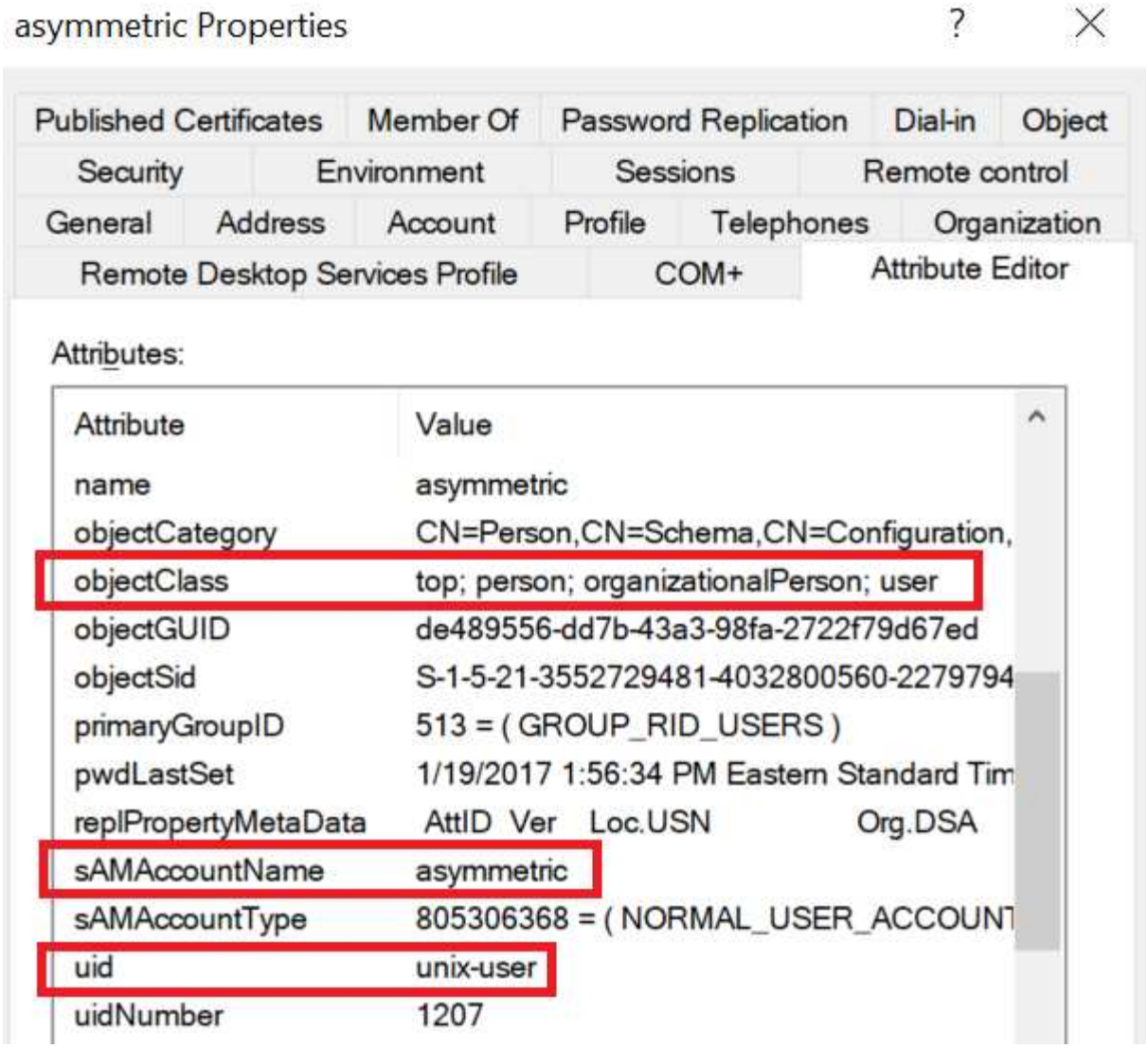
En la siguiente tabla se muestran los atributos que se deben rellenar en LDAP para la funcionalidad de asignación de nombres asimétrica. En la mayoría de los casos, Active Directory ya está configurado para hacerlo.

Atributo Cloud Volumes Service	Qué hace	Valor que utiliza Cloud Volumes Service para la asignación de nombres
Clase de objetos de Windows a UNIX	Especifica el tipo de objeto que se está utilizando. (Es decir, usuario, grupo, posixcuenta, 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 su creación. Cloud Volumes Service lo utiliza para búsquedas de Windows a UNIX.	No se necesita ningún cambio aquí; sAMAccountName es igual que el nombre de inicio de sesión de Windows.
UID	Define el nombre de usuario UNIX.	Nombre de usuario UNIX deseado.

Cloud Volumes Service actualmente no utiliza prefijos de dominio en las búsquedas LDAP, de modo que varios entornos LDAP de dominio no funcionan correctamente con las búsquedas del mapa de nombres LDAP.

En el ejemplo siguiente se muestra un usuario con el nombre de Windows `asymmetric`, El nombre UNIX `unix-user`, Y el comportamiento que sigue al escribir archivos tanto de SMB como de NFS.

La figura siguiente muestra el aspecto de los atributos LDAP desde el servidor Windows.



Desde un cliente NFS, puede 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 AS `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 Windows, puede ver que el propietario del archivo está establecido en el usuario de Windows correcto:

```
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, se muestra el propietario UNIX correcto, tal y como se muestra en el texto siguiente.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
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 DC permiten el enlace LDAP.

El impacto para Cloud Volumes Service es el mismo que para cualquier cliente LDAP. Cloud Volumes Service no admite actualmente el enlace de canal. Dado que Cloud Volumes Service admite la firma LDAP de forma predeterminada a través de la negociación, el enlace al canal LDAP no debe ser un problema. Si tiene problemas con la vinculación a LDAP con el enlace de canal activado, siga los pasos de corrección de ADV190023 para permitir que los enlaces LDAP de Cloud Volumes Service tengan éxito.

DNS

Active Directory y Kerberos tienen dependencias en DNS para el nombre de host a IP/IP para la resolución de nombres de host. DNS requiere que el puerto 53 esté abierto. Cloud Volumes Service no realiza modificaciones en los registros DNS ni admite actualmente el uso de "DNS dinámico" en las interfaces de red.

Puede configurar el DNS de Active Directory para restringir qué servidores pueden actualizar los registros DNS. Para obtener más información, consulte "Proteja el DNS de Windows".

Tenga en cuenta que los recursos de un proyecto de Google utilizan de forma predeterminada Google Cloud DNS, que no está conectado con Active Directory DNS. Los clientes que utilizan DNS cloud no pueden resolver las rutas UNC que devuelve Cloud Volumes Service. 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 unirse a un cliente a Active Directory, debe configurar su configuración DNS para utilizar el DNS de Active Directory. Opcionalmente, puede configurar Cloud DNS para reenviar solicitudes a Active Directory DNS. Consulte "¿Por qué mi cliente no puede resolver el nombre NetBIOS de SMB?"si quiere más información.

Cloud Volumes Service no admite actualmente las consultas DNSSEC y las consultas DNS se realizan en texto sin formato.

Auditoría de acceso a los archivos

Actualmente no es compatible con Cloud Volumes Service.

Protección antivirus

Debe realizar análisis antivirus en Cloud Volumes Service en el cliente para un recurso compartido NAS. Actualmente no existe ninguna integración antivirus nativa con Cloud Volumes Service.

Operación de servicio

El equipo de Cloud Volumes Service gestiona los servicios de back-end en Google Cloud y utiliza varias estrategias para proteger la plataforma y evitar el acceso no deseado.

Cada cliente obtiene su propia subred única, que tiene acceso acotado de forma predeterminada a otros clientes; cada cliente de Cloud Volumes Service obtiene su propio espacio de nombres y VLAN para aislar todos los datos. Una vez autenticado un usuario, el motor de entrega de servicios (SDE) sólo puede leer los datos de configuración específicos de ese arrendatario.

Seguridad física

Con la aprobación previa adecuada, solo los ingenieros in situ y los ingenieros de soporte de campo (FSE) con insignia de NetApp tienen acceso a la jaula y los racks para trabajar físicamente. La gestión de almacenamiento y redes no está permitida. Solo estos recursos in situ pueden realizar tareas de mantenimiento del hardware.

Para los ingenieros in situ, se crea un ticket para la descripción del trabajo (SOW, Stament ID) que incluye el identificador de rack y la ubicación del dispositivo (RU), y todos los demás detalles se incluyen en la incidencia. En el caso de los FSE de NetApp, es necesario elevar un ticket de visita a las instalaciones con LA COLOCACIÓN y el ticket incluye los detalles, la fecha y la hora del visitante a efectos de auditoría. La Descripción del Trabajo para el FSE se comunica internamente a NetApp.

Equipo de operaciones

El equipo de operaciones de Cloud Volumes Service consta de ingeniería de producción y un ingeniero de fiabilidad de sitio (SRE) para servicios de volumen de cloud, e ingenieros de soporte de campo y partners de NetApp para hardware. Todos los miembros del equipo de operaciones están acreditados por su trabajo 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 examinada adecuadamente.

El equipo de SRE gestiona el plano de control y cómo se enrutan los datos desde las solicitudes de la interfaz de usuario al hardware y software de back-end en Cloud Volumes Service. El equipo de SRE también gestiona los recursos del sistema, como los máximos de volumen e inodo. Los SRE no pueden interactuar con los datos del cliente ni tener acceso a ellos. Los Sres también proporcionan coordinación con Autorizaciones de devolución de material (RMA), como solicitudes de sustitución de disco o memoria nuevas para el

hardware de backend.

Responsabilidades del Cliente

Los clientes de Cloud Volumes Service gestionan la administración de Active Directory y las funciones de usuario de su empresa, así como las operaciones de volumen y datos. Los clientes pueden tener roles administrativos y pueden delegar permisos en otros usuarios finales dentro del mismo proyecto de Google Cloud con las dos funciones predefinidas que proporcionan NetApp y Google Cloud (Administrador y Visor).

El administrador puede establecer la relación entre iguales de cualquier VPC del proyecto del cliente a Cloud Volumes Service que el cliente determine que es apropiado. Es responsabilidad del cliente gestionar el acceso a su suscripción a Google Cloud Marketplace y gestionar los ordenadores virtuales que tienen acceso al plano de datos.

Protección frente a SRE maliciosa

Una preocupación que podría surgir es cómo protege Cloud Volumes Service frente a situaciones en las que hay una SRE maliciosa o cuando se han comprometido las credenciales de SRE?

El acceso al entorno de producción es sólo con un número limitado de personas que reciben servicios de salud sexual y reproductiva. Los privilegios administrativos se limitan además a un puñado de administradores con experiencia. Todas las acciones realizadas por cualquier persona en el entorno de producción de Cloud Volumes Service se registran y cualquier anomalía en la línea de base o actividades sospechosas es detectada por nuestra plataforma de inteligencia de amenazas de gestión de eventos e información de seguridad (SIEM). Como resultado, se puede realizar un seguimiento y mitigar de acciones maliciosas antes de que se produzcan demasiados daños en el entorno de administración de Cloud Volumes Service.

Ciclo de vida de volumen

Cloud Volumes Service solo gestiona los objetos dentro del servicio, no los datos dentro de los volúmenes. Solo los clientes que acceden a los volúmenes pueden gestionar los datos, las ACL, los propietarios de archivos, etc. Los datos de estos volúmenes se cifran en reposo y el acceso se limita a los inquilinos de la instancia de Cloud Volumes Service.

El ciclo de vida del volumen para Cloud Volumes Service es create-update-delete. Los volúmenes conservan las copias Snapshot de los volúmenes hasta que se eliminan los volúmenes y solo los administradores de Cloud Volumes Service validados pueden eliminar volúmenes en Cloud Volumes Service. Cuando un administrador solicita la eliminación de un volumen, se necesita un paso adicional para introducir el nombre del volumen para verificar la eliminación. Una vez eliminado el volumen, este ya no se puede recuperar.

En los casos en que se termina un contrato de Cloud Volumes Service, NetApp Marca los volúmenes para su eliminación después de un período de tiempo específico. Antes de que caduque ese período de tiempo, puede recuperar volúmenes a petición del cliente.

Certificaciones

Cloud Volumes Services para Google Cloud está certificado actualmente para cumplir los estándares ISO/IEC 27001:2013 e ISO/IEC 27018:2019. El servicio también recibió recientemente su informe de certificación SOC2 de tipo I. Si desea obtener más información sobre el compromiso de NetApp con la privacidad y la seguridad de los datos, consulte "Cumplimiento de normativas: Seguridad y privacidad de los datos".

RGPD

Nuestros compromisos con respecto a la privacidad y el cumplimiento del RGPD están disponibles en diversos de nuestros "contratos con clientes", como nuestro "Adición al procesamiento de datos del cliente",

que incluye la "Cláusulas contractuales estándar" Proporcionado por la Comisión Europea. También asumimos estos compromisos en nuestra Política de privacidad, respaldada por los valores fundamentales establecidos en nuestro Código de conducta corporativo.

Información adicional e información de contacto

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

- Documentación de Google Cloud para Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Acceso a servicios privados 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 módulos de validación criptográfico—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 de NFS en ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Póngase en contacto con nosotros

Háganos saber cómo podemos mejorar este informe técnico.

Póngase en contacto con nosotros en correo electrónico: doccomments@netapp.com [doccomments@netapp.com]. Incluir EL INFORME TÉCNICO 4918 en el asunto.

Backup y recuperación de datos de BlueXP

Backup y recuperación de datos de BlueXP para máquinas virtuales

3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales

Autor: Josh Powell: Ingeniería de soluciones de NetApp

Descripción general

La estrategia de respaldo 3-2-1 es un método de protección de datos aceptado en el sector, que proporciona un enfoque integral para proteger datos valiosos. Esta estrategia es fiable y garantiza que, incluso si se produce algún desastre inesperado, todavía habrá una copia de los datos disponibles.

La estrategia se compone de tres reglas fundamentales:

1. Conserve al menos tres copias de sus datos. Esto garantiza que, incluso si una copia se pierde o está dañada, todavía tiene al menos dos copias restantes para volver a caer.
2. Almacene dos copias de seguridad en dispositivos o medios de almacenamiento diferentes. La diversificación de los medios de almacenamiento ayuda a protegerse contra fallos específicos de dispositivos o de medios. Si un dispositivo se daña o un tipo de soporte falla, la otra copia de seguridad no se ve afectada.
3. Por último, asegúrese de que al menos una copia de backup esté fuera de las instalaciones. El almacenamiento externo actúa como protección ante desastres localizados, como incendios o inundaciones, que podrían inutilizar las copias in situ.

Este documento de solución abarca una solución de backups 3-2-1 mediante el complemento SnapCenter para VMware vSphere (SCV) para crear backups primarios y secundarios de nuestras máquinas virtuales en las instalaciones y backup y recuperación de BlueXP para máquinas virtuales y realizar un backup de una copia de nuestros datos en el almacenamiento en cloud o StorageGRID.

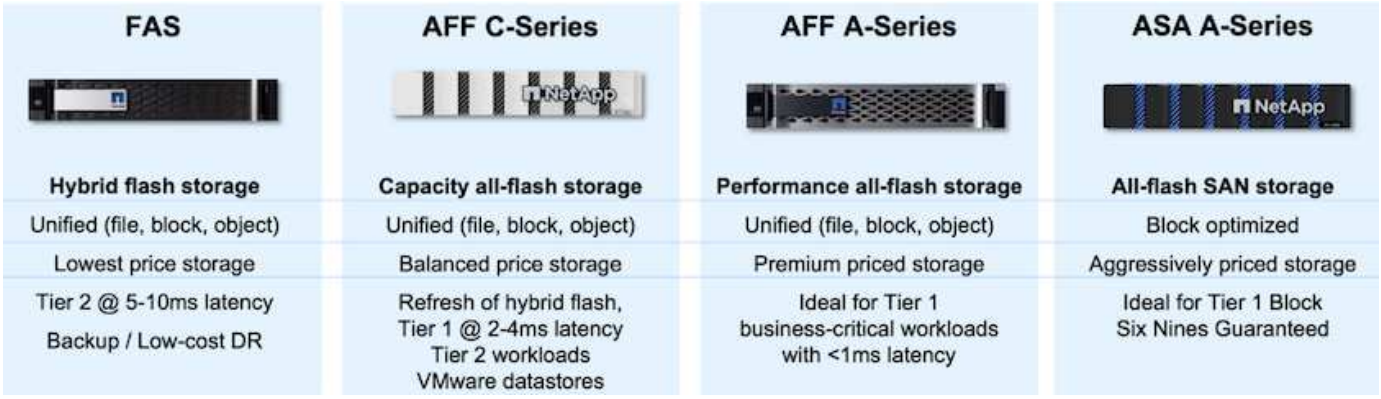
Casos de uso

Esta solución aborda los siguientes casos prácticos:

- Backup y restauración de máquinas virtuales y almacenes de datos en las instalaciones mediante el plugin de SnapCenter para VMware vSphere.
- Backup y restauración de máquinas virtuales y almacenes de datos on-premises, alojadas en clústeres de ONTAP y realizando backups en el almacenamiento de objetos mediante backup y recuperación de BlueXP para máquinas virtuales.

Almacenamiento de datos de NetApp ONTAP

ONTAP es la solución de almacenamiento líder del sector de NetApp que ofrece almacenamiento unificado, tanto si se accede a través de protocolos SAN o NAS. La estrategia de backup 3-2-1 garantiza que los datos en las instalaciones estén protegidos en más de un tipo de medio, y NetApp ofrece plataformas que van desde flash de alta velocidad a medios de bajo coste.



Para obtener más información acerca de toda la plataforma de hardware de NetApp, consulte "Almacenamiento de datos de NetApp".

Plugin de SnapCenter para VMware vSphere

El complemento de SnapCenter para VMware vSphere es una oferta de protección de datos que está perfectamente integrada con VMware vSphere y permite una gestión sencilla de backup y restauraciones de

máquinas virtuales. Como parte de esa solución, SnapMirror proporciona un método rápido y fiable para crear una segunda copia de backup inmutable de datos de un equipo virtual en un clúster de almacenamiento de ONTAP secundario. Con esta arquitectura en vigor, las operaciones de restauración de máquinas virtuales pueden iniciarse fácilmente desde ubicaciones de backup principales o secundarias.

SCV se pone en marcha como dispositivo virtual linux mediante un archivo OVA. El plugin ahora utiliza un plugin remoto
arquitectura. El plugin remoto se ejecuta fuera del servidor vCenter y se aloja en el dispositivo virtual SCV.

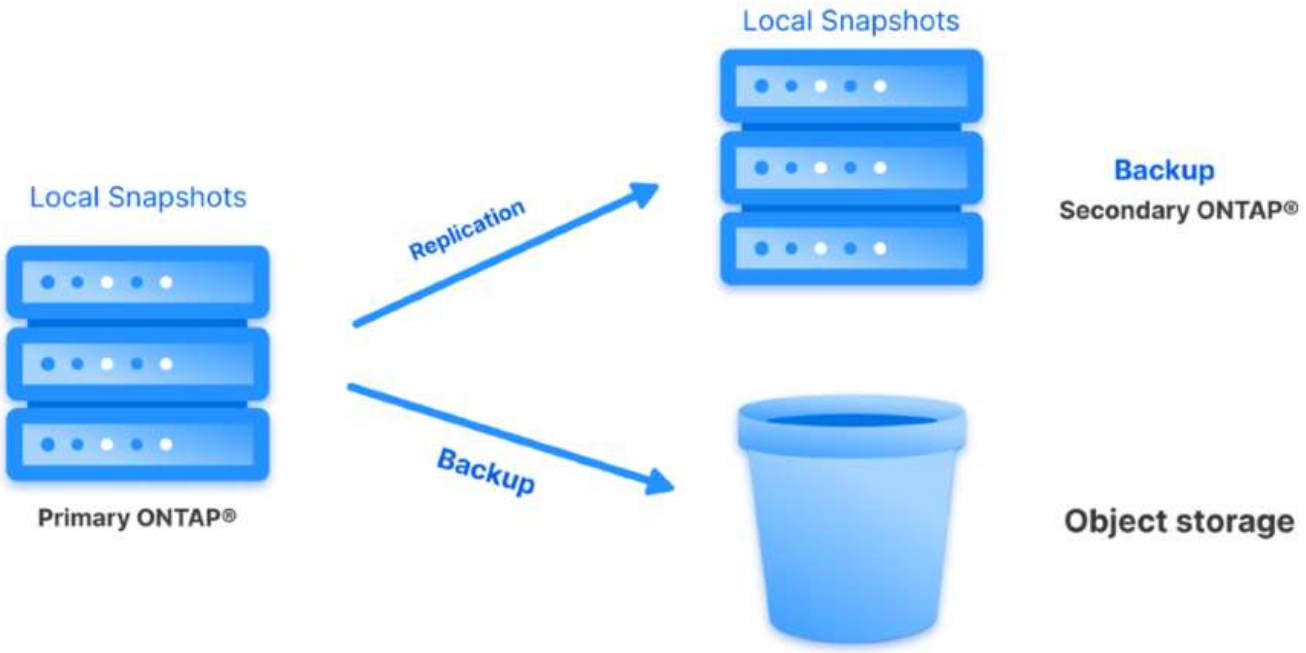
Para obtener información detallada sobre SCV, consulte "Documentación del plugin de SnapCenter para VMware vSphere".

Backup y recuperación de BlueXP para máquinas virtuales

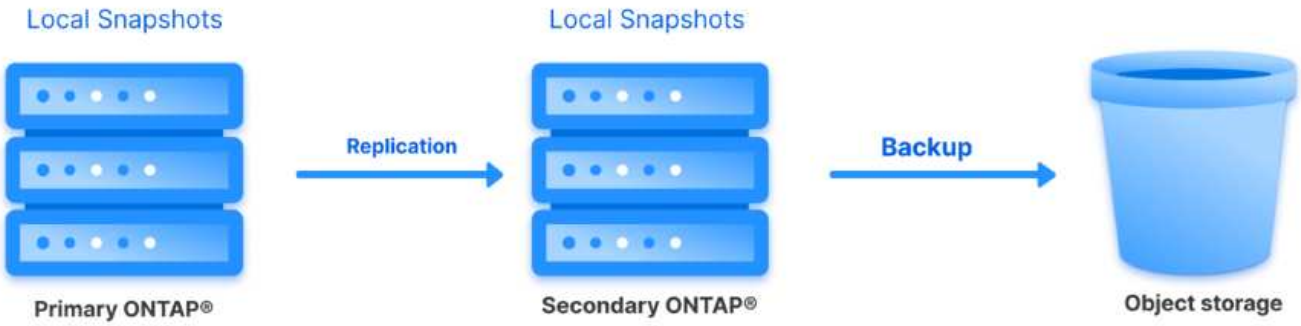
El backup y recuperación de datos de BlueXP es una herramienta basada en la nube para la gestión de datos que proporciona un único plano de control para una amplia gama de operaciones de backup y recuperación tanto en entornos on-premises como en la nube. Parte de la suite de backup y recuperación de datos de NetApp BlueXP es una función que se integra con el complemento SnapCenter para VMware vSphere (en las instalaciones) para ampliar una copia de los datos al almacenamiento de objetos en el cloud. De este modo se establece una tercera copia de los datos fuera de las instalaciones que se obtiene a partir de los backups del almacenamiento principal o secundario. El backup y la recuperación de datos de BlueXP facilita la configuración de políticas de almacenamiento que transfieren copias de tus datos desde cualquiera de estas dos ubicaciones on-premises.

Si se elige entre los backups primarios y secundarios como origen en el backup y recuperación de BlueXP, se implementará una de las dos topologías:

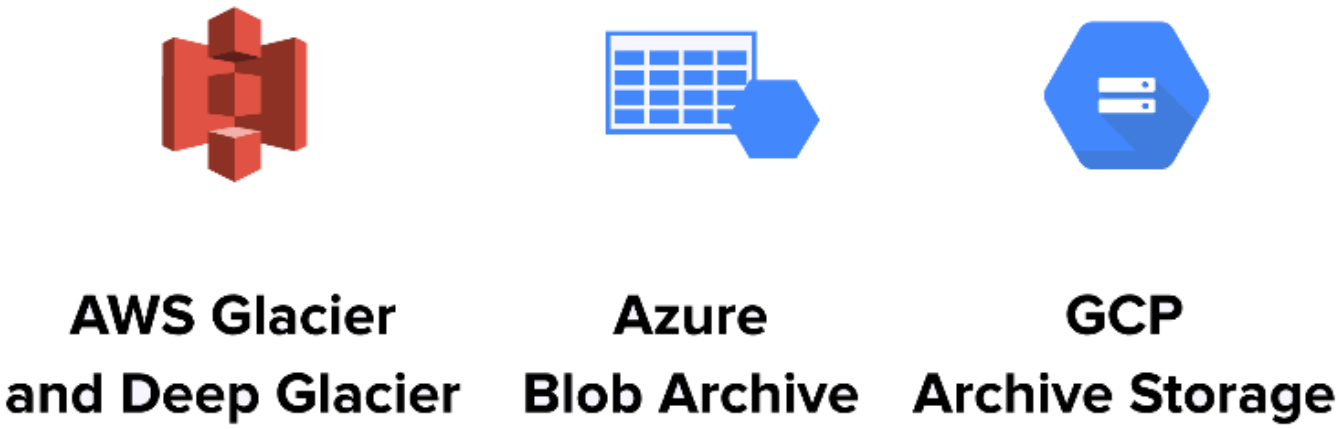
Topología de Fan-Out – Cuando el plugin de SnapCenter inicia una copia de seguridad para VMware vSphere, se toma inmediatamente una instantánea local. A continuación, SCV inicia una operación de SnapMirror que replica la snapshot más reciente en el clúster de ONTAP secundario. En el backup y recuperación de BlueXP, una política especifica el clúster de ONTAP principal como el origen de una copia Snapshot de los datos que se transferirán al almacenamiento de objetos en el proveedor de cloud de su elección.



Topología en cascada – Crear las copias de datos primarias y secundarias usando SCV es idéntica a la topología de fan-out mencionada anteriormente. Sin embargo, esta vez se crea una política en BlueXP Backup and Recovery que especifica que el backup en el almacenamiento de objetos se originará en el clúster de ONTAP secundario.



El backup y la recuperación de datos de BlueXP puede crear copias de backup de copias de Snapshot de ONTAP en las instalaciones en el almacenamiento de AWS Glacier, Azure Blob y GCP Archive.



Además, es posible usar NetApp StorageGRID como destino de backup de almacenamiento de objetos. Para obtener más información acerca de StorageGRID, consulte la "Página de destino de StorageGRID".

Descripción general de la puesta en marcha de soluciones

Esta lista proporciona los pasos altos necesarios para configurar esta solución y ejecutar las operaciones de backup y restauración a partir de backup y recuperación de SCV y BlueXP:

1. Configure la relación de SnapMirror entre los clústeres de ONTAP que se van a utilizar para copias de datos primarias y secundarias.
2. Configure el plugin de SnapCenter para VMware vSphere.
    a. Añadir sistemas de almacenamiento
    b. Cree políticas de backup
    c. Crear grupos de recursos
    d. Ejecute las primeras tareas de backup
3. Configurar el backup y la recuperación de datos de BlueXP para máquinas virtuales
    a. Agregar entorno de trabajo
    b. Detectar dispositivos SCV y vCenter
    c. Cree políticas de backup
    d. Activar backups
4. Restaure máquinas virtuales del almacenamiento principal y secundario con SCV.
5. Restaura las máquinas virtuales desde el almacenamiento de objetos mediante el backup y la restauración de BlueXP.

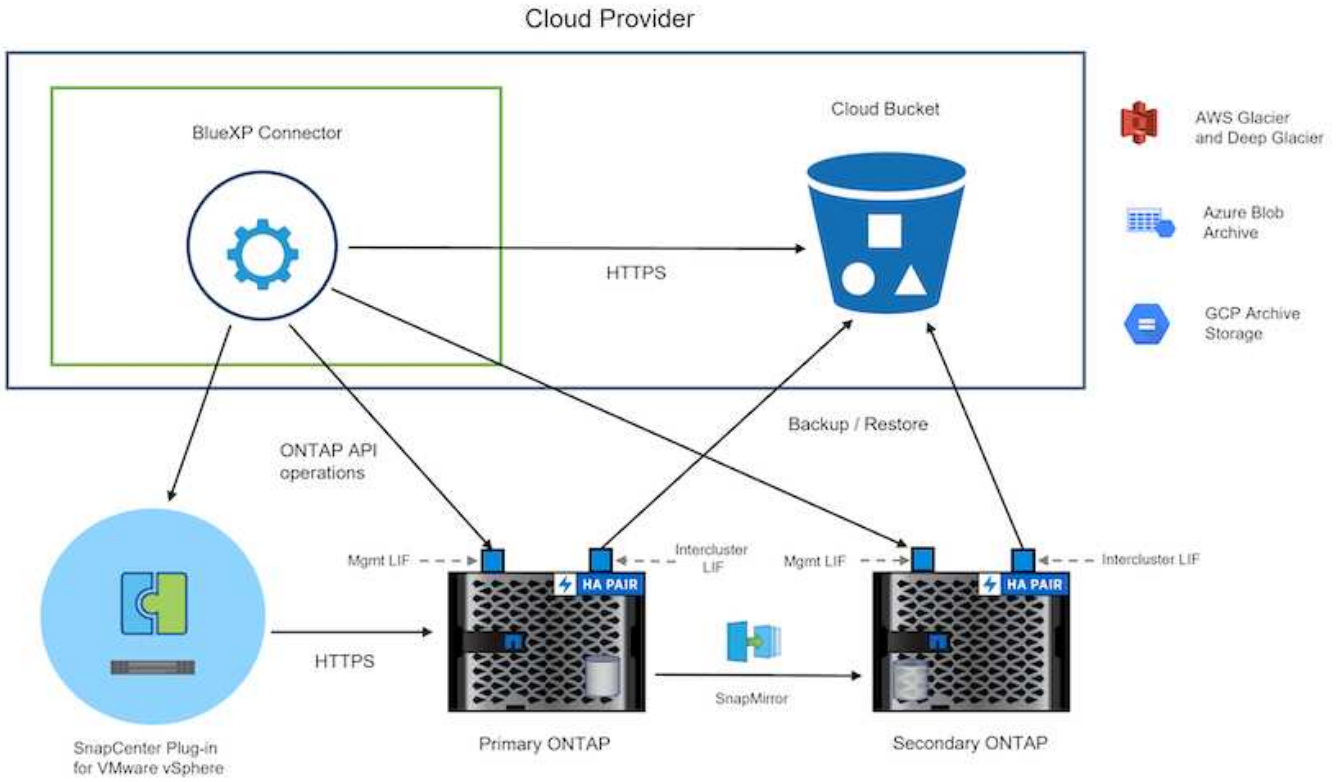
Requisitos previos

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

1. Clúster de almacenamiento de 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 secundario de ONTAP con relaciones de SnapMirror establecidas para volúmenes utilizados para almacenes de datos NFS.
3. El conector BlueXP instalado para el proveedor cloud se utiliza para los backups de almacenamiento de objetos.
4. Las máquinas virtuales a las que se va a realizar un backup se encuentran en almacenes de datos NFS que residen en el clúster de almacenamiento de ONTAP principal.
5. Conectividad de red entre el conector de BlueXP y las interfaces de gestión del clúster de almacenamiento de ONTAP en las instalaciones.
6. Conectividad de red entre el conector BlueXP y la máquina virtual del dispositivo SCV en las instalaciones, y entre el conector de BlueXP y vCenter.
7. La conectividad de red entre las LIF de interconexión de clústeres de ONTAP en las instalaciones y el servicio de almacenamiento de objetos.
8. DNS configurado para la SVM de gestión en clústeres de almacenamiento de ONTAP principales y secundarios. Para obtener más información, consulte "Configure DNS para la resolución de nombres de host".

Arquitectura de alto nivel

Las pruebas y la validación de esta solución se llevaron a cabo en un laboratorio que puede o no coincidir con el entorno de puesta en marcha final.



Puesta en marcha de la solución

Con esta solución, ofrecemos instrucciones detalladas para poner en marcha y validar una solución que utilice el plugin de SnapCenter para VMware vSphere, junto con backup y recuperación de datos de BlueXP, para realizar backups y recuperaciones de máquinas virtuales de Windows y Linux en un clúster de VMware vSphere ubicado en un centro de datos en las instalaciones. Las máquinas virtuales incluidas en esta configuración se almacenan en almacenes de datos NFS alojados en un clúster de almacenamiento de ONTAP A300. Además, un clúster de almacenamiento independiente A300 de ONTAP sirve como destino secundario para los volúmenes replicados con SnapMirror. Además, el almacenamiento de objetos alojado en Amazon Web Services y Azure Blob se emplearon como objetivos para una tercera copia de los datos.

Continuaremos creando relaciones de SnapMirror para copias secundarias de nuestros backups gestionados por SCV y la configuración de trabajos de backup tanto en el backup y recuperación de SCV como en BlueXP.

Para obtener información detallada sobre el plugin de SnapCenter para VMware vSphere, consulte la "Documentación del plugin de SnapCenter para VMware vSphere".

Para obtener información detallada sobre el backup y la recuperación de BlueXP, consulte la "Documentación de backup y recuperación de BlueXP".

Establecer relaciones de SnapMirror entre clústeres de ONTAP

El plugin de SnapCenter para VMware vSphere utiliza la tecnología SnapMirror de ONTAP para gestionar el transporte de copias de SnapMirror o SnapVault secundarias a un clúster de ONTAP secundario.

Las políticas de backup de SCV tienen la opción de usar relaciones de SnapMirror o SnapVault. La diferencia principal radica en que, al utilizar la opción de SnapMirror, el programa de retención configurado para backups en la política será el mismo en las ubicaciones primaria y secundaria. El SnapVault se ha diseñado para archivado y cuando se utiliza esta opción, se puede establecer un programa de retención independiente con la relación de SnapMirror para las copias snapshot en el clúster de almacenamiento de ONTAP secundario.

La configuración de las relaciones de SnapMirror puede realizarse en BlueXP, donde muchos de los pasos se automatizan, o bien puede realizarse mediante System Manager y la interfaz de línea de comandos de ONTAP. Todos estos métodos se discuten a continuación.

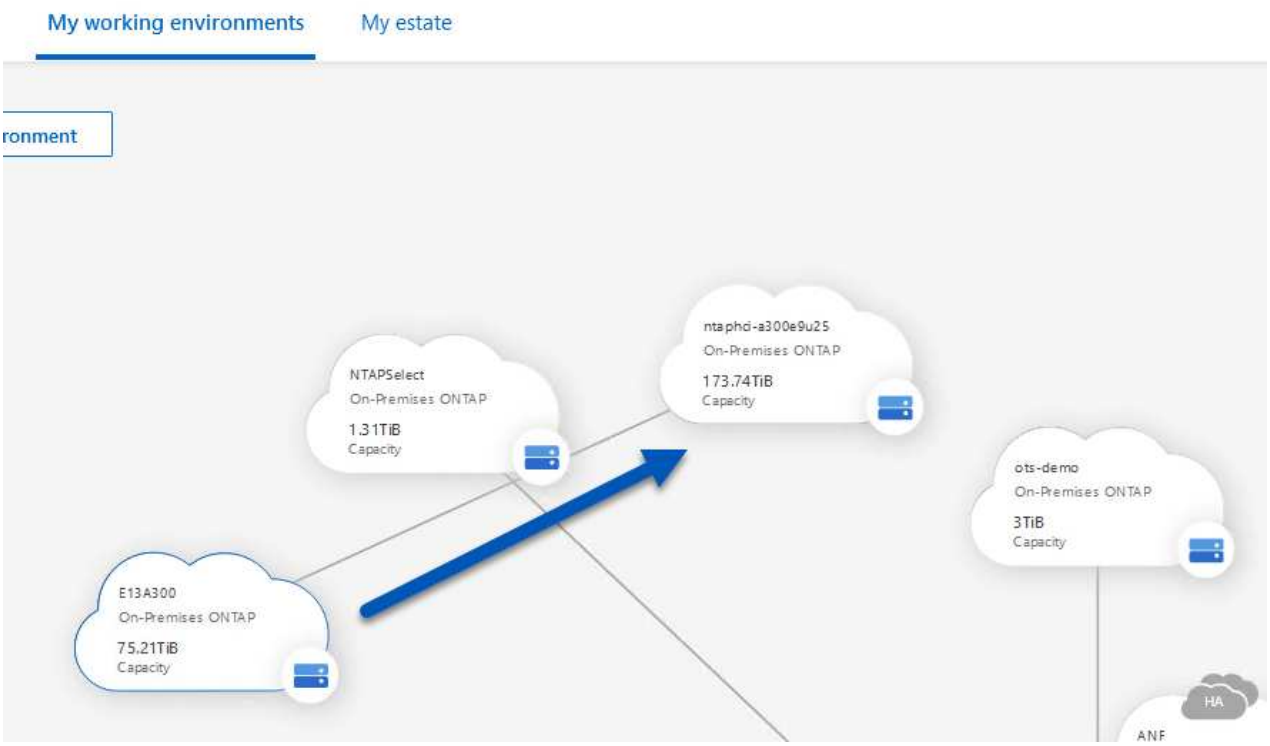
Establece relaciones de SnapMirror con BlueXP

Se deben completar los siguientes pasos desde la consola web de BlueXP:

Configuración de replicación para sistemas de almacenamiento de ONTAP principales y secundarios

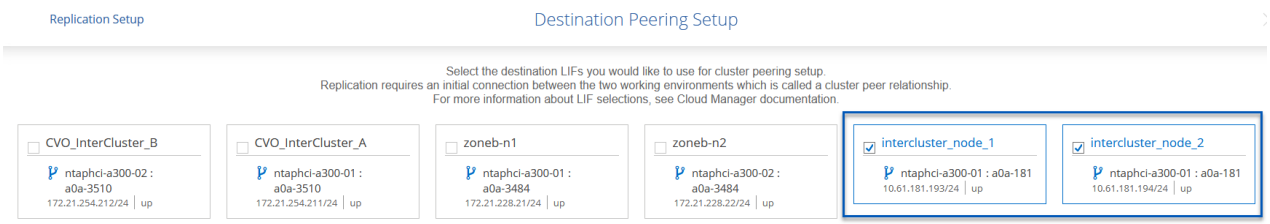
Para empezar, inicie sesión en la consola web de BlueXP y vaya a Canvas.

1. Arrastre y suelte el sistema de almacenamiento ONTAP de origen (principal) en el sistema de almacenamiento ONTAP (secundario) de destino.

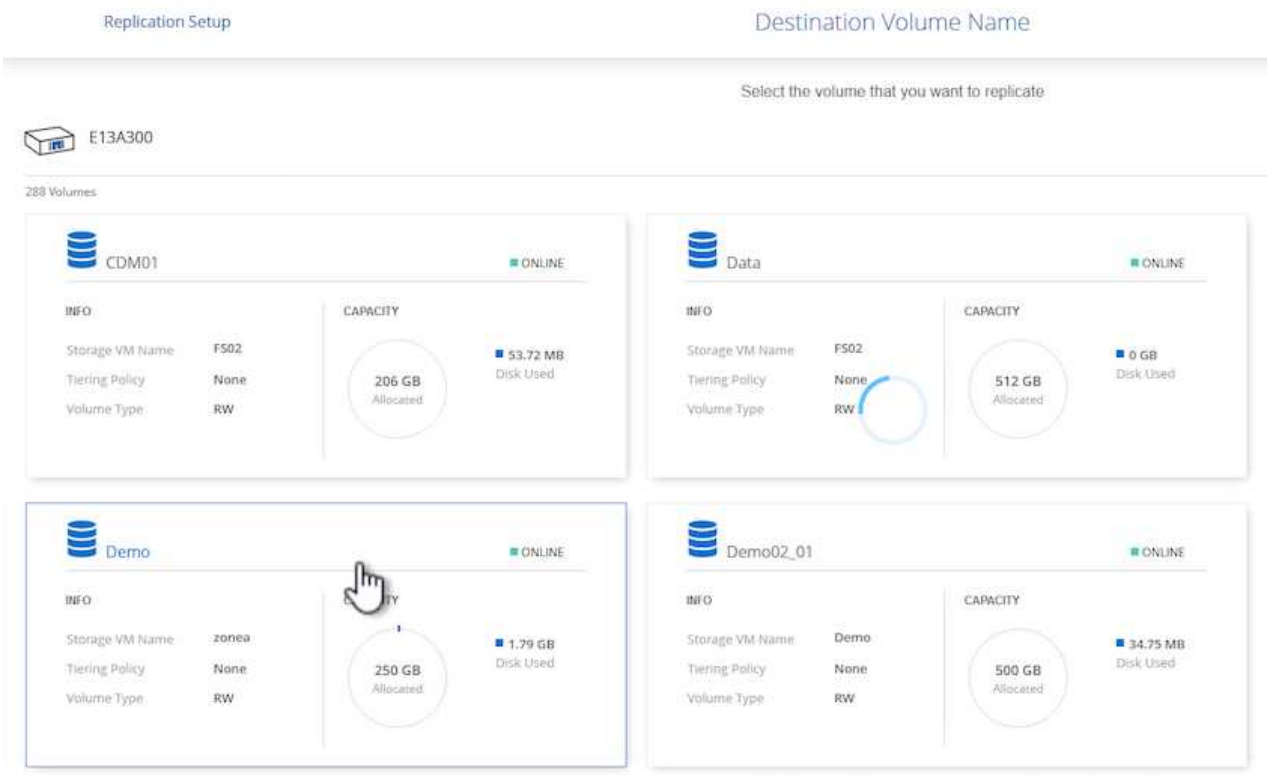


2. En el menú que aparece seleccione **Replicación**.

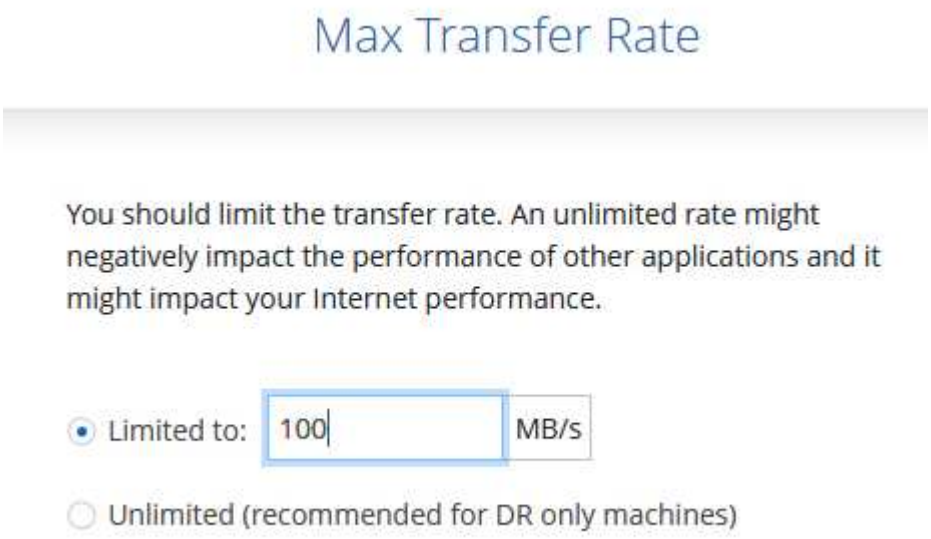
3. En la página **Configuración de pares de destino**, seleccione las LIF de interconexión de clústeres de destino que se utilizarán para la conexión entre sistemas de almacenamiento.



4. En la página **Nombre del volumen de destino**, seleccione primero el volumen de origen y, a continuación, rellene el nombre del volumen de destino y seleccione la SVM de destino y el agregado. Haga clic en **Siguiente** para continuar.



5. Elija la velocidad de transferencia máxima para que se produzca la replicación.



6. Seleccione la política que determinará la programación de retención para backups secundarios. 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 lo desea.

7. Por último, revise toda la información y haga clic en el botón **Go** para iniciar el proceso de configuración de la replicación.

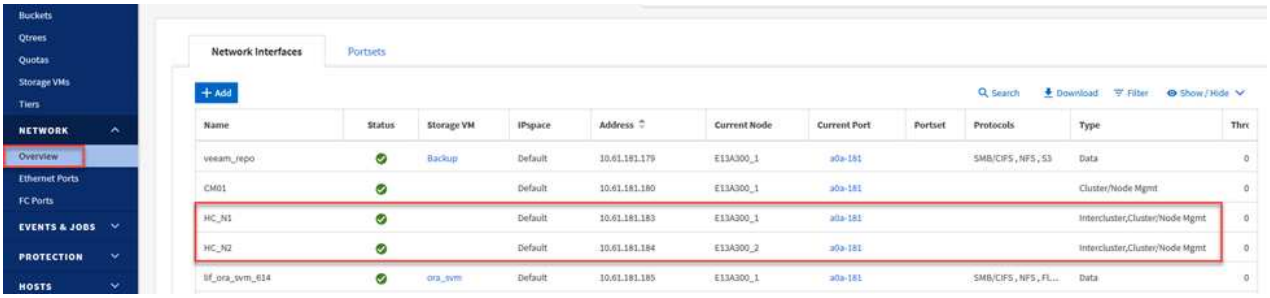
Establezca relaciones de SnapMirror con System Manager y la interfaz de línea de comandos de ONTAP

Todos los pasos necesarios para establecer relaciones de SnapMirror pueden realizarse con System Manager o la interfaz de línea de comandos de ONTAP. En la siguiente sección se proporciona información detallada para ambos métodos:

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

Para los clústeres de ONTAP de origen y de destino, puede recuperar la información de LIF entre clústeres desde System Manager o desde la CLI.

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



2. Para recuperar las direcciones IP de interconexión de clústeres mediante la CLI, ejecute el siguiente comando:

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

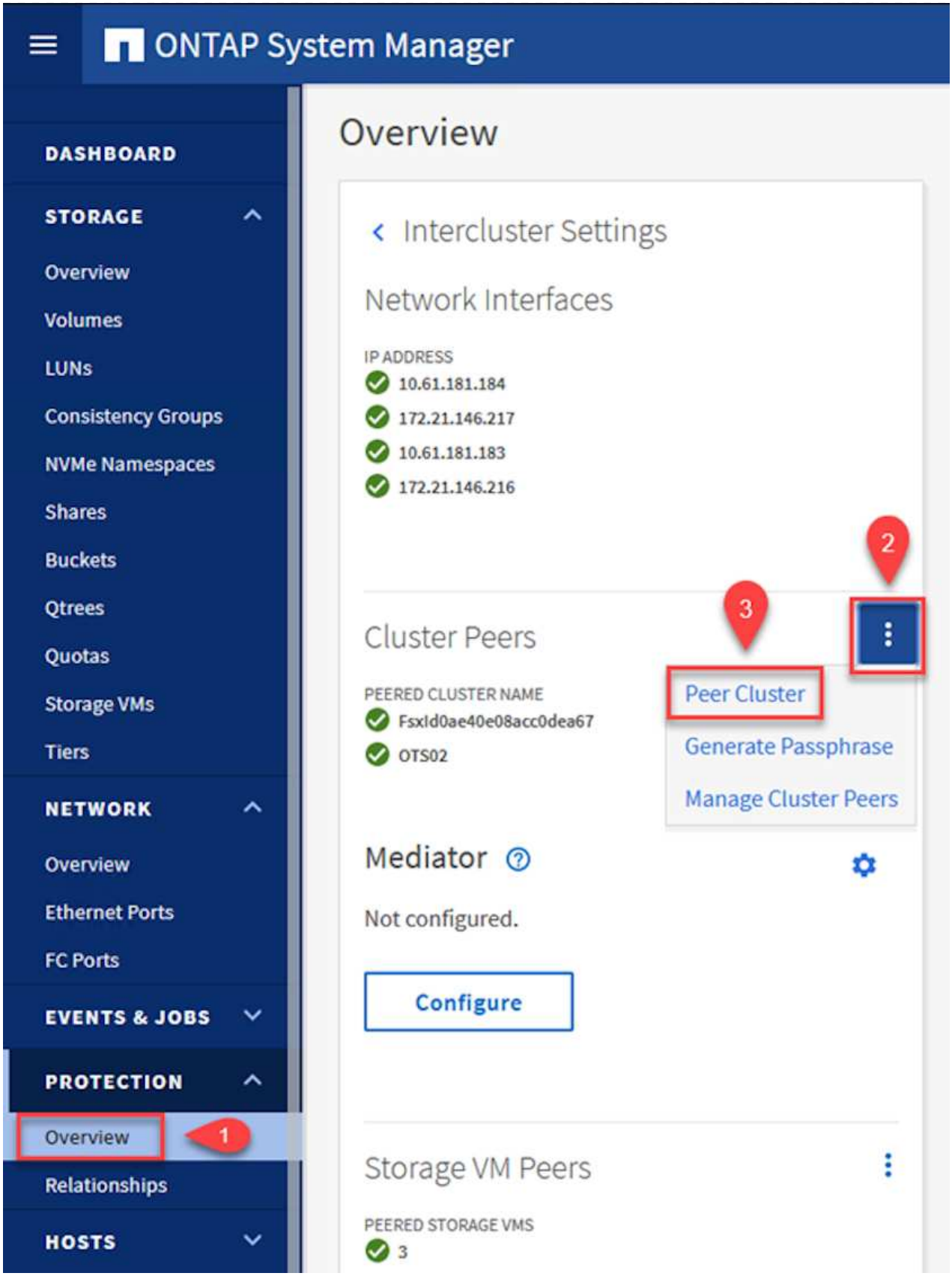
Establezca las relaciones de clústeres entre iguales entre clústeres de ONTAP

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

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

```
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 paridad de clústeres mediante ONTAP System Manager o CLI. En ONTAP System Manager, desplácese hasta Protection > Overview y seleccione Peer Cluster.

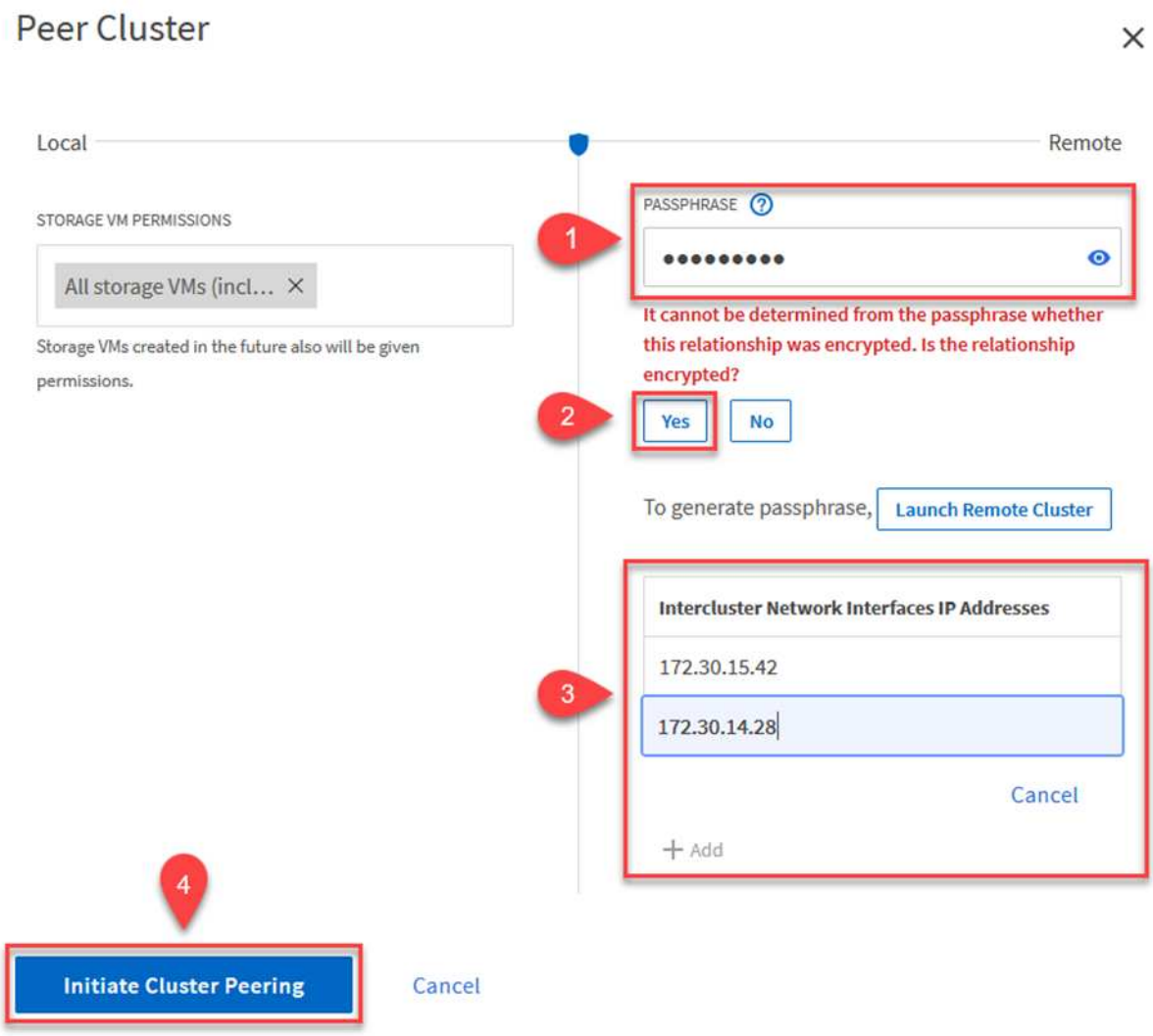


3. En el cuadro de diálogo Peer Cluster, rellene la información que corresponda:
   a. Introduzca la clave de acceso que se utilizó para establecer la relación entre iguales del clúster en el clúster de ONTAP de destino.

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

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

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



4. Compruebe el estado de la relación entre iguales de clústeres en el clúster de ONTAP de destino con el siguiente comando:

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

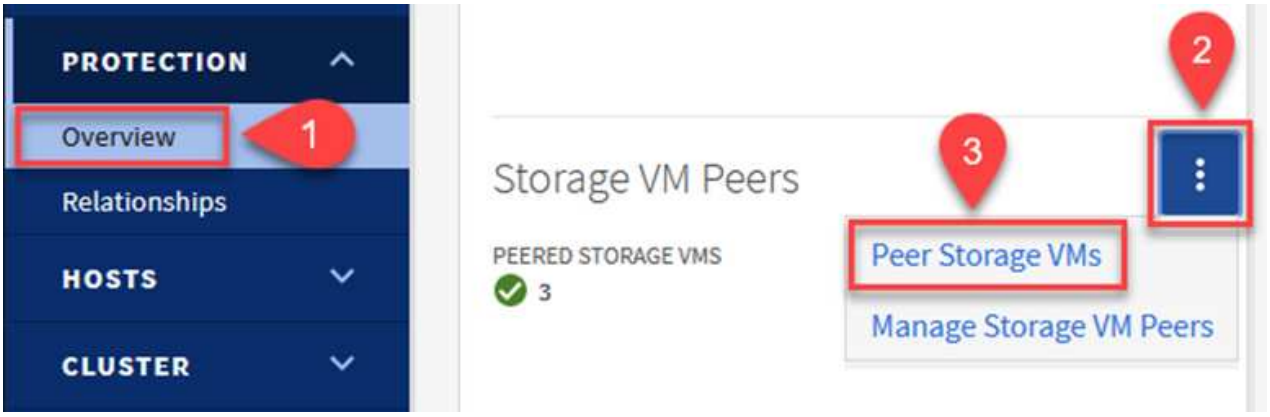
Establecer la relación de paridad de SVM

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

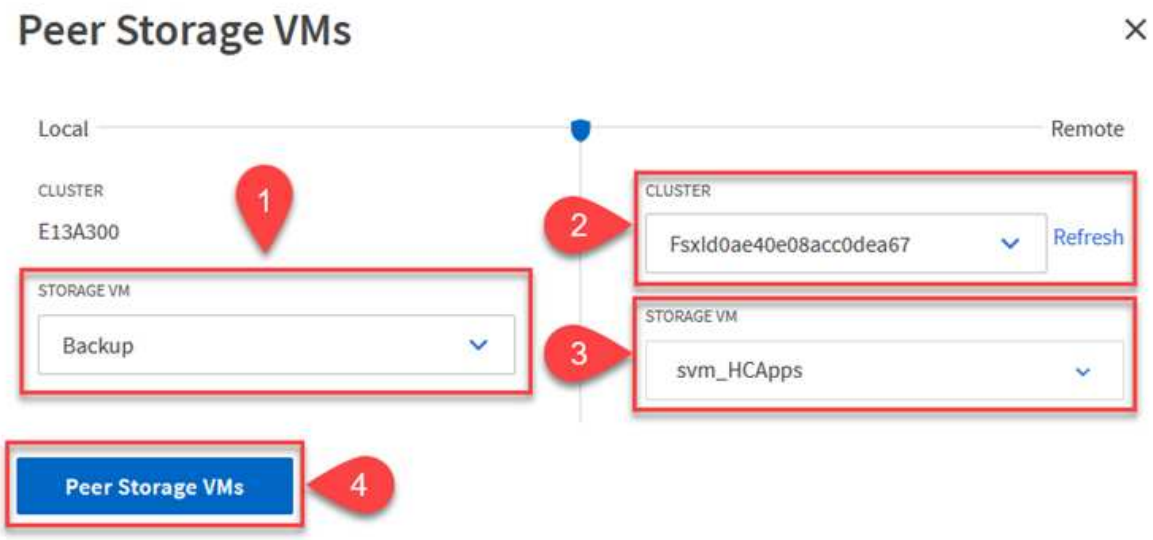
1. Desde el clúster de ONTAP de destino, utilice el siguiente comando desde la interfaz de línea de comandos para crear la relación entre iguales de SVM:

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

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



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



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

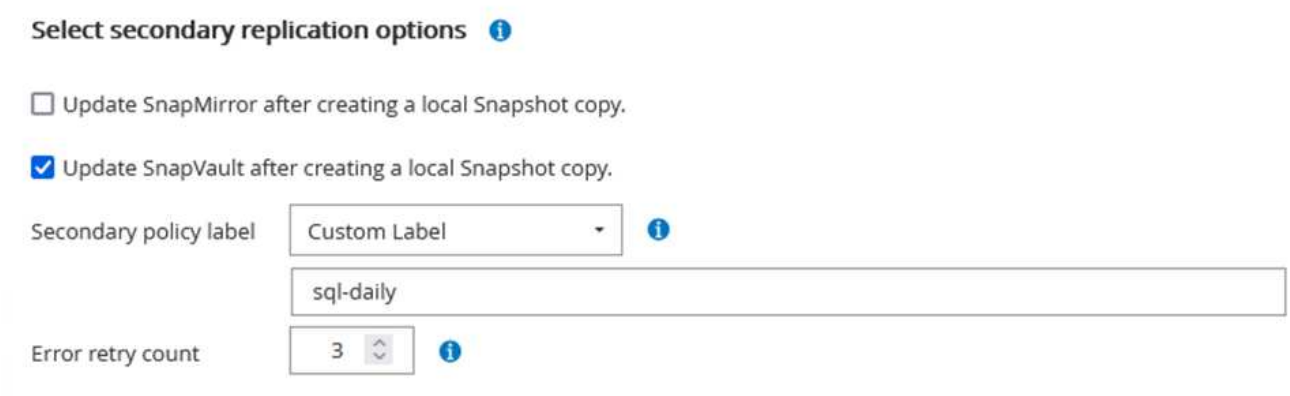
Crear una política de retención de snapshots

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

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

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

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



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

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

1. Cree la política SnapMirror en el clúster FSX.

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

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

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

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

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

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

Crear volúmenes de destino

Para crear un volumen de destino en ONTAP que será el destinatario de las copias Snapshot 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
```

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

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

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

Inicializar las relaciones de SnapMirror

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

Para crear un volumen, ejecute el siguiente comando en el clúster de ONTAP de destino:

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

Configure el plugin de SnapCenter para VMware vSphere

Una vez instalado, puede accederse al plugin de SnapCenter para VMware vSphere desde la interfaz de gestión de vCenter Server Appliance. SCV gestionará backups para los almacenes de datos NFS montados en los hosts ESXi y que contienen máquinas virtuales Windows y Linux.

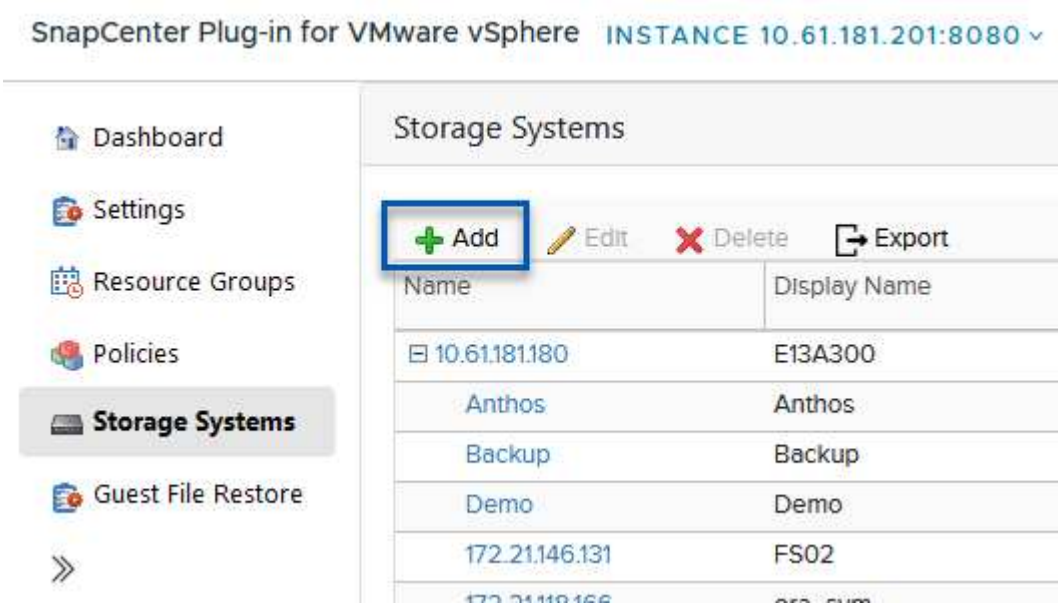
Revise la "Flujo de trabajo de protección de datos" Sección de la documentación de SCV, para obtener más información sobre los pasos involucrados en la configuración de backups.

Para configurar backups de las máquinas virtuales y los almacenes de datos, será necesario completar los siguientes pasos desde la interfaz del plugin.

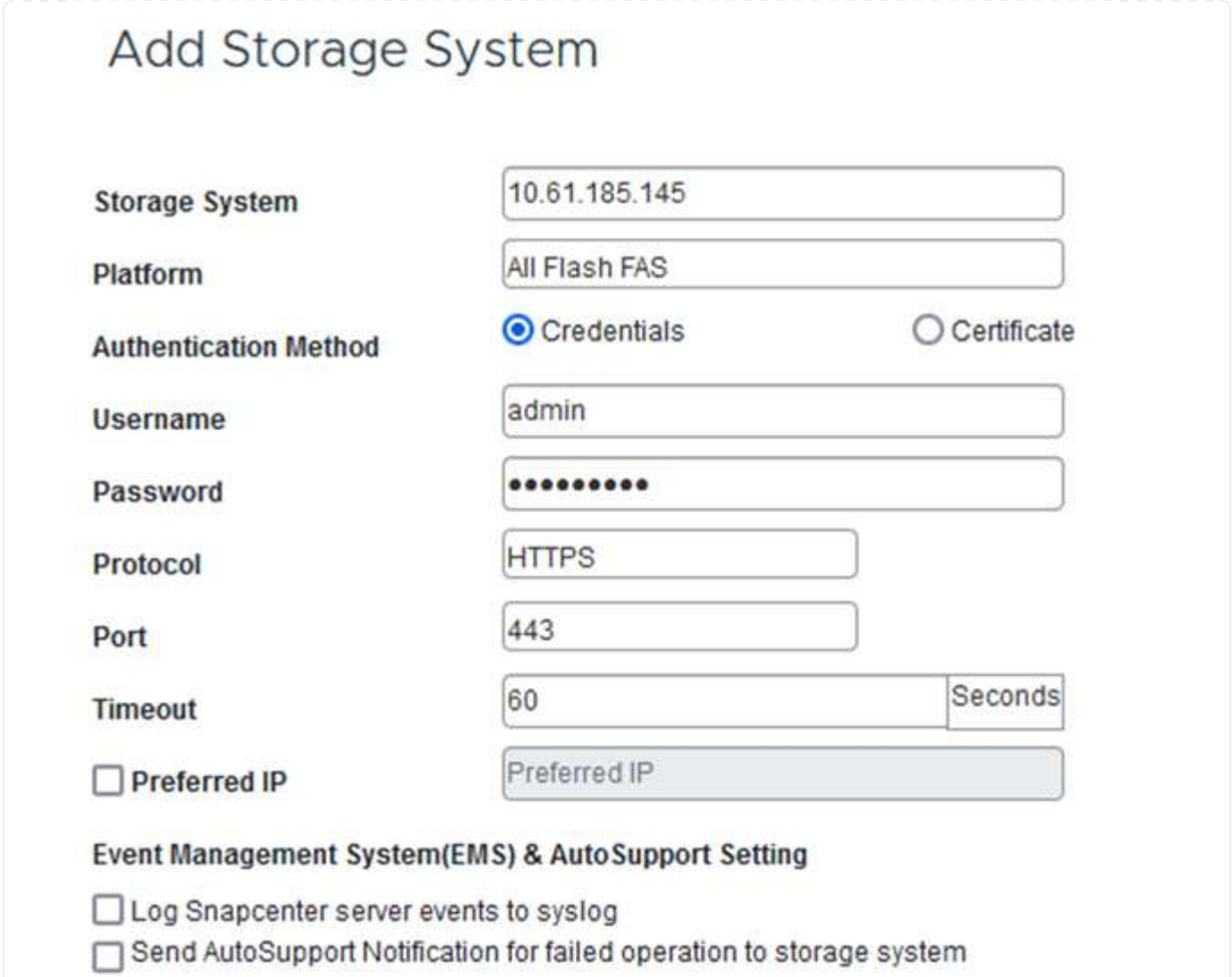
Detección de sistemas de almacenamiento ONTAP

Detectar los clústeres de almacenamiento de ONTAP que se usarán para backups primarios y secundarios.

1. En el plug-in de SnapCenter para 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.

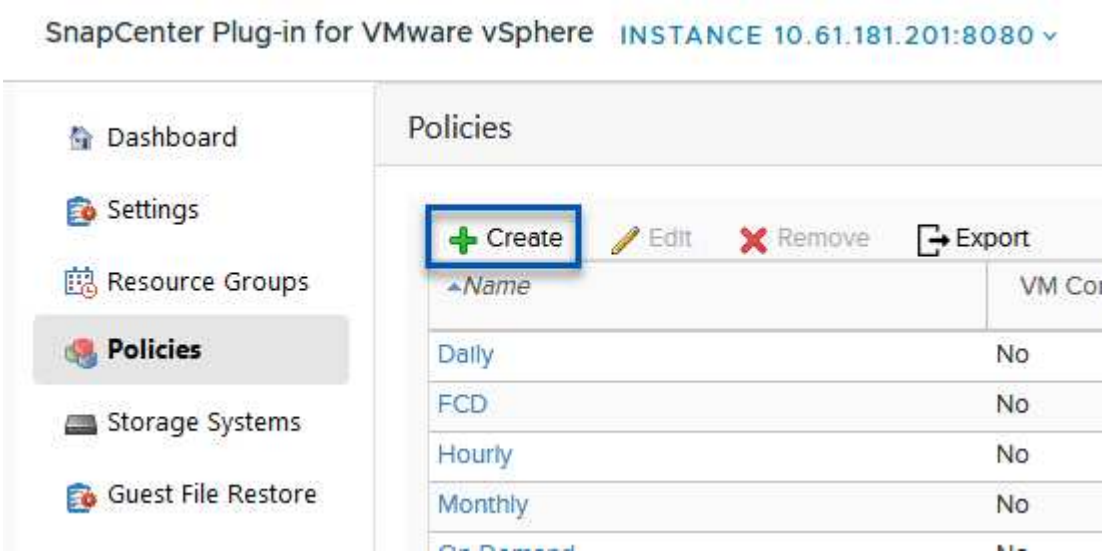
Crear políticas de backup de SCV

Las políticas especifican el período de retención, la frecuencia y las opciones de replicación para los backups gestionados por SCV.

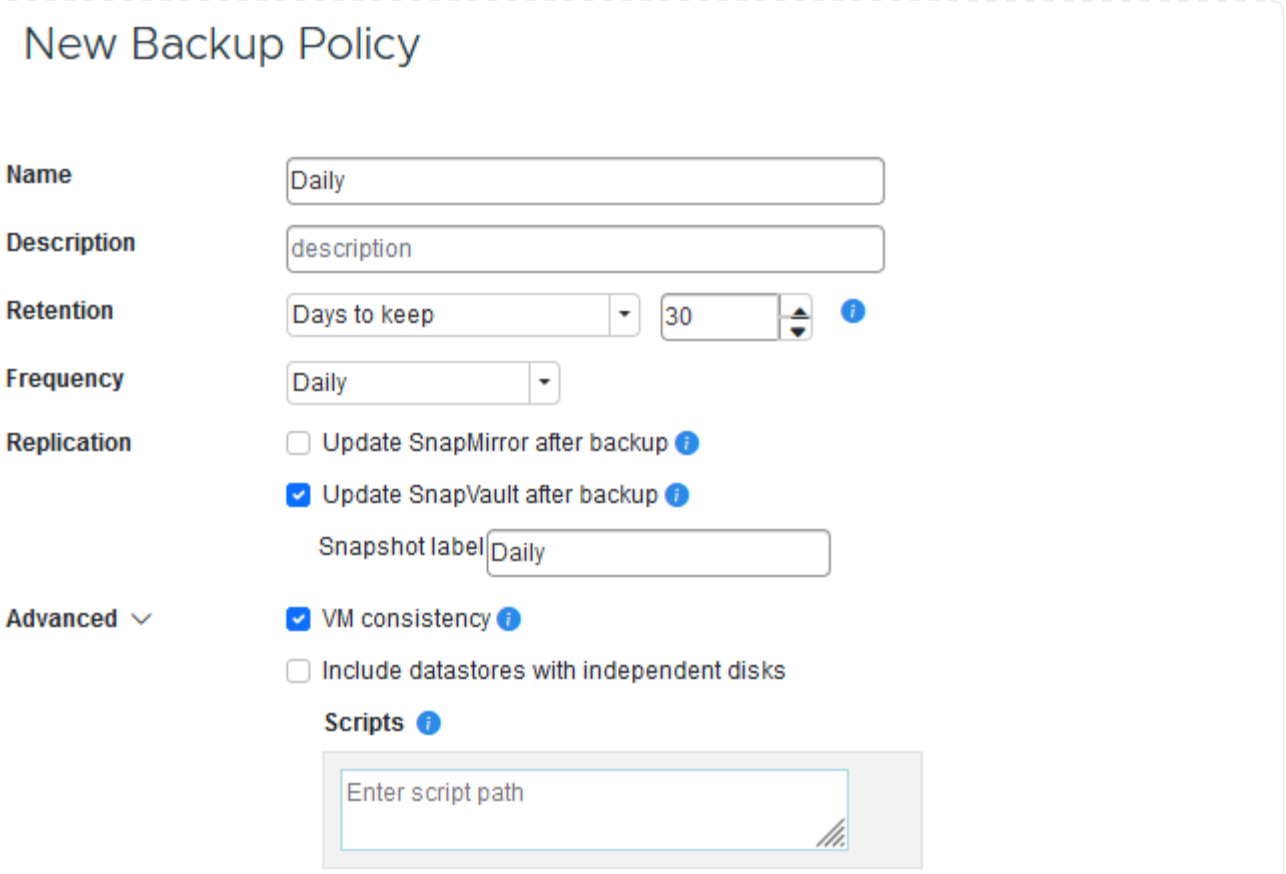
Revise la "Crear políticas de backup para máquinas virtuales y almacenes de datos" sección de la documentación para más información.

Para crear políticas de backup complete los siguientes pasos:

1. En el complemento de SnapCenter para VMware vSphere, navegue hasta **Políticas** en el menú de la izquierda y haga clic en el botón **Crear**.



2. Escriba un nombre para la política, el período de retención, las opciones de frecuencia y replicación y la etiqueta de la snapshot.



Al crear una política en el plugin de SnapCenter, verá opciones para SnapMirror y SnapVault. Si elige SnapMirror, la programación de retención especificada en la política será la misma para las copias de Snapshot primarias y secundarias. Si elige SnapVault, la programación de retención de la snapshot secundaria se basará en una programación independiente implementada con la relación de SnapMirror. Esto es útil cuando se desean períodos de retención más largos para backups secundarios.

Las etiquetas de Snapshot son útiles porque se pueden usar para aplicar políticas con un período de retención específico para las copias de SnapVault replicadas en el clúster de ONTAP secundario. Cuando SCV se utiliza con BlueXP Backup and Restore, el campo de etiqueta de Snapshot debe estar en blanco o Match la etiqueta especificada en la política de backup de BlueXP.

3. Repita el procedimiento para cada política necesaria. Por ejemplo, políticas independientes para backups diarios, semanales y mensuales.

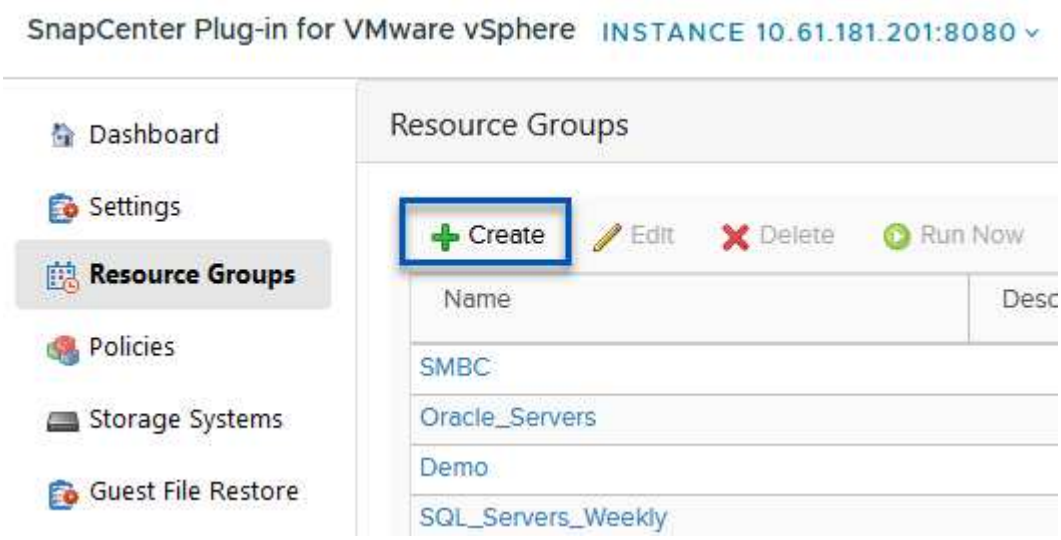
Crear grupos de recursos

Los grupos de recursos contienen los almacenes de datos y las máquinas virtuales que se incluirán en un trabajo de backup, junto con la política y la programación de backup asociadas.

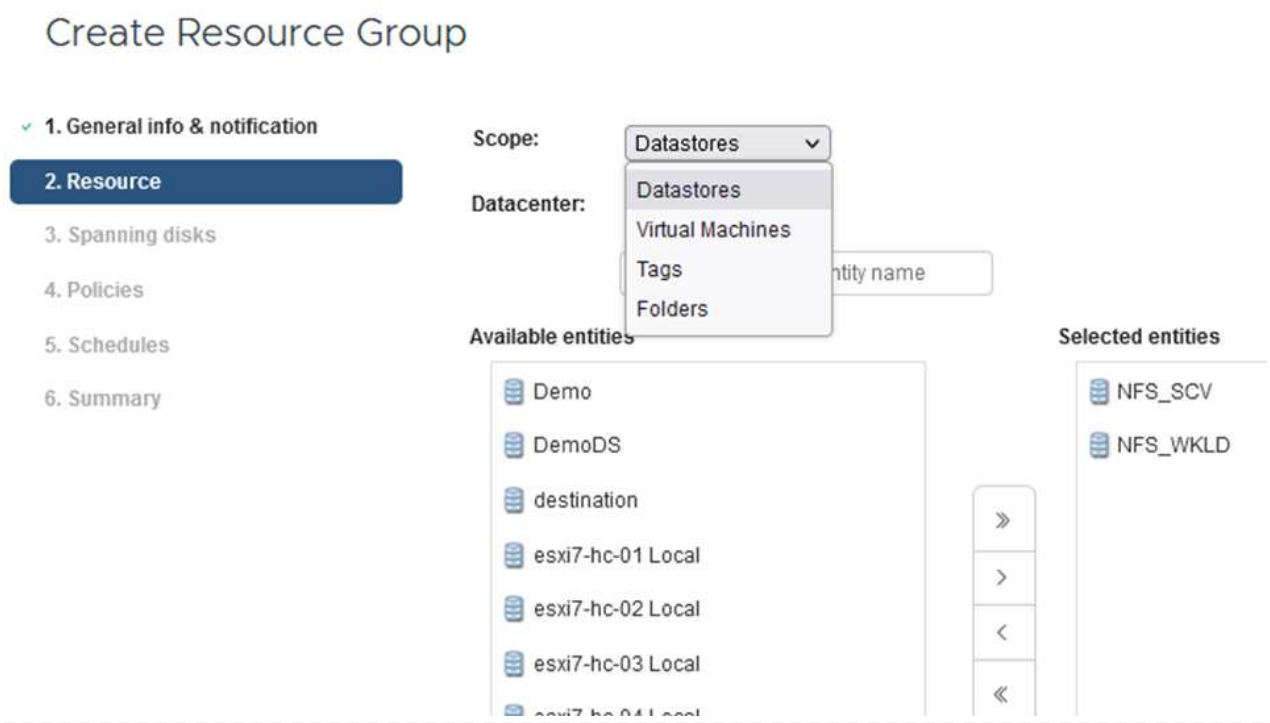
Revise la "Crear grupos de recursos" sección de la documentación para más información.

Para crear grupos de recursos, complete los siguientes pasos.

1. En el plugin de SnapCenter para VMware vSphere, navegue hasta **Grupos de recursos** en el menú de la izquierda y haga clic en el botón **Crear**.

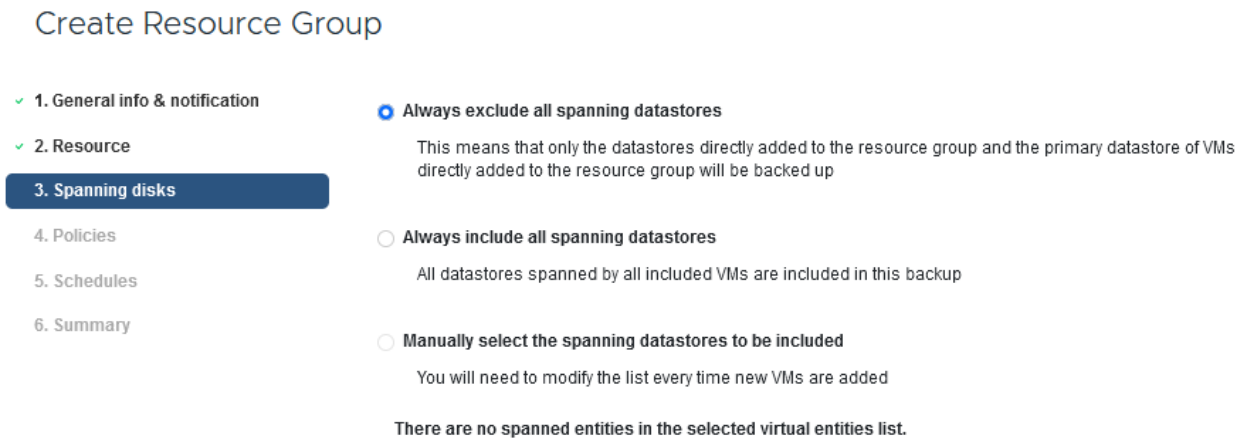


2. En el asistente Create Resource Group, escriba un nombre y una descripción para el grupo, así como la información necesaria para recibir notificaciones. Haga clic en **Siguiente**
3. En la página siguiente, seleccione los almacenes de datos y las máquinas virtuales que desean incluirse en el trabajo de copia de seguridad y luego haga clic en **Siguiente**.



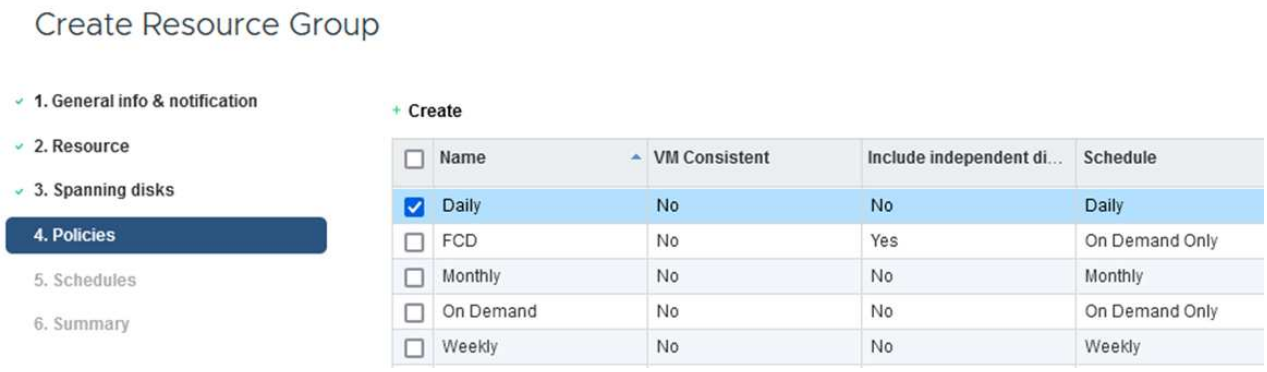
Puede seleccionar máquinas virtuales específicas o almacenes de datos completos. Independientemente del lugar que elija, se realiza el backup de todo el volumen (y el almacén de datos), ya que el backup es el resultado de tomar una snapshot del volumen subyacente. En la mayoría de los casos, es más fácil elegir todo el almacén de datos. Sin embargo, si desea limitar la lista de máquinas virtuales disponibles al restaurar, puede seleccionar solo un subconjunto de máquinas virtuales para realizar backups.

4. Elija opciones para ampliar almacenes de datos para máquinas virtuales con VMDK que residen en varios almacenes de datos y luego haga clic en **Siguiente**.



El backup y la recuperación de datos de BlueXP no admite actualmente el backup de máquinas virtuales con VMDK que abarquen varios almacenes de datos.

5. En la página siguiente, seleccione las políticas que se asociarán con el grupo de recursos y haga clic en **Siguiente**.



Al realizar un backup de las snapshots gestionadas de SCV en el almacenamiento de objetos mediante el backup y recuperación de BlueXP, cada grupo de recursos solo puede estar asociado con una sola política.

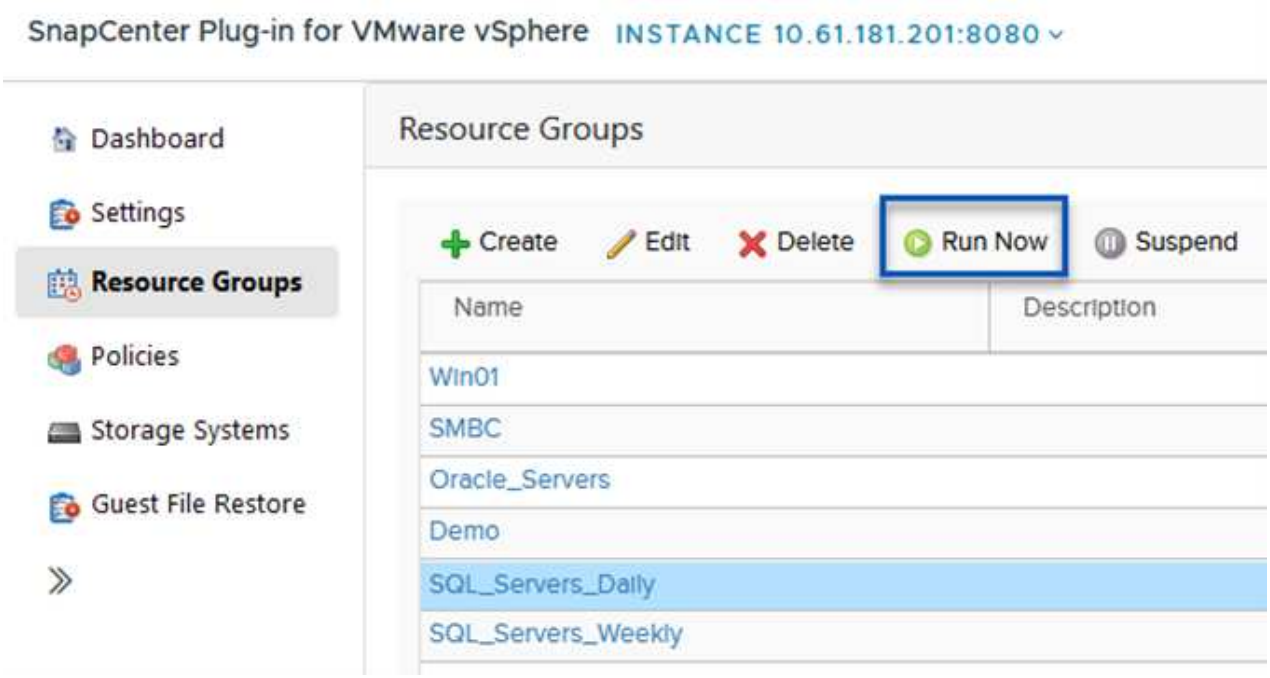
6. Seleccione un programa que determinará en qué momento se ejecutarán las copias de seguridad. Haga clic en **Siguiente**.

7. Finalmente, revise la página de resumen y luego en **Finish** para completar la creación del grupo de recursos.

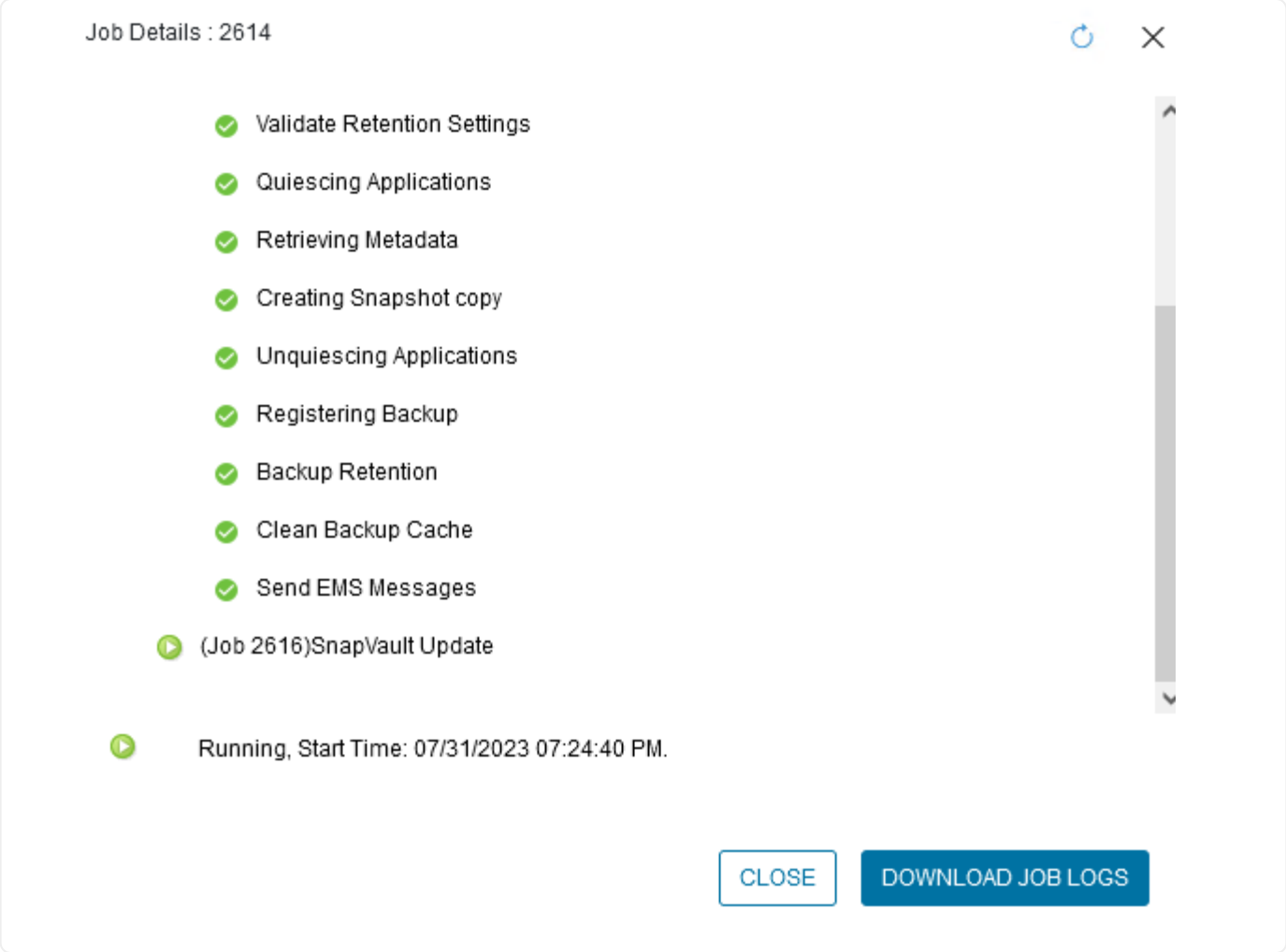
Ejecute una tarea de backup

En este paso final, ejecute un trabajo de copia de seguridad y supervise su progreso. Se debe completar correctamente al menos una tarea de backup en SCV antes de que se puedan detectar los recursos desde el backup y la recuperación de BlueXP.

1. En el plugin de SnapCenter para VMware vSphere, desplácese hasta **Resource Groups** en el menú de la izquierda.
2. Para iniciar una tarea de copia de seguridad, seleccione el grupo de recursos deseado y haga clic en el botón **Ejecutar ahora**.



3. Para supervisar el trabajo de copia de seguridad, navegue hasta **Dashboard** en el menú de la izquierda. En **Actividades recientes del trabajo**, haga clic en el número de ID del trabajo para supervisar el progreso del trabajo.



Configura backups en el almacenamiento de objetos en el backup y la recuperación de BlueXP

Para que BlueXP gestione la infraestructura de datos de forma eficaz, hace falta instalar antes un Connector. El conector ejecuta las acciones involucradas en la detección de recursos y la gestión de operaciones de datos.

Para obtener más información sobre el conector BlueXP, consulte "Más información sobre conectores" En la documentación de BlueXP.

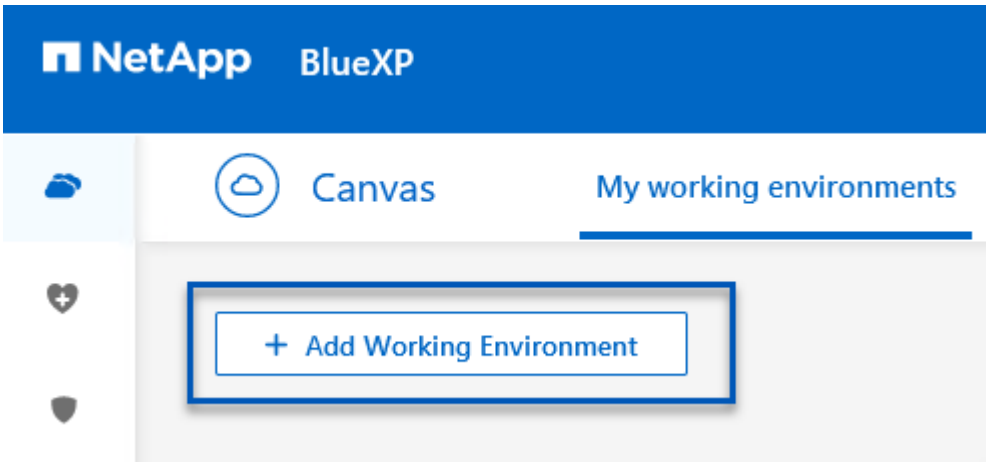
Una vez instalado el conector para el proveedor de nube que se está utilizando, se podrá ver una representación gráfica del almacenamiento de objetos desde Canvas.

Para configurar el backup y la recuperación de BlueXP en los datos de backup gestionados por SCV on-premises, complete los siguientes pasos:

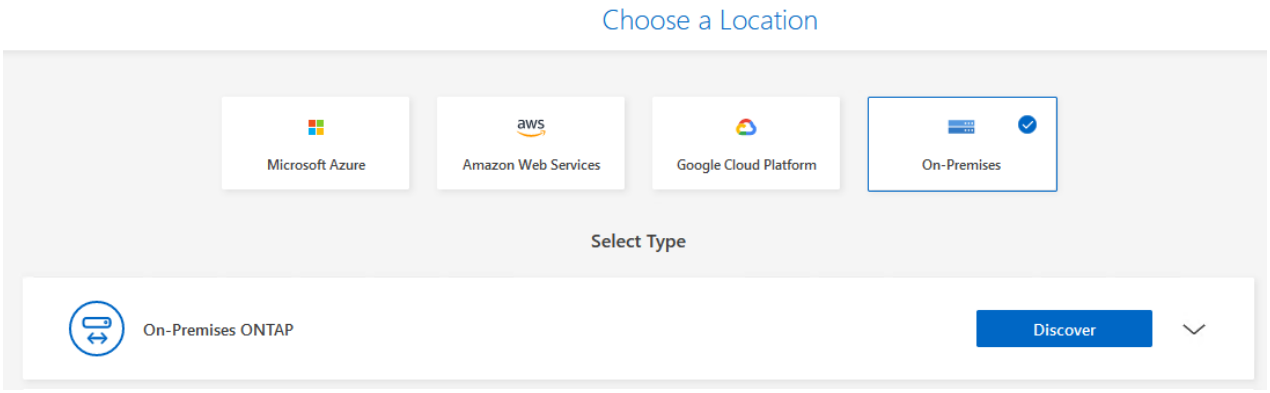
Agregue entornos de trabajo al lienzo

El primer paso es añadir los sistemas de almacenamiento de ONTAP on-premises a BlueXP

1. En el lienzo seleccione **Agregar entorno de trabajo** para comenzar.



2. Seleccione **on-premises** de la selección de ubicaciones y luego haga clic en el botón **Discover**.



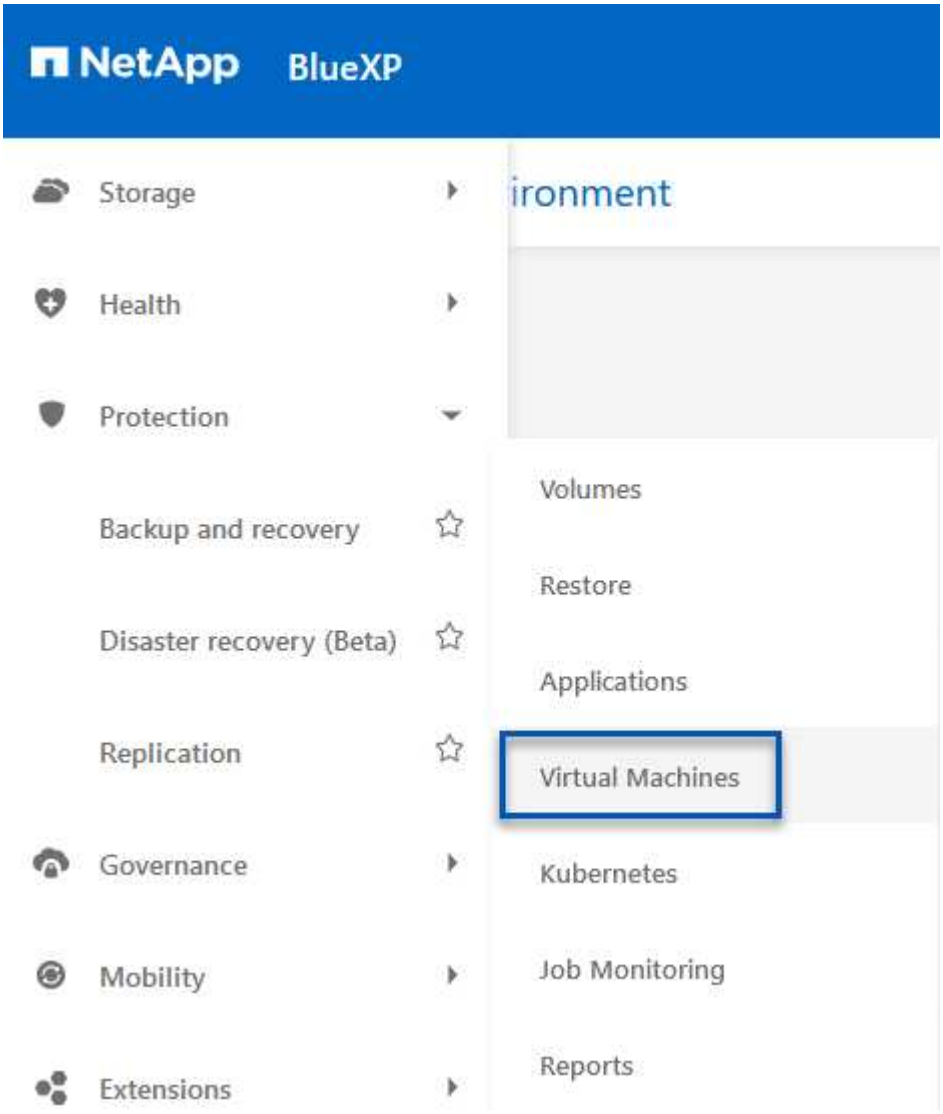
3. Rellene las credenciales del sistema de almacenamiento ONTAP y haga clic en el botón **Descubrir** para agregar el entorno de trabajo.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

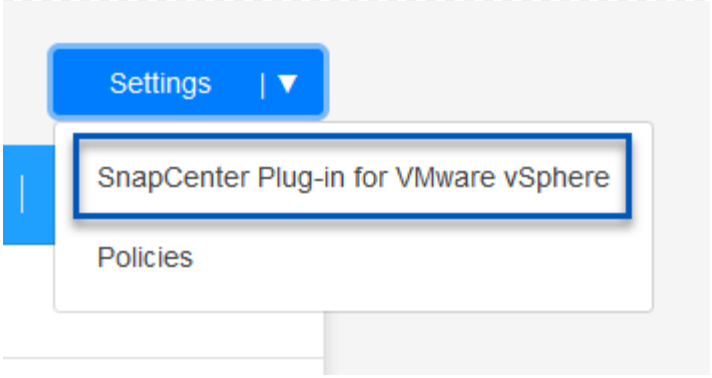
Detecte el dispositivo SCV local y vCenter

Para detectar el almacén de datos en las instalaciones y los recursos de máquinas virtuales, añada información del agente de datos SCV y las credenciales para el dispositivo de gestión de vCenter.

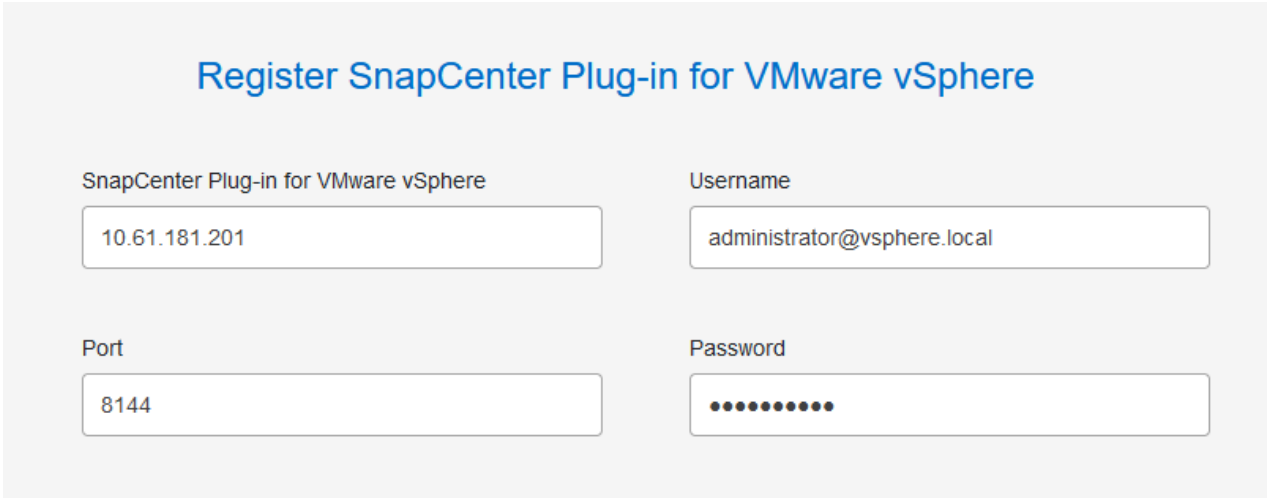
1. En el menú de la izquierda de BlueXP, seleccione **Protección > Copia de seguridad y recuperación > Máquinas virtuales**



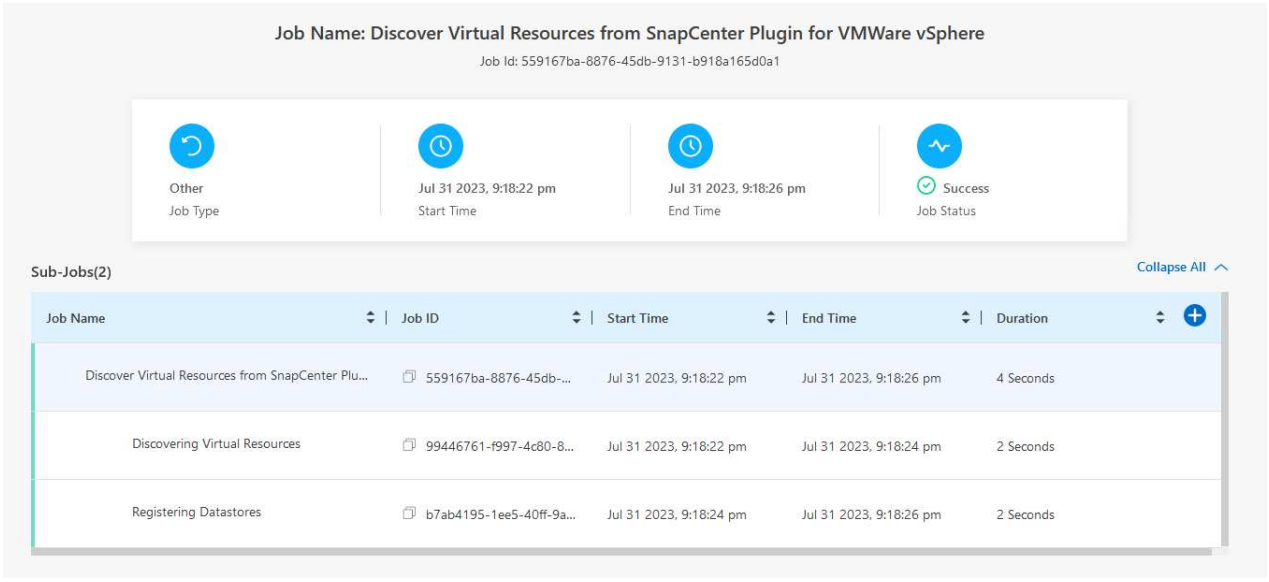
2. Desde la pantalla principal de Máquinas virtuales, acceda al menú desplegable **Configuración** y seleccione **SnapCenter Plug-in for VMware vSphere**.



3. Haga clic en el botón **Registrar** y, a continuación, introduzca la dirección IP y el número de puerto para el dispositivo de complemento de SnapCenter y el nombre de usuario y la contraseña para el dispositivo de administración de vCenter. Haga clic en el botón **Registrar** para comenzar el proceso de descubrimiento.



4. El progreso de los trabajos se puede supervisar desde la pestaña Supervisión de trabajos.



5. Una vez completada la detección, podrá ver los almacenes de datos y las máquinas virtuales en todos los dispositivos SCV detectados.

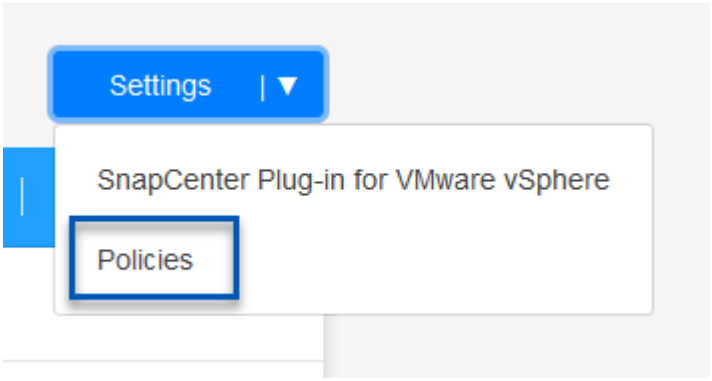
Image::bxp-scw-hybrid-23.png[Ver los recursos disponibles]

Cree políticas de backup de BlueXP

En el backup y recuperación de datos de BlueXP para máquinas virtuales, cree políticas que especifiquen el período de retención, el origen de backup y la política de archivado.

Para obtener más información sobre la creación de políticas, consulte "Crear una política para realizar backups de almacenes de datos".

1. Desde la página principal de copia de seguridad y recuperación de BlueXP para máquinas virtuales, accede al menú desplegable **Configuración** y selecciona **Políticas**.



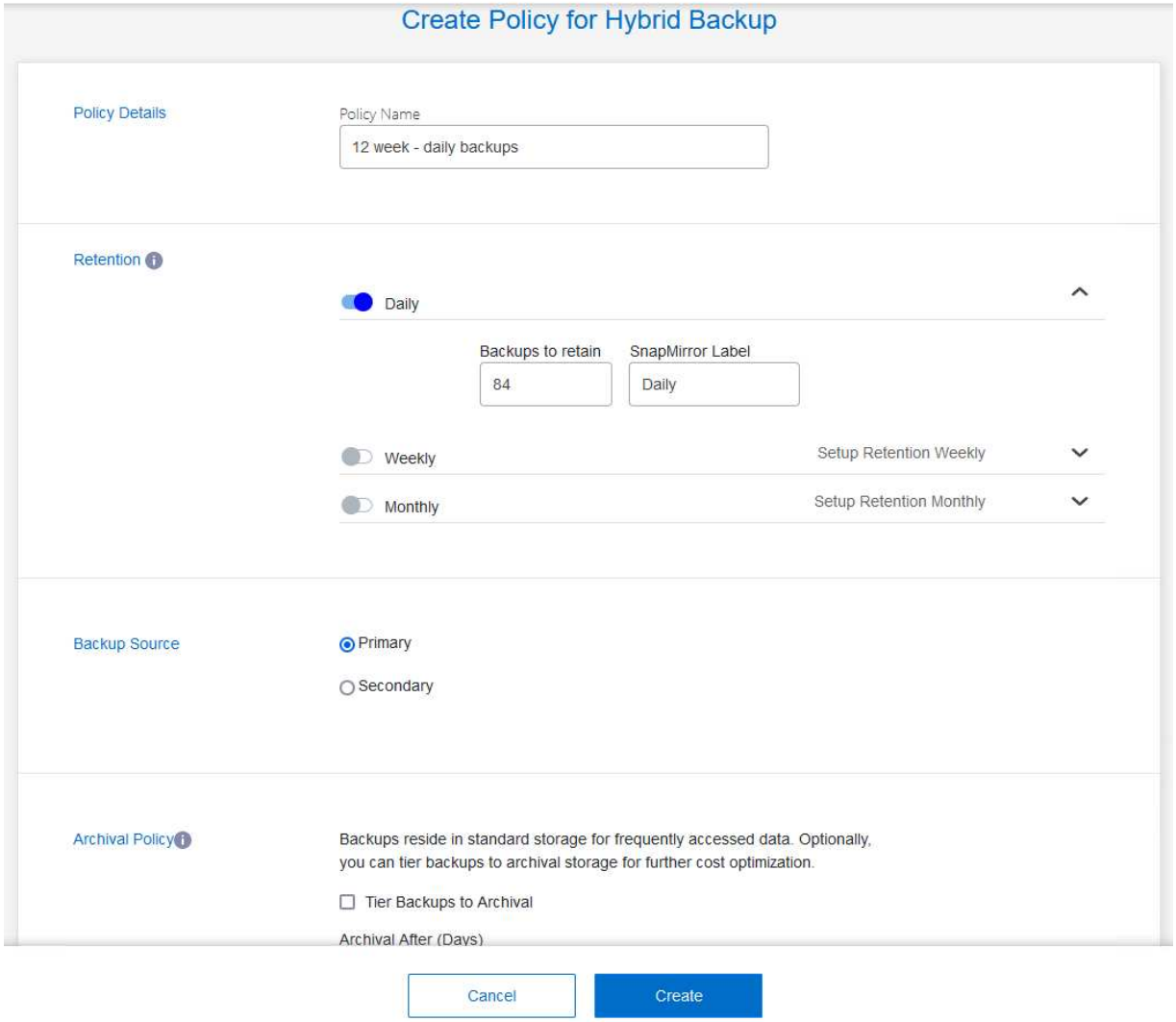
2. Haga clic en **Crear política** para acceder a la ventana **Crear política para copia de seguridad híbrida**.

   a. Agregue un nombre para la política

   b. Seleccione el período de retención deseado

   c. Seleccione si se asignarán los backups del sistema de almacenamiento de ONTAP principal o secundario en las instalaciones

   d. Opcionalmente, especifique tras qué período de tiempo se organizarán los backups en niveles en el almacenamiento archivado para reducir aún más los costes.



La etiqueta de SnapMirror introducida aquí se utiliza también para identificar qué backups aplicarán la política. El nombre de etiqueta debe coincidir con el nombre de etiqueta en la política de SCV en las instalaciones correspondiente.

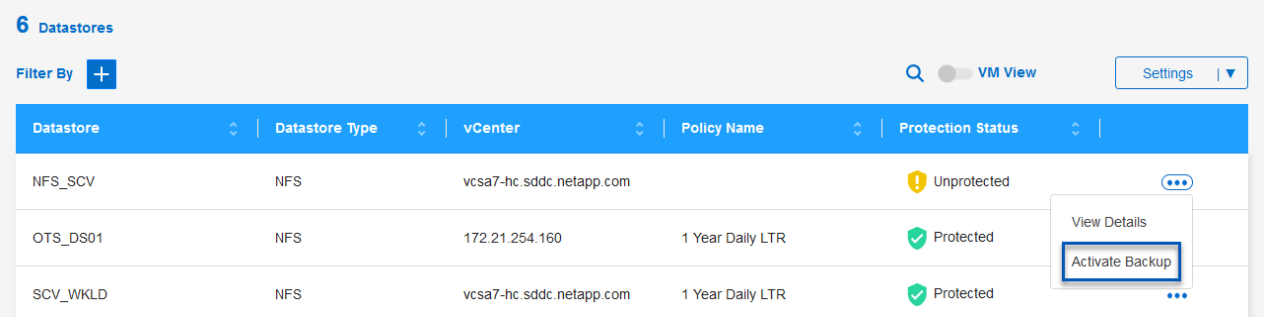
3. Haga clic en **Crear** para completar la creación de la política.

Backup de almacenes de datos en Amazon Web Services

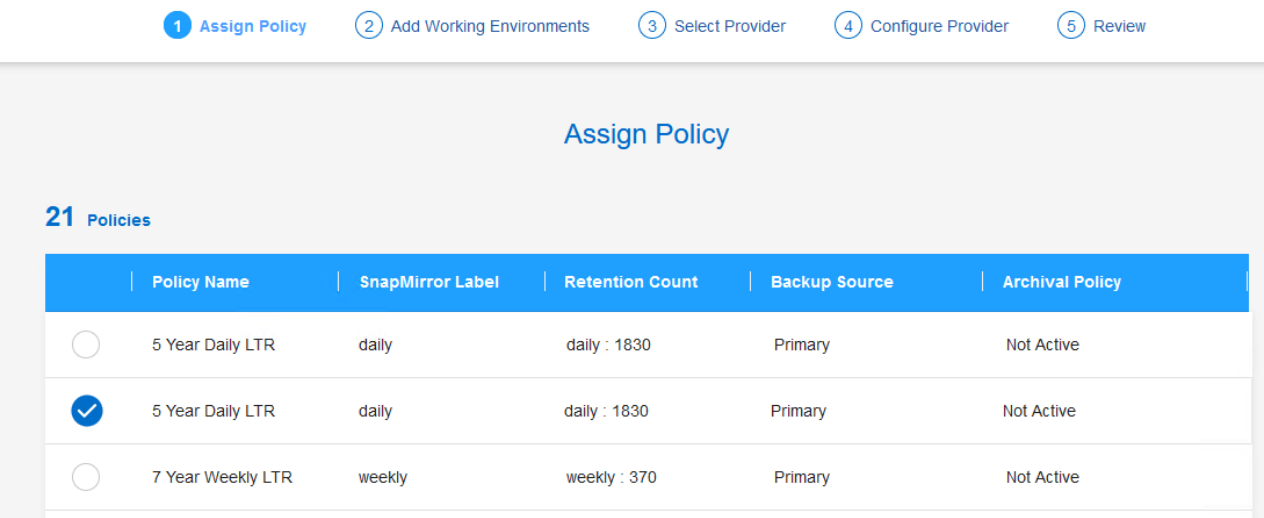
El paso final es activar la protección de datos para los almacenes de datos individuales y los equipos virtuales. Los siguientes pasos describen cómo activar copias de seguridad en AWS.

Para obtener más información, consulte "Backup de almacenes de datos en Amazon Web Services".

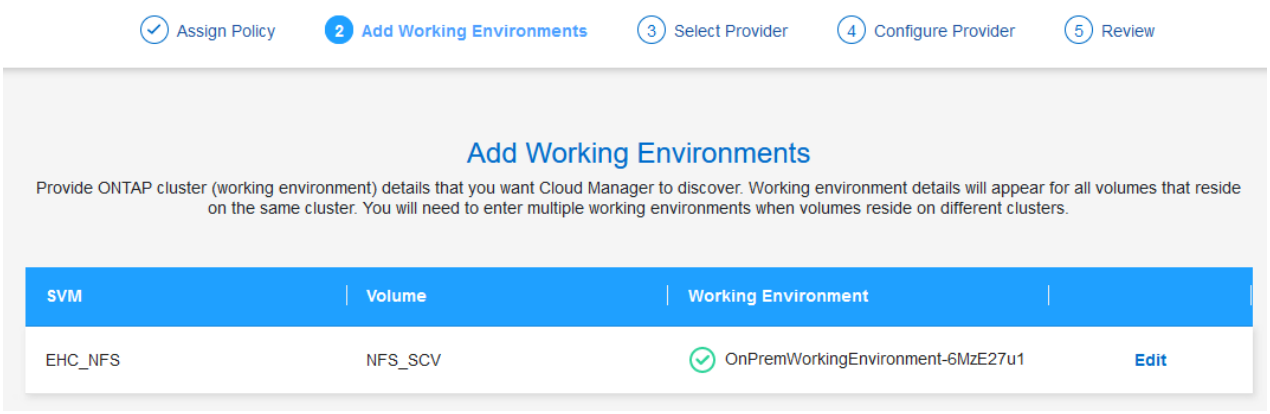
1. Desde la página principal de copia de seguridad y recuperación de BlueXP para máquinas virtuales, accede a la lista desplegable de configuración para que se realice una copia de seguridad del almacén de datos y selecciona **Activar copia de seguridad**.



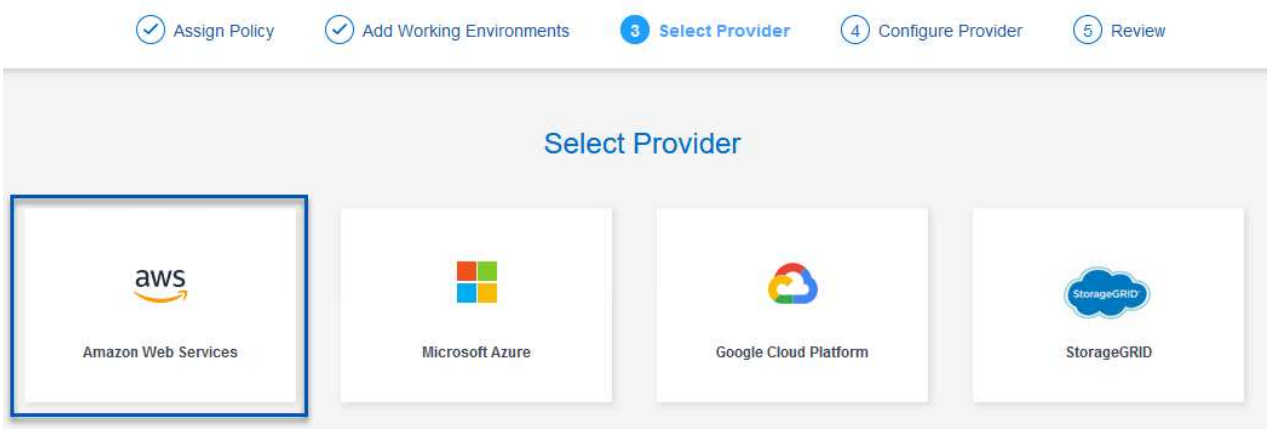
2. Asigne la política que se utilizará para la operación de protección de datos y haga clic en **Siguiente**.



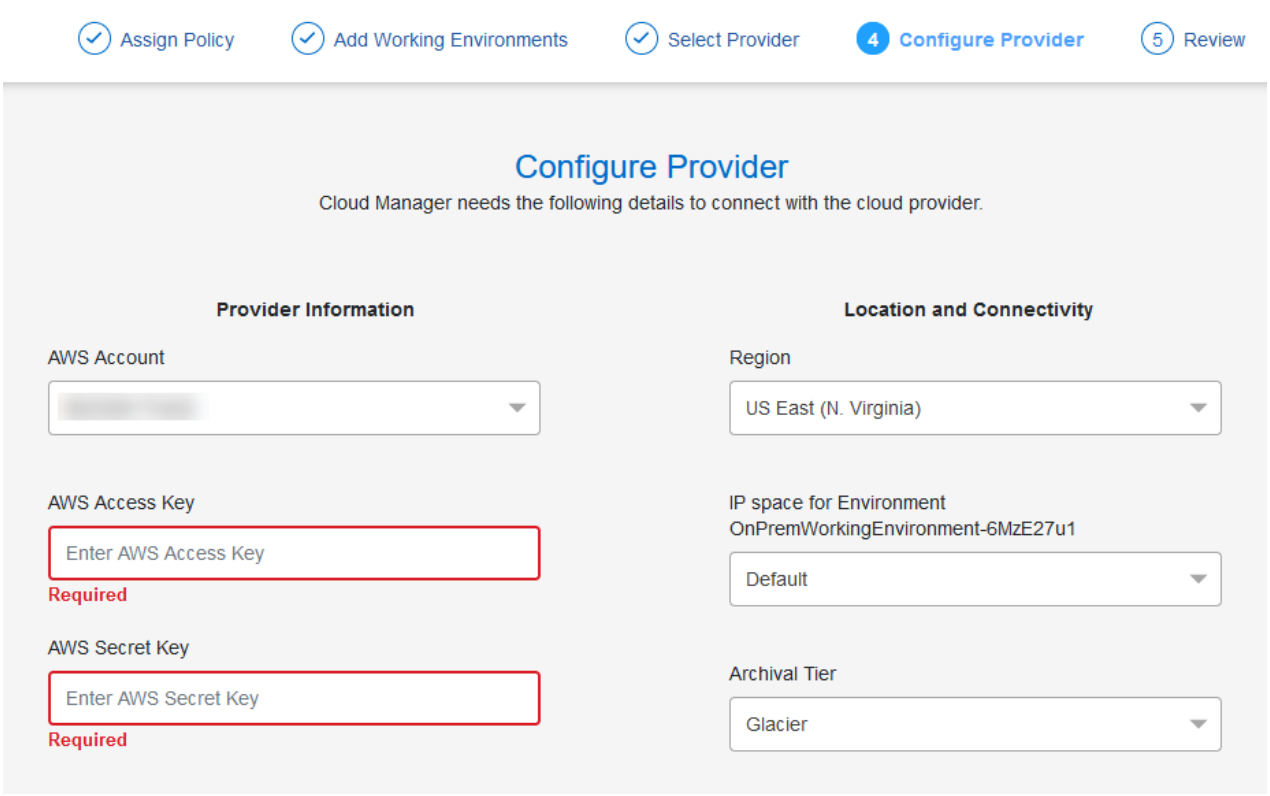
3. En la página **Agregar entornos de trabajo**, el almacén de datos y el entorno de trabajo con una marca de verificación deben aparecer si el entorno de trabajo se ha detectado previamente. Si el entorno de trabajo no se ha detectado anteriormente, puede agregarlo aquí. Haga clic en **Siguiente** para continuar.



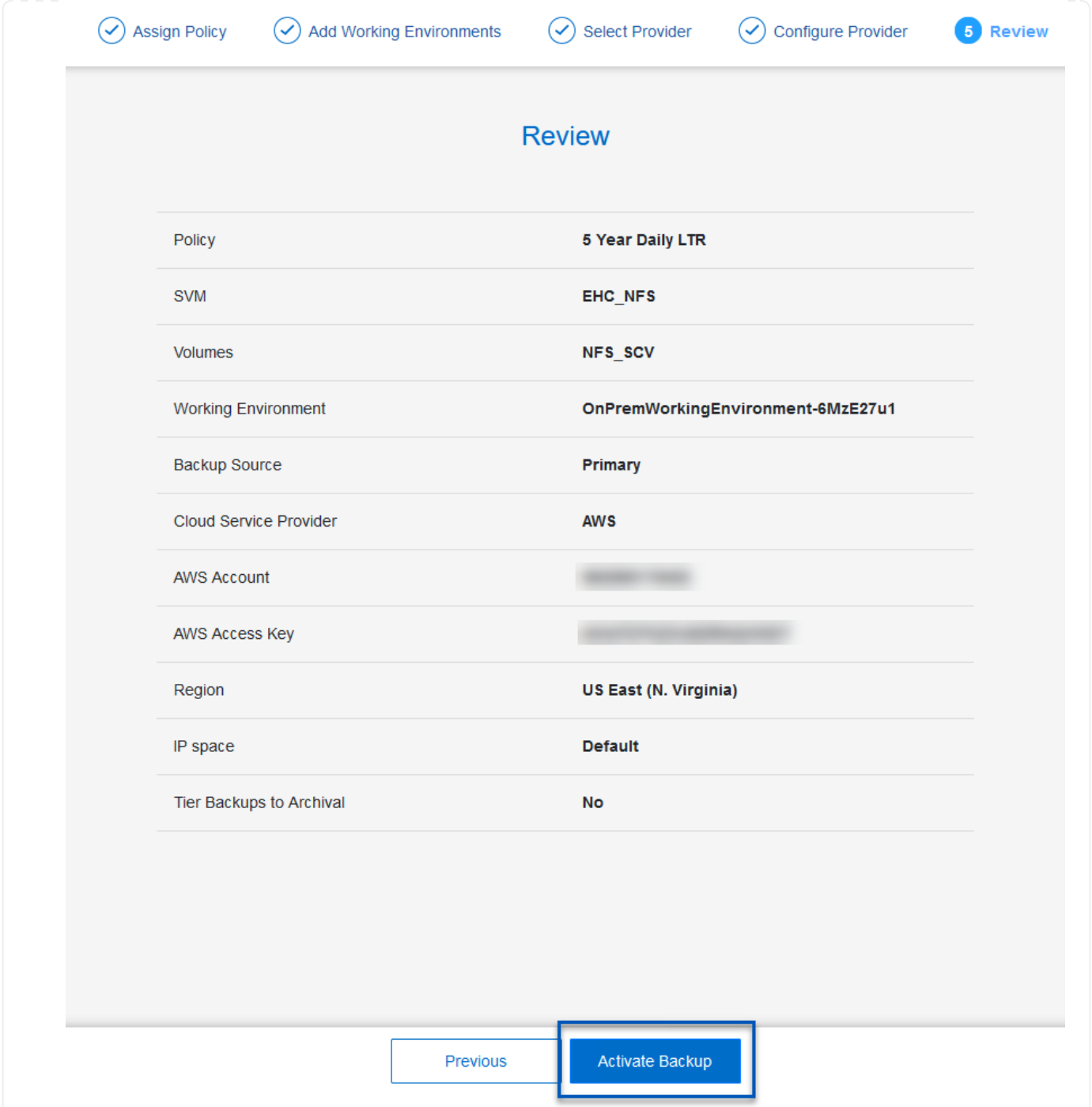
4. En la página **Seleccionar proveedor**, haga clic en AWS y luego haga clic en el botón **Siguiente** para continuar.



5. Rellene la información de credenciales específica del proveedor para AWS, incluida la clave de acceso de AWS y la clave secreta, la región y el nivel de archivado que se va a utilizar. Además, seleccione el espacio IP de ONTAP para el sistema de almacenamiento de ONTAP en las instalaciones. Haga clic en **Siguiente**.



6. Por último, revise los detalles del trabajo de copia de seguridad y haga clic en el botón **Activar copia de seguridad** para iniciar la protección de datos del almacén de datos.



En este punto, la transferencia de datos puede no comenzar inmediatamente. El backup y la recuperación de BlueXP analiza todas las copias Snapshot pendientes cada hora y luego las transfiere al almacenamiento de objetos.

Restauración de máquinas virtuales en caso de pérdida de datos

Garantizar la protección de los datos es tan solo un aspecto de la protección de datos completa. Igualmente importante es la capacidad de restaurar datos rápidamente desde cualquier ubicación en caso de pérdida de datos o ataque de ransomware. Esta funcionalidad es esencial para mantener operaciones empresariales transparentes y cumplir con los objetivos de punto de recuperación.

NetApp ofrece una estrategia 3-2-1 altamente adaptable que proporciona un control personalizado de los programas de retención en las ubicaciones de almacenamiento principal, secundario y de objetos. Esta estrategia proporciona la flexibilidad necesaria para adaptar los enfoques de protección de datos a necesidades específicas.

En esta sección se ofrece una descripción general del proceso de restauración de datos desde el plugin de SnapCenter para VMware vSphere y backup y recuperación de BlueXP para máquinas virtuales.

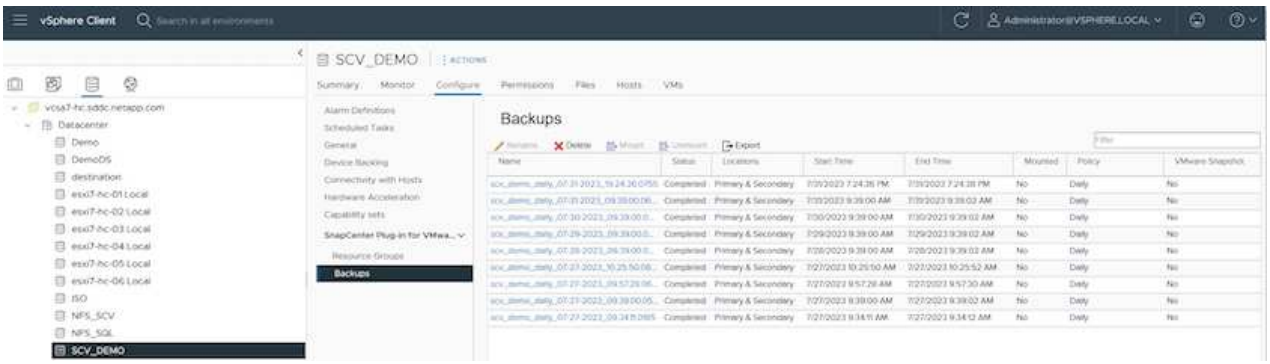
Restaurar máquinas virtuales desde el plugin de SnapCenter para VMware vSphere

Para esta solución, se restauraron las máquinas virtuales en ubicaciones originales y alternativas. No todos los aspectos de las funcionalidades de restauración de datos de SCV se tratarán en esta solución. Para obtener información detallada sobre todo lo que SCV tiene para ofrecer, consulte la "Restaurar máquinas virtuales desde backups" en la documentación del producto.

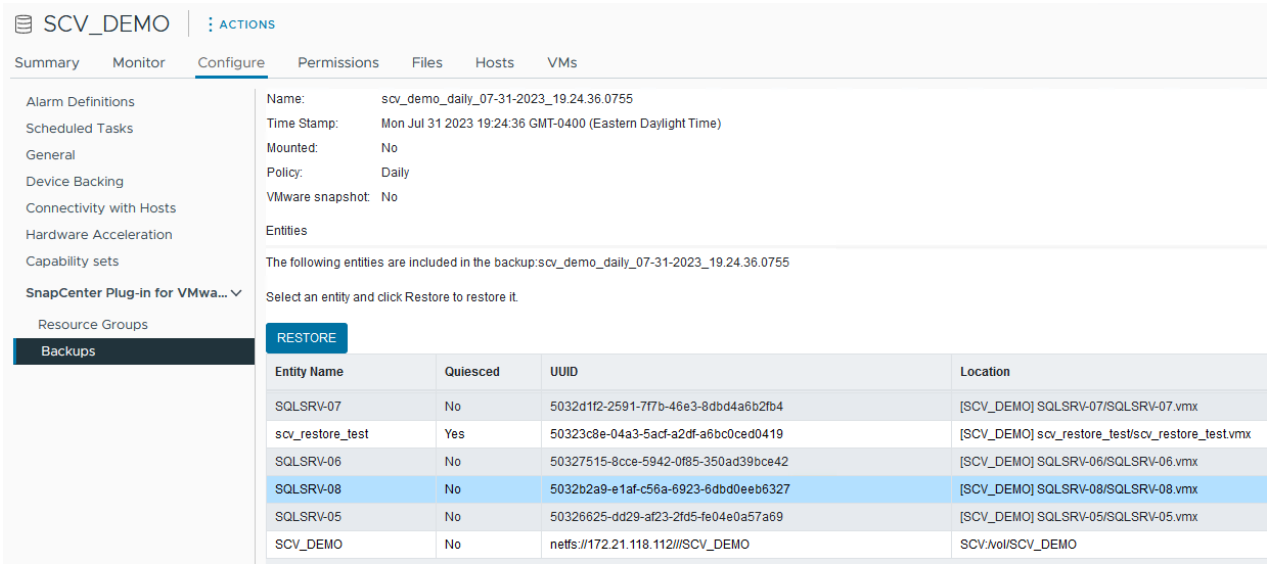
Restaurar máquinas virtuales desde SCV

Complete los siguientes pasos para restaurar una restauración de máquina virtual a partir de un almacenamiento principal o secundario.

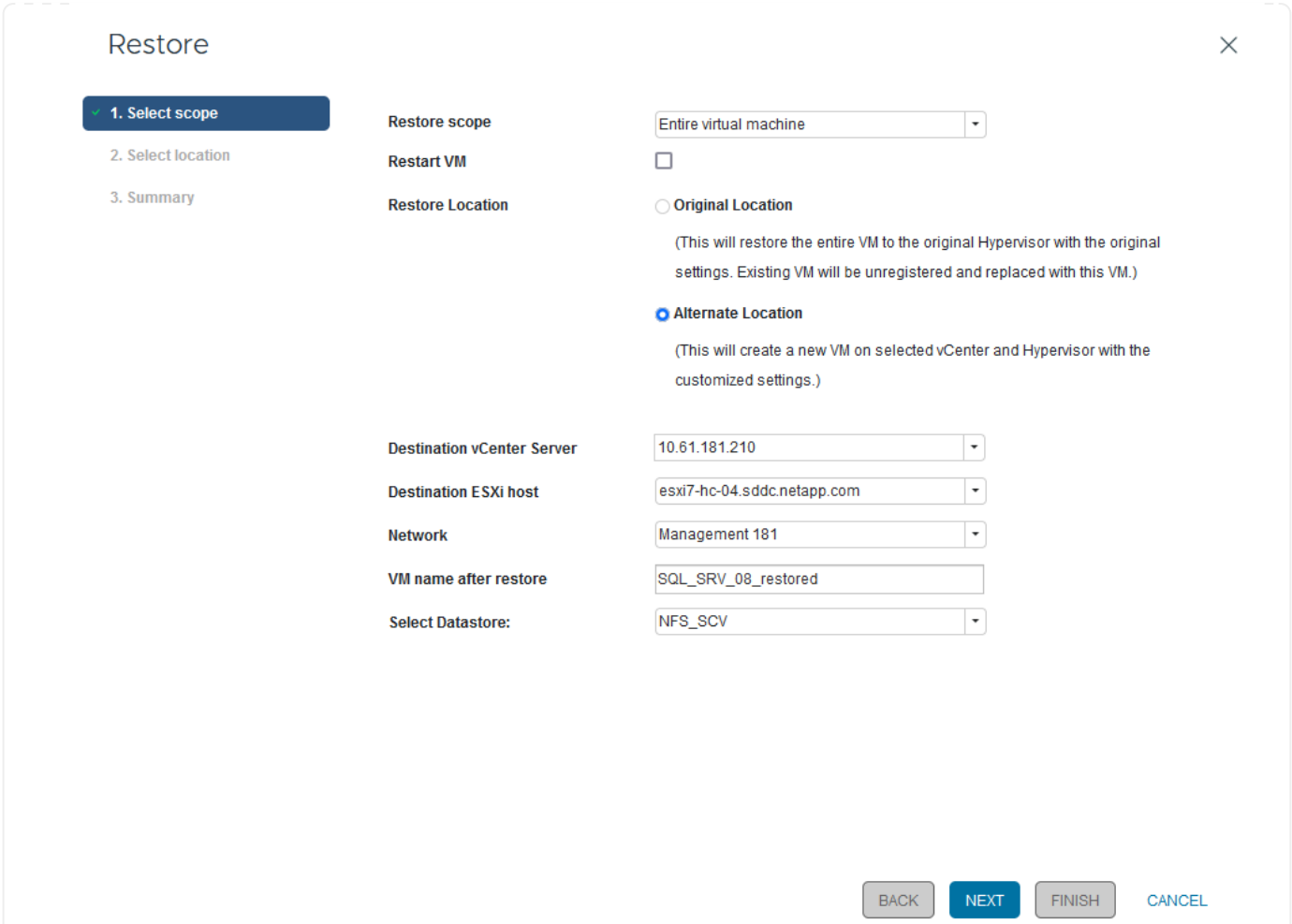
1. Desde el cliente de vCenter, navegue hasta **Inventory > Storage** y haga clic en el almacén de datos que contiene las máquinas virtuales que desea restaurar.
2. Desde la pestaña **Configure**, haga clic en **backups** para acceder a la lista de copias de seguridad disponibles.



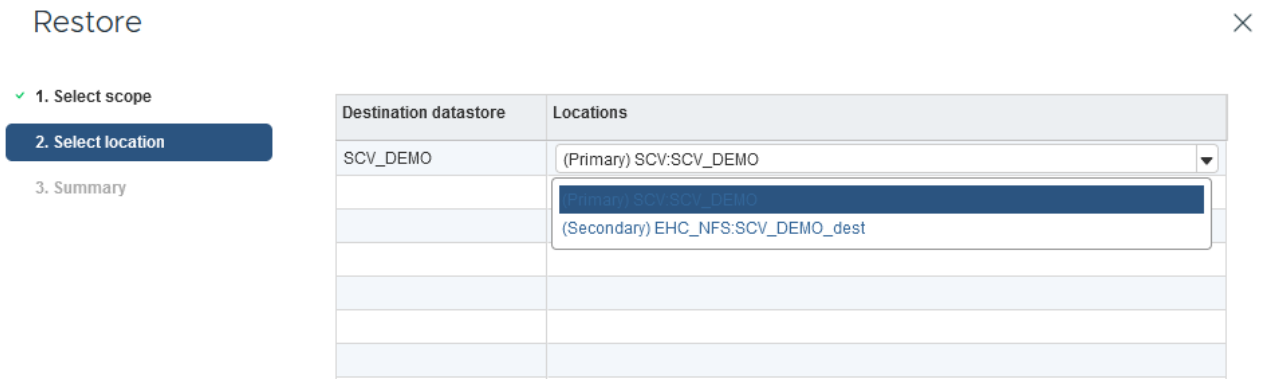
3. Haga clic en un backup para acceder a la lista de máquinas virtuales y, a continuación, seleccione una máquina virtual para restaurar. Haga clic en **Restaurar**.



4. En el asistente Restore, seleccione para restaurar toda la máquina virtual o un VMDK específico. Seleccione para instalar en la ubicación original o la ubicación alternativa, proporcione el nombre de máquina virtual después de la restauración y el almacén de datos de destino. Haga clic en **Siguiente**.



5. Seleccione realizar un backup desde la ubicación del almacenamiento principal o secundario.



6. Por último, revise un resumen del trabajo de copia de seguridad y haga clic en Finalizar para comenzar el proceso de restauración.

Restaurar máquinas virtuales a partir de backup y recuperación de datos de BlueXP para máquinas virtuales

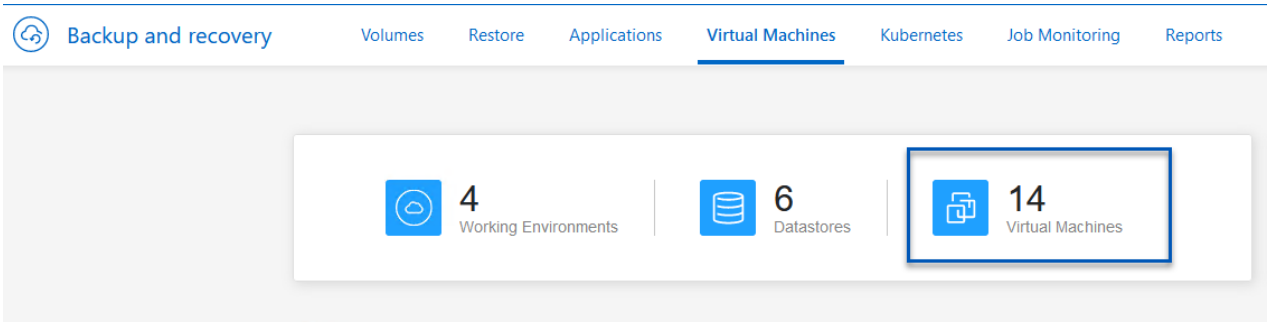
El backup y recuperación de datos de BlueXP para máquinas virtuales permite restaurar las máquinas virtuales a su ubicación original. Para acceder a las funciones de restauración a través de la consola web de BlueXP.

Para obtener más información, consulte "Restaure datos de máquinas virtuales desde el cloud".

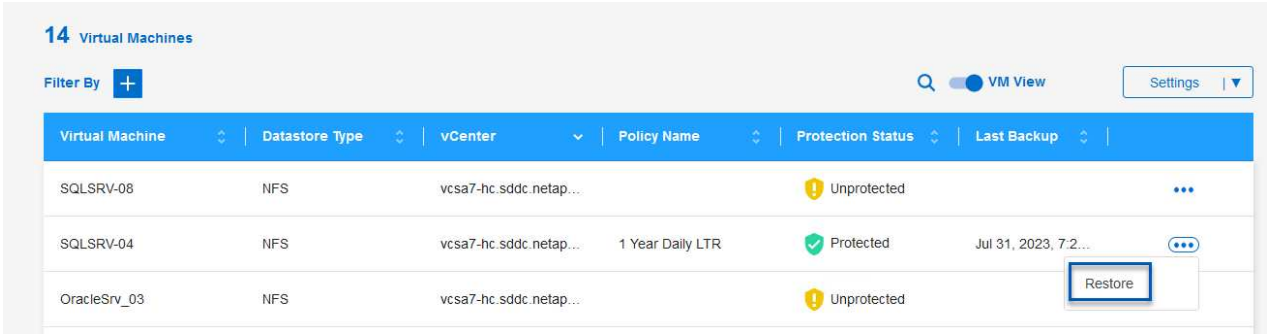
Restaura las máquinas virtuales desde el backup y la recuperación de BlueXP

Para restaurar una máquina virtual a partir de backup y recuperación de BlueXP, lleve a cabo los siguientes pasos.

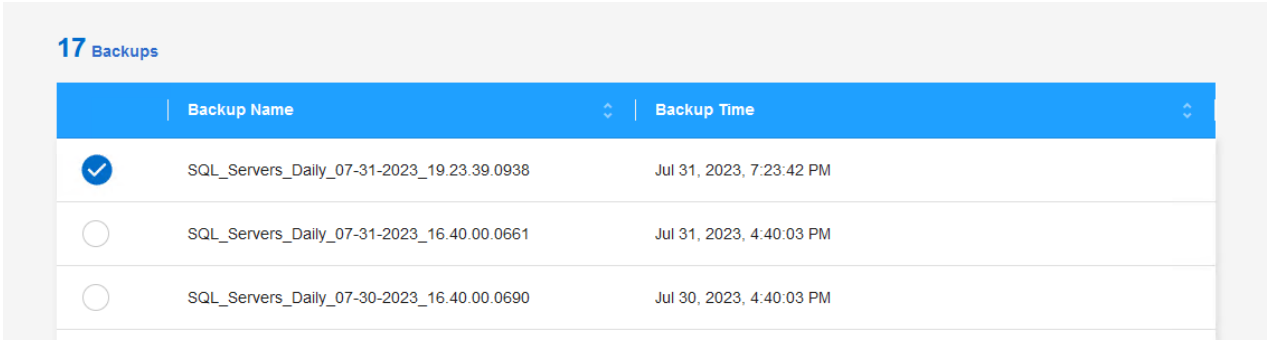
1. Vaya a **Protección > Copia de seguridad y recuperación > Máquinas virtuales** y haga clic en Máquinas virtuales para ver la lista de máquinas virtuales disponibles para restaurar.



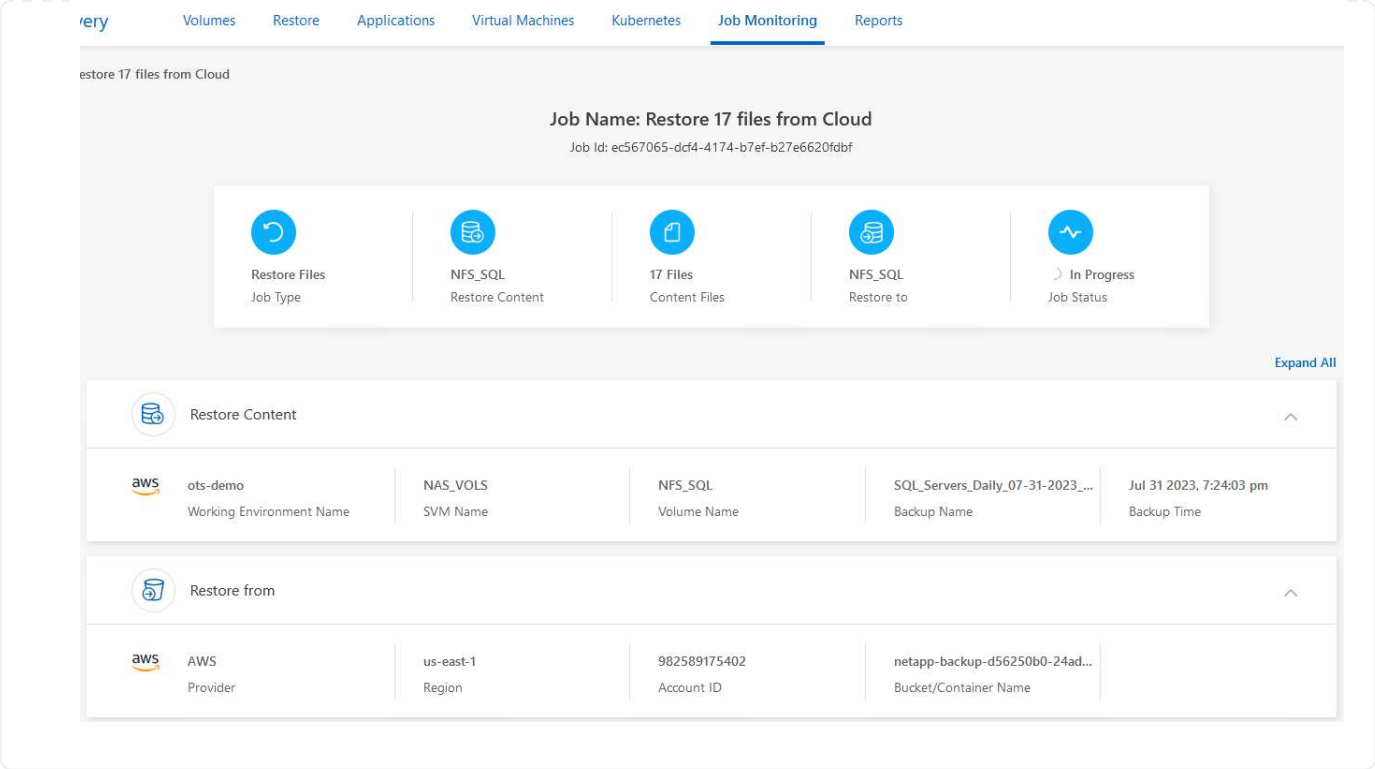
2. Acceda al menú desplegable de configuración de la máquina virtual que se va a restaurar y seleccione



3. Seleccione la copia de seguridad para restaurar y haga clic en **Siguiente**.



4. Revise un resumen del trabajo de copia de seguridad y haga clic en **Restaurar** para iniciar el proceso de restauración.
5. Supervise el progreso del trabajo de restauración desde la pestaña **Job Monitoring**.



Conclusión

La estrategia de backup 3-2-1, cuando se implementa con el complemento SnapCenter para VMware vSphere y backup y recuperación de datos BlueXP para máquinas virtuales, ofrece una solución sólida, fiable y rentable para la protección de datos. Esta estrategia no solo garantiza la redundancia de datos y la accesibilidad, sino que también proporciona la flexibilidad de restaurar datos desde cualquier ubicación y tanto desde sistemas de almacenamiento de ONTAP on-premises como desde el almacenamiento de objetos basado en la nube.

El caso de uso que se presenta en esta documentación se centra en las tecnologías de protección de datos demostradas que destacan la integración entre NetApp, VMware y los principales proveedores de cloud. El complemento de SnapCenter para VMware vSphere se integra sin problemas con VMware vSphere, lo que permite una gestión eficiente y centralizada de las operaciones de protección de datos. Esta integración optimiza los procesos de respaldo y recuperación para máquinas virtuales, lo que permite operaciones sencillas de programación, supervisión y restauración flexibles dentro del ecosistema VMware. El backup y recuperación de datos de BlueXP para máquinas virtuales ofrece un (1) en 3-2-1 al proporcionar backups seguros y aislados de datos de máquinas virtuales al almacenamiento de objetos basado en la nube. 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 obtener más información sobre las tecnologías presentadas en esta solución, consulte la siguiente información adicional.

- "Documentación del plugin de SnapCenter para VMware vSphere"
- "Documentación de BlueXP"

Nube soberana de VMware

Recursos de VMware para Sovereign Cloud

NetApp y VMware Sovereign Cloud

Descripción general de VMware Sovereign Cloud

El concepto de soberanía se está convirtiendo en un componente necesario del cloud computing para muchas entidades que procesan y mantienen datos altamente confidenciales, como los gobiernos nacionales y estatales, y sectores altamente regulados, como las finanzas y la sanidad. Los gobiernos nacionales también buscan expandir la funcionalidad económica digital y reducir la dependencia de empresas multinacionales para sus servicios de cloud.

Iniciativa de cloud soberano de VMware

VMware define un cloud soberano como uno que:

- Protege y libera el valor de los datos críticos (por ejemplo, datos nacionales, corporativos y datos personales) para organizaciones del sector privado y público
- Ofrece una funcionalidad nacional para la economía digital
- Protege los datos con controles de seguridad auditados
- Garantiza el cumplimiento de leyes de privacidad de datos
- Mejora el control de los datos al proporcionar tanto la residencia de datos como la soberanía de datos con un control jurisdiccional total

Asociación con un proveedor de servicios cloud soberano de VMware de confianza

Para garantizar el éxito, las organizaciones deben trabajar con partners en los que confíen y que sean capaces de alojar plataformas de cloud soberano auténticas y autónomas. Los proveedores de nube de VMware reconocidos dentro de la iniciativa VMware Sovereign Cloud se comprometen a diseñar y operar soluciones de nube basadas en arquitecturas modernas y definidas por software que incorporan los principios clave y las mejores prácticas descritas en el marco de VMware Sovereign Cloud.

- **Soberanía de datos y control jurisdiccional** – Todos los datos son residentes y están sujetos al control exclusivo y autoridad del estado nacional donde se recopilaron esos datos. Las operaciones se gestionan completamente dentro de la jurisdicción
- **Acceso e integridad de datos** – La infraestructura en la nube es resiliente y está disponible en al menos dos ubicaciones de centros de datos dentro de la jurisdicción con opciones de conectividad seguras y privadas disponibles.
- **Seguridad y cumplimiento de datos** – Los controles del sistema de gestión de la seguridad de la información están certificados según un estándar global (o regional) reconocido por la industria y se auditan regularmente.
- * Independencia de datos y movilidad *: Soporte para arquitecturas de aplicaciones modernas para evitar el bloqueo en la nube de proveedores y permitir la portabilidad e independencia de las aplicaciones

Para obtener más información de VMware, visite:

- "Descripción general de la nube soberana de VMware"
- "¿Qué es VMware Sovereign Cloud?"
- "Presentamos la nueva iniciativa VMware Sovereign Cloud"
- "Whitepaper técnico de VMware Sovereign Cloud"

Netpp con VMware Sovereign Cloud: Casos de uso

NetApp ofrece compatibilidad con los conceptos de nube soberana de VMware mediante la integración de varias tecnologías de NetApp.

Utilice los siguientes enlaces para obtener más información acerca de las integraciones de la tecnología de NetApp con VMware Sovereign Cloud:

- "NetApp StorageGRID como extensión de almacén de objetos"

NetApp StorageGRID como extensión de almacén de objetos

NetApp ha colaborado con VMware para integrar NetApp StorageGRID en VMware Cloud Director en apoyo de la nube soberana de VMware. Este complemento para VMware Cloud Director permite que los proveedores de servicios utilicen StorageGRID como su oferta de almacenamiento de objetos (independientemente del caso de uso) y permite la gestión de StorageGRID mediante la misma solución multi-tenant de VMware (Cloud Director de VMware) utilizada por los proveedores de servicios para gestionar otras partes de su catálogo de ofertas.

Los partners que ofrecen clouds soberanos de VMware pueden elegir NetApp StorageGRID para que les ayude a gestionar y mantener los entornos de cloud con datos no estructurados. Su compatibilidad universal en su compatibilidad nativa con API estándar del sector, como la API de Amazon S3, ayuda a garantizar una interoperabilidad fluida entre diversos entornos de cloud, así como innovaciones únicas, como la gestión automatizada del ciclo de vida, ayudan a garantizar una protección y un almacenamiento más rentables y una conservación a largo plazo de los datos no estructurados de los clientes.

Integración del cloud soberano de NetApp con los proveedores de Cloud Director clientes con:

- Garantía de que los datos confidenciales, incluidos los metadatos, permanecen bajo control soberano al tiempo que impiden el acceso por parte de autoridades extranjeras que podrían violar las leyes de privacidad de los datos.
- Mayor seguridad y cumplimiento de normativas que protege las aplicaciones y los datos de los vectores de ataque en rápida evolución, a la vez que mantiene un cumplimiento continuo con un local de confianza. de infraestructura, marcos incorporados y expertos locales.
- Infraestructura preparada para el futuro que reacciona con rapidez a los cambios en las normativas de privacidad de datos, las amenazas de seguridad y la política geográfica.
- La capacidad de desbloquear el valor de los datos con análisis y uso compartido de datos seguros para impulsar la innovación sin infringir las leyes de privacidad. La integridad de los datos está protegida para garantizar la precisión de la información.

Si quiere más información sobre la integración de StorageGRID, consulte lo siguiente:

- "Anuncio de NetApp"

Multicloud híbrido de NetApp con cargas de trabajo de contenedores de Red Hat OpenShift

Soluciones de multicloud híbrido de NetApp para cargas de trabajo de contenedores de Red Hat OpenShift

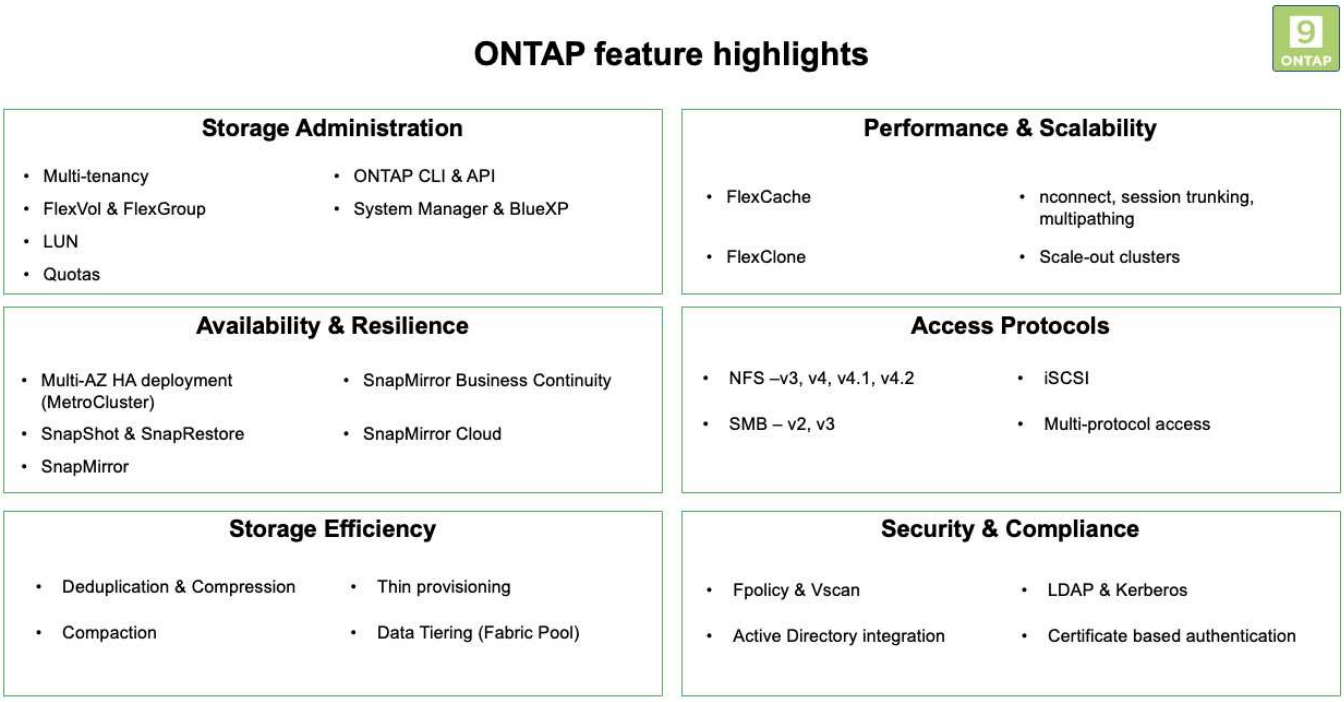
Descripción general

NetApp está viendo un aumento significativo en los clientes que modernizan sus aplicaciones empresariales heredadas y crean nuevas aplicaciones con contenedores y plataformas de orquestación creadas en torno a Kubernetes. Red Hat OpenShift Container Platform es un ejemplo que consideramos adoptado por muchos de nuestros clientes.

A medida que más y más clientes empiezan a adoptar contenedores dentro de sus empresas, NetApp está perfectamente posicionada para poder dar respuesta a las necesidades de almacenamiento persistente de sus aplicaciones con estado y las necesidades de gestión de datos clásicas como la protección de datos, la seguridad de datos y la migración de datos. Sin embargo, estas necesidades se satisfacen utilizando diferentes estrategias, herramientas y métodos.

Las opciones de almacenamiento basado en ONTAP de NetApp que se enumeran a continuación, ofrecen seguridad, protección de datos, fiabilidad y flexibilidad para implementaciones de contenedores y Kubernetes.

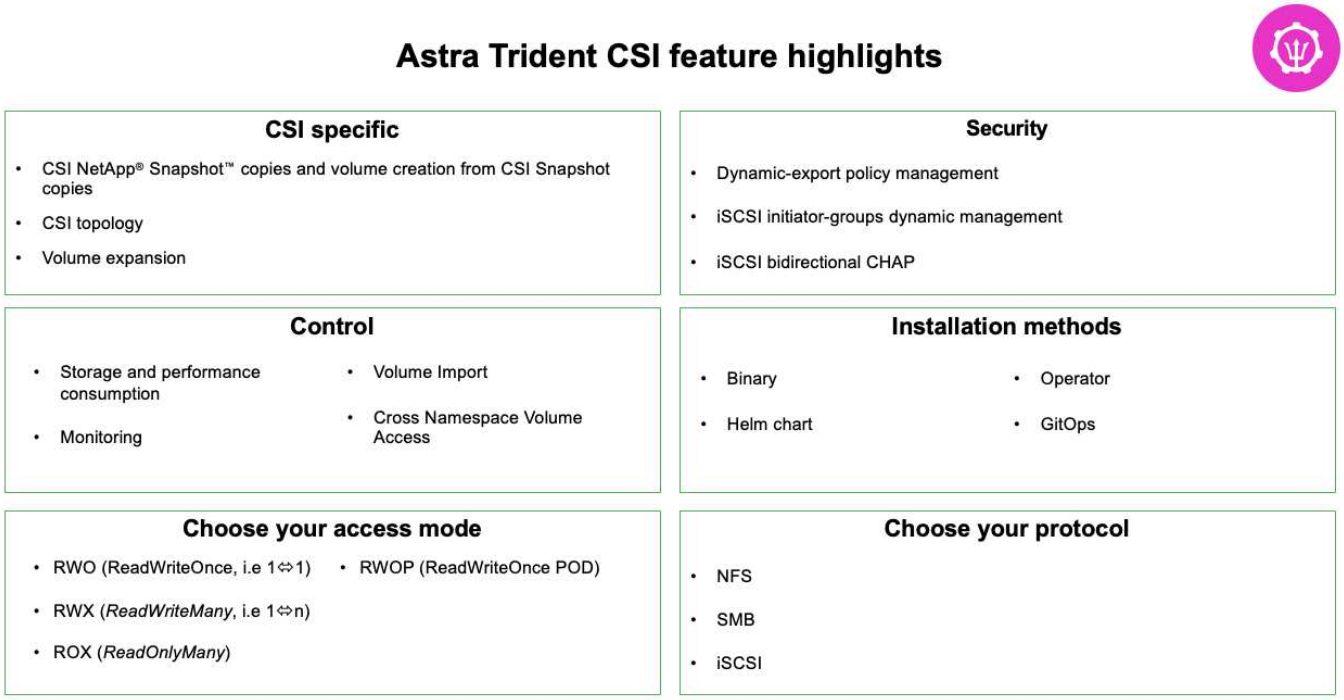
- Almacenamiento autogestionado en las instalaciones:
  - Almacenamiento estructural (FAS) de NetApp, cabinas All Flash FAS (AFF), cabina All SAN (ASA) y ONTAP Select
- Almacenamiento gestionado por el proveedor en las instalaciones:
  - NetApp Keystone proporciona almacenamiento como servicio (STaaS)
- Almacenamiento autogestionado en el cloud:
  - Cloud Volumes ONTAP (CVO) de NetApp proporciona almacenamiento autogestionado en los proveedores a hiperescala
- Almacenamiento en el cloud gestionado por el proveedor:
  - Cloud Volumes Service para Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx para ONTAP de NetApp ofrecen un almacenamiento totalmente gestionado en los proveedores a hiperescala



NetApp BlueXP le permite gestionar todos sus activos de almacenamiento y datos desde una única interfaz o plano de control.

Puedes usar BlueXP para crear y administrar almacenamiento en nube (por ejemplo, Cloud Volumes ONTAP y Azure NetApp Files), para mover, proteger y analizar datos, y para controlar muchos dispositivos de almacenamiento on-premises y en la periferia.

Astra Trident de NetApp es un orquestador de almacenamiento compatible con CSI que permite consumir almacenamiento persistente de forma rápida y sencilla, respaldado por diversas opciones de almacenamiento de NetApp mencionadas anteriormente. Es un software de código abierto que tiene soporte y mantenimiento de NetApp.



Las cargas de trabajo de contenedores vitales para el negocio necesitan más que volúmenes persistentes. Sus requisitos de gestión de datos requieren la protección y la migración de los objetos de aplicaciones kubernetes también.

> 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, PVCs, despliegues, servicios - objetos de configuración personalizados como mapas de configuración y secretos - datos persistentes como copias Snapshot, copias de seguridad, clones - recursos personalizados como CRS y CRD

Astra Control de NetApp, disponible como software totalmente gestionado y autogestionado, proporciona orquestación para una gestión de datos de aplicaciones sólida. Consulte la "Documentación de Astra" Para obtener más información sobre la familia de productos Astra.

Esta documentación de referencia proporciona la validación de la migración y la protección de aplicaciones basadas en contenedores, puestas en marcha en la plataforma de contenedores RedHat OpenShift, mediante Astra Control Center de NetApp. Además, la solución proporciona detalles de alto nivel para la implementación y el uso de Red Hat Advanced Cluster Management (ACM) para la gestión de las plataformas de contenedores. En el documento también se destacan los detalles de la integración del almacenamiento de NetApp con las plataformas de contenedor Red Hat OpenShift mediante el aprovisionador CSI de Astra Trident. Astra Control Center se pone en marcha en el clúster de concentradores y se utiliza para gestionar las aplicaciones de contenedores y su ciclo de vida de almacenamiento persistente. Por último, proporciona una solución de replicación y conmutación al nodo de respaldo y conmutación de retorno tras recuperación para cargas de trabajo de contenedores en clústeres de Red Hat OpenShift gestionados en AWS (ROSA) utilizando Amazon FSx para NetApp ONTAP (FSxN) como almacenamiento persistente.

Propuestas de valor de las soluciones de multicloud híbrido de NetApp para cargas de trabajo de contenedor de Red Hat OpenShift

La mayoría de los clientes no empiezan a crear entornos basados en Kubernetes sin ninguna infraestructura existente. Tal vez sean un centro TECNOLÓGICO tradicional que

ejecuta la mayoría de sus aplicaciones empresariales en máquinas virtuales (en grandes entornos VMware, por ejemplo). A continuación, empiezan a crear pequeños entornos basados en contenedores para satisfacer las necesidades de los equipos de desarrollo de aplicaciones modernos. Estas iniciativas suelen comenzar poco a poco y comienzan a ser más generalizadas a medida que los equipos aprenden estas nuevas tecnologías y habilidades, y comienzan a reconocer los muchos beneficios de adoptarlas. La buena noticia para los clientes es que NetApp puede atender las necesidades de ambos entornos. Este conjunto de soluciones para la multinube híbrida con Red Hat OpenShift capacitará a los clientes de NetApp para adoptar tecnologías y servicios de nube modernos sin tener que actualizar toda su infraestructura y organización. Tanto si las aplicaciones y los datos de los clientes están alojados en las instalaciones, en el cloud, ejecutados en máquinas virtuales o en contenedores, NetApp puede proporcionar gestión, protección, seguridad y portabilidad de datos consistentes. Con estas nuevas soluciones, el mismo valor que NetApp ha proporcionado en entornos de centros de datos on-premises durante décadas estará disponible en todo el horizonte de datos de la empresa, sin necesidad de realizar una inversión significativa para rediseñar la herramienta, adquirir nuevas habilidades o crear nuevos equipos. NetApp se encuentra bien posicionado para ayudar a los clientes a resolver estos retos empresariales, independientemente de la fase de su transición al cloud en la que se encuentren.

Multicloud híbrido de NetApp con Red Hat OpenShift:

- Ofrece a los clientes diseños y prácticas validados que demuestran las mejores formas de gestionar, proteger, proteger y migrar sus datos y aplicaciones al utilizar Red Hat OpenShift con soluciones de almacenamiento basadas en NetApp.
- Presente las mejores prácticas para clientes que ejecuten Red Hat OpenShift con almacenamiento de NetApp en entornos VMware, una infraestructura básica o una combinación de ambas opciones.
- Muestra estrategias y opciones tanto para entornos on-premises como en la nube, así como entornos híbridos donde se utilizan ambas.

Soluciones compatibles del multicloud híbrido de NetApp para cargas de trabajo de contenedor de Red Hat OpenShift

La solución prueba y valida la migración y la protección de datos centralizada con la plataforma de contenedores OpenShift (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp BlueXP y Astra Control Center (ACC) de NetApp.

Para esta solución, NetApp ha probado y validado los siguientes supuestos. La solución se separa en varios escenarios según las siguientes características:

- localmente
- oferta
  - Clústeres de OpenShift autogestionados y almacenamiento autogestionado de NetApp
  - Clústeres de OpenShift gestionados por proveedores y almacenamiento de NetApp gestionado por proveedores

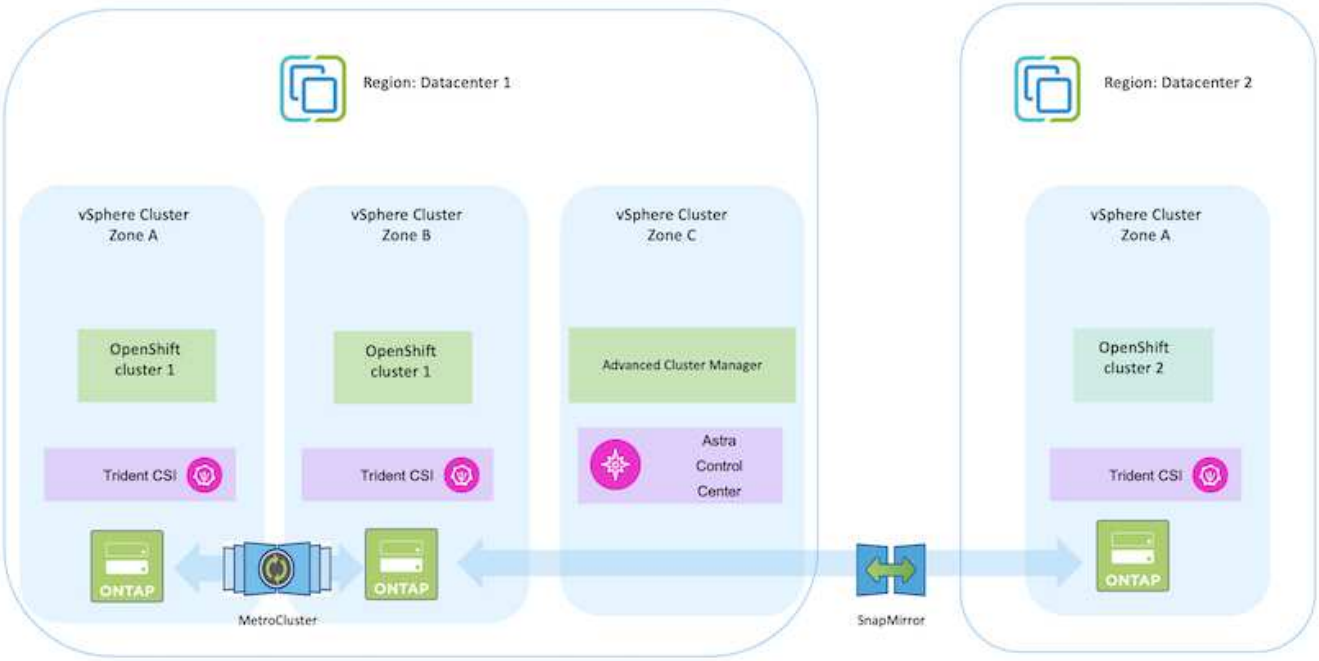
Estaremos construyendo soluciones adicionales y casos de uso en el futuro.

Escenario 1: Protección y migración de datos dentro del entorno local mediante ACC

En las instalaciones: Clústeres OpenShift autogestionados y almacenamiento NetApp autogestionado

- Con ACC, cree copias Snapshot, backups y restauraciones para proteger los datos.
- Con ACC, realice una replicación de SnapMirror de las aplicaciones de contenedor.

Situación 1

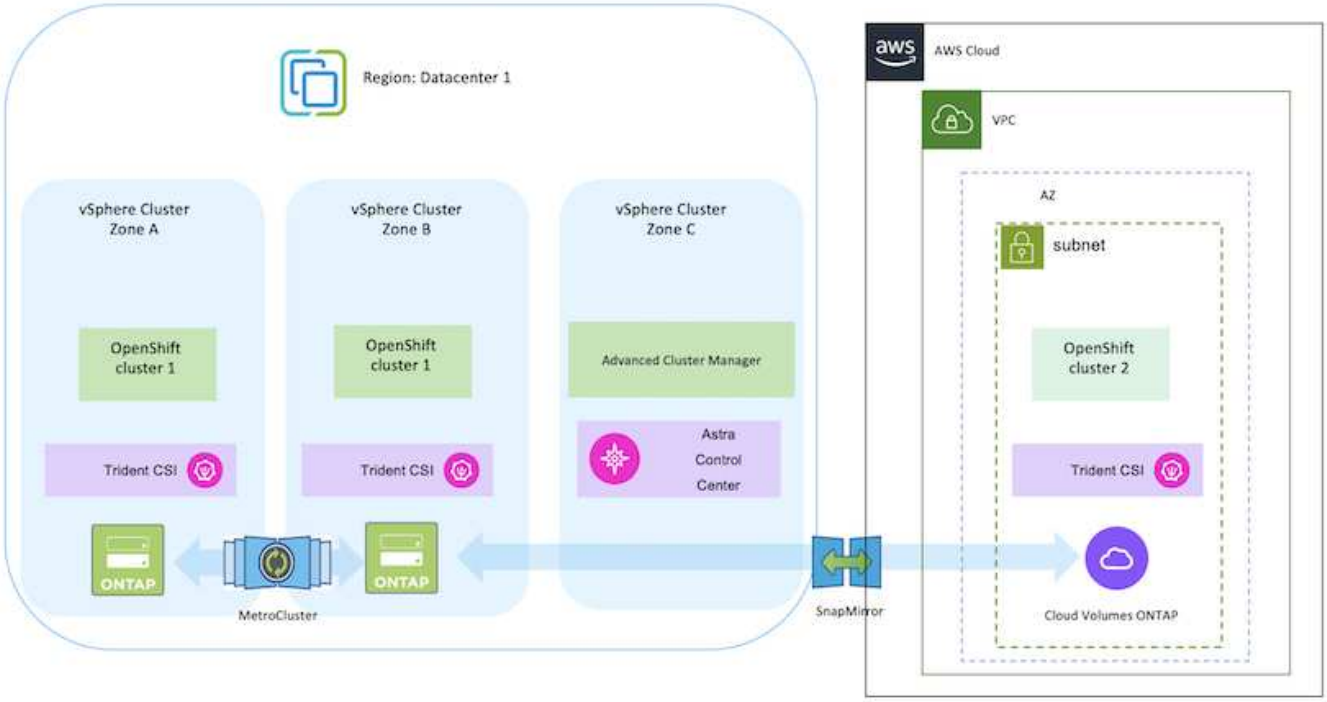


Escenario 2: Protección de datos y migración del entorno local al entorno AWS mediante ACC

En las instalaciones: Clúster OpenShift autogestionado y almacenamiento autogestionado AWS Cloud: Clúster OpenShift autogestionado y almacenamiento autogestionado

- Con ACC, realice backups y restauraciones para la protección de datos.
- Con ACC, realice una replicación de SnapMirror de las aplicaciones de contenedor.

Situación 2

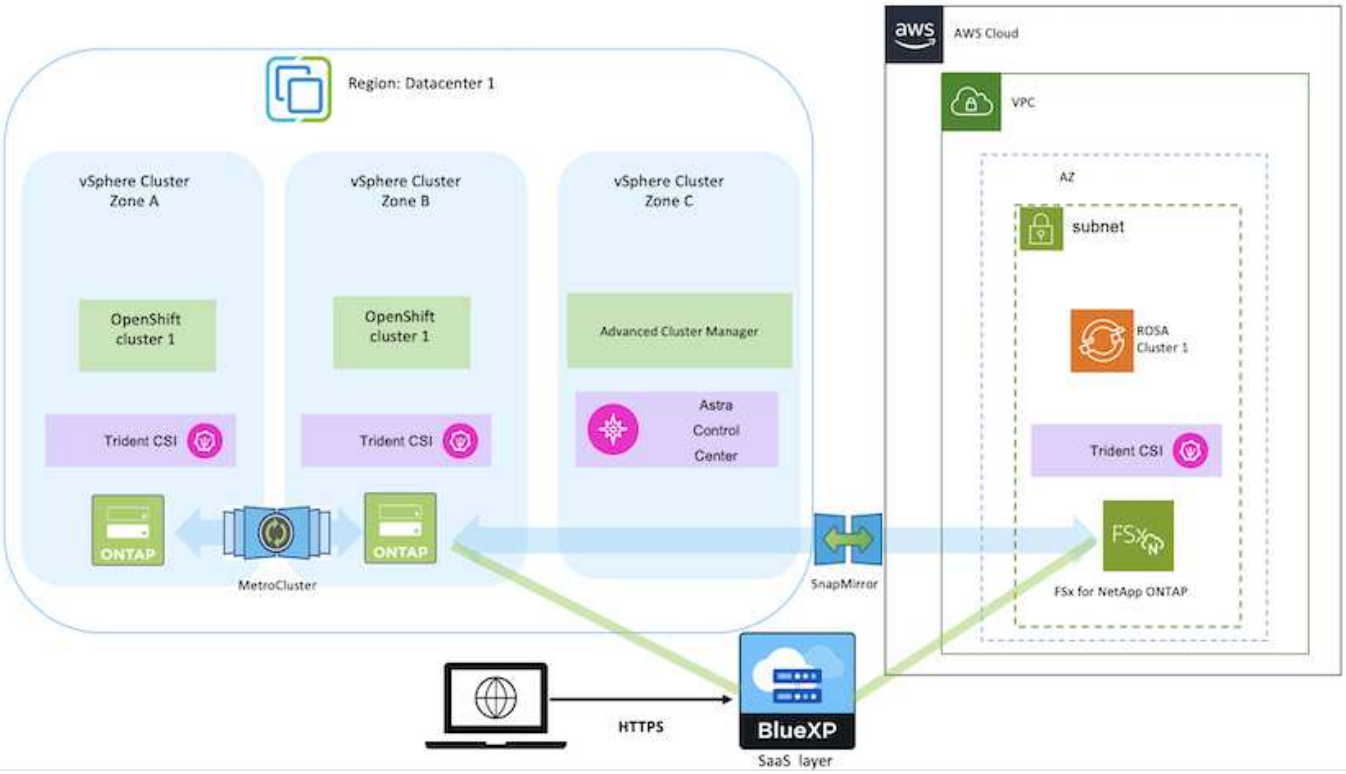


Situación 3: Protección y migración de datos del entorno on-premises a un entorno AWS

En las instalaciones: Clúster OpenShift autogestionado y almacenamiento autogestionado AWS Cloud: Clúster OpenShift (ROSA) gestionado por el proveedor y almacenamiento gestionado por el proveedor (FSxN)

- Con BlueXP, realiza la replicación de volúmenes persistentes (FSxN).
- Con OpenShift GitOps, vuelva a crear los metadatos de la aplicación.

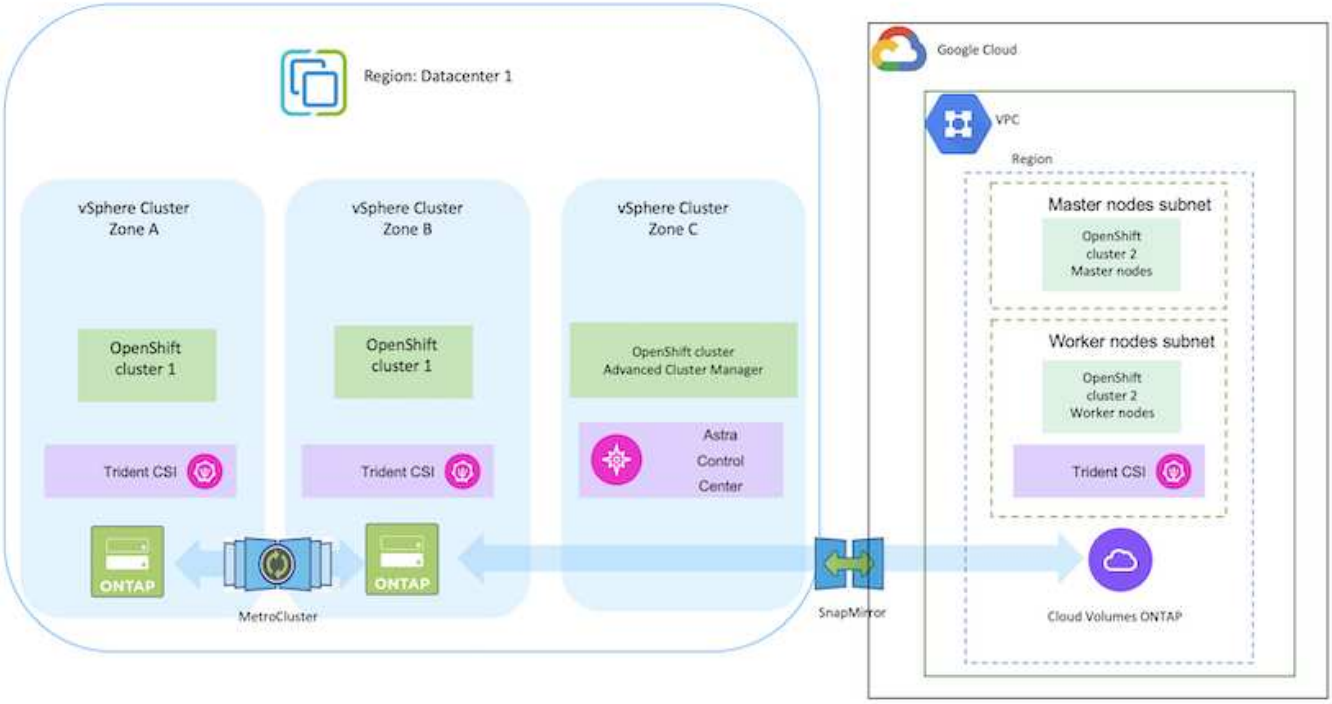
Situación 3



Escenario 4: Protección de datos y migración desde el entorno on-premises a un entorno GCP mediante ACC

En las instalaciones: Clúster OpenShift autogestionado y almacenamiento autogestionado Google Cloud: Clúster OpenShift autogestionado y almacenamiento autogestionado

- Con ACC, realice backups y restauraciones para la protección de datos.
- Con ACC, realice una replicación de SnapMirror de las aplicaciones de contenedor.

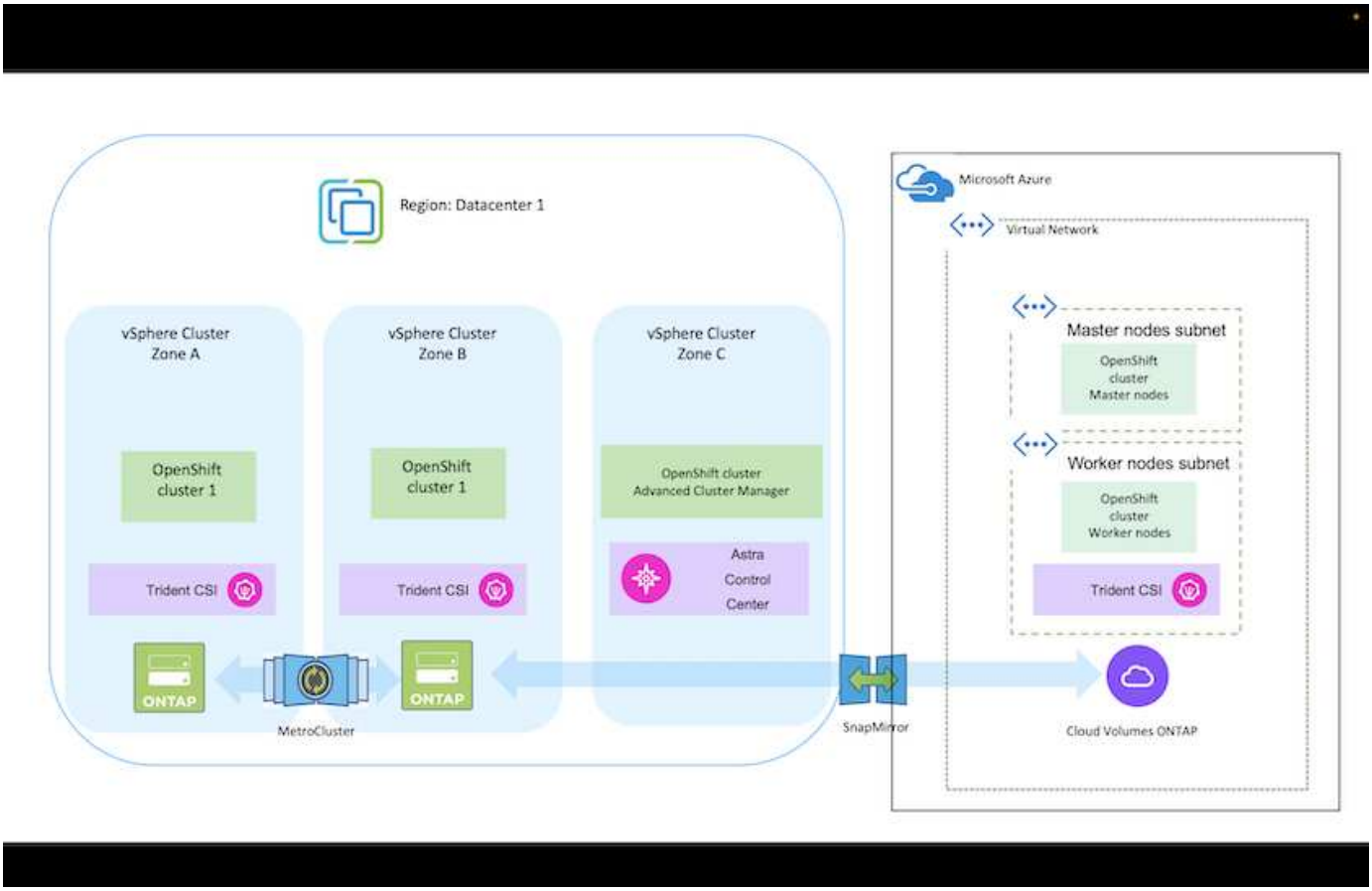


Para obtener información acerca del uso de ONTAP en una configuración de MetroCluster, consulte "aquí".

Escenario 5: Protección de datos y migración del entorno on-premises a un entorno de Azure mediante ACC

En las instalaciones: Clúster OpenShift autogestionado y almacenamiento autogestionado
Azure Cloud: Clúster OpenShift autogestionado y almacenamiento autogestionado

- Con ACC, realice backups y restauraciones para la protección de datos.
- Con ACC, realice una replicación de SnapMirror de las aplicaciones de contenedor.



Para obtener información acerca del uso de 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 Astra Control Center de NetApp.

Los escenarios 1, 2 y 3 de la solución se validaron utilizando las versiones como se muestra en la tabla siguiente:

Componente	Versión
VMware	VSphere Client versión 8.0.0.10200 VMware ESXi, 8,0.0, 20842819
Hub Cluster	OpenShift 4.11.34
Clusters de origen y destino	OpenShift 4.12.9 en las instalaciones y en AWS
Astra Trident de NetApp	Trident Server y Client 23.04.0
Centro de control de Astra de NetApp	ACC 22.11.0-82
ONTAP DE NETAPP	ONTAP 9.12.1
AWS FSx para ONTAP de NetApp	Zona de acceso única

El escenario 4 de la solución se validó usando las versiones como se muestra en la tabla siguiente:

Componente	Versión
VMware	VSphere Client versión 8.0.2.00000 VMware ESXi, 8,0.2, 22380479
Hub Cluster	OpenShift 4.13.13
Clusters de origen y destino	OpenShift 4.13.12 En las instalaciones y en Google Cloud
Astra Trident de NetApp	Trident Server y Client 23.07.0
Centro de control de Astra de NetApp	ACC 23.07.0-25
ONTAP DE NETAPP	ONTAP 9.12.1
Cloud Volumes ONTAP	Un espacio de disponibilidad, nodo único, 9.14.0

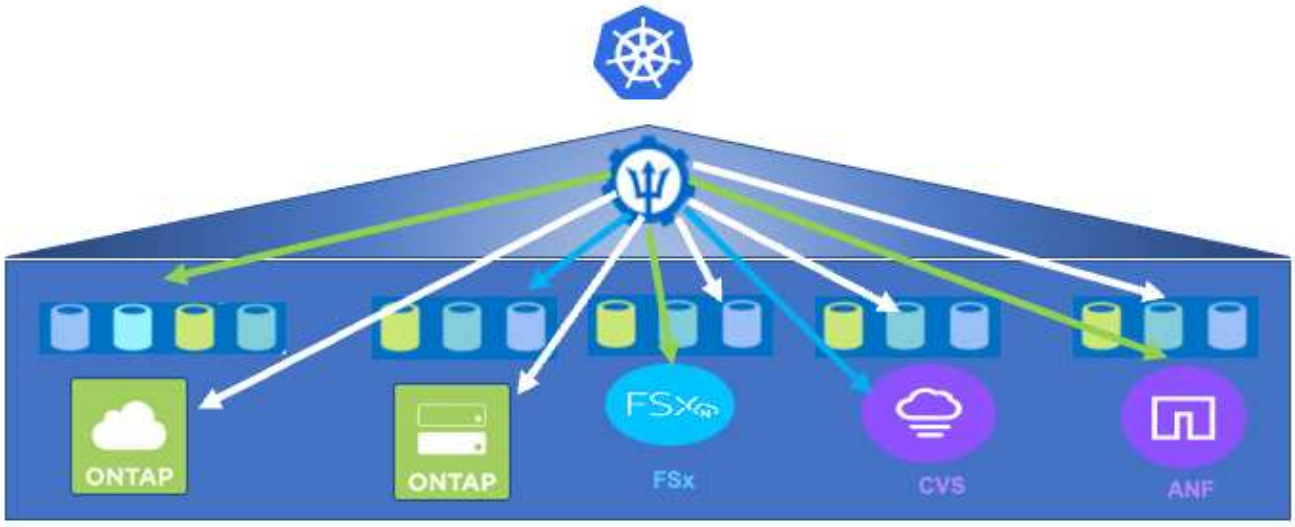
El escenario 5 de la solución se validó usando las versiones como se muestra en la tabla siguiente:

Componente	Versión
VMware	VSphere Client versión 8.0.2.00000 VMware ESXi, 8,0.2, 22380479
Clusters de origen y destino	OpenShift 4.13.25 On-premises y en Azure
Astra Trident de NetApp	Trident Server y Client y Astra Control Provisioning 23.10.0
Centro de control de Astra de NetApp	ACC 23,10
ONTAP DE NETAPP	ONTAP 9.12.1
Cloud Volumes ONTAP	Un espacio de disponibilidad, nodo único, 9.14.0

Integraciones de almacenamiento de NetApp compatibles con contenedores de Red Hat Open Shift

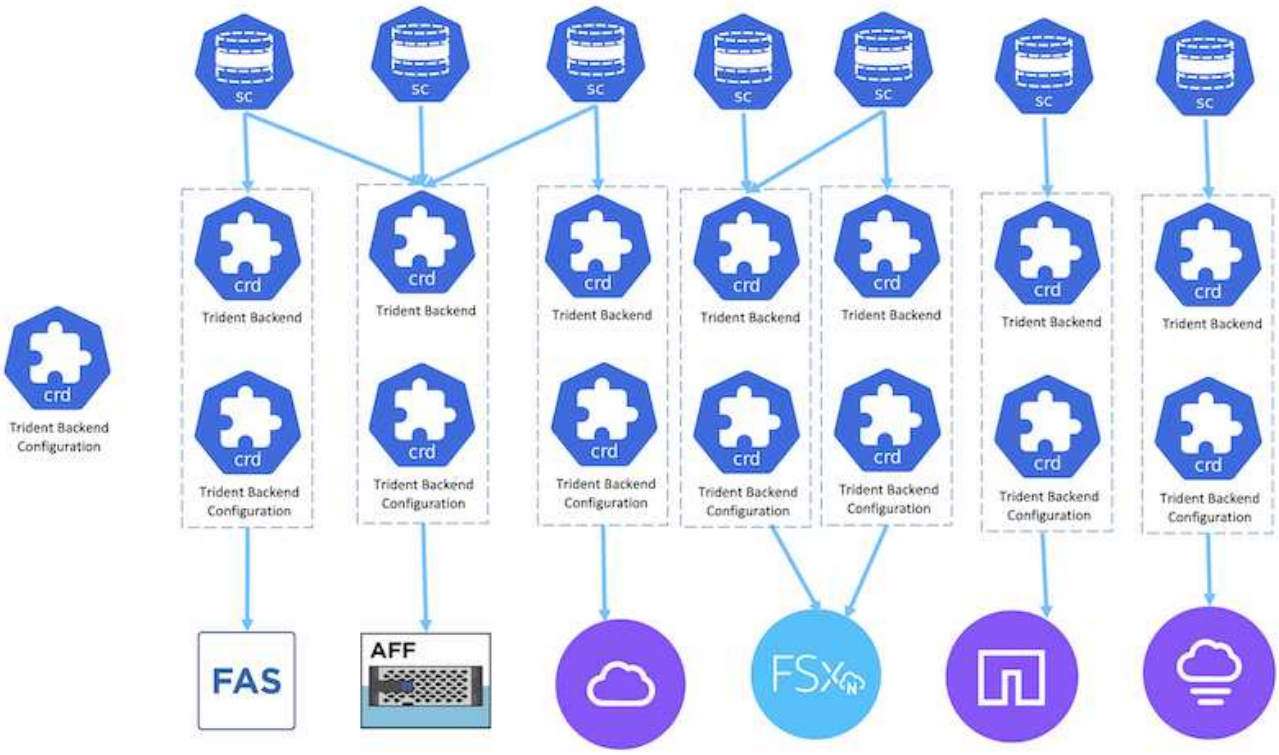
Tanto si los contenedores de Red Hat Open Shift se ejecutan en VMware como en proveedores a hiperescala, Astra Trident de NetApp puede utilizarse como aprovisionador de CSI para los distintos tipos de almacenamiento back-end de NetApp compatibles.

El siguiente diagrama muestra los diversos sistemas de almacenamiento back-end de NetApp que se pueden integrar con clústeres OpenShift utilizando Astra Trident de NetApp.

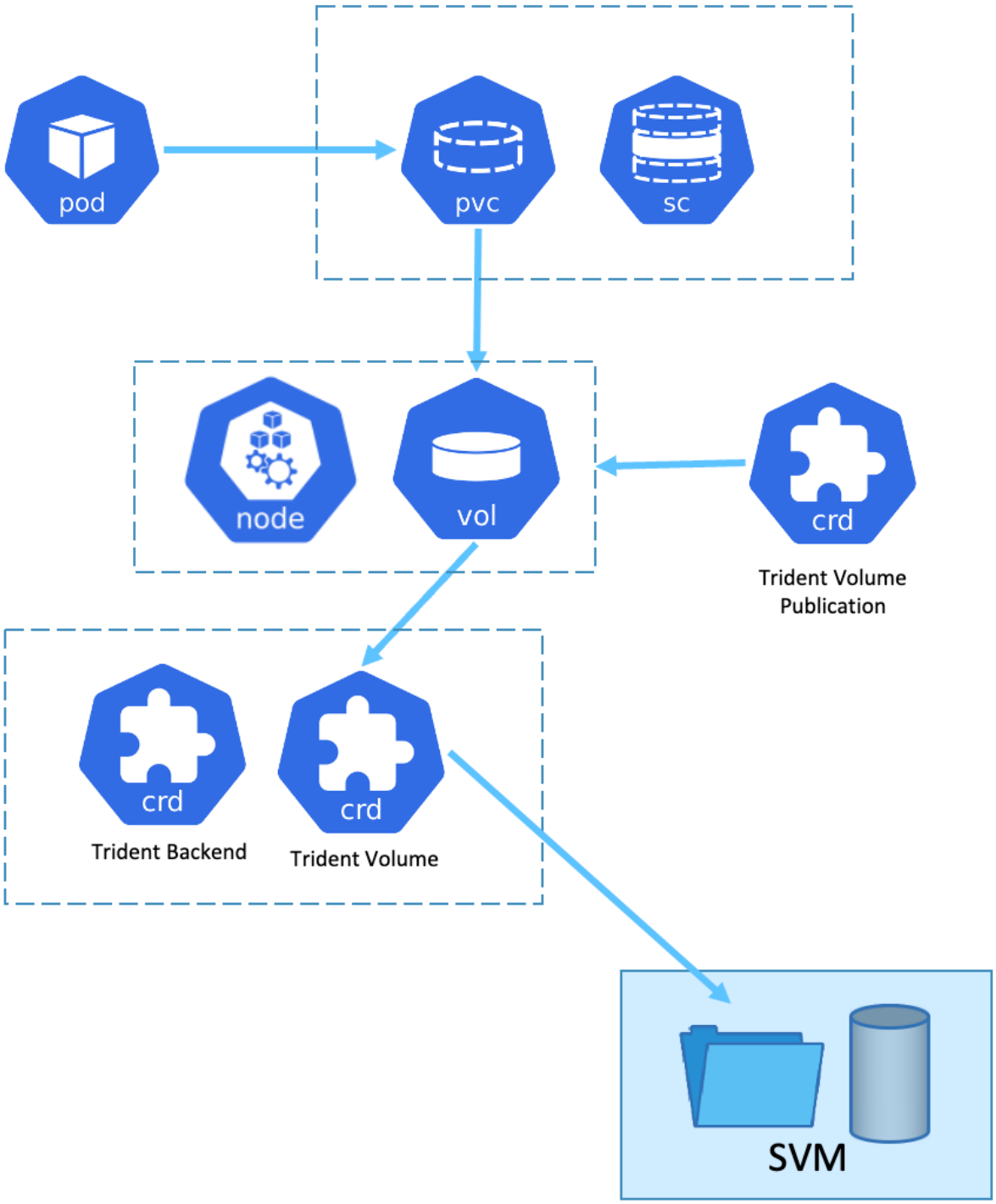


Storage Virtual Machine (SVM) de ONTAP proporciona multi-tenancy seguro. Un único clúster de OpenShift se puede conectar a una única SVM o a varias SVM o incluso a varios clústeres de ONTAP. La clase de almacenamiento filtra el almacenamiento de backend en función de parámetros o por etiquetas. Los administradores de almacenamiento definen los parámetros para conectarse al sistema de almacenamiento mediante la configuración de back-end trident. Al establecer correctamente la conexión, crea el backend trident y rellena la información que la clase de almacenamiento puede filtrar.

A continuación se muestra la relación entre storageclass y backend.



El propietario de la aplicación solicita un volumen persistente mediante la clase de almacenamiento. La clase de almacenamiento filtra el almacenamiento back-end. A continuación se muestra la relación entre el pod y el almacenamiento back-end.



Opciones de la interfaz de almacenamiento de contenedores (CSI)

En entornos vSphere, los clientes pueden elegir el controlador CSI de VMware o Astra Trident CSI para integrarse 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 modos de acceso RWX con ONTAP, las aplicaciones deben utilizar Trident CSI si se requiere el modo RWX. Con las puestas en marcha basadas en FC, es preferible VMware CSI, y SnapMirror Business Continuity (SMBC) proporciona alta disponibilidad a nivel de zona.

Compatibilidad con VMware CSI

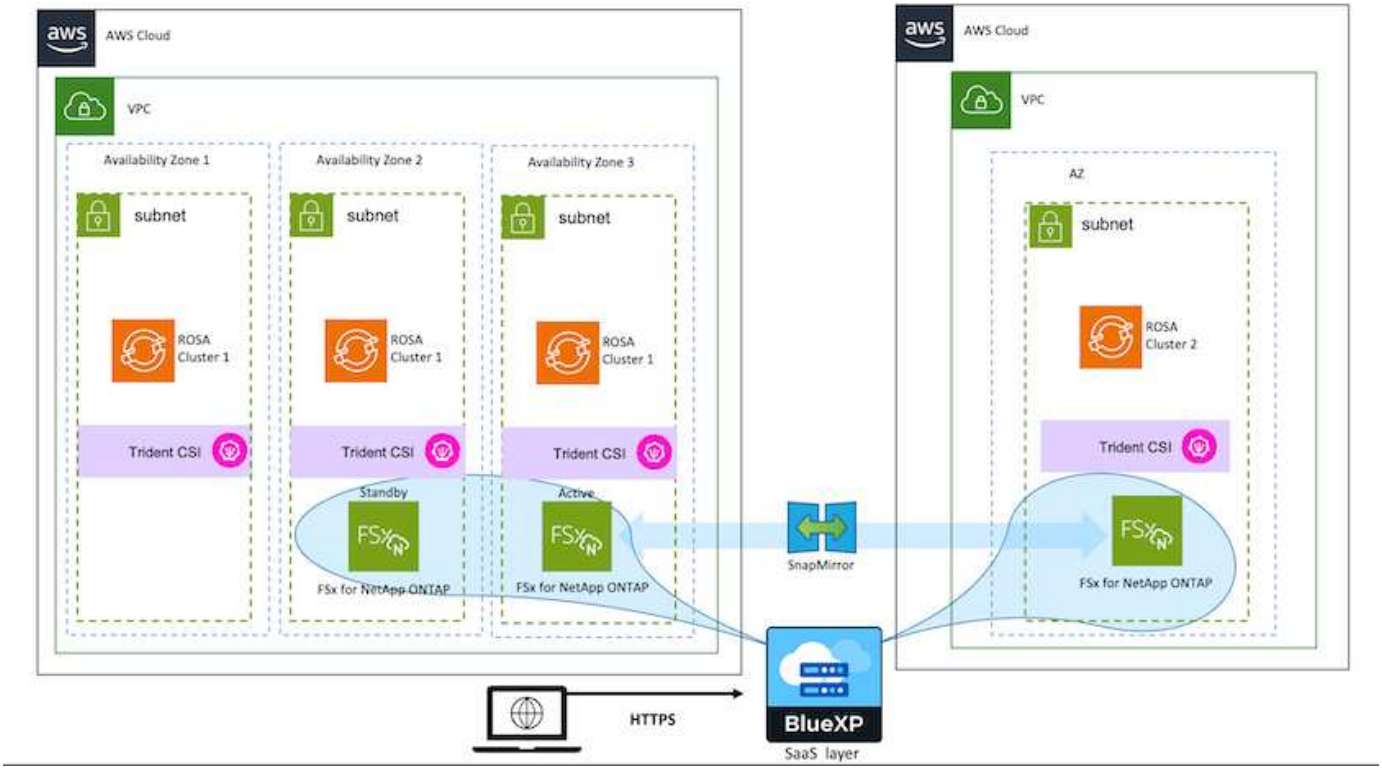
- Almacenes de datos basados en bloques principales (FC, FCoE, iSCSI, NVMeoF)
- Almacenes de datos principales basados en archivos (NFS v3, v4)
- Almacenes de datos de VVol (bloque y archivo)

Trident cuenta con los siguientes controladores para admitir ONTAP

- ontap-san (volumen dedicado)
- economía ontap-san (volumen compartido)
- ontap-nas (volumen dedicado)
- economía ontap-nas (volumen compartido)
- ontap-nas-flexgroup (volumen a gran escala dedicado)

Para VMware CSI y Astra Trident CSI, ONTAP admite nconnect, trunking de sesión, kerberos, etc. para NFS y multivía, autenticación CHAP, etc. para los protocolos de bloque.

En AWS, FSx para ONTAP de NetApp (FSxN) puede ponerse en marcha en una zona de disponibilidad única (AZ) o en varias zonas. Para cargas de trabajo de producción que requieren alta disponibilidad, multi-AZ ofrece tolerancia a fallos de nivel de zona y ofrece una mejor caché de lectura NVMe que una única zona de disponibilidad. Para obtener más información, consulte "Directrices de rendimiento de AWS".
Para ahorrar costes en el sitio de recuperación ante desastres, se puede utilizar un único AZ FSx ONTAP.



Para obtener más información sobre el número de SVM que admite FSx ONTAP, consulte "Gestión de la máquina virtual de almacenamiento FSx ONTAP"

Soluciones de multicloud híbrido de NetApp para cargas de trabajo de contenedores de Red Hat OpenShift

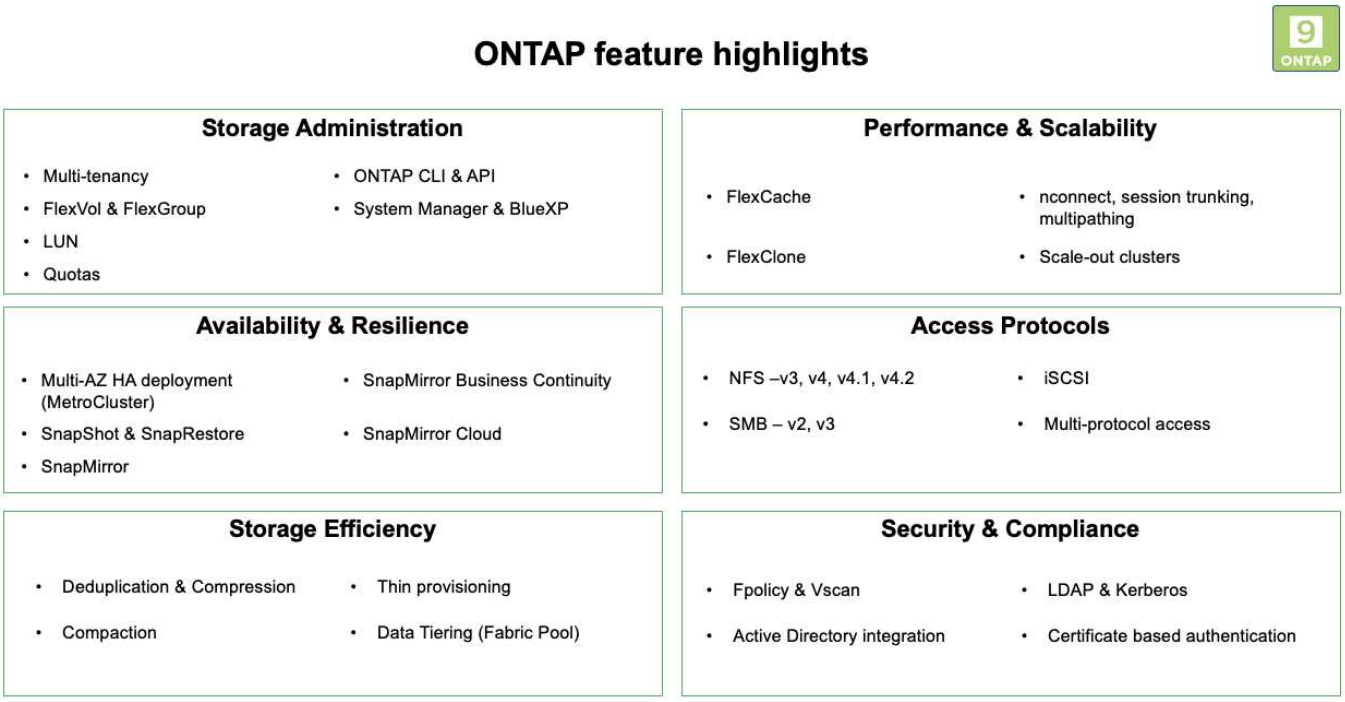
Descripción general

NetApp está viendo un aumento significativo en los clientes que modernizan sus aplicaciones empresariales heredadas y crean nuevas aplicaciones con contenedores y plataformas de orquestación creadas en torno a Kubernetes. Red Hat OpenShift Container Platform es un ejemplo que consideramos adoptado por muchos de nuestros clientes.

A medida que más y más clientes empiezan a adoptar contenedores dentro de sus empresas, NetApp está perfectamente posicionada para poder dar respuesta a las necesidades de almacenamiento persistente de sus aplicaciones con estado y las necesidades de gestión de datos clásicas como la protección de datos, la seguridad de datos y la migración de datos. Sin embargo, estas necesidades se satisfacen utilizando diferentes estrategias, herramientas y métodos.

Las opciones de almacenamiento basado en ONTAP de NetApp que se enumeran a continuación, ofrecen seguridad, protección de datos, fiabilidad y flexibilidad para implementaciones de contenedores y Kubernetes.

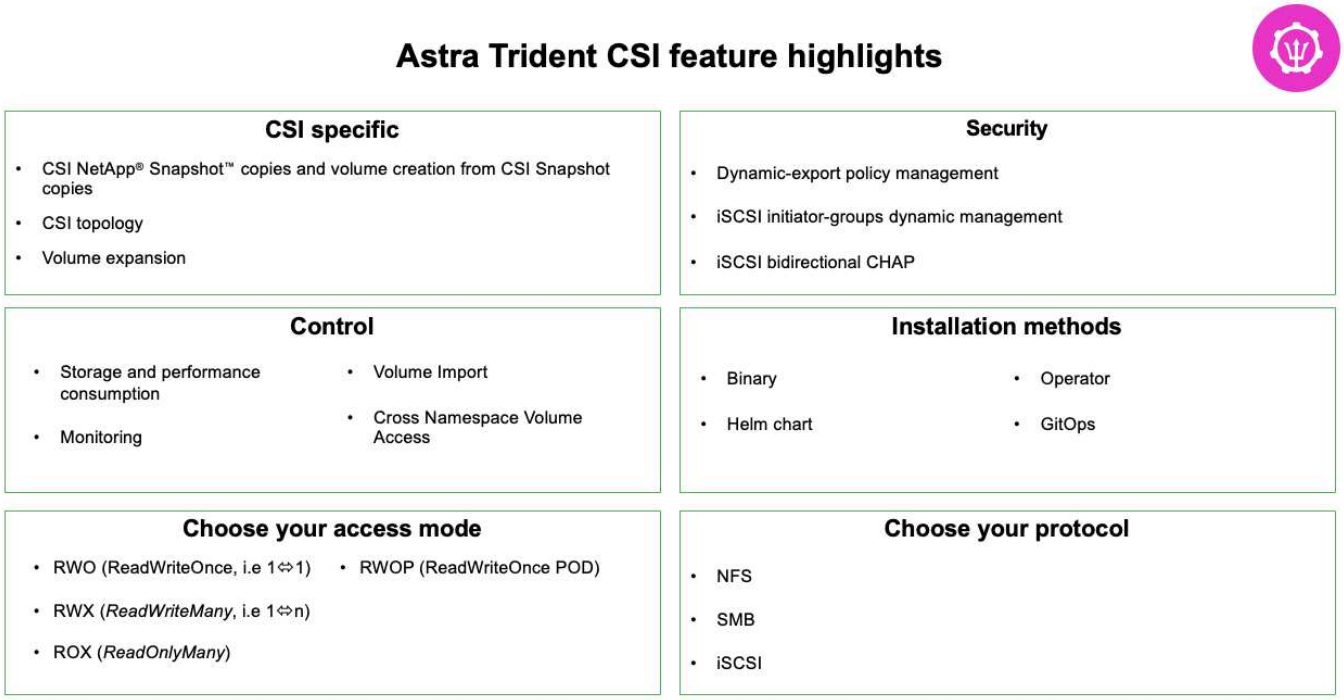
- Almacenamiento autogestionado en las instalaciones:
  - Almacenamiento estructural (FAS) de NetApp, cabinas All Flash FAS (AFF), cabina All SAN (ASA) y ONTAP Select
- Almacenamiento gestionado por el proveedor en las instalaciones:
  - NetApp Keystone proporciona almacenamiento como servicio (STaaS)
- Almacenamiento autogestionado en el cloud:
  - Cloud Volumes ONTAP (CVO) de NetApp proporciona almacenamiento autogestionado en los proveedores a hiperescala
- Almacenamiento en el cloud gestionado por el proveedor:
  - Cloud Volumes Service para Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx para ONTAP de NetApp ofrecen un almacenamiento totalmente gestionado en los proveedores a hiperescala



NetApp BlueXP le permite gestionar todos sus activos de almacenamiento y datos desde una única interfaz o plano de control.

Puedes usar BlueXP para crear y administrar almacenamiento en nube (por ejemplo, Cloud Volumes ONTAP y Azure NetApp Files), para mover, proteger y analizar datos, y para controlar muchos dispositivos de almacenamiento on-premises y en la periferia.

Astra Trident de NetApp es un orquestador de almacenamiento compatible con CSI que permite consumir almacenamiento persistente de forma rápida y sencilla, respaldado por diversas opciones de almacenamiento de NetApp mencionadas anteriormente. Es un software de código abierto que tiene soporte y mantenimiento de NetApp.



Las cargas de trabajo de contenedores vitales para el negocio necesitan más que volúmenes persistentes. Sus requisitos de gestión de datos requieren la protección y la migración de los objetos de aplicaciones kubernetes también.

> 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, PVCs, despliegues, servicios - objetos de configuración personalizados como mapas de configuración y secretos - datos persistentes como copias Snapshot, copias de seguridad, clones - recursos personalizados como CRS y CRD

Astra Control de NetApp, disponible como software totalmente gestionado y autogestionado, proporciona orquestación para una gestión de datos de aplicaciones sólida. Consulte la "Documentación de Astra" Para obtener más información sobre la familia de productos Astra.

Esta documentación de referencia proporciona la validación de la migración y la protección de aplicaciones basadas en contenedores, puestas en marcha en la plataforma de contenedores RedHat OpenShift, mediante Astra Control Center de NetApp. Además, la solución proporciona detalles de alto nivel para la implementación y el uso de Red Hat Advanced Cluster Management (ACM) para la gestión de las plataformas de contenedores. En el documento también se destacan los detalles de la integración del almacenamiento de NetApp con las plataformas de contenedor Red Hat OpenShift mediante el aprovisionador CSI de Astra Trident. Astra Control Center se pone en marcha en el clúster de concentradores y se utiliza para gestionar las aplicaciones de contenedores y su ciclo de vida de almacenamiento persistente. Por último, proporciona una solución de replicación y conmutación al nodo de respaldo y conmutación de retorno tras recuperación para cargas de trabajo de contenedores en clústeres de Red Hat OpenShift gestionados en AWS (ROSA) utilizando Amazon FSx para NetApp ONTAP (FSxN) como almacenamiento persistente.

Solución de NetApp con cargas de trabajo de la plataforma de contenedores Red Hat OpenShift en VMware

Si los clientes necesitan ejecutar sus aplicaciones modernas en contenedores en una infraestructura en sus centros de datos privados, pueden hacerlo. Deben planificar e

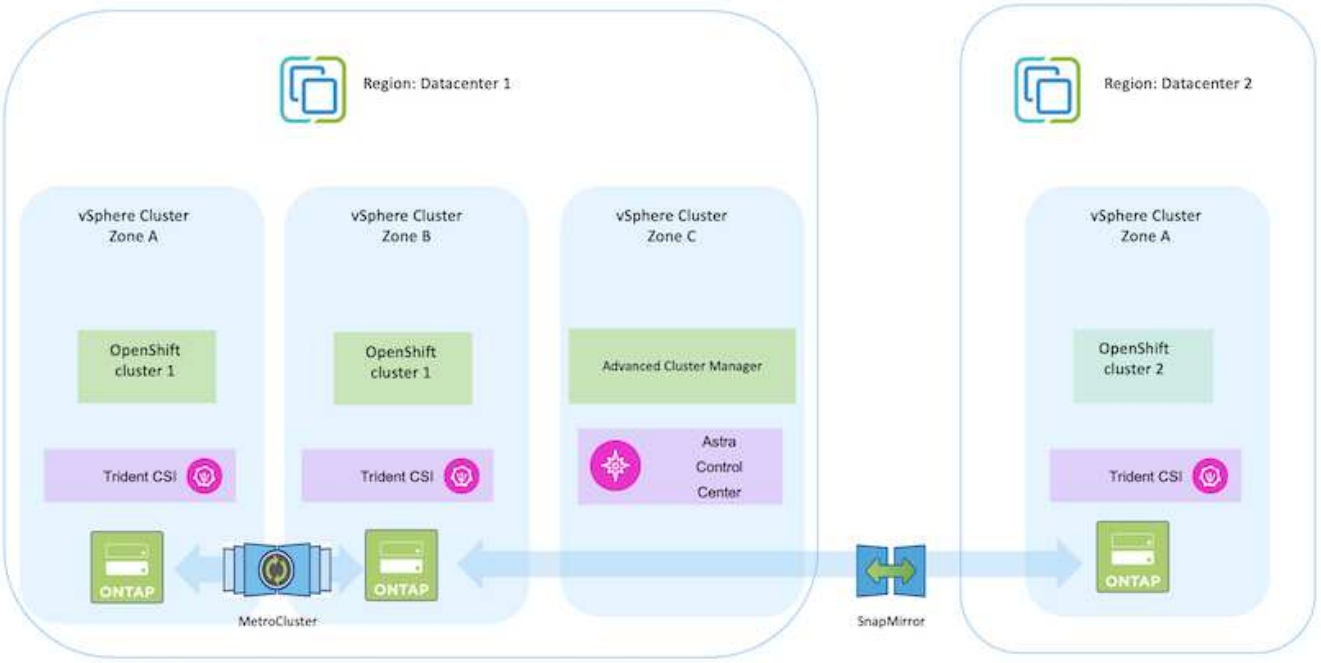
implementar Red Hat OpenShift Container Platform (OCP) para un entorno preparado para la producción con éxito para implementar sus cargas de trabajo de contenedores. Sus clústeres OCP se pueden poner en marcha en VMware o bare metal.

El almacenamiento ONTAP de NetApp ofrece protección de datos, fiabilidad y flexibilidad para puestas en marcha de contenedores. Astra Trident sirve como aprovisionador de almacenamiento dinámico para consumir almacenamiento ONTAP persistente para las aplicaciones con estado de los clientes. Se puede usar Astra Control Center para orquestar los muchos requisitos de gestión de datos de aplicaciones con estado, como la protección de datos, la migración y la continuidad del negocio.

Con VMware vSphere, las herramientas de ONTAP de NetApp proporcionan un complemento para vCenter que se puede utilizar para aprovisionar almacenes de datos. Aplique etiquetas y utilícelas con OpenShift para almacenar la configuración y los datos del nodo. El almacenamiento basado en NVMe proporciona una latencia menor y un alto rendimiento.

Esta solución proporciona detalles para la protección de datos y migración de cargas de trabajo de contenedores mediante Astra Control Center. Para esta solución, las cargas de trabajo de contenedores se ponen en marcha en clústeres de Red Hat OpenShift en vSphere dentro del entorno en las instalaciones. NOTA: Proporcionaremos una solución para cargas de trabajo de contenedores en clústeres OpenShift en bare metal en el futuro.

Solución de protección de datos y migración para cargas de trabajo de contenedores de OpenShift con Astra Control Center



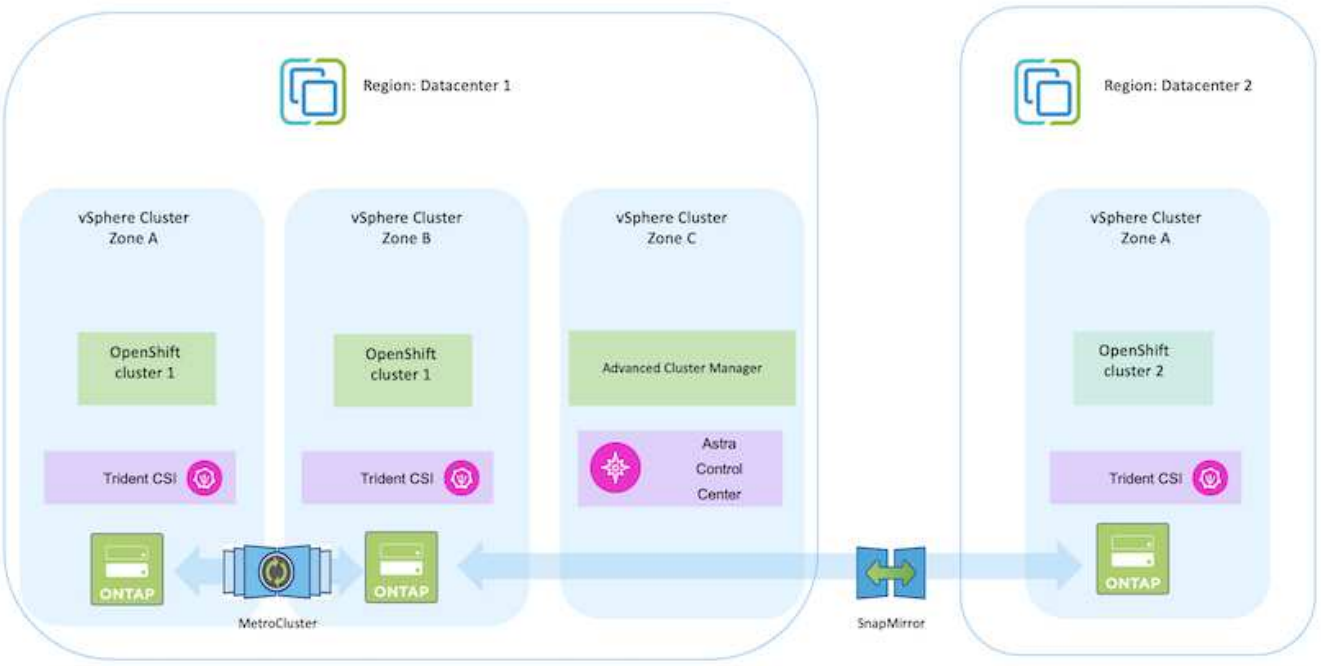
Implemente y configure la plataforma Red Hat OpenShift Container en VMware

En esta sección se describe un flujo de trabajo de alto nivel sobre cómo configurar y gestionar clústeres de OpenShift y administrar aplicaciones con estado en ellos. Muestra el uso de las cabinas de almacenamiento ONTAP de NetApp con la ayuda de Astra Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso

de Astra Control Center para realizar actividades de protección de datos y migración para las aplicaciones con estado.

Existen varias formas de implementar los clústeres de plataformas de contenedores de Red Hat OpenShift. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

A continuación encontrará un diagrama que muestra los clústeres implementados en VMware en un centro de datos.



El proceso de configuración puede dividirse en los siguientes pasos:

Desplegar y configurar una VM CentOS

- Se pone en marcha en el entorno VMware vSphere.
- Esta máquina virtual se utiliza para poner en marcha algunos componentes como Astra Trident de NetApp y Astra Control Center de NetApp para la solución.
- Se configura un usuario raíz en esta máquina virtual durante la instalación.

Ponga en marcha y configure un clúster de plataforma de contenedores de OpenShift en VMware vSphere (clúster de Hub)

Consulte las instrucciones del "Puesta en marcha asistida" Método para desplegar un cluster de OCP.

Recuerde lo siguiente: - Crear ssh clave pública y privada para proporcionar al instalador. Estas claves se utilizarán para conectarse a los nodos maestro y trabajador si es necesario. - Descargar el programa de instalación desde el instalador asistido. Este programa se utiliza para arrancar las máquinas virtuales que cree en el entorno de VMware vSphere para los nodos principal y de trabajo. - Las máquinas virtuales deben tener el requisito mínimo de CPU, memoria y disco duro. (Consulte los comandos de creación de la máquina virtual en "este" Para los nodos maestro y trabajador que proporcionan esta información) - El diskUUID debe estar activado en todas las máquinas virtuales. - Crear un mínimo de 3 nodos para el maestro y 3 nodos para el trabajador. - Una vez que sean descubiertos por el instalador, active el botón de conmutación de integración de VMware vSphere.

Instale Advanced Cluster Management en el cluster Hub

Esto se instala mediante el operador de gestión de clúster avanzado del cluster del hub. Consulte las instrucciones "aquí".

Instale un registro interno de Red Hat Quay en el cluster de hub.

- Se necesita un registro interno para insertar la imagen de Astra. Se instala un registro interno de muelle mediante el operador en el clúster del concentrador.
- Consulte las instrucciones "aquí"

Instalar dos clusters OCP adicionales (origen y destino)

- Los clusters adicionales se pueden desplegar mediante ACM en el cluster del hub.
- Consulte las instrucciones "aquí".

Configurar el almacenamiento ONTAP de NetApp

- Instale un clúster de ONTAP con conectividad a las máquinas virtuales de OCP en el entorno VMware.
- Cree una SVM.
- Configure el LIF de datos de NAS para acceder al almacenamiento en SVM.

Instale Trident de NetApp en los clústeres de OCP

- Instale Trident de NetApp en los tres clústeres: Clústeres de concentrador, origen y destino
- Consulte las instrucciones "aquí".
- Cree un back-end de almacenamiento para ontap-nas .
- Cree una clase de almacenamiento para ontap-nas.
- Consulte las instrucciones "aquí".

Instale Astra Control Center de NetApp

- Astra Control Center de NetApp se instala mediante el operador Astra en el clúster Hub.
- Consulte las instrucciones "aquí".

Puntos que hay que recordar: * Descargue la imagen del Centro de control de Astra de NetApp desde el sitio de soporte. * Empuje la imagen a un registro interno. * Consulte las instrucciones aquí.

Desplegar una Aplicación en el Cluster de Origen

Utilice OpenShift GitOps para desplegar una aplicación. (p. ej., Postgres, fantasma)

Añada los clústeres de origen y destino a Astra Control Center.

Después de agregar un clúster a la gestión de Astra Control, podrá instalar las aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página Aplicaciones de Astra Control para definir las aplicaciones y sus recursos. Consulte "Empieza a gestionar la sección de aplicaciones de Astra Control Center".

El siguiente paso es utilizar Astra Control Center para la protección de datos y la migración de datos desde el origen al clúster de destino.

Protección de datos con Astra

Esta página muestra las opciones de protección de datos para aplicaciones basadas en contenedores Red Hat OpenShift que se ejecutan en VMware vSphere mediante Astra Control Center (ACC).

A medida que los usuarios realizan el proceso de modernización de sus aplicaciones con Red Hat OpenShift, debe implementarse una estrategia de protección de datos para protegerlos de la eliminación accidental o de cualquier otro error humano. A menudo, también es necesaria una estrategia de protección para los fines normativos o de cumplimiento de normativas con el fin de proteger sus datos contra un diaster.

Los requisitos de protección de datos varían desde volver a una copia puntual hasta conmutar automáticamente por error a un dominio de fallo diferente sin intervención humana alguna. Muchos clientes eligen ONTAP como su plataforma de almacenamiento preferida para las aplicaciones de Kubernetes por sus completas funciones, como multi-tenancy, multiprotocolo, ofertas de alto rendimiento y capacidad, replicación y almacenamiento en caché para ubicaciones multisitio, seguridad y flexibilidad.

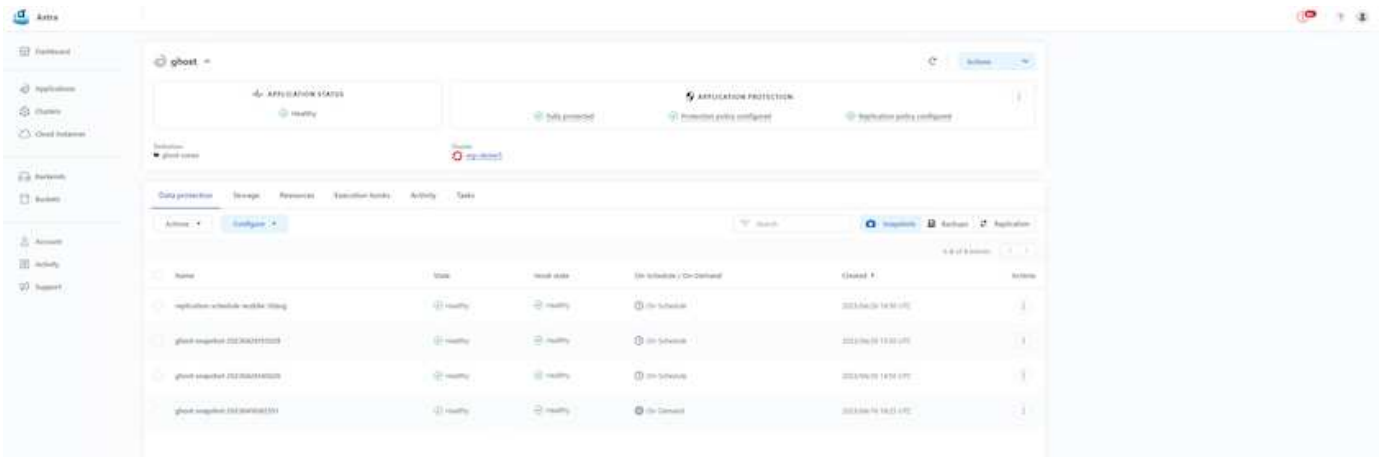
La protección de datos en ONTAP se puede lograr usando ad-hoc o controlados por políticas - **Snapshot** - **copia de seguridad y restauración**

Tanto las copias Snapshot como las copias backup protegen los siguientes tipos de datos: - **Los metadatos de la aplicación que representan el estado de la aplicación**. **Los volúmenes de datos persistentes asociados con la aplicación**. **Cualquier artefacto de recursos que pertenezca a la aplicación**

Instantánea con ACC

Se puede capturar una copia puntual de los datos mediante Snapshot con ACC. La política de protección define el número de copias de Snapshot que se deben conservar. La opción de programación mínima disponible es por horas. Las copias Snapshot manuales bajo demanda se pueden realizar en cualquier momento y en intervalos inferiores a las copias Snapshot programadas. Las copias Snapshot se almacenan en el mismo volumen aprovisionado que la aplicación.

Configuración de instantánea con ACC

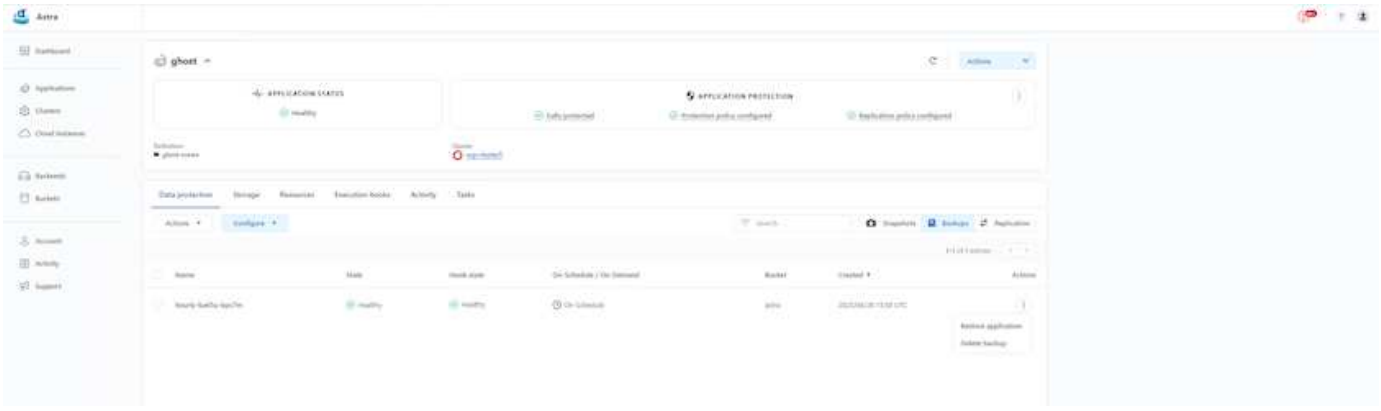


Copia de seguridad y restauración con ACC

Un backup se basa en una snapshot. ACC puede realizar copias Snapshot mediante CSI y realizar backups utilizando la copia snapshot puntual. El backup se almacena en un almacén de objetos externo (cualquier compatible con S3, incluido ONTAP S3 en una ubicación diferente). La política de protección puede configurarse para los backups programados y la cantidad de versiones de backup que deben conservarse. El objetivo de punto de recuperación mínimo es de una hora.

Restauración de una aplicación a partir de una copia de seguridad mediante ACC

ACC restaura la aplicación desde el bloque de S3, donde se almacenan los backups.



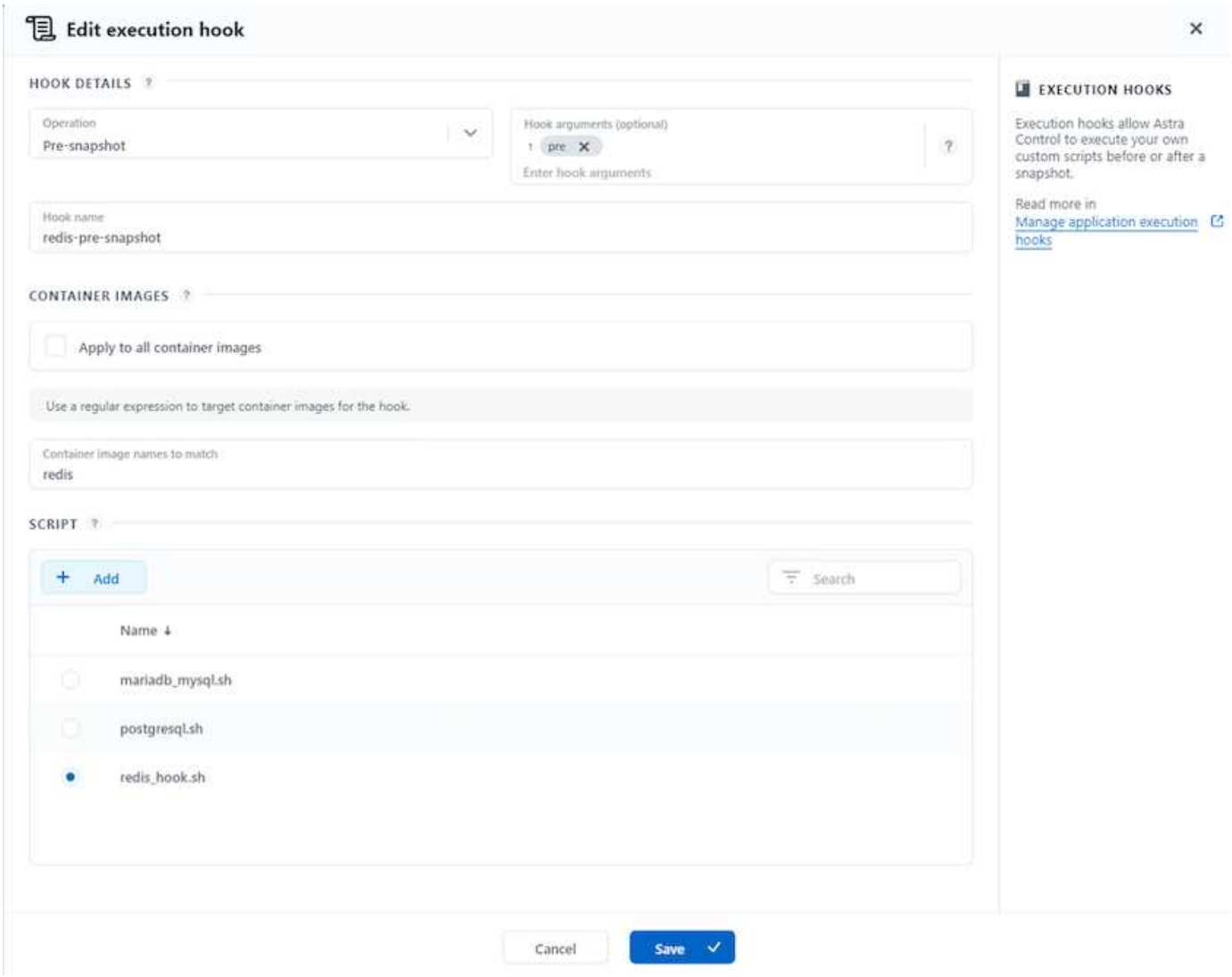
Enlaces de ejecución específicos de la aplicación

Además, los ganchos de ejecución se pueden configurar para que se ejecuten junto con una operación de protección de datos de una aplicación administrada. A pesar de que están disponibles las funciones de protección de datos al nivel de cabina de almacenamiento, a menudo se necesitan pasos adicionales para realizar backups y restauraciones de datos consistentes con la aplicación. Los pasos adicionales específicos de la aplicación pueden ser: - Antes o después de crear una copia snapshot. - antes o después de crear una copia de seguridad. - Después de restaurar a partir de una copia Snapshot o copia de seguridad.

Astra Control puede ejecutar estos pasos específicos de la aplicación codificados como scripts personalizados denominados «enlaces de ejecución».

"Proyecto Verda GitHub de NetApp" proporciona ganchos de ejecución para aplicaciones nativas de la nube populares para que la protección de aplicaciones sea sencilla, robusta y fácil de orquestar. Siéntase libre de contribuir a ese proyecto si tiene suficiente información para una aplicación que no está en el repositorio.

Enlace de ejecución de ejemplo para la instantánea previa de una aplicación de redis.



Replicación con ACC

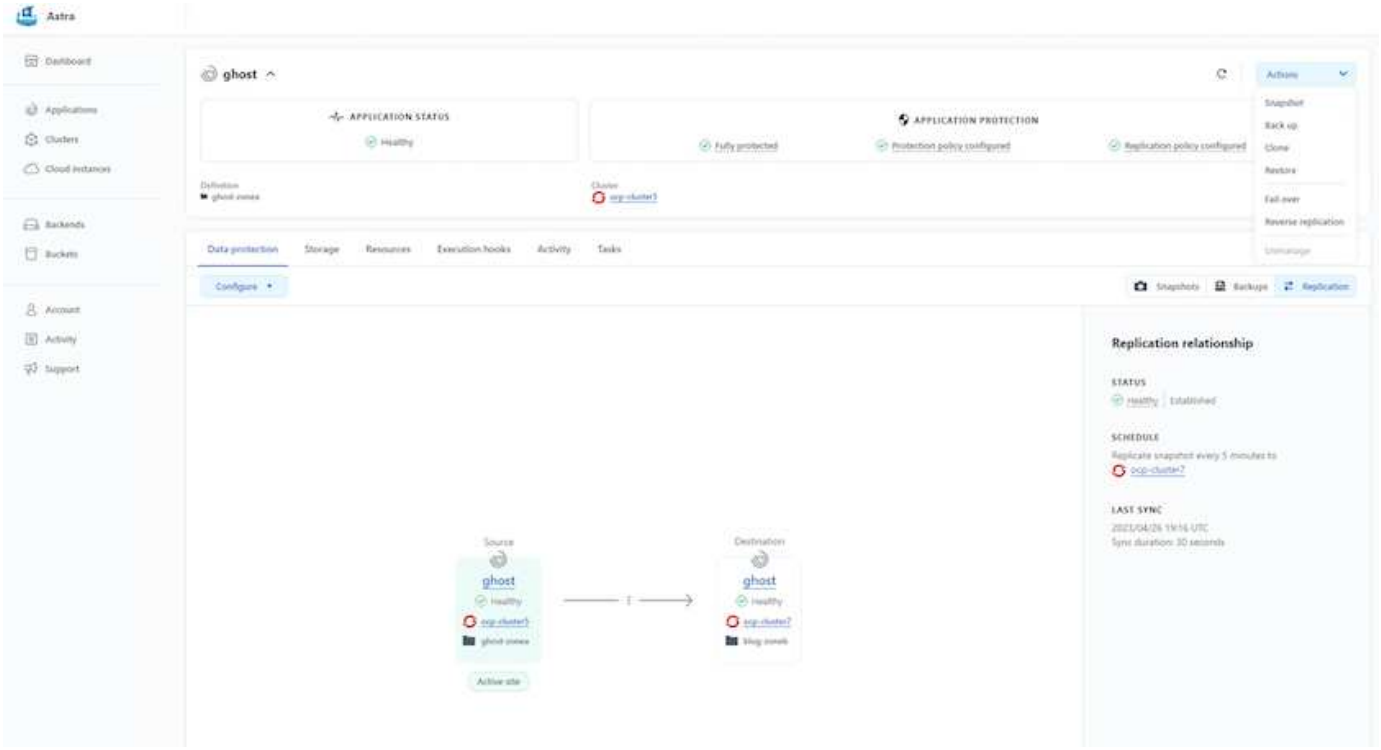
Para la protección regional o para una solución de objetivo de punto de recuperación y objetivo de tiempo de recuperación bajos, una aplicación se puede replicar en otra instancia de Kubernetes que se ejecute en otro sitio, preferiblemente en otra región. ACC utiliza SnapMirror asíncrono de ONTAP con un objetivo de punto de

recuperación mínimo de 5 minutos. La replicación se realiza mediante la replicación en ONTAP y, a continuación, una conmutación por error crea los recursos de Kubernetes en el clúster de destino.

Tenga en cuenta que la replicación es diferente de la copia de seguridad y restauración donde la copia de seguridad va a S3 y la restauración se realiza a partir de S3. Consulte el enlace here para obtener detalles adicionales sobre las diferencias entre los dos tipos de protección de datos.

Consulte "aquí" Para obtener instrucciones de configuración de SnapMirror.

SnapMirror con ACC



los controladores de almacenamiento san y nas económicos no admiten la función de replicación. Consulte "aquí" para obtener más detalles.

Vídeo de demostración:

"Vídeo de demostración de la recuperación de desastres con Astra Control Center"

Protección de datos con Astra Control Center

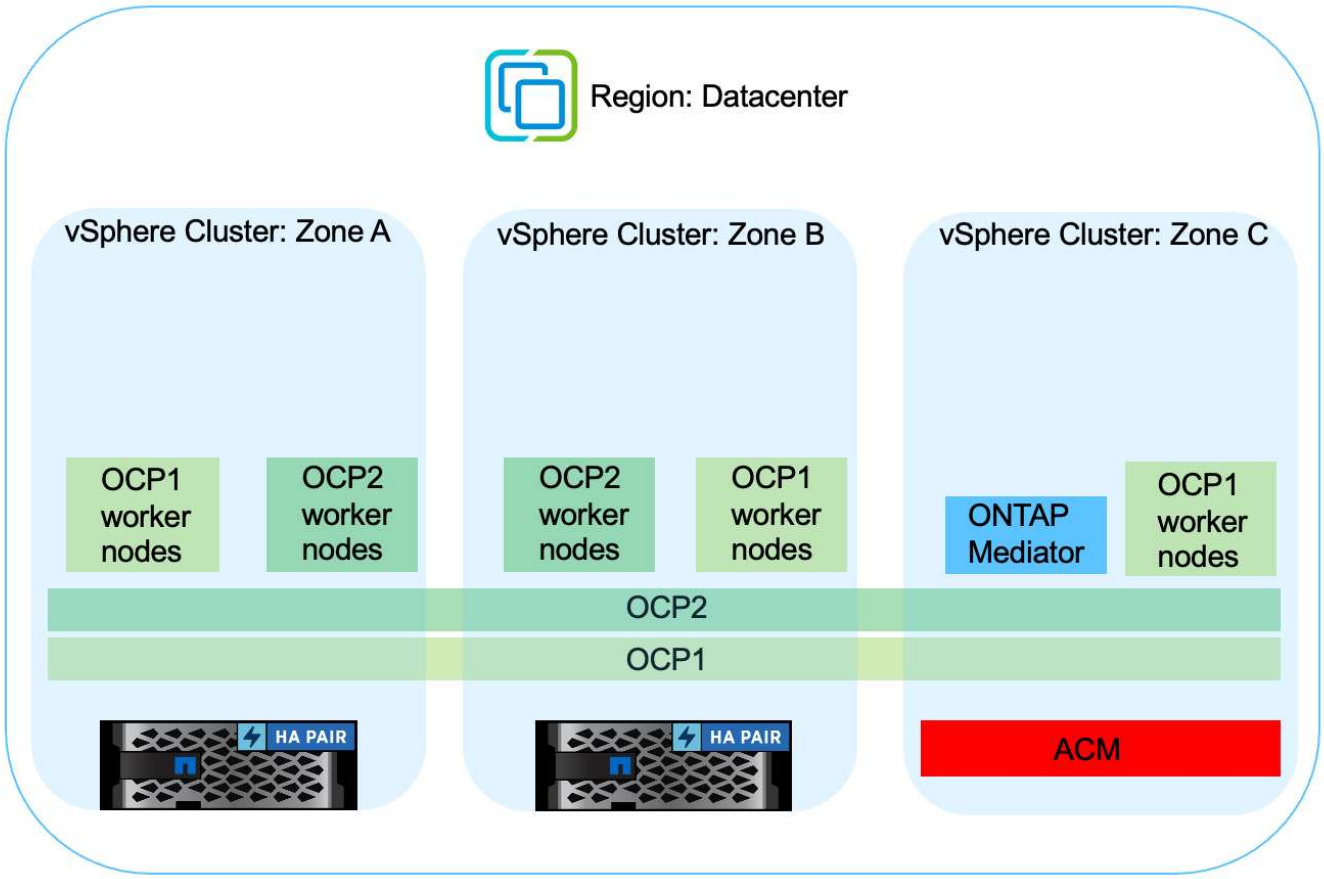
Continuidad del negocio con MetroCluster

La mayoría de nuestra plataforma de hardware para ONTAP tiene características de alta disponibilidad para proteger de fallos en los dispositivos, lo que evita la necesidad de realizar la recuperación de diaster. Sin embargo, para protegerse de incendios o cualquier otro desastre y para continuar el negocio con un objetivo de punto de recuperación nulo y un objetivo de tiempo de recuperación bajo, a menudo se usa una solución MetroCluster.

Los clientes que actualmente tienen un sistema ONTAP pueden extenderse a MetroCluster añadiendo sistemas ONTAP compatibles dentro de las limitaciones de distancia para proporcionar recuperación ante

desastres a nivel de zona. Astra Trident, CSI (Container Storage Interface) es compatible con ONTAP de NetApp, incluida la configuración de MetroCluster, así como otras opciones como Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx para ONTAP de NetApp, etc. Astra Trident proporciona cinco opciones de controladores de almacenamiento para ONTAP y todas son compatibles con la configuración MetroCluster. Consulte "aquí" Para obtener más información sobre los controladores de almacenamiento de ONTAP admitidos por Astra Trident.

La solución de MetroCluster requiere una funcionalidad o una extensión de red de capa 2 para acceder a la misma dirección de red desde ambos dominios de fallo. Una vez que se ha instalado la configuración de MetroCluster, la solución es transparente para los propietarios de aplicaciones, ya que todos los volúmenes de la svm de MetroCluster están protegidos y disfrutan de las ventajas de SyncMirror (objetivo de punto de recuperación cero).



Para la configuración del back-end de Trident (TBC), no especifique la LIF de datos ni la SVM cuando se utilice la configuración de MetroCluster. Especifique la IP de gestión de SVM para la LIF de gestión y utilice las credenciales de rol vsadmin.

Hay disponible más información sobre las funciones de protección de datos de Astra Control Center "aquí"

Migración de datos mediante Astra Control Center

Esta página muestra las opciones de migración de datos para las cargas de trabajo de contenedor en clústeres de Red Hat OpenShift con Astra Control Center (ACC).

A menudo, las aplicaciones de Kubernetes tienen que moverse de un entorno a otro. Para migrar una aplicación junto con sus datos persistentes, se puede utilizar ACC de NetApp.

Migración de datos entre distintos entornos de Kubernetes

ACC es compatible con varios tipos de Kubernetes, como Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, upstream Kubernetes, etc. Para obtener más información, consulte "aquí".

Para migrar una aplicación de un cluster a otro, puede utilizar una de las siguientes funciones de ACC:

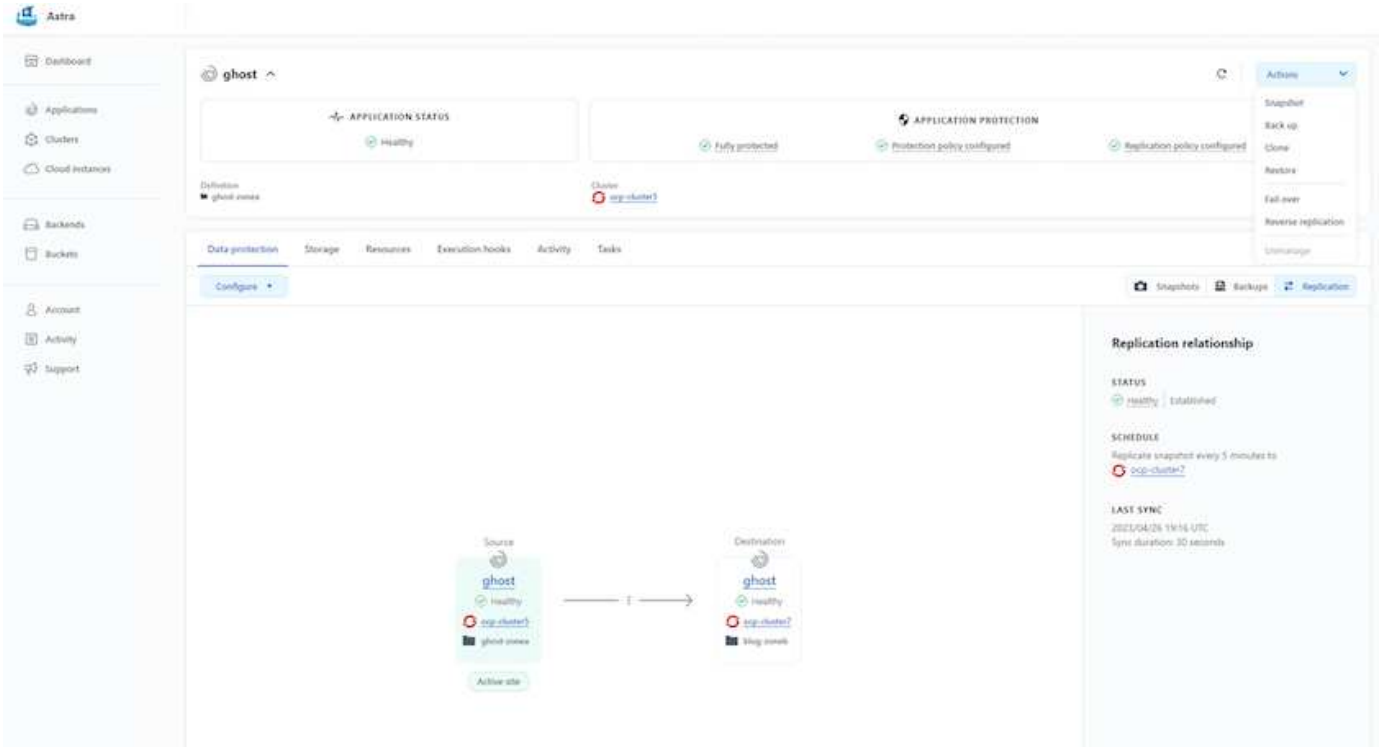
- **replicación**
- **copia de seguridad y restauración**
- **clone**

Consulte la "sección de protección de datos" para las opciones **replicación y copia de seguridad y restauración**.

Consulte "aquí" para más detalles acerca de **clonación**.

> La función de replicación de Astra solo se admite con Trident Container Storage Interface (CSI). Sin embargo, la replicación no es compatible con los controladores de economía nas y san.

Realización de la replicación de datos mediante ACC



Soluciones de multicloud híbrido de NetApp para cargas de trabajo de contenedores de Red Hat OpenShift

Descripción general

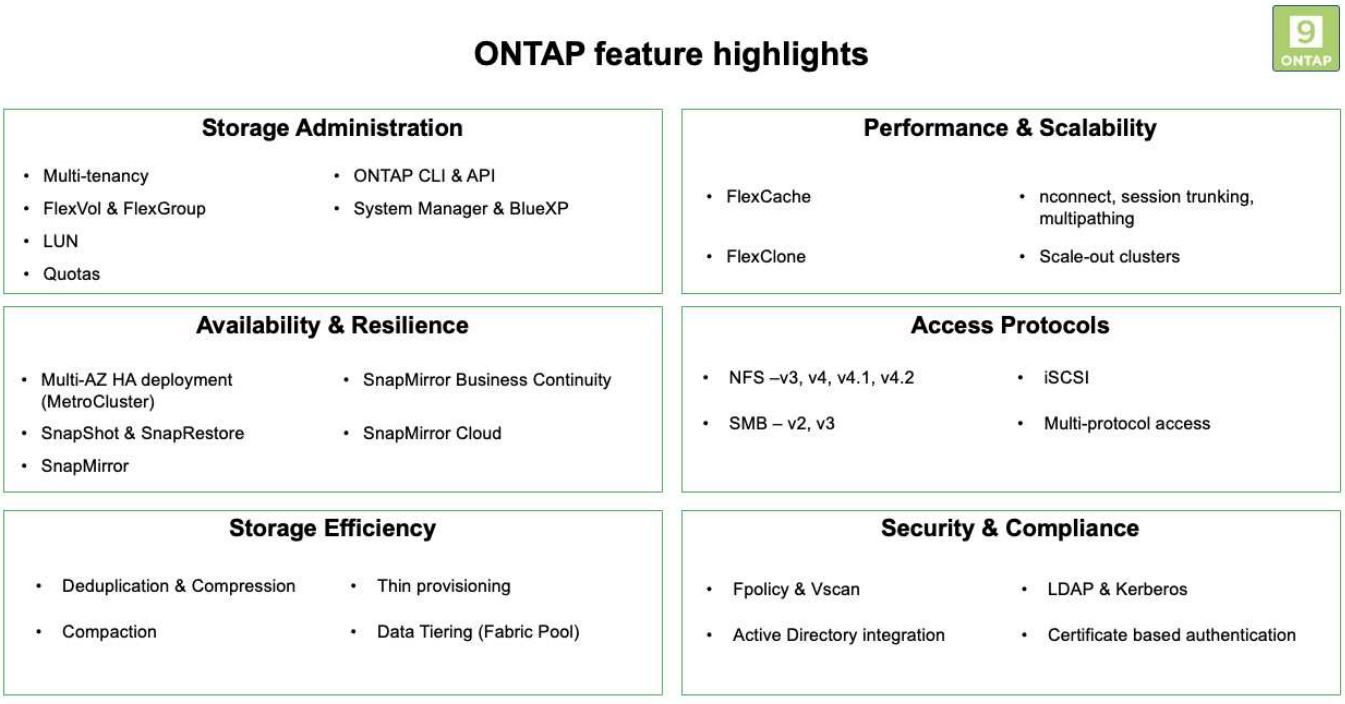
NetApp está viendo un aumento significativo en los clientes que modernizan sus aplicaciones empresariales heredadas y crean nuevas aplicaciones con contenedores y plataformas de orquestación creadas en torno a Kubernetes. Red Hat OpenShift Container Platform es un ejemplo que consideramos adoptado por muchos de

nuestros clientes.

A medida que más y más clientes empiezan a adoptar contenedores dentro de sus empresas, NetApp está perfectamente posicionada para poder dar respuesta a las necesidades de almacenamiento persistente de sus aplicaciones con estado y las necesidades de gestión de datos clásicas como la protección de datos, la seguridad de datos y la migración de datos. Sin embargo, estas necesidades se satisfacen utilizando diferentes estrategias, herramientas y métodos.

Las opciones de almacenamiento basado en ONTAP de NetApp que se enumeran a continuación, ofrecen seguridad, protección de datos, fiabilidad y flexibilidad para implementaciones de contenedores y Kubernetes.

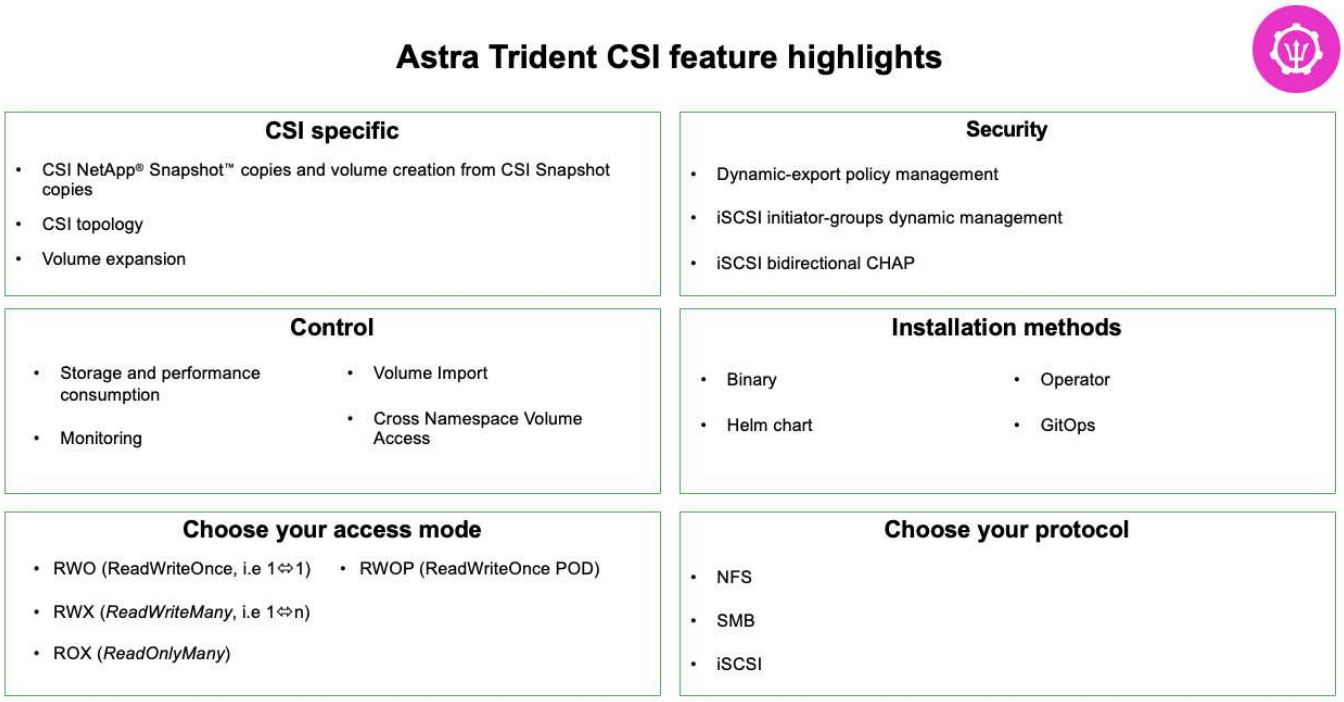
- Almacenamiento autogestionado en las instalaciones:
  - Almacenamiento estructural (FAS) de NetApp, cabinas All Flash FAS (AFF), cabina All SAN (ASA) y ONTAP Select
- Almacenamiento gestionado por el proveedor en las instalaciones:
  - NetApp Keystone proporciona almacenamiento como servicio (STaaS)
- Almacenamiento autogestionado en el cloud:
  - Cloud Volumes ONTAP (CVO) de NetApp proporciona almacenamiento autogestionado en los proveedores a hiperescala
- Almacenamiento en el cloud gestionado por el proveedor:
  - Cloud Volumes Service para Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx para ONTAP de NetApp ofrecen un almacenamiento totalmente gestionado en los proveedores a hiperescala



NetApp BlueXP le permite gestionar todos sus activos de almacenamiento y datos desde una única interfaz o plano de control.

Puedes usar BlueXP para crear y administrar almacenamiento en nube (por ejemplo, Cloud Volumes ONTAP y Azure NetApp Files), para mover, proteger y analizar datos, y para controlar muchos dispositivos de almacenamiento on-premises y en la periferia.

Astra Trident de NetApp es un orquestador de almacenamiento compatible con CSI que permite consumir almacenamiento persistente de forma rápida y sencilla, respaldado por diversas opciones de almacenamiento de NetApp mencionadas anteriormente. Es un software de código abierto que tiene soporte y mantenimiento de NetApp.



Las cargas de trabajo de contenedores vitales para el negocio necesitan más que volúmenes persistentes. Sus requisitos de gestión de datos requieren la protección y la migración de los objetos de aplicaciones kubernetes también.

> 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, PVCs, despliegues, servicios - objetos de configuración personalizados como mapas de configuración y secretos - datos persistentes como copias Snapshot, copias de seguridad, clones - recursos personalizados como CRS y CRD

Astra Control de NetApp, disponible como software totalmente gestionado y autogestionado, proporciona orquestación para una gestión de datos de aplicaciones sólida. Consulte la "Documentación de Astra" Para obtener más información sobre la familia de productos Astra.

Esta documentación de referencia proporciona la validación de la migración y la protección de aplicaciones basadas en contenedores, puestas en marcha en la plataforma de contenedores RedHat OpenShift, mediante Astra Control Center de NetApp. Además, la solución proporciona detalles de alto nivel para la implementación y el uso de Red Hat Advanced Cluster Management (ACM) para la gestión de las plataformas de contenedores. En el documento también se destacan los detalles de la integración del almacenamiento de NetApp con las plataformas de contenedor Red Hat OpenShift mediante el aprovisionador CSI de Astra Trident. Astra Control Center se pone en marcha en el clúster de concentradores y se utiliza para gestionar las aplicaciones de contenedores y su ciclo de vida de almacenamiento persistente. Por último, proporciona una solución de replicación y conmutación al nodo de respaldo y conmutación de retorno tras recuperación para cargas de trabajo de contenedores en clústeres de Red Hat OpenShift gestionados en AWS (ROSA) utilizando Amazon FSx para NetApp ONTAP (FSxN) como almacenamiento persistente.

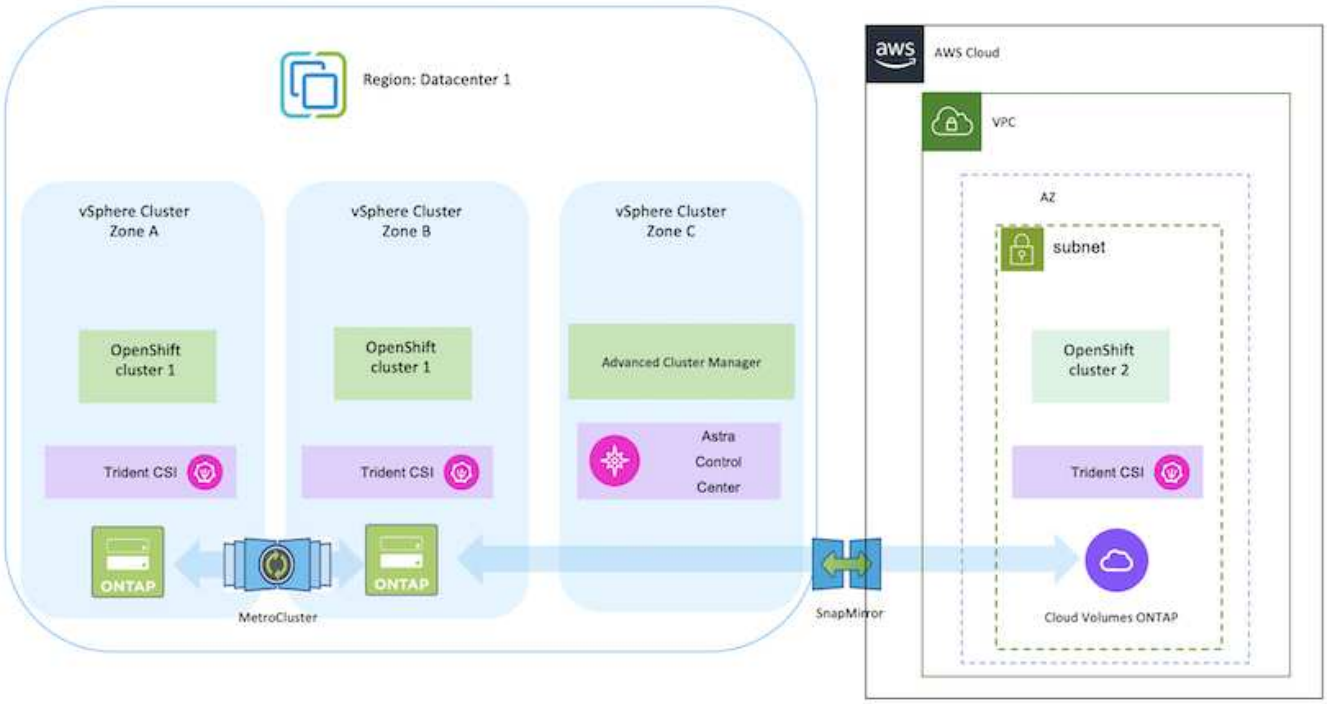
Solución de NetApp con cargas de trabajo de la plataforma de contenedores Red Hat OpenShift en un cloud híbrido

Los clientes pueden estar en un momento de su proceso de modernización cuando estén listos para mover algunas cargas de trabajo seleccionadas o todas las cargas de trabajo de sus centros de datos al cloud. Pueden optar por usar contenedores OpenShift autogestionados y almacenamiento autogestionado de NetApp en la nube por diversos motivos. Deben planificar e implementar la plataforma de contenedores Red Hat OpenShift (OCP) en la nube para un entorno preparado para la producción con éxito para migrar las cargas de trabajo de contenedores desde sus centros de datos. Sus clústeres de 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.

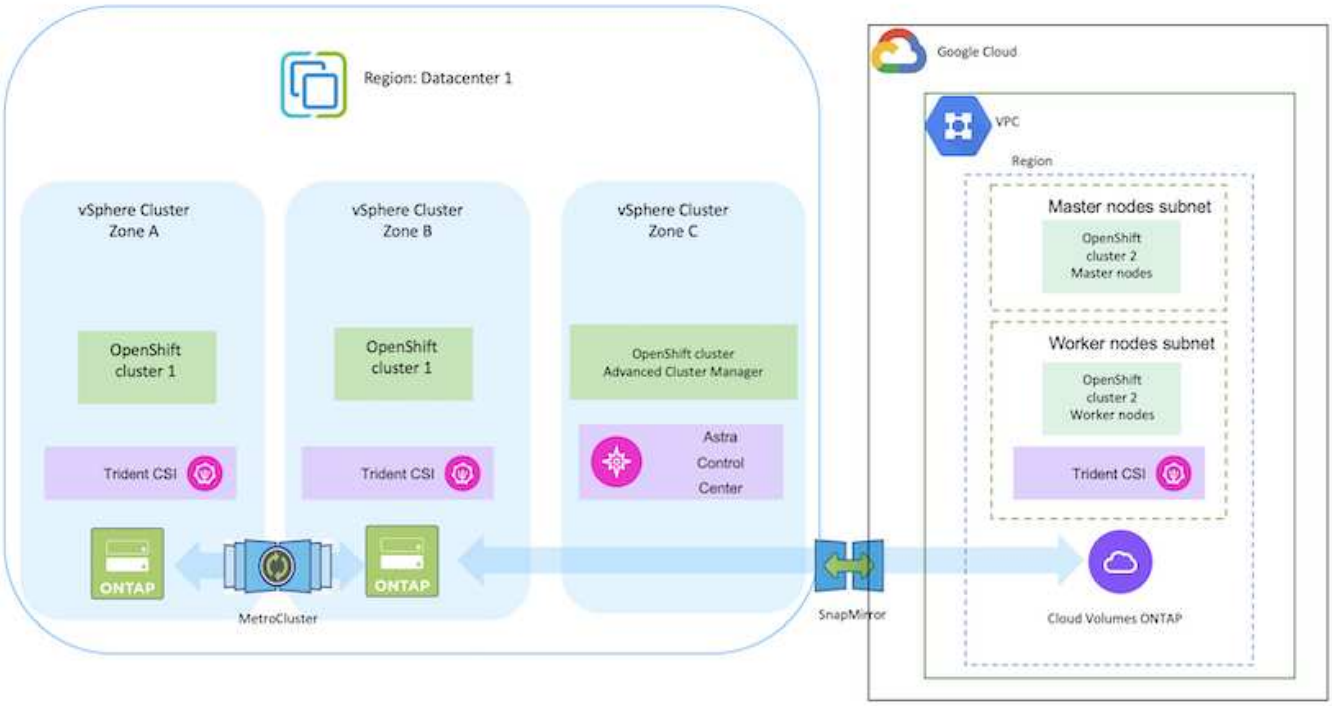
El almacenamiento de NetApp Cloud Volumes ONTAP ofrece protección de datos, fiabilidad y flexibilidad para puestas en marcha de contenedores en AWS, Azure y en Google Cloud. Astra Trident sirve como aprovisionador de almacenamiento dinámico para consumir almacenamiento persistente de Cloud Volumes ONTAP para las aplicaciones con estado de los clientes. Se puede usar Astra Control Center para orquestar los muchos requisitos de gestión de datos de aplicaciones con estado, como la protección de datos, la migración y la continuidad del negocio.

Solución de protección y migración de datos para cargas de trabajo de contenedores de OpenShift en un cloud híbrido mediante Astra Control Center

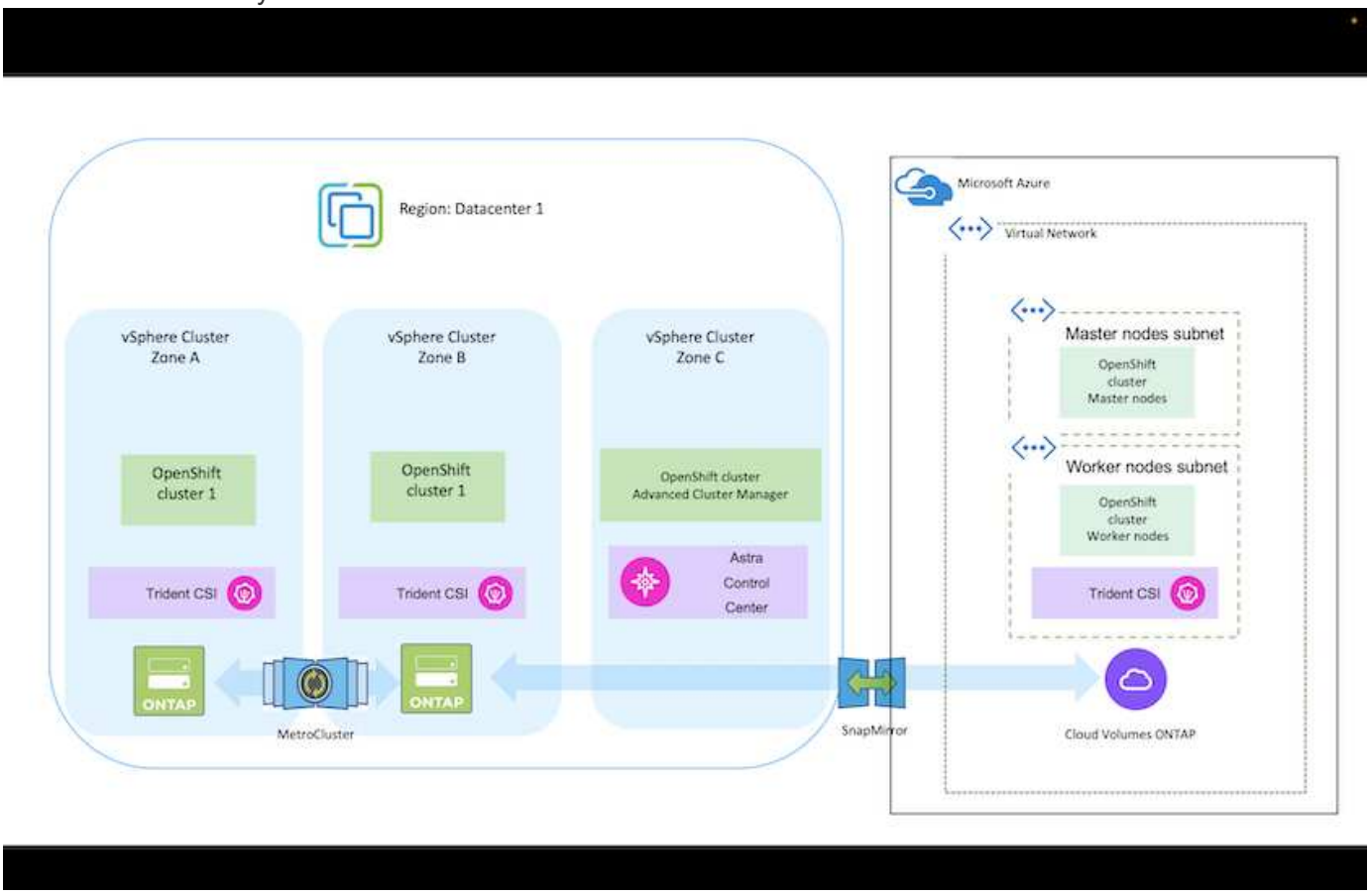
On-premises y AWS



En las instalaciones y Google Cloud



En las instalaciones y Azure Cloud



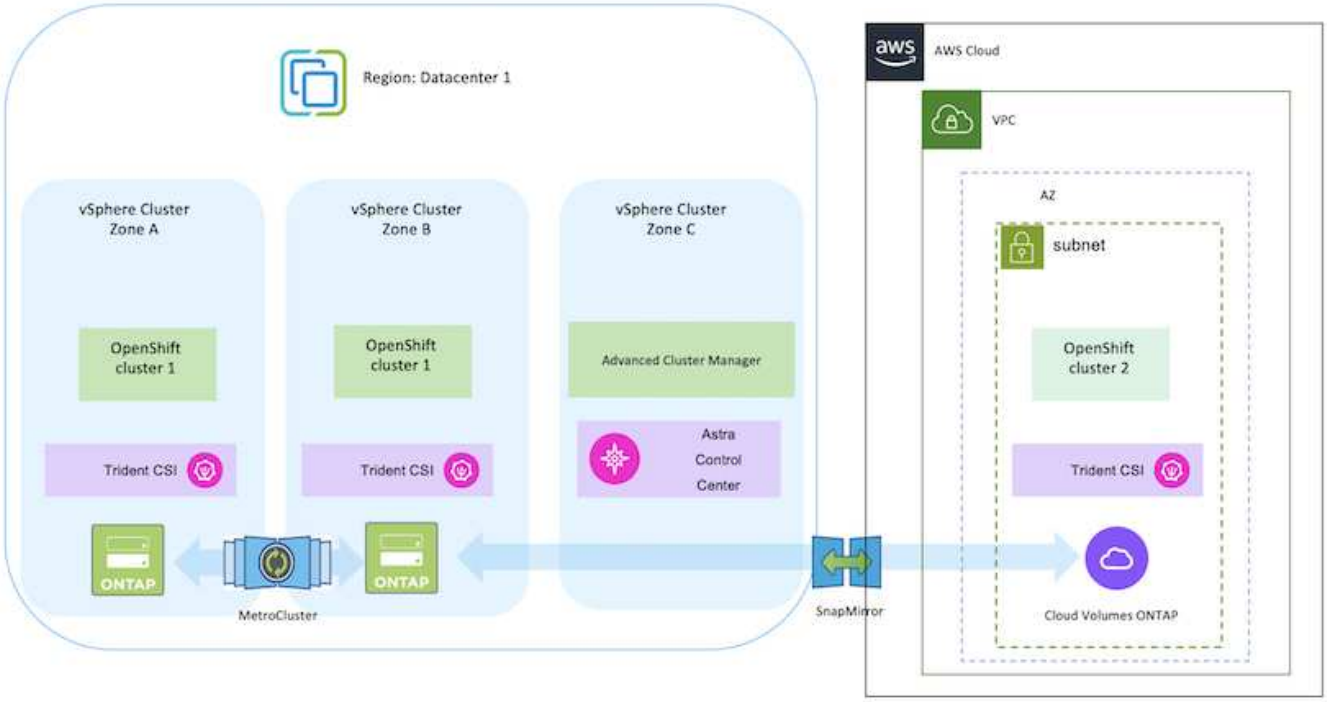
Implemente y configure la plataforma Red Hat OpenShift Container en AWS

En esta sección se describe un flujo de trabajo de alto nivel sobre cómo configurar y

gestionar clústeres de OpenShift en AWS e implementar aplicaciones con estado en ellos. Muestra el uso del almacenamiento Cloud Volumes ONTAP de NetApp con la ayuda de Astra Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Astra Control Center para realizar actividades de protección de datos y migración para las aplicaciones con estado.

Existen varias formas de implementar los clústeres de plataformas de contenedores de Red Hat OpenShift en AWS. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

A continuación se muestra un diagrama que muestra los clústeres implementados en AWS y conectados al centro de datos mediante una VPN.



El proceso de configuración puede dividirse en los siguientes pasos:

Instale un clúster de OCP en AWS desde Advanced Cluster Management.

- Cree una VPC con una conexión VPN de sitio a sitio (mediante pfsense) para conectarse a la red local.
- La red local tiene conectividad a Internet.
- Cree 3 subredes privadas en 3 AZs diferentes.
- Cree una zona alojada privada de Route 53 y una resolución de DNS para la VPC.

Cree un clúster de OpenShift en AWS desde el Asistente de administración avanzada de clústeres (ACM). Consulte las instrucciones "aquí".

También puede crear el clúster en AWS desde la consola de OpenShift Hybrid Cloud. Consulte "aquí" si desea obtener instrucciones.

Al crear el clúster con ACM, tiene la capacidad de personalizar la instalación editando el archivo yaml después de completar los detalles en la vista de formulario. Después de crear el clúster, puede iniciar sesión ssh en los nodos del clúster para solucionar problemas o utilizar otra configuración manual. Utilice la clave ssh que proporcionó durante la instalación y el núcleo de nombre de usuario para iniciar sesión.

Pon en marcha Cloud Volumes ONTAP en AWS mediante BlueXP.

- Instale el conector en un entorno VMware en las instalaciones. Consulte las instrucciones "aquí".
- Pon en marcha una instancia de CVO en AWS usando el conector. Consulte las instrucciones "aquí".

El conector también se puede instalar en el entorno de nube. Consulte "aquí" para obtener más información.

Instale Astra Trident en el clúster de OCP

- Ponga en marcha el operador Trident mediante Helm. Consulte las instrucciones "aquí"
- Cree un back-end y una clase de almacenamiento. Consulte las instrucciones "aquí".

Añada el clúster OCP en AWS al Astra Control Center.

Añada el clúster OCP en AWS a Astra Control Center.

Uso de la función de topología CSI de Trident para arquitecturas de varias zonas

Los proveedores de cloud, hoy en día, permiten que los administradores de clústeres de Kubernetes/OpenShift generen nodos de los clústeres basados en zonas. Los nodos se pueden ubicar 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 de varias zonas, Astra Trident utiliza la topología CSI. Con la función de topología CSI, el acceso a los volúmenes puede limitarse a un subconjunto de nodos, en función de regiones y zonas de disponibilidad. Consulte "aquí" para obtener más detalles.

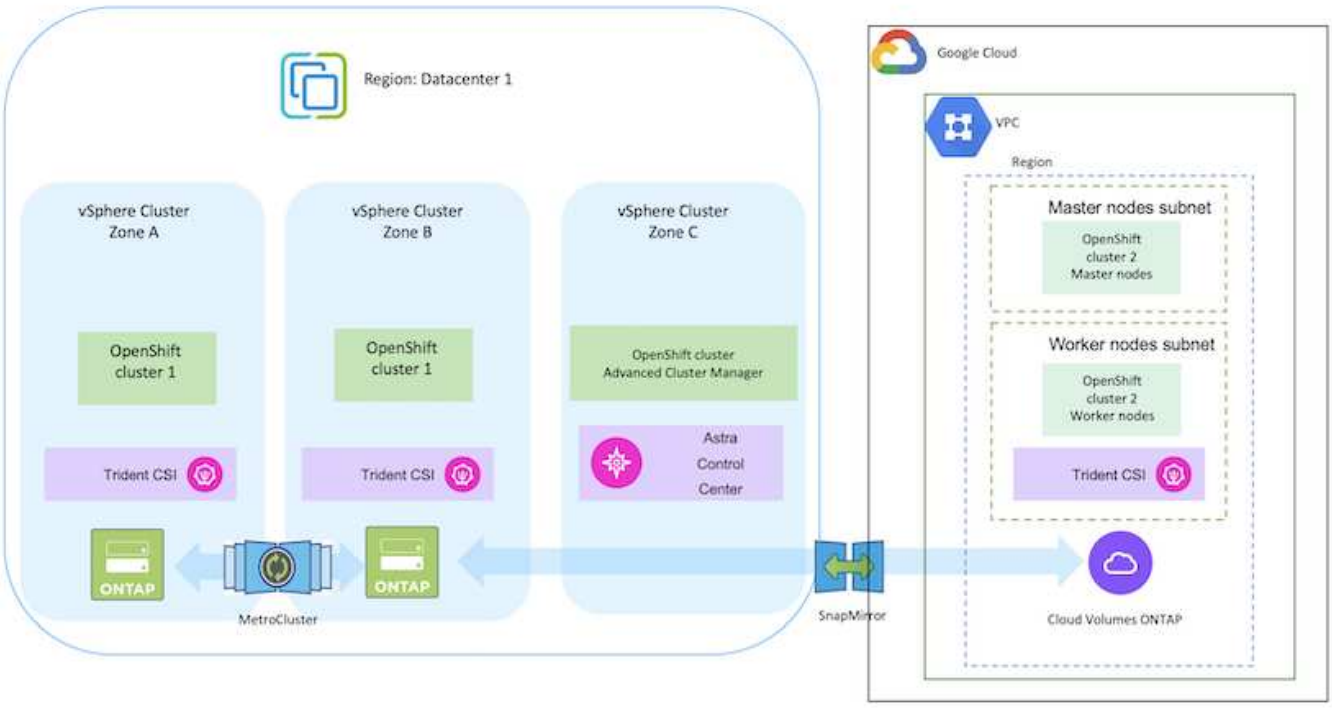
Kubernetes admite dos modos de vinculación de volúmenes: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Astra Trident crea el volumen sin reconocimiento de topología. Los volúmenes persistentes se crean sin dependencia alguna de los requisitos de programación del POD solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y vinculación de un Volumen persistente para una RVP se retrasa hasta que se programe y cree un pod que utilice la RVP. De esta forma, se crean volúmenes con el fin de cumplir las restricciones de programación que se aplican en los requisitos de topología. Los back-ends de almacenamiento de Astra Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (back-end compatible con topología). En el caso de StorageClasses que utilizan dicho back-end, solo se creará un volumen si lo solicita una aplicación programada en una región/zona admitida. (Clase StorageClass compatible con topología) "aquí" para obtener más detalles.

Implemente y configure la plataforma Red Hat OpenShift Container en GCP

Implemente y configure la plataforma Red Hat OpenShift Container en GCP

En esta sección se describe un flujo de trabajo de alto nivel sobre cómo configurar y gestionar clústeres de OpenShift en GCP e implementar aplicaciones con estado en ellos. Muestra el uso del almacenamiento Cloud Volumes ONTAP de NetApp con la ayuda de Astra Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Astra Control Center para realizar actividades de protección de datos y migración para las aplicaciones con estado.

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 plataformas de contenedores Red Hat OpenShift en GCP. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

El proceso de configuración puede dividirse en los siguientes pasos:

Instale un clúster OCP en GCP desde la CLI.

- Asegúrese de haber cumplido todos los requisitos previos indicados "aquí".
- Para la conectividad VPN entre on-premises y GCP, se creó y configuró una VM pfsense. Para ver instrucciones, consulte "aquí".
  - La dirección de la puerta de enlace remota en pfsense solo se puede configurar después de haber creado una puerta de enlace VPN en Google Cloud Platform.
  - Las direcciones IP de red remota para la fase 2 solo se pueden configurar después de que el programa de instalación del clúster de OpenShift 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 cree los componentes de infraestructura para el clúster.
- Ahora instale el clúster OpenShift en GCP.
  - Obtenga el programa de instalación y el secreto de extracción e implemente el clúster siguiendo los pasos que se proporcionan en la documentación "aquí".
  - La instalación crea una red VPC en Google Cloud Platform. También crea una zona privada en Cloud DNS y añade Un registro.
    - Utilice la dirección de bloque CIDR de la red VPC para configurar pfsense y establecer la conexión VPN. Asegúrese de que los firewalls están configurados correctamente.
    - Agregue registros 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.

Pon en marcha Cloud Volumes ONTAP en GCP mediante BlueXP.

- Instala un conector en Google Cloud. Consulte las instrucciones "aquí".
- Pon en marcha una instancia de CVO en Google Cloud mediante el conector. Consulte las instrucciones aquí. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Instale Astra Trident en el clúster OCP de GCP

- Como se muestra, hay muchos métodos para poner en marcha Astra Trident "aquí".
- Para este proyecto, se instaló Astra Trident poniendo en marcha el operador Astra Trident de forma manual mediante las instrucciones "aquí".
- Crear backend y clases de almacenamiento. Consulte las instrucciones "aquí".

Añade el clúster OCP en GCP a Astra Control Center.

- Crea un archivo KubeConfig independiente con un rol de clúster que contenga los permisos mínimos necesarios para que Astra Control gestione un clúster. Se pueden encontrar las instrucciones "aquí".
- Añada el clúster a Astra Control Center siguiendo las instrucciones "aquí"

Uso de la función de topología CSI de Trident para arquitecturas de varias zonas

Los proveedores de cloud, hoy en día, permiten que los administradores de clústeres de Kubernetes/OpenShift generen nodos de los clústeres basados en zonas. Los nodos se pueden ubicar 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 de varias zonas, Astra Trident utiliza la topología CSI. Con la función de topología CSI, el acceso a los volúmenes puede limitarse a un subconjunto de nodos, en función de regiones y zonas de disponibilidad. Consulte "aquí" para obtener más detalles.

> Kubernetes admite dos modos de vinculación de volúmenes: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Astra Trident crea el volumen sin reconocimiento de topología. Los volúmenes persistentes se crean sin dependencia alguna de los requisitos de programación del POD solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y vinculación de un Volumen persistente para una RVP se retrasa hasta que se programe y cree un pod que utilice la RVP. De esta forma, se crean volúmenes con el fin de cumplir las restricciones de programación que se aplican en los requisitos de topología. Los back-ends de almacenamiento de Astra Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (back-end compatible con topología). En el caso de StorageClasses que utilizan dicho back-end, solo se creará un volumen si lo solicita una aplicación programada en una región/zona admitida. (Clase StorageClass compatible con topología) "aquí" para obtener más detalles.

Vídeo de demostración

Instalación de OpenShift Cluster en Google Cloud Platform

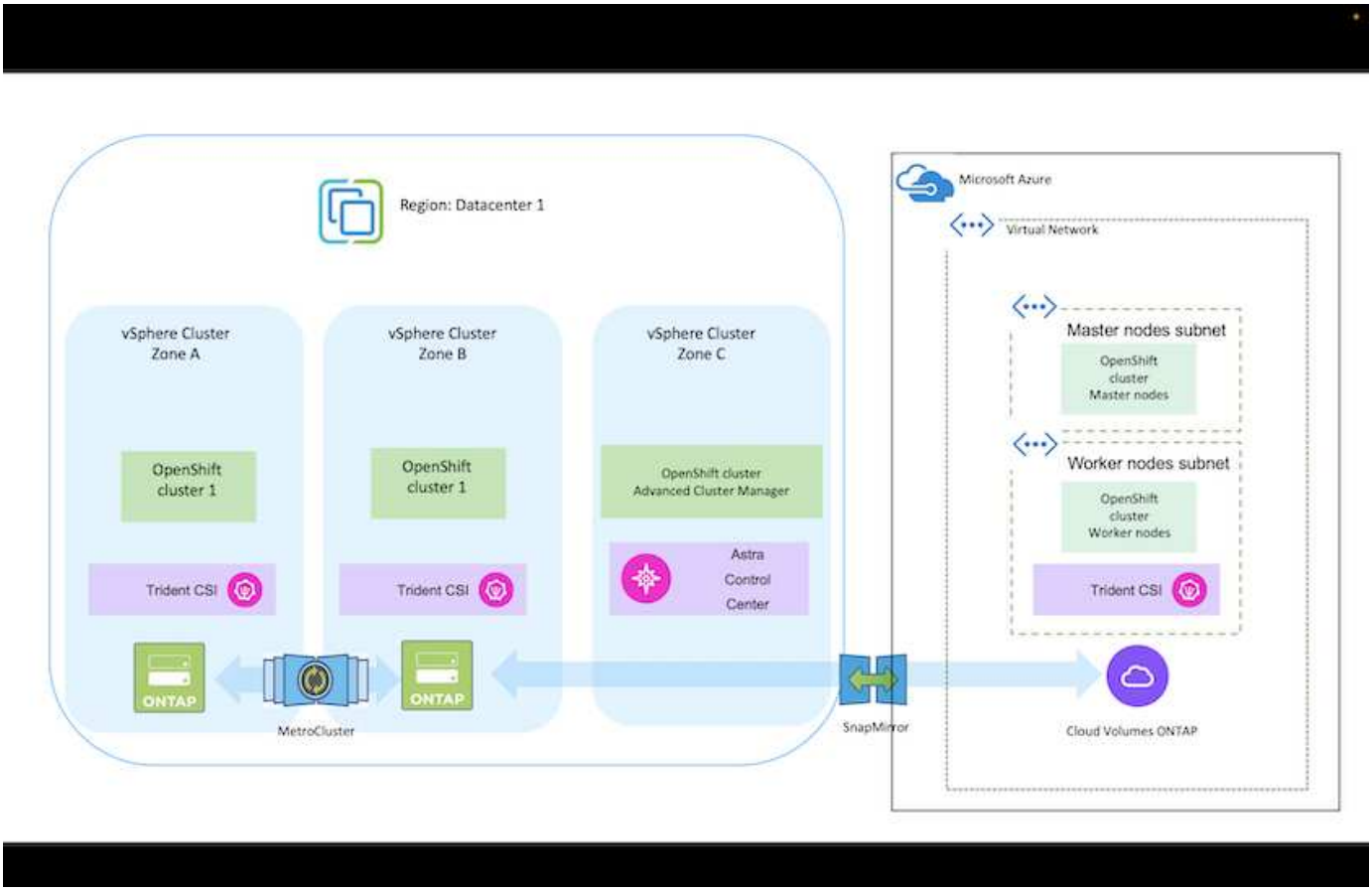
Importar clústeres de OpenShift a Astra Control Center

Implemente y configure la plataforma Red Hat OpenShift Container en Azure

Implemente y configure la plataforma Red Hat OpenShift Container en Azure

En esta sección se describe un flujo de trabajo de alto nivel sobre cómo configurar y gestionar clústeres OpenShift en Azure e implementar aplicaciones con estado en ellos. Muestra el uso del almacenamiento de NetApp Cloud Volumes ONTAP con la ayuda del aprovisionador de Astra Trident/Astra Control para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Astra Control Center para realizar actividades de protección de datos y migración 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 los clústeres de plataformas de contenedores de Red Hat OpenShift en Azure. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

El proceso de configuración puede dividirse en los siguientes pasos:

Instale un clúster OCP en Azure desde la CLI.

- Asegúrese de haber cumplido todos los requisitos previos indicados "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 y Azure, se creó y configuró una máquina virtual pfsense. Para ver instrucciones, consulte "aquí".
- Obtenga el programa de instalación y el secreto de extracción e implemente el clúster siguiendo los pasos que se proporcionan 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 proporciona un archivo install-config.yaml de ejemplo.

```
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:
```

Pon en marcha Cloud Volumes ONTAP en Azure mediante BlueXP.

- Instale un conector en Azure. Consulte las instrucciones "aquí".
- Pon en marcha una instancia de CVO en Azure usando el conector. Consulte el enlace de instrucciones:https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [aquí.]

Instale Astra Control Provisioner en el clúster OCP en Azure

- Para este proyecto, Astra Control Provisioner (ACP) se instaló en todos los clústeres (clúster en las instalaciones, clúster en las instalaciones donde se puso en marcha Astra Control Center y el clúster en Azure). Obtenga más información sobre el aprovisionador de Astra Control "aquí".
- Crear backend y clases de almacenamiento. Consulte las instrucciones "aquí".

Añada el clúster OCP en Azure al Astra Control Center.

- Crea un archivo KubeConfig independiente con un rol de clúster que contenga los permisos mínimos necesarios para que Astra Control gestione un clúster. Se pueden encontrar las instrucciones "aquí".
- Añada el clúster a Astra Control Center siguiendo las instrucciones "aquí"

Uso de la función de topología CSI de Trident para arquitecturas de varias zonas

Los proveedores de cloud, hoy en día, permiten que los administradores de clústeres de Kubernetes/OpenShift generen nodos de los clústeres basados en zonas. Los nodos se pueden ubicar 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 de varias zonas, Astra Trident utiliza la topología CSI. Con la función de topología CSI, el acceso a los volúmenes puede limitarse a un subconjunto de nodos, en función de regiones y zonas de disponibilidad. Consulte "aquí" para obtener más detalles.

Kubernetes admite dos modos de vinculación de volúmenes: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Astra Trident crea el volumen sin reconocimiento de topología. Los volúmenes persistentes se crean sin dependencia alguna de los requisitos de programación del POD solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y vinculación de un Volumen persistente para una RVP se retrasa hasta que se programe y cree un pod que utilice la RVP. De esta forma, se crean volúmenes con el fin de cumplir las restricciones de programación que se aplican en los requisitos de topología. Los back-ends de almacenamiento de Astra Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (back-end compatible con topología). En el caso de StorageClasses que utilizan dicho back-end, solo se creará un volumen si lo solicita una aplicación programada en una región/zona admitida. (Clase StorageClass compatible con topología) "aquí" para obtener más detalles.

Vídeo de demostración

Utilizar Astra Control para la conmutación al nodo de respaldo y la conmutación de retorno tras recuperación de aplicaciones

Protección de datos mediante Astra Control Center

Esta página muestra las opciones de protección de datos para aplicaciones basadas en contenedores Red Hat OpenShift que se ejecutan en VMware vSphere o en la nube mediante Astra Control Center (ACC).

A medida que los usuarios realizan el proceso de modernización de sus aplicaciones con Red Hat OpenShift, debe implementarse una estrategia de protección de datos para protegerlos de la eliminación accidental o de cualquier otro error humano. A menudo, también es necesaria una estrategia de protección para los fines normativos o de cumplimiento de normativas con el fin de proteger sus datos contra un diaster.

Los requisitos de protección de datos varían desde volver a una copia puntual hasta conmutar automáticamente por error a un dominio de fallo diferente sin intervención humana alguna. Muchos clientes eligen ONTAP como su plataforma de almacenamiento preferida para las aplicaciones de Kubernetes por sus completas funciones, como multi-tenancy, multiprotocolo, ofertas de alto rendimiento y capacidad, replicación

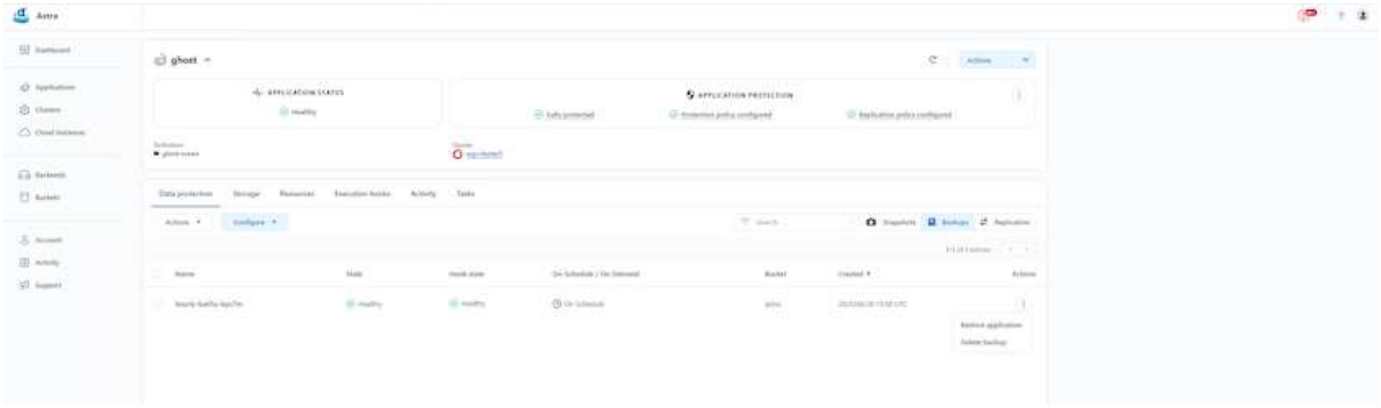
y almacenamiento en caché para ubicaciones multisitio, seguridad y flexibilidad.

Es posible que los clientes tengan configurado un entorno cloud como extensión de su centro de datos, para que puedan aprovechar las ventajas del cloud y estar bien posicionados para mover sus cargas de trabajo en el futuro. Para estos clientes, realizar backup de sus aplicaciones OpenShift y sus datos en el entorno de cloud se convierte en una opción inevitable. Luego, pueden restaurar las aplicaciones y los datos asociados en un clúster de OpenShift en la nube o en el centro de datos.

Copia de seguridad y restauración con ACC

Los propietarios de aplicaciones pueden revisar y actualizar las aplicaciones descubiertas por ACC. ACC puede realizar copias Snapshot mediante CSI y realizar backups utilizando la copia snapshot puntual. El destino de backup puede ser un almacén de objetos en el entorno de cloud. La política de protección puede configurarse para los backups programados y la cantidad de versiones de backup que deben conservarse. El objetivo de punto de recuperación mínimo es de una hora.

Restauración de una aplicación a partir de una copia de seguridad mediante ACC

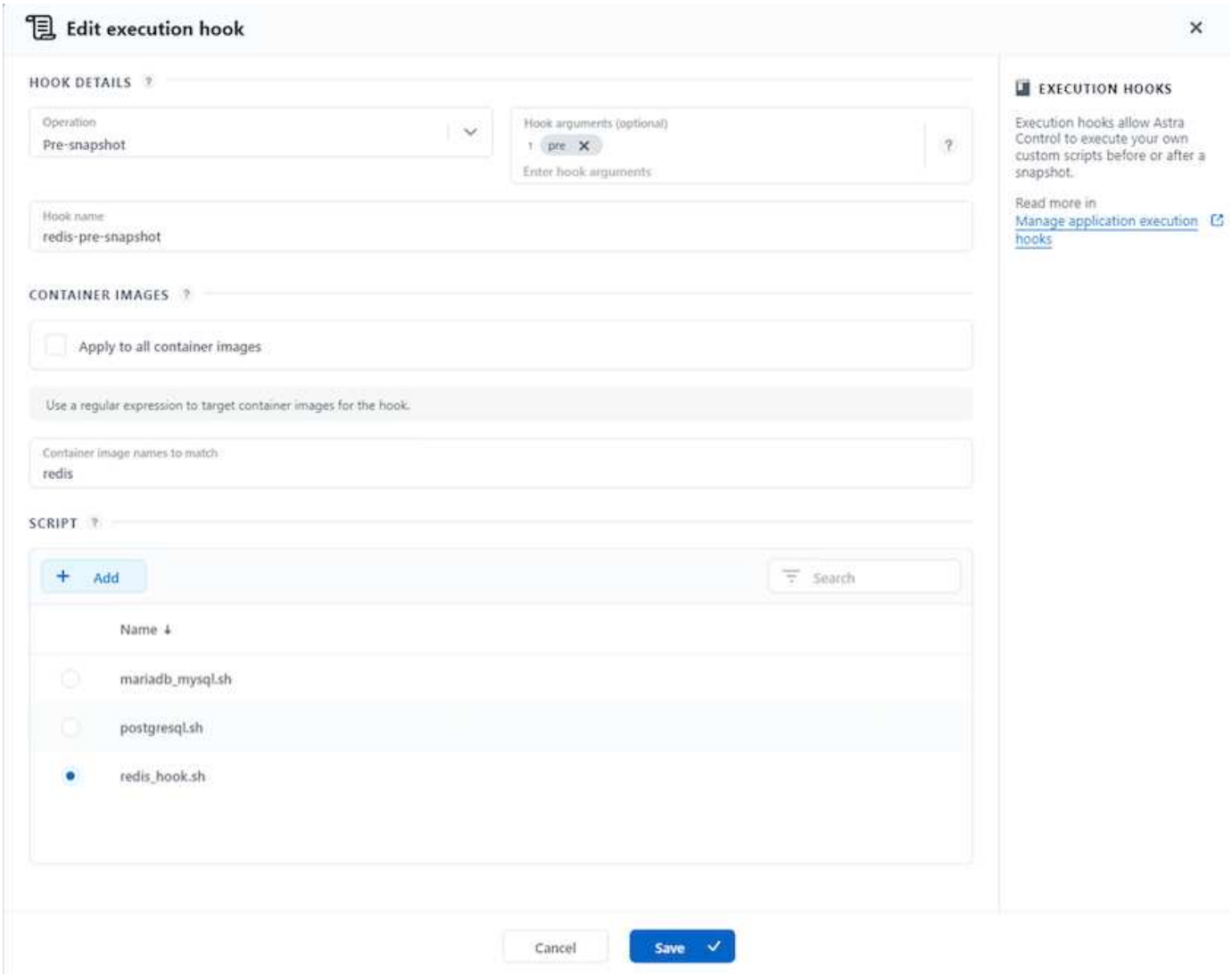


Enlaces de ejecución específicos de la aplicación

Aunque las funciones de protección de datos en el arreglo de almacenamiento están disponibles, a menudo se necesitan pasos adicionales para realizar backups y restaurar la consistencia de la aplicación. Los pasos adicionales específicos de la aplicación pueden ser: - Antes o después de crear una copia snapshot. - antes o después de crear una copia de seguridad. - Después de restaurar a partir de una copia Snapshot o copia de seguridad. Astra Control puede ejecutar estos pasos específicos de la aplicación codificados como scripts personalizados denominados «enlaces de ejecución».

La de NetApp "Proyecto de código abierto Verda" proporciona ganchos de ejecución para aplicaciones nativas de la nube populares para que la protección de aplicaciones sea sencilla, robusta y fácil de orquestar. Siéntase libre de contribuir a ese proyecto si tiene suficiente información para una aplicación que no está en el repositorio.

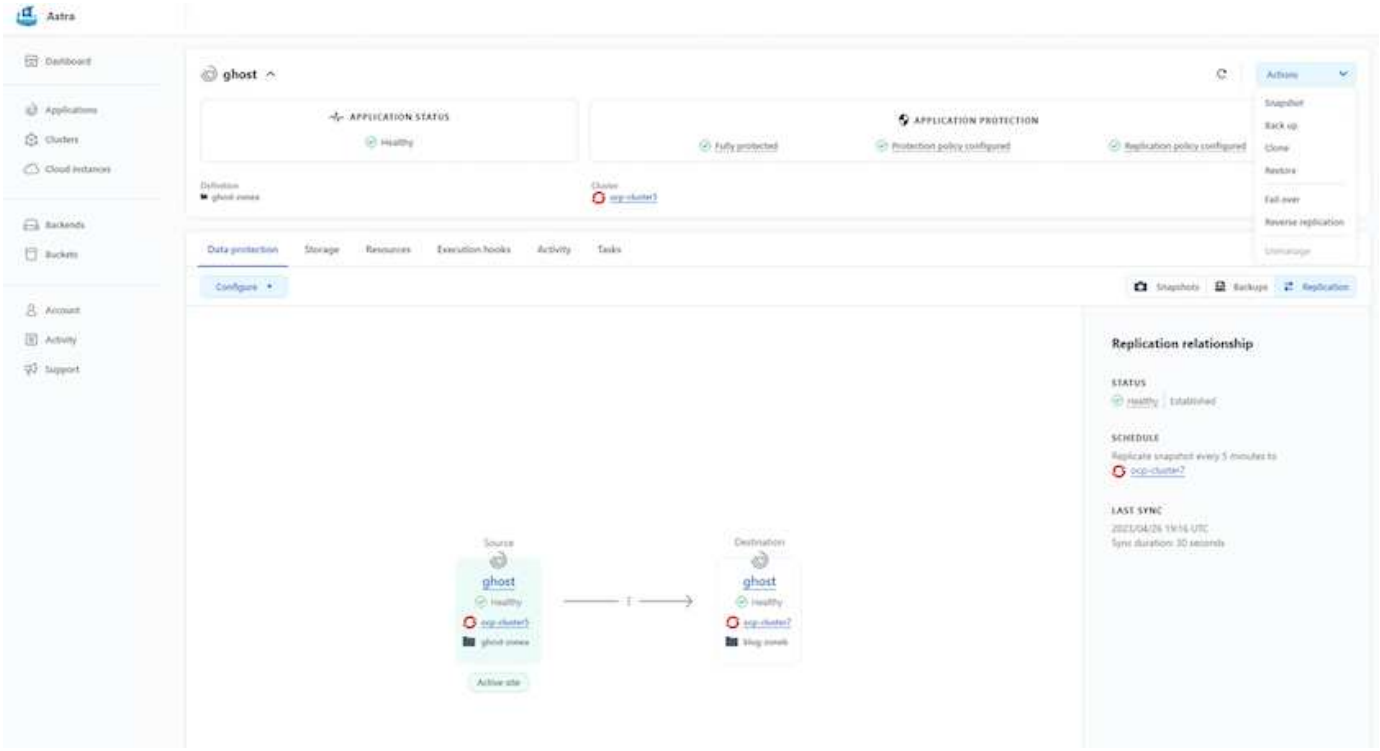
Enlace de ejecución de ejemplo para la instantánea previa de una aplicación de redis.



Replicación con ACC

Para la protección regional o para una solución de objetivo de punto de recuperación y objetivo de tiempo de recuperación bajos, una aplicación se puede replicar en otra instancia de Kubernetes que se ejecute en otro sitio, preferiblemente en otra región. ACC utiliza SnapMirror asíncrono de ONTAP con un objetivo de punto de recuperación mínimo de 5 minutos. Consulte "aquí" Para obtener instrucciones de configuración de SnapMirror.

SnapMirror con ACC



los controladores de almacenamiento san y nas económicos no admiten la función de replicación. Consulte "aquí" para obtener más detalles.

Vídeo de demostración:

"Vídeo de demostración de la recuperación de desastres con Astra Control Center"

Protección de datos con Astra Control Center

Hay disponible más información sobre las funciones de protección de datos de Astra Control Center "aquí"

Recuperación ante desastres (conmutación por error y conmutación tras recuperación con replicación) con ACC

Utilizar Astra Control para la conmutación al nodo de respaldo y la conmutación de retorno tras recuperación de aplicaciones

Migración de datos mediante Astra Control Center

Esta página muestra las opciones de migración de datos para las cargas de trabajo de contenedor en clústeres de Red Hat OpenShift con Astra Control Center (ACC). Concretamente, los clientes pueden utilizar ACC para mover algunas cargas de trabajo seleccionadas o todas las cargas de trabajo de sus centros de datos en las instalaciones al cloud; clonar sus aplicaciones al cloud para fines de pruebas o trasladarlas del centro de datos al cloud

Migración de datos

Para migrar una aplicación de un entorno a otro, puede utilizar una de las siguientes funciones de ACC:

- **replicación**

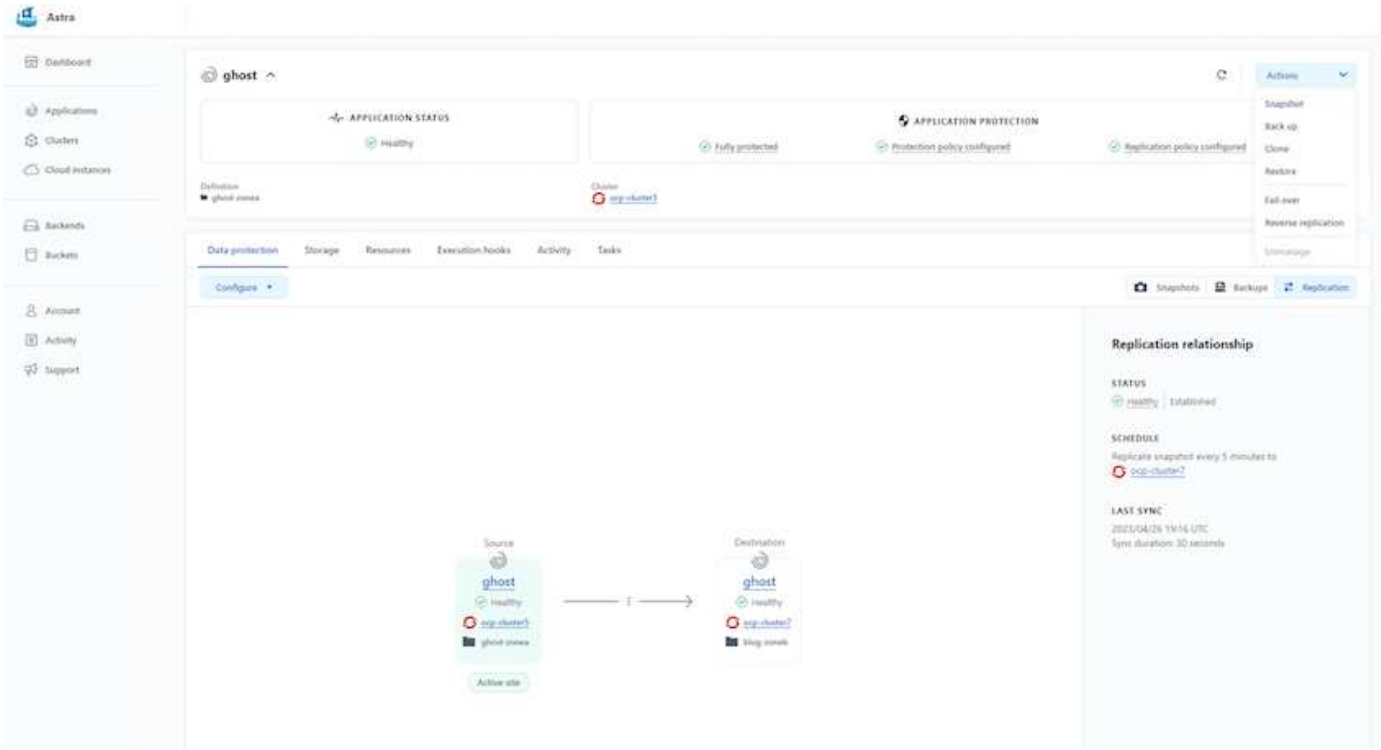
- **copia de seguridad y restauración**
- **clone**

Consulte la "sección de protección de datos" para las opciones **replicación y copia de seguridad y restauración**.

Consulte "aquí" para más detalles acerca de **clonación**.

> La función de replicación de Astra solo se admite con Trident Container Storage Interface (CSI). Sin embargo, la replicación no es compatible con los controladores de economía nas y san.

Realización de la replicación de datos mediante ACC



Soluciones de multicloud híbrido de NetApp para cargas de trabajo de contenedores de Red Hat OpenShift

Descripción general

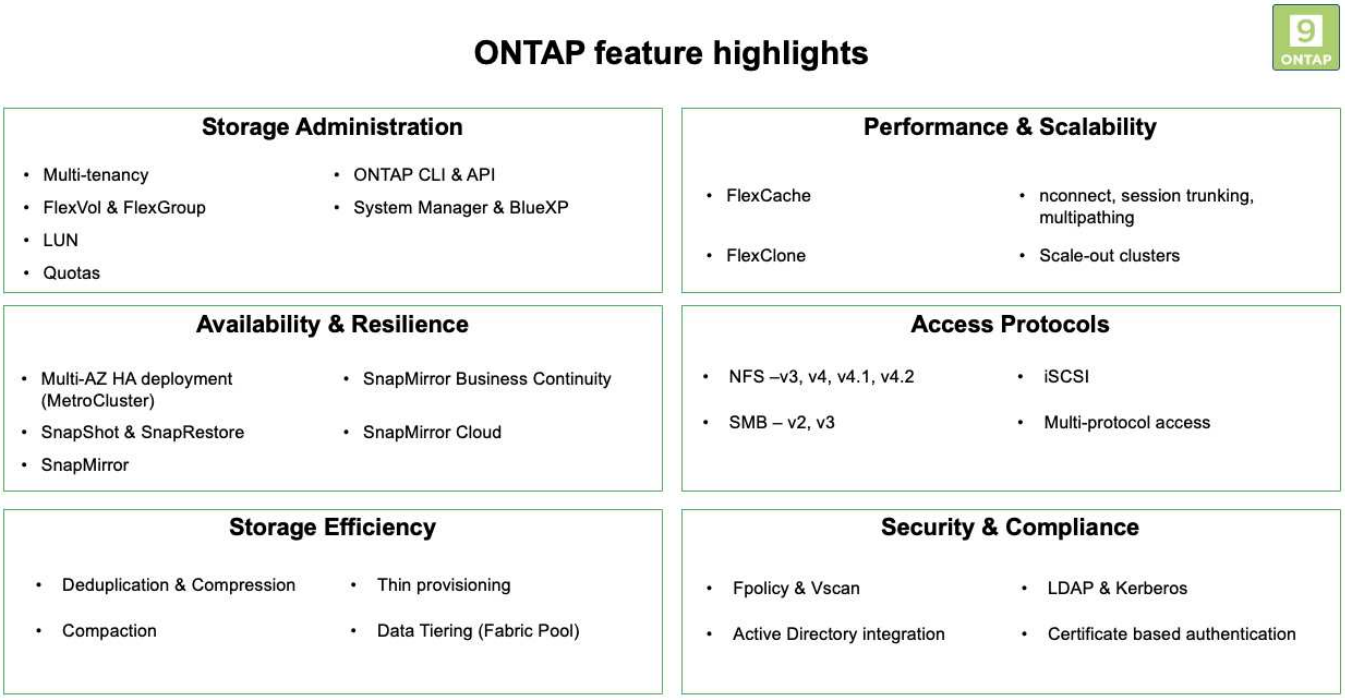
NetApp está viendo un aumento significativo en los clientes que modernizan sus aplicaciones empresariales heredadas y crean nuevas aplicaciones con contenedores y plataformas de orquestación creadas en torno a Kubernetes. Red Hat OpenShift Container Platform es un ejemplo que consideramos adoptado por muchos de nuestros clientes.

A medida que más y más clientes empiezan a adoptar contenedores dentro de sus empresas, NetApp está perfectamente posicionada para poder dar respuesta a las necesidades de almacenamiento persistente de sus aplicaciones con estado y las necesidades de gestión de datos clásicas como la protección de datos, la seguridad de datos y la migración de datos. Sin embargo, estas necesidades se satisfacen utilizando diferentes estrategias, herramientas y métodos.

Las opciones de almacenamiento basado en ONTAP de NetApp que se enumeran a continuación, ofrecen

seguridad, protección de datos, fiabilidad y flexibilidad para implementaciones de contenedores y Kubernetes.

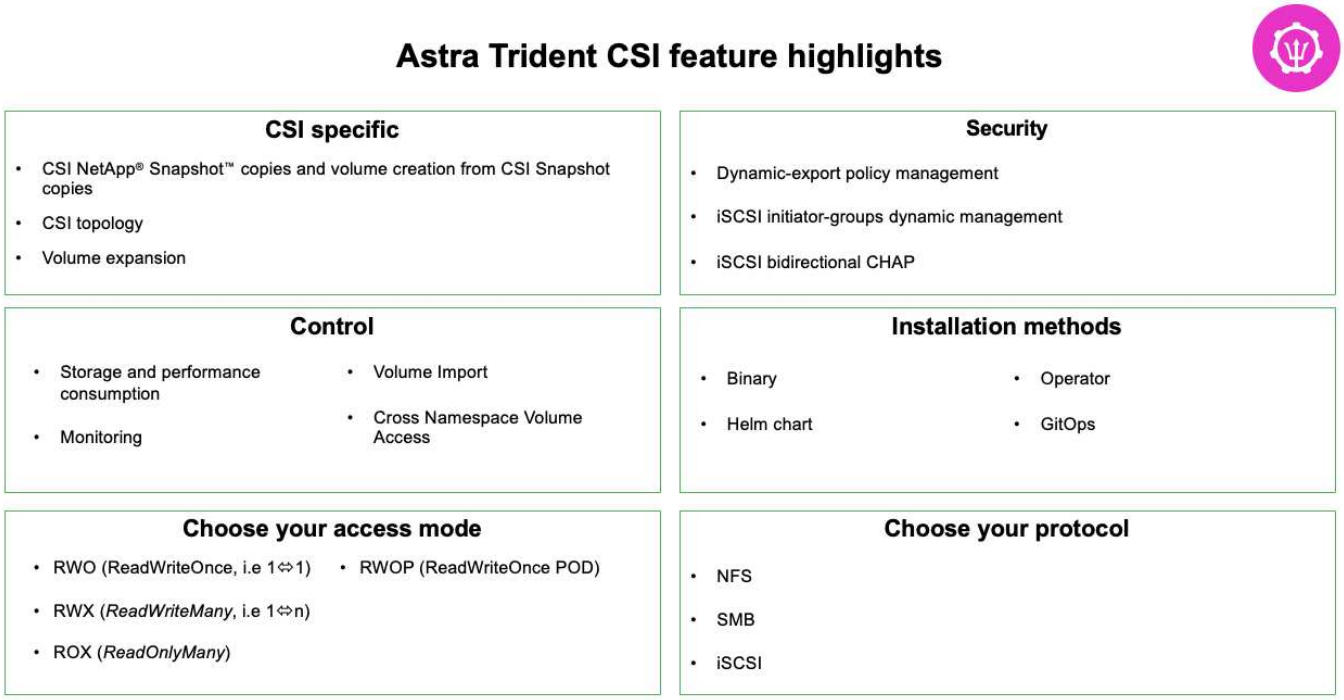
- Almacenamiento autogestionado en las instalaciones:
  - Almacenamiento estructural (FAS) de NetApp, cabinas All Flash FAS (AFF), cabina All SAN (ASA) y ONTAP Select
- Almacenamiento gestionado por el proveedor en las instalaciones:
  - NetApp Keystone proporciona almacenamiento como servicio (STaaS)
- Almacenamiento autogestionado en el cloud:
  - Cloud Volumes ONTAP (CVO) de NetApp proporciona almacenamiento autogestionado en los proveedores a hiperescala
- Almacenamiento en el cloud gestionado por el proveedor:
  - Cloud Volumes Service para Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx para ONTAP de NetApp ofrecen un almacenamiento totalmente gestionado en los proveedores a hiperescala



NetApp BlueXP le permite gestionar todos sus activos de almacenamiento y datos desde una única interfaz o plano de control.

Puedes usar BlueXP para crear y administrar almacenamiento en nube (por ejemplo, Cloud Volumes ONTAP y Azure NetApp Files), para mover, proteger y analizar datos, y para controlar muchos dispositivos de almacenamiento on-premises y en la periferia.

Astra Trident de NetApp es un orquestador de almacenamiento compatible con CSI que permite consumir almacenamiento persistente de forma rápida y sencilla, respaldado por diversas opciones de almacenamiento de NetApp mencionadas anteriormente. Es un software de código abierto que tiene soporte y mantenimiento de NetApp.



Las cargas de trabajo de contenedores vitales para el negocio necesitan más que volúmenes persistentes. Sus requisitos de gestión de datos requieren la protección y la migración de los objetos de aplicaciones kubernetes también.

> 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, PVCs, despliegues, servicios - objetos de configuración personalizados como mapas de configuración y secretos - datos persistentes como copias Snapshot, copias de seguridad, clones - recursos personalizados como CRS y CRD

Astra Control de NetApp, disponible como software totalmente gestionado y autogestionado, proporciona orquestación para una gestión de datos de aplicaciones sólida. Consulte la "Documentación de Astra" Para obtener más información sobre la familia de productos Astra.

Esta documentación de referencia proporciona la validación de la migración y la protección de aplicaciones basadas en contenedores, puestas en marcha en la plataforma de contenedores RedHat OpenShift, mediante Astra Control Center de NetApp. Además, la solución proporciona detalles de alto nivel para la implementación y el uso de Red Hat Advanced Cluster Management (ACM) para la gestión de las plataformas de contenedores. En el documento también se destacan los detalles de la integración del almacenamiento de NetApp con las plataformas de contenedor Red Hat OpenShift mediante el aprovisionador CSI de Astra Trident. Astra Control Center se pone en marcha en el clúster de concentradores y se utiliza para gestionar las aplicaciones de contenedores y su ciclo de vida de almacenamiento persistente. Por último, proporciona una solución de replicación y conmutación al nodo de respaldo y conmutación de retorno tras recuperación para cargas de trabajo de contenedores en clústeres de Red Hat OpenShift gestionados en AWS (ROSA) utilizando Amazon FSx para NetApp ONTAP (FSxN) como almacenamiento persistente.

Solución de NetApp con cargas de trabajo de la plataforma de contenedores Red Hat OpenShift gestionadas en AWS

Solución de NetApp con cargas de trabajo de la plataforma de contenedores Red Hat OpenShift gestionadas en AWS

Los clientes pueden haber «nacido en el cloud» o pueden estar en un momento en su

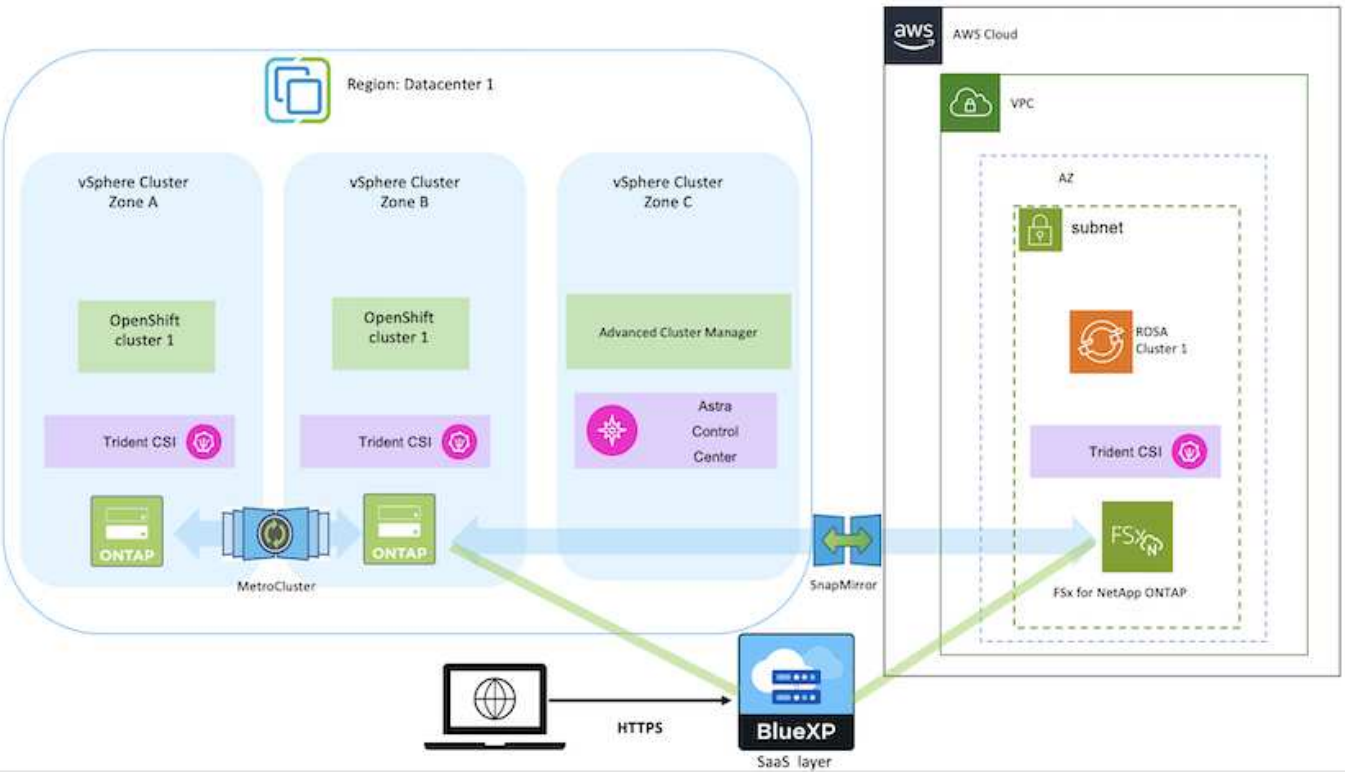
proceso de modernización cuando estén listos para mover algunas cargas de trabajo selectas o todas las cargas de trabajo de sus centros de datos al cloud. Pueden elegir usar contenedores OpenShift gestionados por proveedores y almacenamiento NetApp gestionado por proveedores en la nube para ejecutar sus cargas de trabajo. Deben planificar e implementar los clústeres de contenedores Managed Red Hat OpenShift (ROSA) en la nube para un entorno de producción adecuado para sus cargas de trabajo de contenedores. Cuando están en el cloud de AWS, también podrían poner en marcha FSx para ONTAP de NetApp para cubrir las necesidades de almacenamiento.

FSX para ONTAP de NetApp ofrece protección de datos, fiabilidad y flexibilidad para las puestas en marcha de contenedores en AWS. Astra Trident actúa como el aprovisionador de almacenamiento dinámico para consumir el almacenamiento FSxN persistente para las aplicaciones con estado de los clientes.

Como ROSA se puede poner en marcha en modo de alta disponibilidad con nodos del plano de control repartidos por varias zonas de disponibilidad, FSx ONTAP también se puede aprovisionar con la opción Multi-AZ que proporciona alta disponibilidad y protección frente a fallos de AZ.

No hay cargos de transferencia de datos al acceder a un sistema de archivos Amazon FSx desde la zona de disponibilidad (AZ) preferida del sistema de archivos. Para obtener más información sobre los precios, consulte "aquí".

Solución de protección y migración de datos para las cargas de trabajo de contenedores de OpenShift

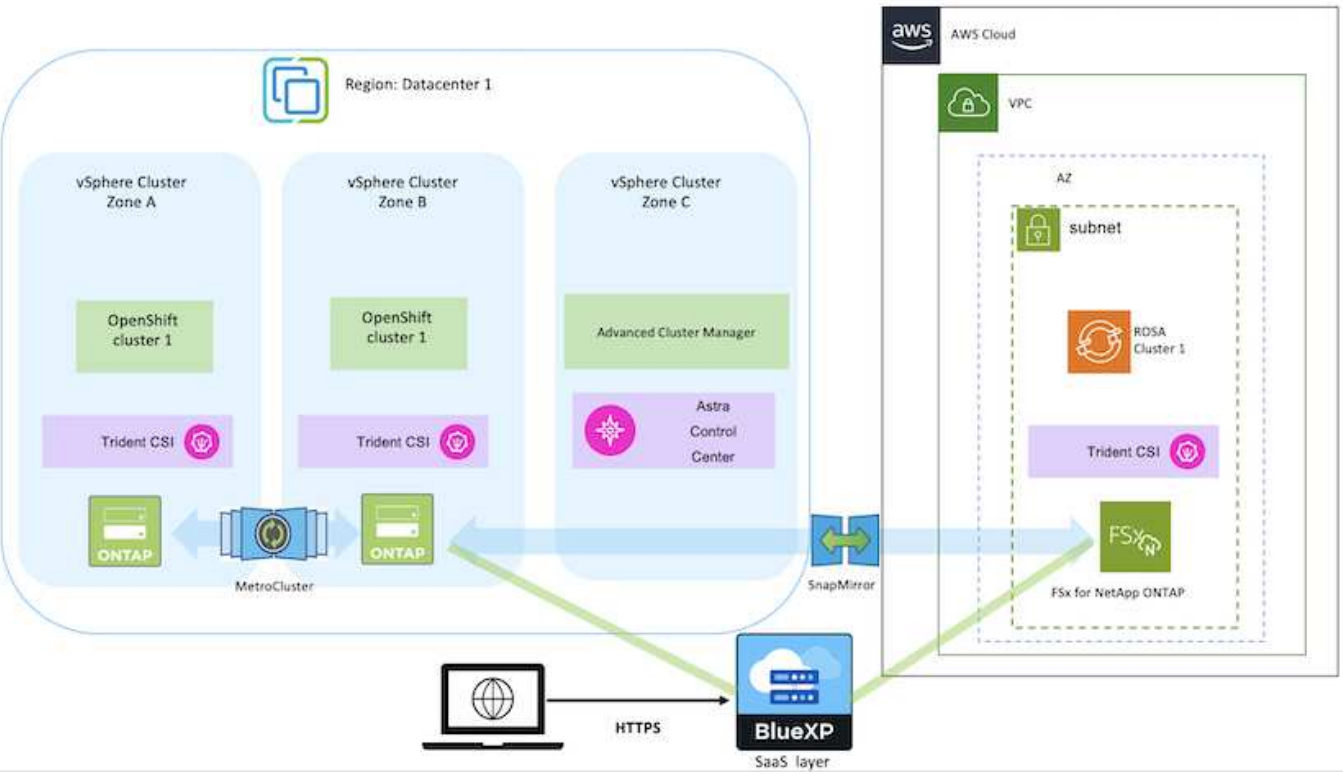


Implemente y configure la plataforma Managed Red Hat OpenShift Container en AWS

En esta sección se describe un flujo de trabajo de alto nivel de configuración de los clústeres gestionados de Red Hat OpenShift en AWS (ROSA). Muestra el uso de Managed FSx para ONTAP de NetApp (FSxN) como back-end de almacenamiento por

parte de Astra Trident para proporcionar volúmenes persistentes. Encontrará más detalles sobre la implementación de FSxN en AWS mediante BlueXP. Además, se incluyen más detalles sobre el uso de BlueXP y OpenShift GitOps (Argo CD) para realizar actividades de protección y migración de datos para las aplicaciones con estado en los clústeres de ROSA.

A continuación se muestra un diagrama que muestra los clústeres ROSA implementados en AWS y utilizando FSxN como almacenamiento back-end.



Esta solución se verificó mediante el uso de dos clústeres ROSA en dos VPC en AWS. Cada clúster ROSA se integró con FSxN mediante Astra Trident. Hay varias formas de implementar los clusters ROSA y FSxN en AWS. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

El proceso de configuración puede dividirse en los siguientes pasos:

Instale los clusters ROSA

- Cree dos VPC y configure la conectividad entre iguales entre los VPC.
- Consulte "aquí" Para obtener instrucciones para instalar los clusters ROSA.

Instale FSxN

- Instala FSxN en los PC de BlueXP. Consulte "aquí" Para la creación de cuenta de BlueXP y para comenzar a usarla. Consulte "aquí" Para instalar FSxN. Consulte "aquí" Para crear un conector en AWS para gestionar FSxN.
- Implemente FSxN con AWS. Consulte "aquí" Para la puesta en marcha mediante la consola de AWS.

Instalación de Trident en clústeres ROSA (usando el gráfico Helm)

- Use el gráfico Helm para instalar Trident en clústeres ROSA. url para el diagrama Helm: https://netapp.github.io/trident-helm-chart

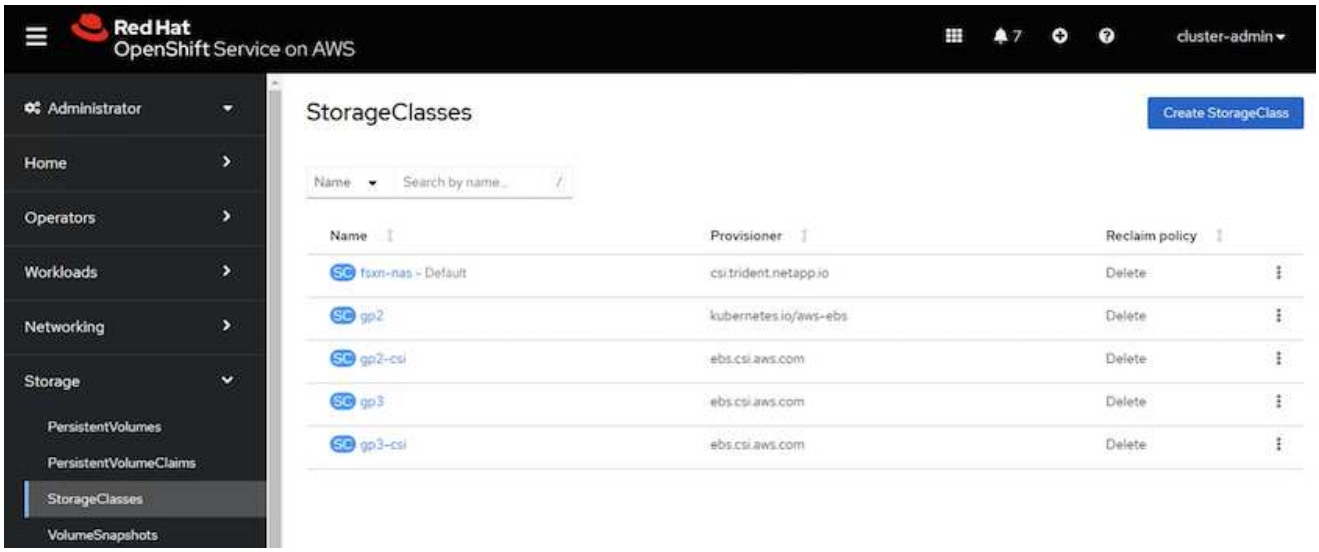
Integración de FSxN con Astra Trident para clústeres ROSA

OpenShift GitOps se puede utilizar para implementar Astra Trident CSI en todos los clústeres gestionados 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 back-end con Trident (para FSxN)

- Consulte "aquí" para obtener detalles sobre la creación del back-end y la clase de almacenamiento.
- Convierta la clase de almacenamiento creada para FsxN con Trident CSI por defecto en OpenShift Console. Consulte la captura de pantalla a continuación:



Desplegar una aplicación usando OpenShift GitOps (CD de Argo)

- Instale el operador OpenShift GitOps en el clúster. Consulte las instrucciones "aquí".
- Configure una nueva instancia de CD de Argo para el cluster. Consulte las instrucciones "aquí".

Abre la consola del CD de Argo e implementa una aplicación. Como ejemplo, puedes implementar una aplicación Jenkins usando Argo CD con un Helm Chart. Al crear la aplicación, se proporcionaron los siguientes detalles: Proyecto: Clúster predeterminado: https://kubernetes.default.svcEspacio de nombres: Jenkins La url del diagrama Helm: https://charts.bitnami.com/bitnami

Parámetros del timón: Global.storageClass: Fsxn-nas

Protección de datos

Esta página muestra las opciones de protección de datos para clústeres de Red Hat OpenShift gestionados en AWS (ROSA) mediante Astra Control Service. Astra Control Service (ACS) proporciona una interfaz gráfica de usuario fácil de usar con la que puedes añadir clústeres, definir aplicaciones en ellas y realizar actividades de gestión de datos para aplicaciones. También se puede acceder a las funciones de ACS mediante una API que permite la automatización de flujos de trabajo.

Astra Trident de NetApp es el motor de Astra Control (ACS o ACC). Astra Trident integra varios tipos de clústeres de Kubernetes, como Red Hat OpenShift, EKS, AKS, SUSE Rancher, Anthos, etc. con diversos tipos de almacenamiento de NetApp ONTAP, como FAS/AFF, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files y Amazon FSx para NetApp ONTAP.

En esta sección se proporcionan detalles sobre las siguientes opciones de protección de datos mediante ACS:

- Un vídeo que muestra la copia de seguridad y restauración de una aplicación ROSA que se ejecuta en una región y la restauración en otra.
- Un vídeo que muestra la instantánea y la restauración de una aplicación ROSA.
- Detalles paso a paso de la instalación de un clúster ROSA, Amazon FSx para NetApp ONTAP, mediante Astra Trident de NetApp para su integración con el back-end de almacenamiento, la instalación de una aplicación posgresql en un clúster ROSA, el uso de ACS para crear una instantánea de la aplicación y la restauración de la aplicación a partir de ella.
- Un blog en el que se muestran detalles paso a paso de la creación y restauración a partir de una instantánea para una aplicación mysql en un clúster ROSA con FSx para ONTAP mediante ACS.

Copia de seguridad/Restaurar desde copia de seguridad

El siguiente vídeo muestra la copia de seguridad de una aplicación ROSA que se ejecuta en una región y se restaura en otra región.

FSX NetApp ONTAP para el servicio Red Hat OpenShift en AWS

Snapshot/Restaurar de la instantánea

En el siguiente vídeo se muestra la toma de una instantánea de una aplicación ROSA y la restauración de la instantánea después.

Snapshot/Restore para aplicaciones en Red Hat OpenShift Service en clústeres de AWS (ROSA) con almacenamiento de Amazon FSx para NetApp ONTAP

Blog

- "Mediante Astra Control Service para la gestión de datos de aplicaciones en CLÚSTERES ROSA con el almacenamiento de Amazon FSx"

Detalles paso a paso para crear la instantánea y restaurarla a partir de ella

Configuración de requisitos previos

- "Cuenta de AWS"
- "Cuenta de Red Hat OpenShift"
- Usuario de IAM con "permisos apropiados" Para crear y acceder al clúster ROSA
- "CLI DE AWS"
- "ROSA CLI"
- "CLI de OpenShift"(oc)
- VPC con subredes y puertas de enlace y rutas correspondientes
- "ROSA Cluster instalado" En el VPC
- "Amazon FSX para ONTAP de NetApp" Creadas en el mismo VPC
- Acceso al clúster ROSA desde "Consola de nube híbrida de OpenShift"

Siguientes pasos

1. Cree un usuario administrador e inicie sesión en el clúster.

2. Cree un archivo kubeconfig para el cluster.
3. Instale Astra Trident en el clúster.
4. Cree una configuración de back-end, clase de almacenamiento y clase de snapshot con el aprovisionador CSI de Trident.
5. Despliegue una aplicación postgresql en el cluster.
6. Cree una base de datos y agregue un registro.
7. Añada el clúster a ACS.
8. Defina la aplicación en ACS.
9. Cree una instantánea mediante ACS.
10. Suprima la base de datos en la aplicación postgresql.
11. Restaurar desde una instantánea mediante ACS.
12. Verifique que su aplicación se ha restaurado de la instantánea.

1. Cree un usuario administrador e inicie sesión en el clúster

Acceda al clúster ROSA creando un usuario administrador con el siguiente comando : (solo necesita crear un usuario administrador si no creó uno en el momento de la instalación).

```
rosa create admin --cluster=<cluster-name>
```

El comando proporcionará un resultado que se parecerá a la siguiente. Inicie sesión en el clúster mediante el `oc login` el comando proporcionado en la salida.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

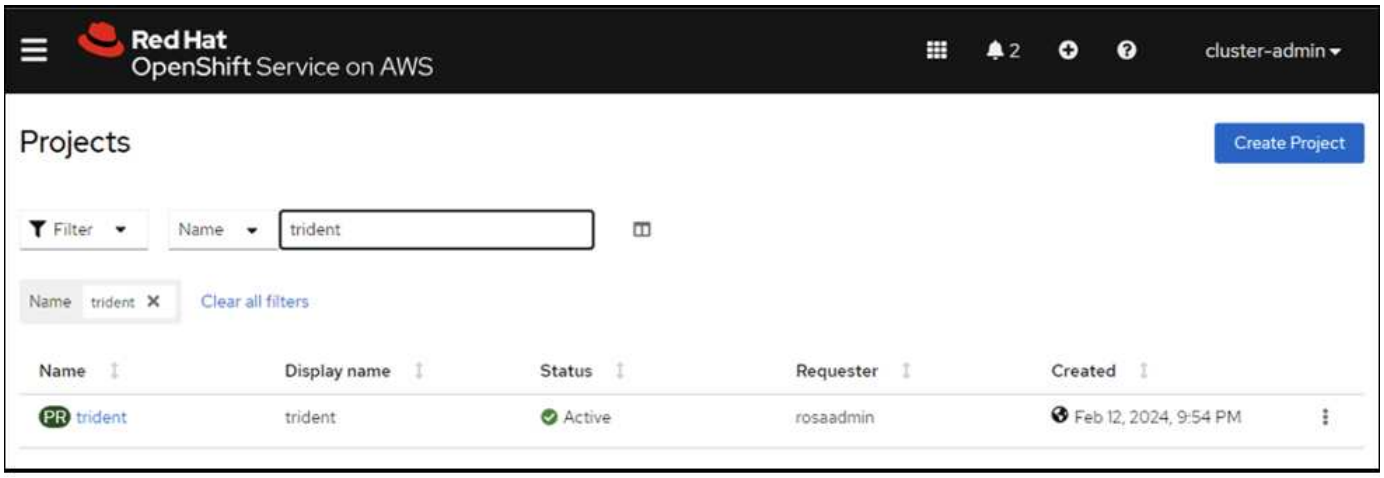
> También puede iniciar sesión en el clúster mediante un token. Si ya creó un usuario administrador en el momento de la creación del clúster, puede iniciar sesión en el clúster desde la consola de Red Hat OpenShift Hybrid Cloud con las credenciales de usuario administrador. A continuación, haciendo clic en la esquina superior derecha donde se muestra el nombre del usuario que ha iniciado sesión, puede obtener el `oc login` comando (token login) para la línea de comandos.

2. Cree un archivo kubeconfig para el cluster

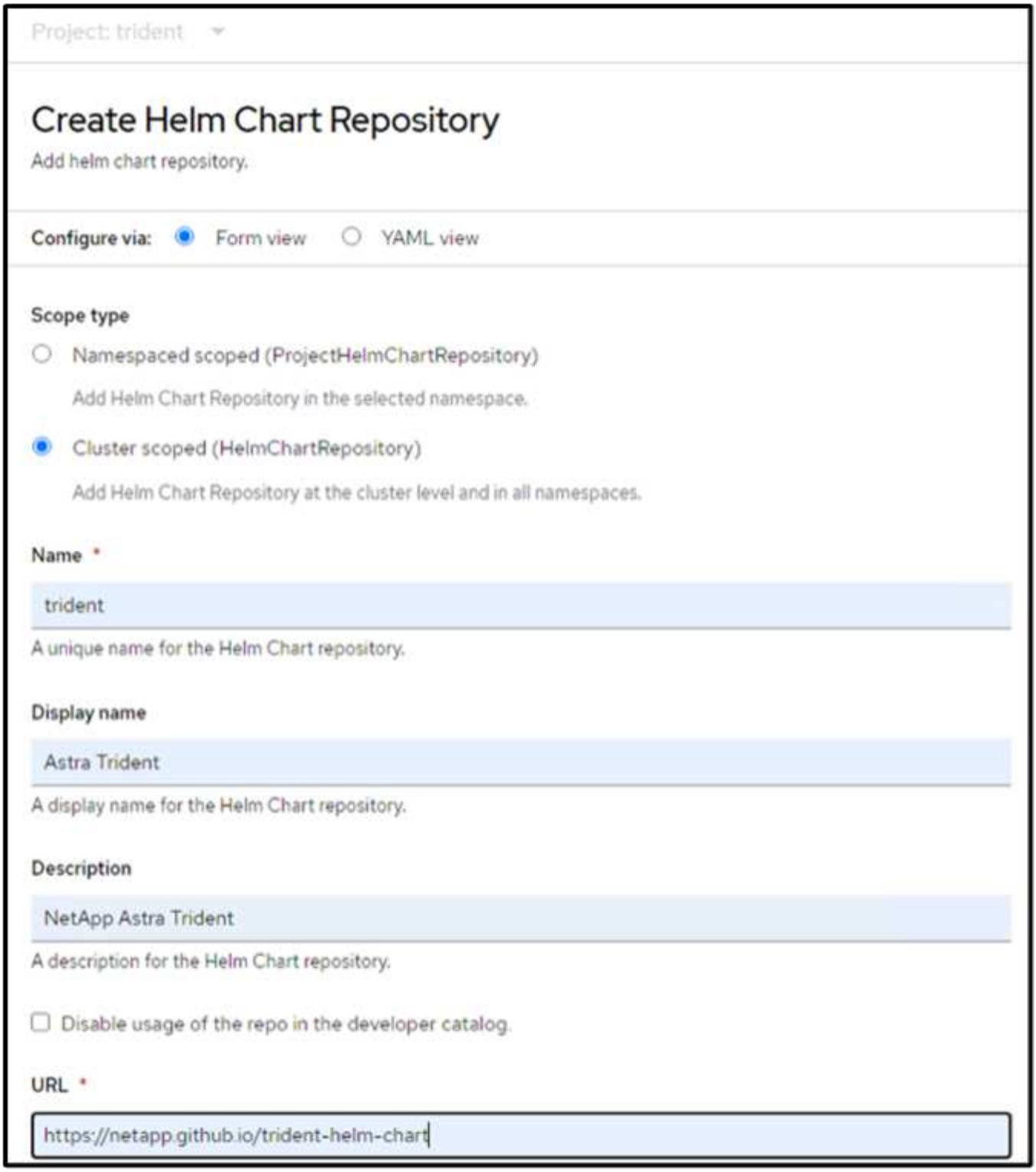
Siga los procedimientos "aquí" Para crear un archivo kubeconfig para el clúster ROSA. Este archivo kubeconfig se utilizará más adelante cuando agregue el clúster a ACS.

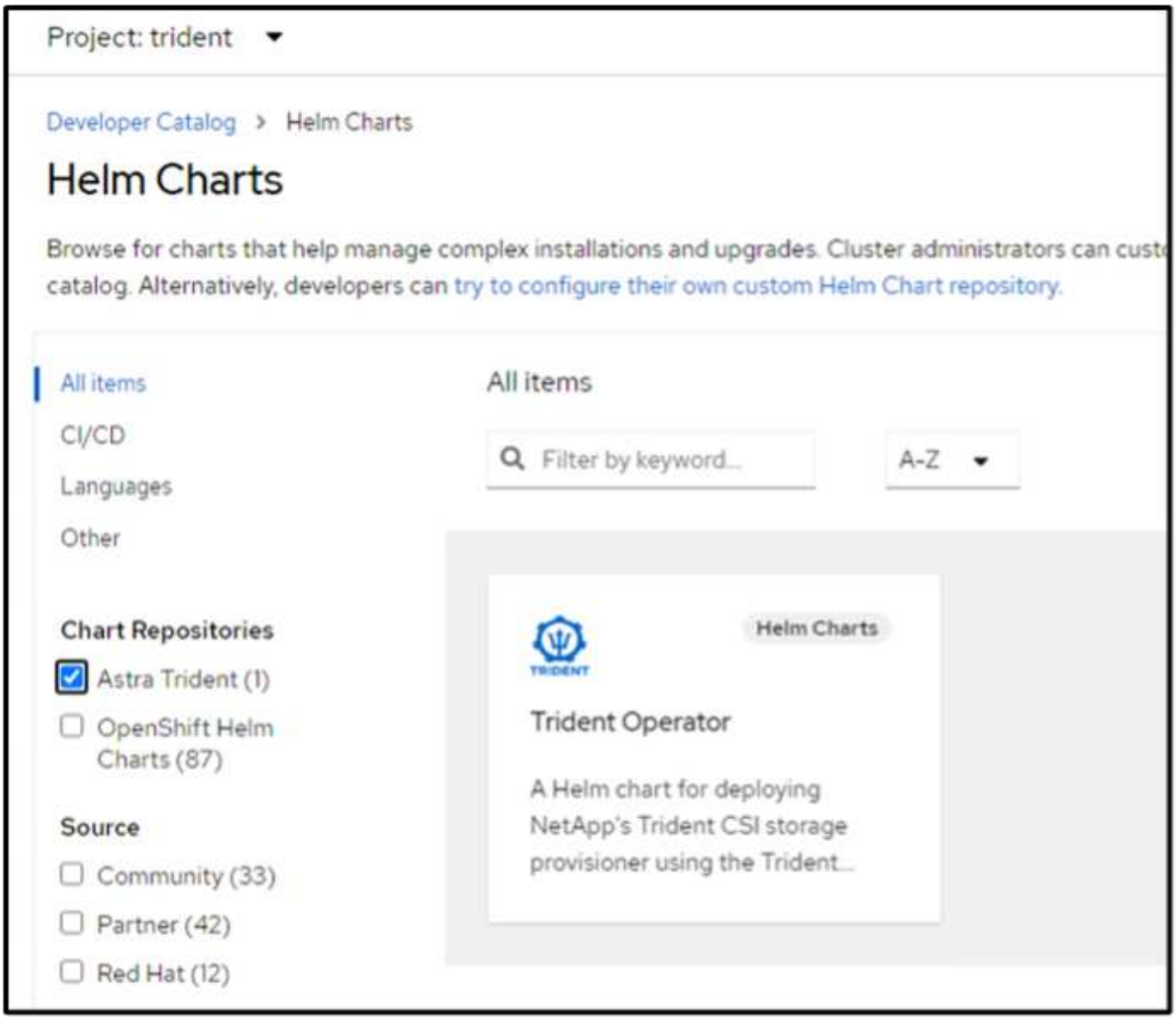
3. Instale Astra Trident en el clúster

Instale Astra Trident (versión más reciente) en el clúster ROSA. Para hacer esto, puede seguir cualquiera de los procedimientos dados "aquí". Para instalar Trident usando helm desde la consola del clúster, cree primero un proyecto denominado Trident.

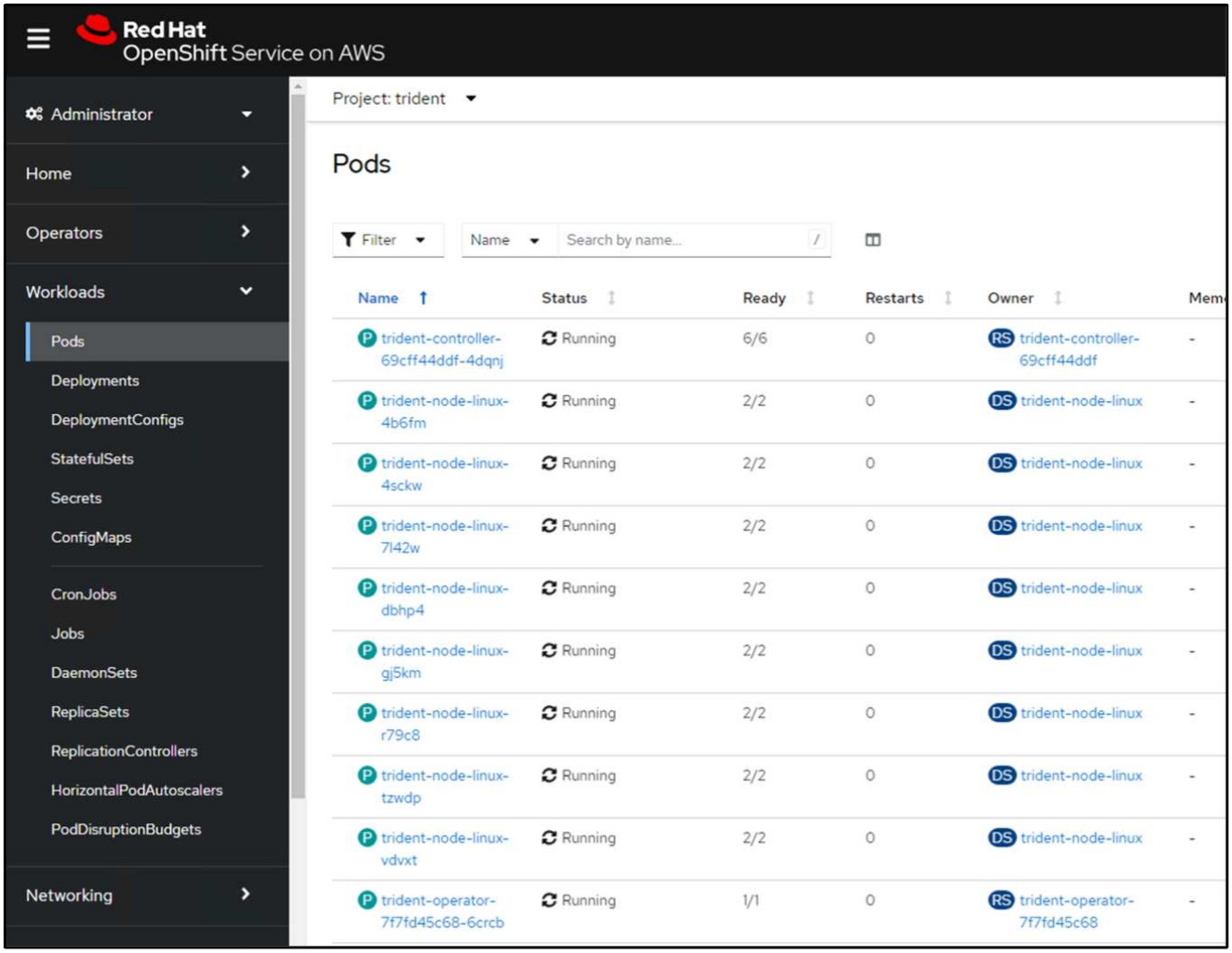


A continuación, desde la vista Desarrollador, cree un repositorio de gráficos Helm. Para utilizar el campo URL `'https://netapp.github.io/trident-helm-chart'`. A continuación, cree una liberación de timón para el operador Trident.


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



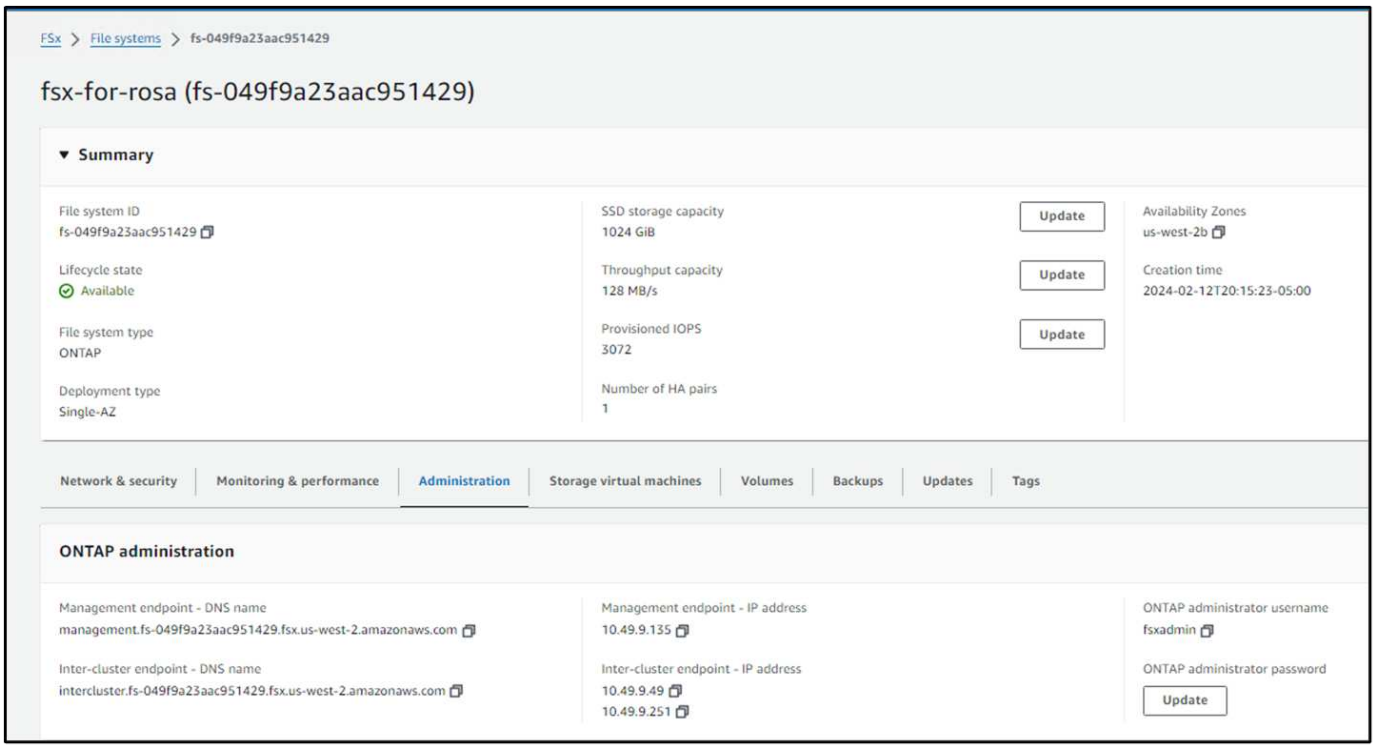
Compruebe que todos los pods de trident se están ejecutando volviendo a la vista Administrador en la consola y seleccionando pods en el proyecto de trident.



4. Cree una configuración de backend, clase de almacenamiento y clase de snapshot usando el aprovisionador CSI de Trident

Utilice los archivos yaml que se muestran a continuación para crear un objeto backend trident, un objeto de clase de almacenamiento y el objeto Volumesnapshot. Asegúrese de proporcionar las credenciales a su sistema de archivos Amazon FSx para NetApp ONTAP que creó, la LIF de gestión y el nombre Vserver de su sistema de archivos en la configuración yaml para el backend. Para obtener esos detalles, ve a la consola de AWS para Amazon FSx y selecciona el sistema de archivos, navega a la pestaña Administración. También, haga clic en Actualizar para establecer la contraseña del `fsxadmin` usuario.

Puede utilizar la línea de comandos para crear los objetos o crearlos con los archivos yaml desde la consola de la nube híbrida.



Configuración de backend Trident

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

Clase de almacenamiento

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

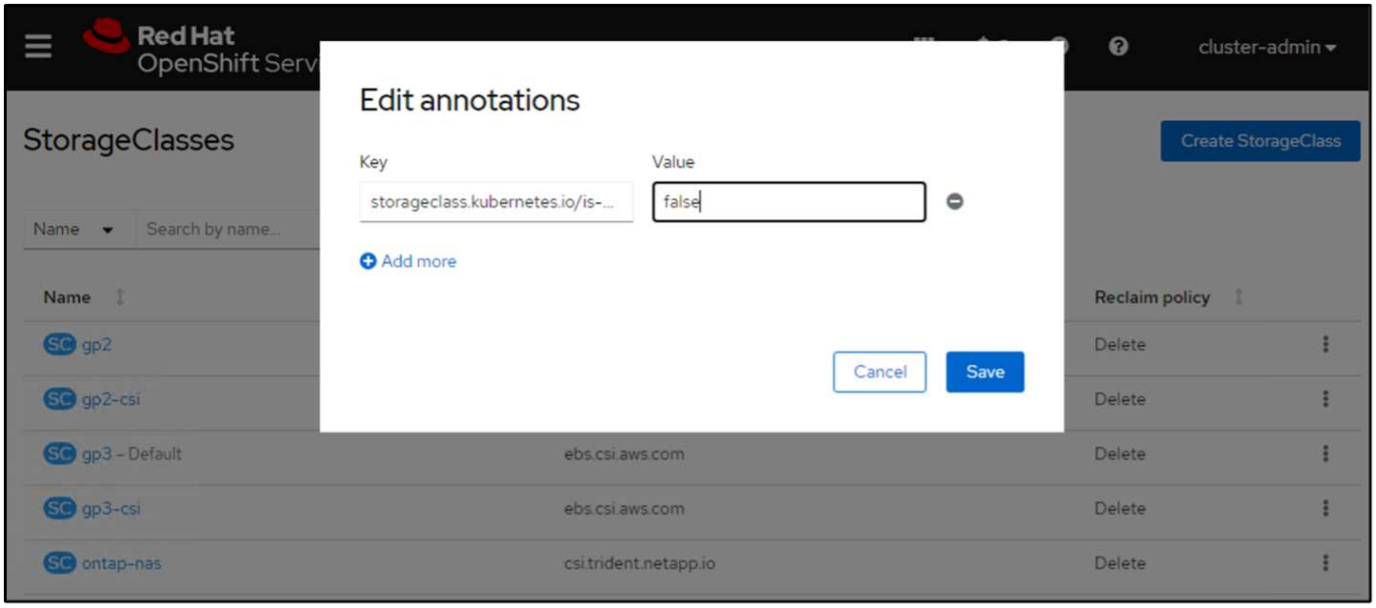
clase de instantánea

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Verifique que el back-end, la clase storage y los objetos trident-snapshotclass se han creado utilizando los comandos que se muestran a continuación.

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

En este momento, una importante modificación que hay que realizar es establecer ontap-nas como la clase de almacenamiento predeterminada en lugar de GP3 para que la aplicación postgresql que ponga en marcha más adelante pueda utilizar la clase de almacenamiento predeterminada. En la consola de OpenShift de su clúster, en Storage seleccione StorageClasses. Edite la anotación de la clase predeterminada actual como false y añada la anotación storageclass.kubernetes.io/is-default-class establecida como true para la clase de almacenamiento ontap-nas.



5. Implementar una aplicación postgresql en el clúster

Puede desplegar la aplicación desde la línea de comandos de la siguiente manera:

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

Si no ve los pods de la aplicación en ejecución, es posible que haya un error debido a las restricciones del contexto de seguridad.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                    TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)    AGE
service/postgresql      ClusterIP   172.30.245.50  <none>        5432/TCP   12m
service/postgresql-hl   ClusterIP   None           <none>        5432/TCP   12m

NAME                          READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer   persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate       statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate           statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

Corrija el error editando `runAsUser` y.. `fsGroup` campos de la `statefuleset.apps/postgresql` objeto con el uid que se encuentra en la salida del `oc get project` comando como se muestra a continuación.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

La aplicación de postgresql debería ejecutar y utilizar volúmenes persistentes respaldados por Amazon FSx para el almacenamiento de NetApp ONTAP.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

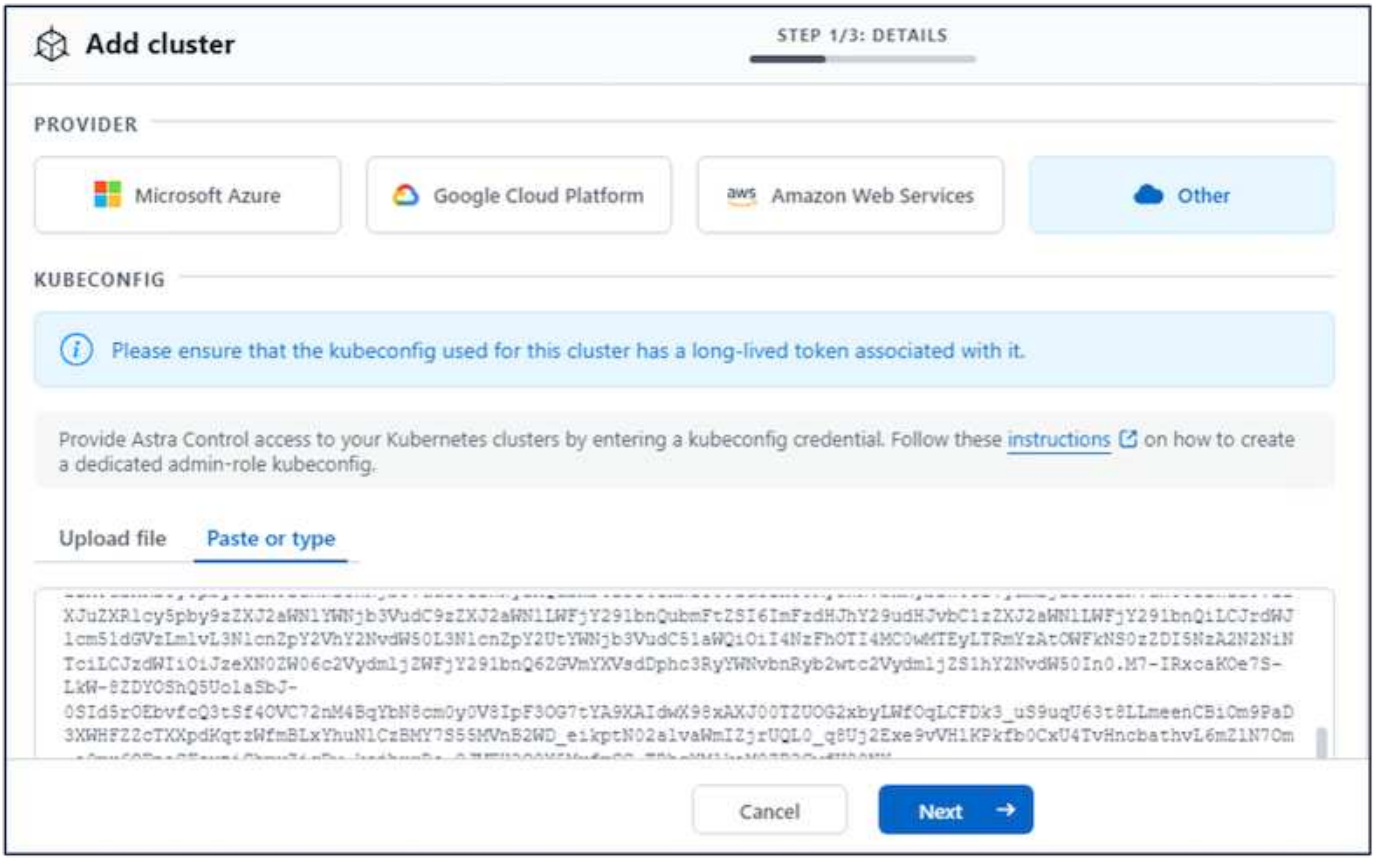
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6. Crear una base de datos y agregar un registro

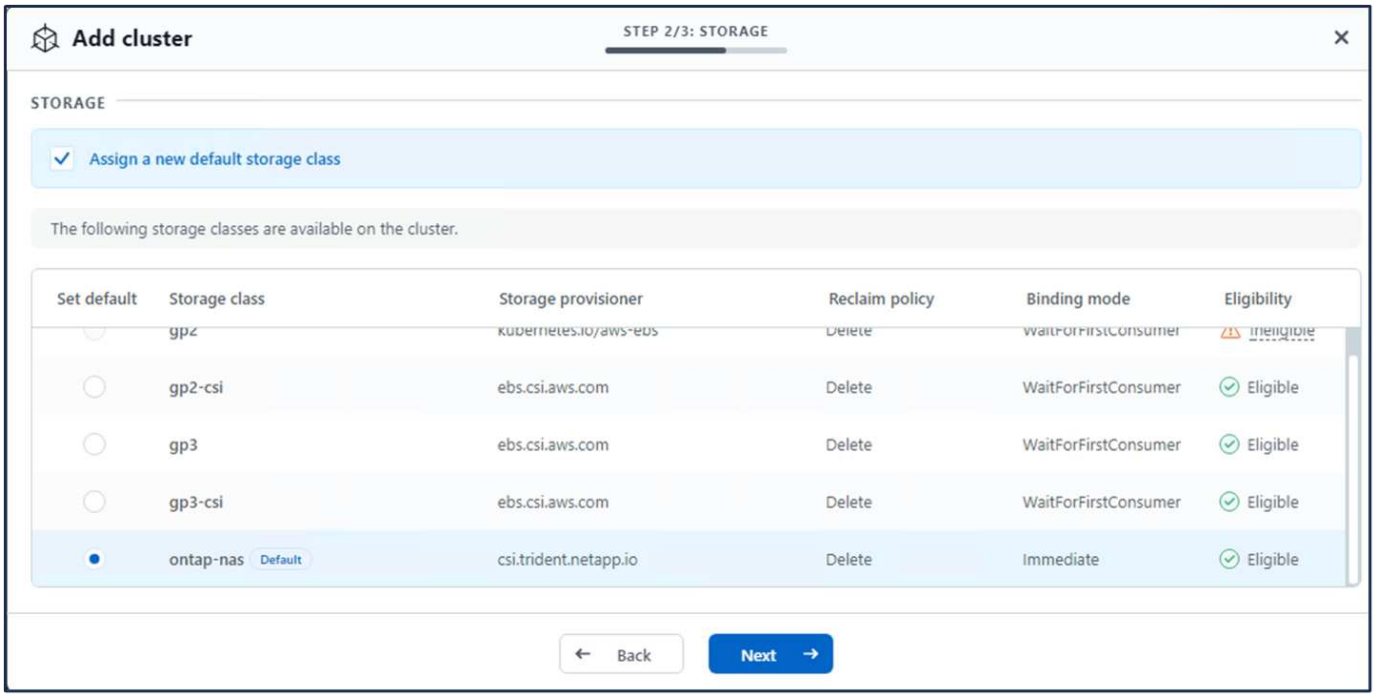
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7. Agregue el clúster a ACS

Inicie sesión en ACS. Seleccione cluster y haga clic en Add. Seleccione Otro y cargue o pegue el archivo kubeconfig.



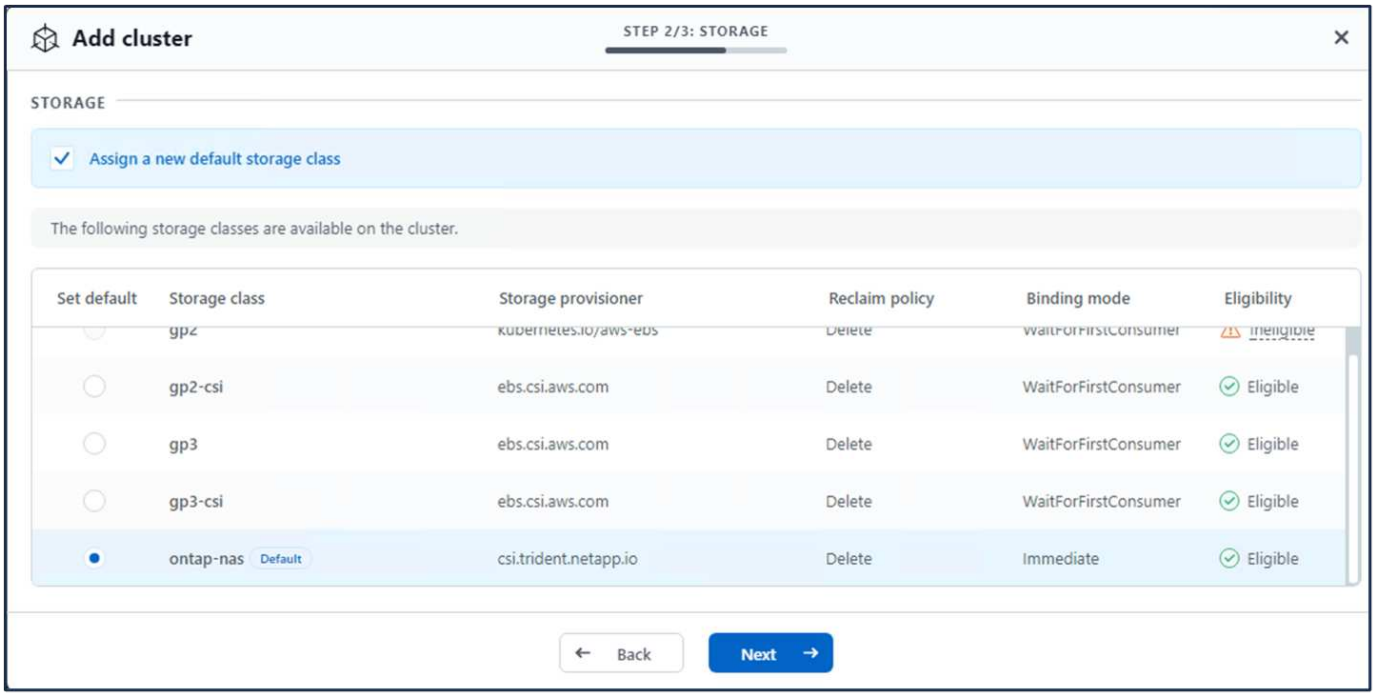
Haga clic en **Next** y seleccione ontap-nas como la clase de almacenamiento predeterminada para ACS. Haga clic en **Siguiente**, revise los detalles y **Agregar** el clúster.



8. Defina la aplicación en ACS

Defina la aplicación postgresql en ACS. En la página de destino, selecciona **Aplicaciones**, **Definir** y rellena los detalles apropiados. Haga clic en **Siguiente** un par de veces, revise los detalles y haga clic en **Definir**. La

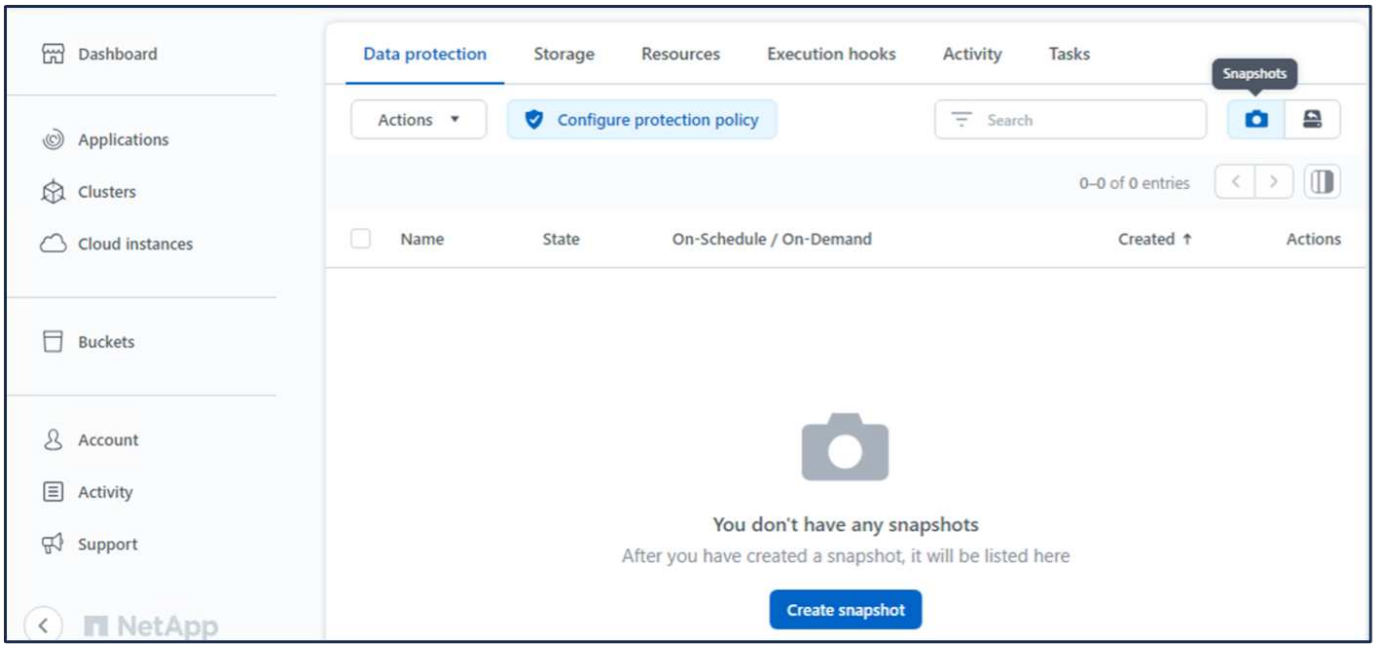
aplicación se agrega a ACS.

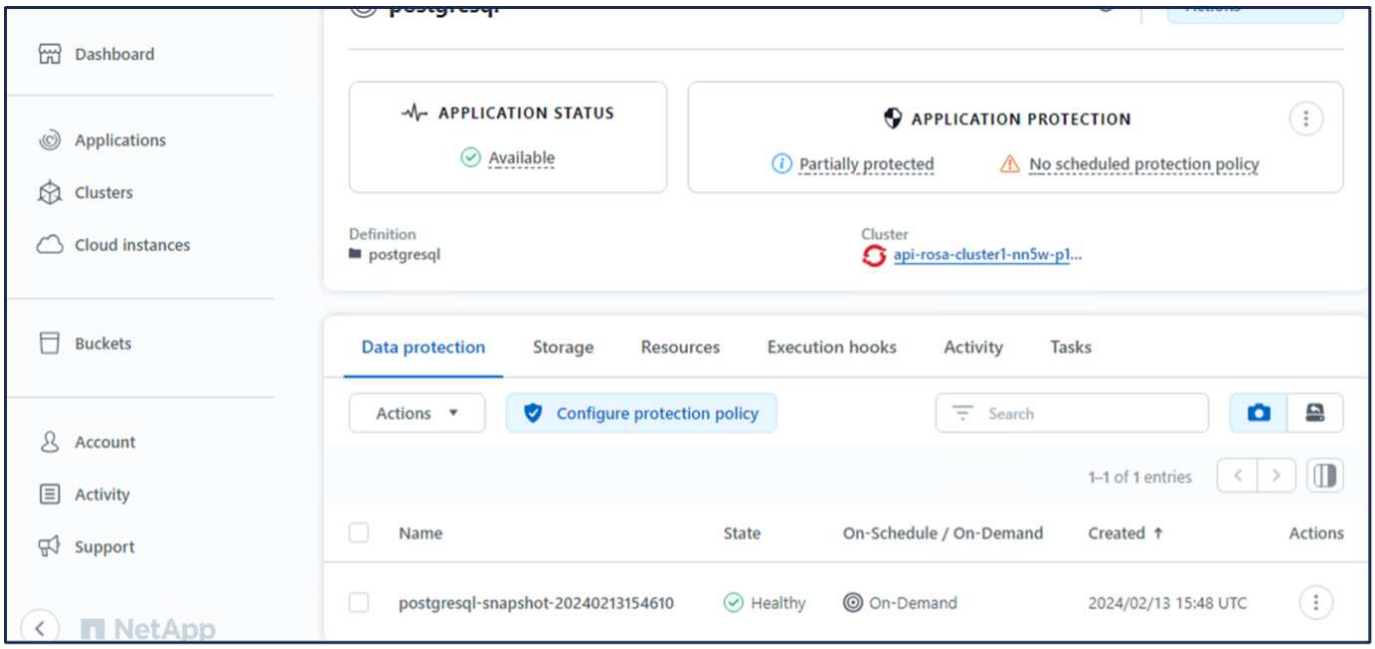


9. Cree una instantánea con ACS

Hay muchas maneras de crear una instantánea en ACS. Puede seleccionar la aplicación y crear una instantánea desde la página que muestra los detalles de la aplicación. Puede hacer clic en Crear snapshot para crear una snapshot bajo demanda o configurar una política de protección.

Cree una instantánea bajo demanda simplemente haciendo clic en **Crear instantánea**, proporcionando un nombre, revisando los detalles y haciendo clic en **Instantánea**. El estado de la Snapshot cambia a correcto una vez que se completa la operación.





10. Elimine la base de datos en la aplicación postgresql

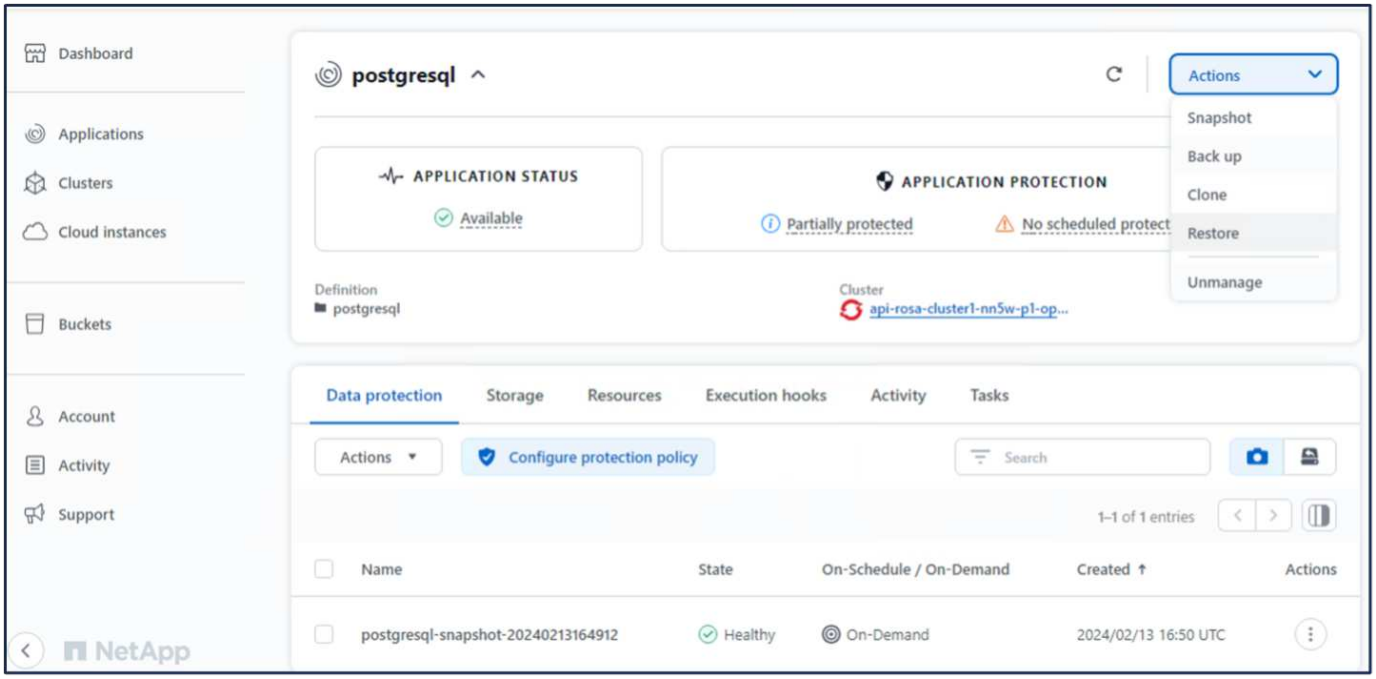
Vuelva a conectarse a postgresql, enumere las bases de datos disponibles, suprima la que creó anteriormente y vuelva a listar para asegurarse de que la base de datos se ha eliminado.

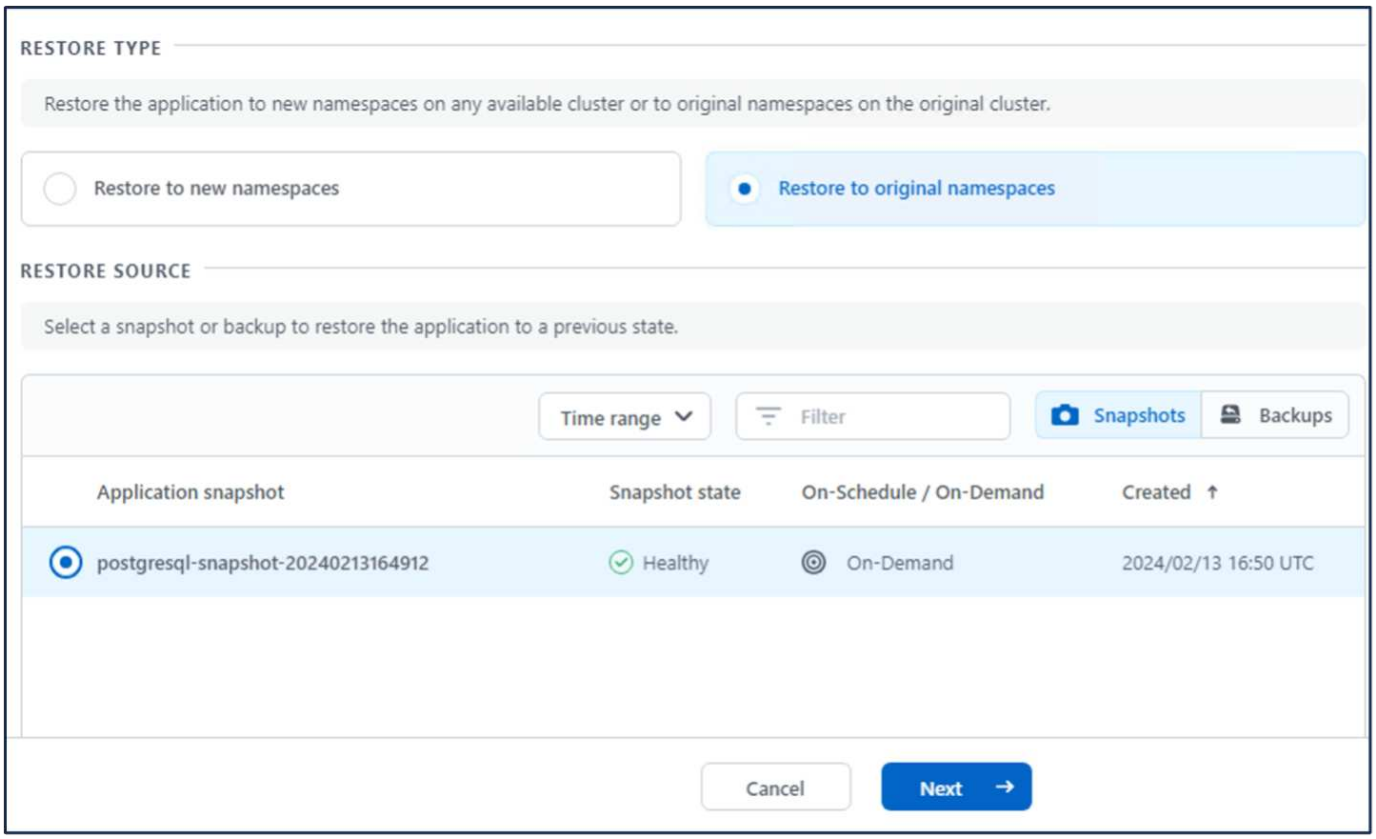
```
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

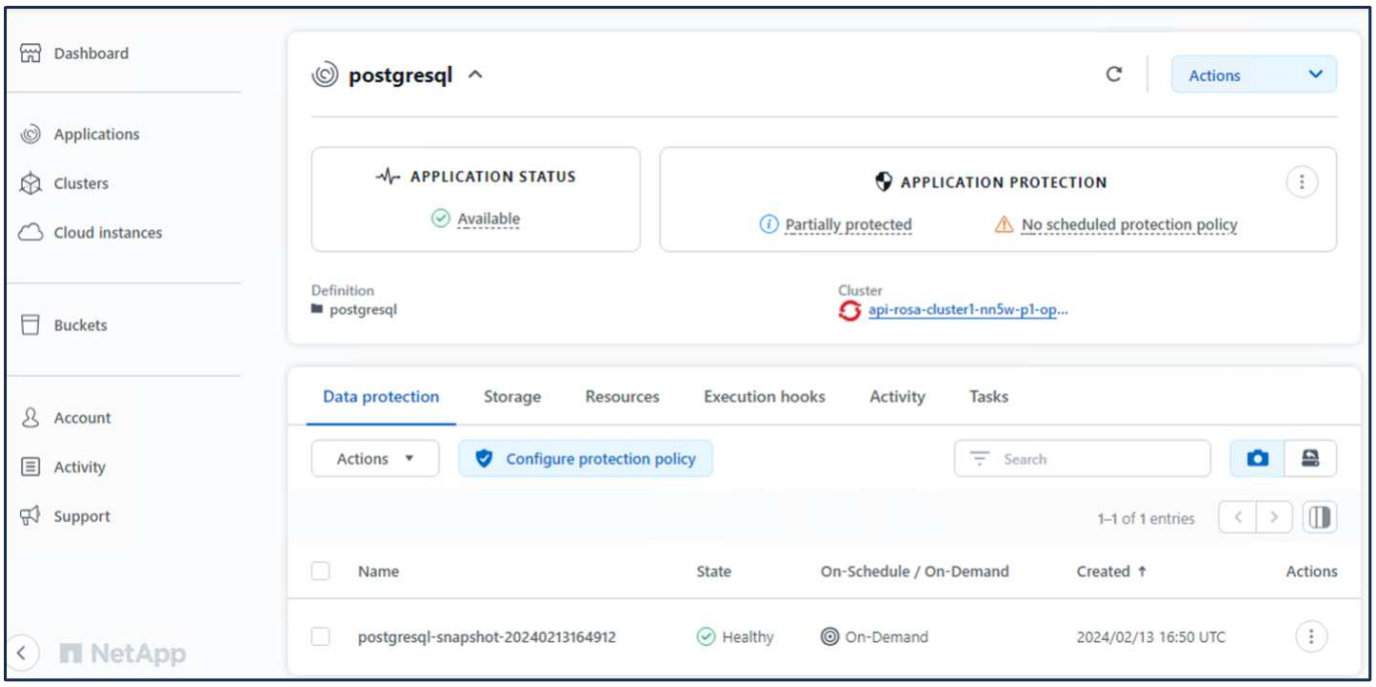
11. Restaurar desde una instantánea mediante ACS

Para restaurar la aplicación desde una instantánea, vaya a la página de inicio de la interfaz de usuario de

ACS, seleccione la aplicación y seleccione Restaurar. Debe elegir la copia Snapshot o un backup desde el que desea restaurar. (Por lo general, tendría varios creados en función de una política que haya configurado). Tome las decisiones adecuadas en el próximo par de pantallas y luego haga clic en **Restaurar**. El estado de la aplicación pasa de restaurar a Disponible después de que se ha restaurado de la copia de Snapshot.







12. Verifique que su aplicación se ha restaurado a partir de la instantánea

Inicie sesión en el cliente postgresql y ahora debería ver la tabla y el registro en la tabla que tenía anteriormente. Eso es todo. Con solo hacer clic en un botón, su aplicación se ha restaurado a un estado anterior. Es así de fácil que conseguimos a nuestros clientes con Astra Control.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
        List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```


Migración de datos

Esta página muestra las opciones de migración de datos para las cargas de trabajo de contenedor en clústeres de Red Hat OpenShift gestionados mediante FSx para NetApp ONTAP para el almacenamiento persistente.

Migración de datos

Red Hat OpenShift Service en AWS, así como FSx para ONTAP de NetApp (FSxN) forman parte de su cartera de servicios de AWS. FSxN está disponible en las opciones de AZ única o Multi-AZ. La opción Multi-AZ proporciona protección de datos frente a un fallo en la zona de disponibilidad. FSxN puede integrarse con Astra Trident para proporcionar almacenamiento persistente para aplicaciones en clústeres de ROSA.

Integración de FSxN con Trident mediante el gráfico Helm

Integración de clústeres ROSA con Amazon FSx para ONTAP

La migración de las aplicaciones de contenedores implica:

- Volúmenes persistentes: Se puede realizar con BlueXP. Otra opción consiste en utilizar Astra Control Center para gestionar las migraciones de aplicaciones de contenedores desde las instalaciones al entorno de cloud. La automatización se puede usar para el mismo propósito.
- Metadatos de la aplicación: Esto se puede realizar con OpenShift GitOps (CD de Argo).

Recuperación tras fallos y conmutación por error de aplicaciones en el cluster ROSA utilizando FSxN para el almacenamiento persistente

El siguiente vídeo es una demostración de los escenarios de conmutación al nodo de respaldo y conmutación de retorno tras recuperación en las aplicaciones con BlueXP y Argo CD.

Failover y failover de aplicaciones en el cluster ROSA

Solución de protección y migración de datos para las cargas de trabajo de contenedores de OpenShift