VMware Cloud Foundation en NetApp

NetApp virtualization solutions

NetApp
August 25, 2025

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions-virtualization/vmware/vmw-vcf-overview.html on August 25, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

VMware Cloud Foundation en NetApp . . . 1
- Simplifique la experiencia de nube híbrida con VMware Cloud Foundation y ONTAP . . . 1
- Introducción . . . 1
  - Introducción a NetApp ONTAP . . . 1
  - Introducción a VMware Cloud Foundation . . . 1
  - Dominios VCF . . . 2
  - Almacenamiento con VCF . . . 3
  - ¿Por qué ONTAP para VCF? . . . 3
  - Información adicional: . . . 4
  - Resumen . . . 5
  - Recursos de documentación . . . 5
- Opciones de diseño con VMware Cloud Foundation y ONTAP . . . 6
  - Opciones de almacenamiento . . . 6
  - Planos . . . 7
- Configurar entornos de nube privada con VMware Cloud Foundation y ONTAP . . . 11
  - Implementar una nueva instancia de VCF 9 . . . 11
  - Convergir componentes existentes en VCF 9 . . . 13
  - Actualizar un entorno VCF existente a VCF 9 . . . 14
- Implementación de la recuperación ante desastres con NetApp SnapMirror y BlueXP DRaaS . . . 14
  - Empezando . . . 15
  - Configuración de BlueXP disaster recovery . . . 17
  - Configuración de la replicación de almacenamiento entre la matriz del sitio de origen y la matriz del sitio de destino . . . 17
  - Cómo configurarlo para VMware Disaster Recovery . . . 18
  - ¿Qué puede hacer por usted la BlueXP disaster recovery ? . . . 18
  - Prueba de conmutación por error . . . 23
  - Operación de prueba de conmutación por error de limpieza . . . 25
  - Migración planificada y conmutación por error . . . 26
  - Recuperación por recuperación . . . 27
  - Monitoreo y tablero de control . . . 29
- Convertir clústeres de vSphere existentes a VCF . . . 30
  - Obtenga información sobre cómo convertir un entorno de vSphere con almacenes de datos existentes a VCF . . . 30
  - Convertir una instancia de servidor vCenter en un dominio de administración VCF (almacén de datos NFS) . . . 30
  - Convertir una instancia de servidor vCenter en un dominio de administración VCF (almacén de datos FC) . . . 44
- Aprovisionar VCF con almacenamiento principal . . . 58
  - Proporcionar un entorno VCF con ONTAP como solución de almacenamiento principal . . . 58
  - Utilice un almacén de datos VMFS basado en FC en ONTAP como almacenamiento principal para el dominio de administración de VCF . . . 58
  - Utilice un almacén de datos NFS en ONTAP como almacenamiento principal para el dominio de administración de VCF . . . 60

Utilice un almacén de datos VMFS basado en FC en ONTAP como almacenamiento principal para un dominio de carga de trabajo VI . . . 61
Utilice un almacén de datos NFS en ONTAP como almacenamiento principal para un dominio de carga de trabajo VI . . . 63
Ampliar VCF con almacenamiento complementario . . . 84
Obtenga información sobre cómo ampliar el almacenamiento para un entorno VCF mediante almacenamiento complementario . . . 84
Agregue un almacén de datos iSCSI como almacenamiento complementario para un dominio de administración mediante ONTAP tools for VMware vSphere . . . 84
Agregue un almacén de datos VMFS basado en FC como almacenamiento complementario para un dominio de administración mediante ONTAP tools for VMware vSphere . . . 108
Agregue vVols como almacenamiento complementario a los dominios de carga de trabajo VI mediante ONTAP tools for VMware vSphere . . . 109
Agregue NFS y vVols como almacenamiento complementario a los dominios de carga de trabajo VI mediante ONTAP tools for VMware vSphere . . . 136
Agregue NVMe sobre TCP como almacenamiento complementario a los dominios de carga de trabajo de VI . . . 161
Agregue un almacén de datos VMFS basado en FC como almacenamiento complementario a los dominios de carga de trabajo de VI . . . 185
Proteger VCF con SnapCenter . . . 186
Obtenga información sobre cómo proteger los dominios de carga de trabajo VCF con el complemento SnapCenter para VMware vSphere . . . 186
Proteja un dominio de carga de trabajo VCF con el complemento SnapCenter para VMware vSphere 187
Proteja los dominios de administración y carga de trabajo de VCF mediante el complemento SnapCenter para VMware vSphere . . . 223
Proteja los dominios de carga de trabajo VCF con almacenamiento NVMe sobre TCP y el complemento SnapCenter para VMware vSphere . . . 236
Proteja los almacenes de datos de VMware con BlueXP . . . 244
Obtenga información sobre cómo proteger los almacenes de datos de VMware mediante la BlueXP disaster recovery . . . 244
Configure la protección de datos 3-2-1 para VMware con el complemento SnapCenter para VMware vSphere y la BlueXP backup and recovery . . . 244
Configurar la recuperación ante desastres para almacenes de datos VMFS mediante la BlueXP disaster recovery . . . 290
Configurar la recuperación ante desastres para almacenes de datos NFS mediante la BlueXP disaster recovery . . . 308
Proteja las cargas de trabajo con vSphere Metro Storage Cluster . . . 329
Obtenga información sobre la integración de la alta disponibilidad de ONTAP con VMware vSphere Metro Storage Cluster (vMSC) . . . 329
Configurar un clúster extendido para un dominio de administración de VCF mediante MetroCluster . . . 330
Configurar un clúster extendido para un dominio de carga de trabajo VI mediante MetroCluster . . . 342
Configurar un clúster extendido para un dominio de administración de VCF mediante SnapMirror Active Sync . . . 354
Configurar un clúster extendido para un dominio de carga de trabajo VI mediante SnapMirror Active Sync . . . 356

Migrar máquinas virtuales de VMware vSphere a almacenes de datos de ONTAP . . . 358
Requisitos de red . . . 359
Escenarios de migración de máquinas virtuales . . . 361
Escenarios de migración de plantillas de VM . . . 386
Casos de uso . . . 394
Recursos adicionales . . . 395
Protección autónoma contra ransomware para almacenamiento NFS . . . 395
Supervise el almacenamiento local con Data Infrastructure Insights . . . 405
Supervisión del almacenamiento local con Data Infrastructure Insights . . . 405
Descripción general de la implementación de la solución . . . 406
Prerrequisitos . . . 406
Implementación de la solución . . . 406
Conclusión . . . 423
Información adicional . . . 423

VMware Cloud Foundation en NetApp

Simplifique la experiencia de nube híbrida con VMware Cloud Foundation y ONTAP

NetApp ONTAP se integra con VMware Cloud Foundation (VCF) para ofrecer una solución de almacenamiento unificada compatible con protocolos de bloques y archivos. Esta integración simplifica las implementaciones de nube híbrida, mejora la gestión y el rendimiento de los datos y garantiza servicios de datos consistentes en entornos locales y en la nube.

Introducción

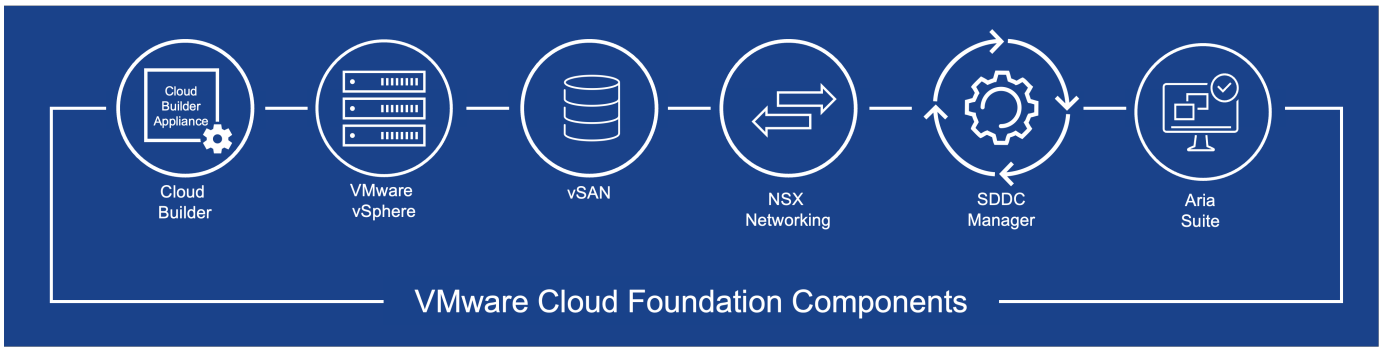
El uso de NetApp con VCF mejora la gestión de datos y la eficiencia del almacenamiento a través de las funciones avanzadas de NetApp, como deduplicación, compresión e instantáneas. Esta combinación proporciona una integración perfecta, alto rendimiento y escalabilidad para entornos virtualizados. Además, simplifica las implementaciones de nube híbrida al permitir servicios de datos consistentes y administración en infraestructuras locales y en la nube.

Introducción a NetApp ONTAP

NetApp ONTAP es un software integral de gestión de datos que ofrece funciones de almacenamiento avanzadas en una amplia línea de productos. ONTAP está disponible como almacenamiento definido por software, como un servicio de primera parte a través de los principales proveedores de nube y como sistema operativo de almacenamiento para las plataformas NetApp ASA (All San Array), AFF (All-flash FAS) y FAS (Fabric-Attached Storage). ONTAP ofrece alto rendimiento y baja latencia para una variedad de casos de uso, incluida la virtualización de VMware, sin crear silos.

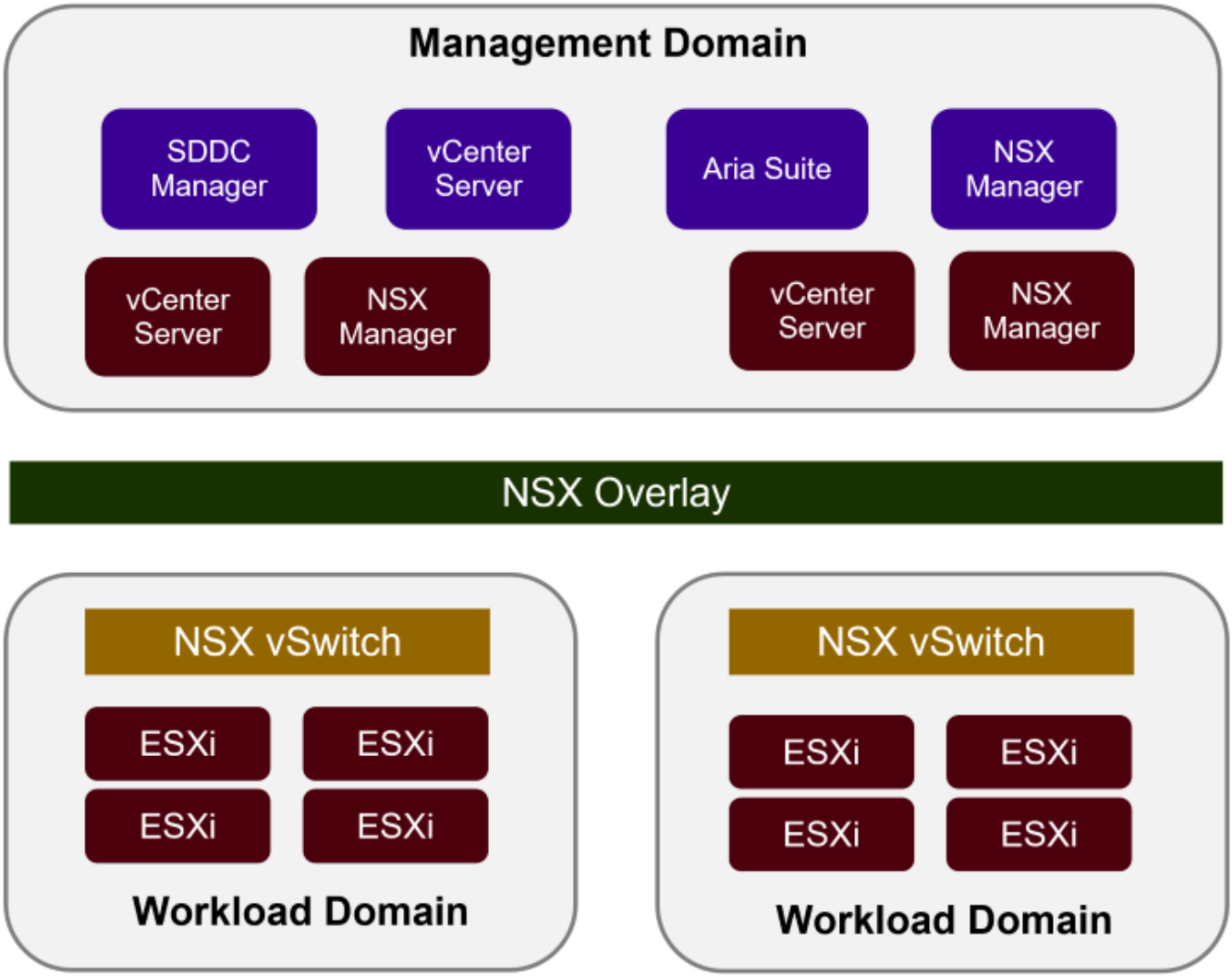
Introducción a VMware Cloud Foundation

VCF integra ofertas de computación, red y almacenamiento con productos VMware e integraciones de terceros, lo que facilita cargas de trabajo nativas basadas en Kubernetes y máquinas virtuales. Esta plataforma de software incluye componentes clave como VMware vSphere, NSX, Aria Suite Enterprise, Tanzu Kubernetes Grid, HCX Enterprise, SDDC Manager y capacidad de almacenamiento vinculada a los núcleos de CPU del host a través de vSAN. NetApp ONTAP se integra perfectamente con una variedad de modelos de implementación de VCF tanto locales como en la nube pública.



Dominios VCF

Los dominios son una construcción fundamental dentro de VCF que permite la organización de recursos en grupos distintos e independientes. Los dominios ayudan a organizar la infraestructura de forma más efectiva, garantizando que los recursos se utilicen de manera eficiente. Cada dominio se implementa con sus propios elementos de computación, red y almacenamiento.



Hay dos tipos principales de dominios con VCF:

- **Dominio de administración**: el dominio de administración incluye componentes responsables de las funciones principales del entorno VCF. Los componentes manejan tareas esenciales como aprovisionamiento de recursos, monitoreo y mantenimiento e incluyen integraciones de complementos de terceros como NetApp ONTAP Tools para VMware. Los dominios de administración se pueden implementar utilizando Cloud Builder Appliance para garantizar que se sigan las mejores prácticas, o se puede convertir un entorno de vCenter existente en un dominio de administración de VCF.
- **Dominio de carga de trabajo de infraestructura virtual**: los dominios de carga de trabajo de infraestructura virtual están diseñados para ser grupos de recursos dedicados a una necesidad operativa, carga de trabajo u organización específica. Los dominios de carga de trabajo se implementan fácilmente a través del SDDC Manager, lo que ayuda a automatizar una serie de tareas complejas. Se pueden aprovisionar hasta 24 dominios de carga de trabajo dentro de un entorno VCF, cada uno de los cuales representa una unidad de infraestructura lista para aplicaciones.

Almacenamiento con VCF

Un aspecto central de la funcionalidad de los dominios es el almacenamiento que consumen. Si bien VCF incluye capacidad vSAN basada en núcleos de CPU para casos de uso hiperconvergentes, también admite una amplia gama de soluciones de almacenamiento externo. Esta flexibilidad es crucial para las empresas que tienen inversiones significativas en matrices de almacenamiento existentes o necesitan soportar protocolos más allá de los que vSAN ofrece. VMware admite múltiples tipos de almacenamiento con VCF.

Hay dos tipos principales de almacenamiento con VCF:

- **Almacenamiento principal**: este tipo de almacenamiento se asigna durante la creación inicial del dominio. Para los dominios de administración, este almacenamiento alberga los componentes administrativos y operativos de VCF. Para los dominios de carga de trabajo, este almacenamiento está diseñado para soportar las cargas de trabajo, las máquinas virtuales o los contenedores para los que se implementó el dominio.
- **Almacenamiento complementario**: se puede agregar almacenamiento complementario a cualquier dominio de carga de trabajo después de la implementación. Este tipo de almacenamiento ayuda a las organizaciones a aprovechar las inversiones existentes en infraestructura de almacenamiento e integrar diversas tecnologías de almacenamiento para optimizar el rendimiento, la escalabilidad y la rentabilidad.

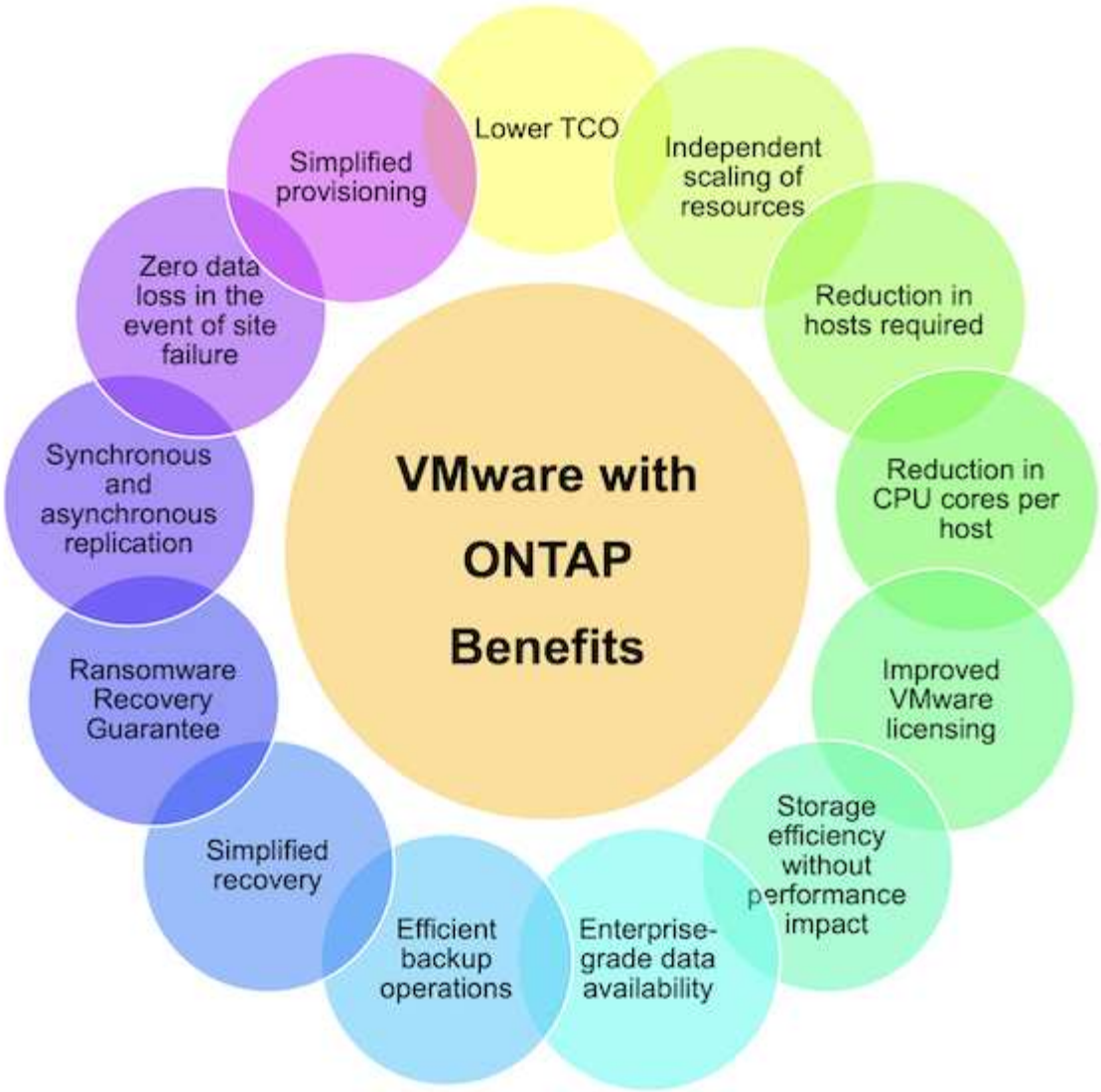
Compatible con tipos de almacenamiento VCF

Tipo de dominio	Almacenamiento principal	Almacenamiento suplementario
Dominio de gestión	vSAN FC* NFS*	vVols (FC, iSCSI o NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA
Dominio de carga de trabajo de infraestructura virtual	vSAN vVols (FC, iSCSI o NFS) FC NFS	vVols (FC, iSCSI o NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA

Nota: *Se proporciona soporte de protocolo específico cuando se utiliza la herramienta de importación VCF con entornos vSphere existentes.

¿Por qué ONTAP para VCF?

Además de los casos de uso que involucran protección de inversiones y soporte de múltiples protocolos, existen muchas razones adicionales para aprovechar el almacenamiento compartido externo dentro de un dominio de carga de trabajo VCF. Se puede suponer que el almacenamiento provisto para un dominio de carga de trabajo es simplemente un repositorio para alojar máquinas virtuales y contenedores. Sin embargo, las necesidades de la organización a menudo superan las capacidades de la licencia y requieren almacenamiento empresarial. El almacenamiento proporcionado por ONTAP, asignado a dominios dentro de VCF, es fácil de implementar y ofrece una solución de almacenamiento compartido a prueba de futuro.



Para obtener más información sobre los principales beneficios de ONTAP para VMware VCF identificados a continuación, consulte"¿Por qué ONTAP para VMware?" .

- Flexibilidad desde el primer día y a medida que escala
- Descargue tareas de almacenamiento a ONTAP
- La mejor eficiencia de almacenamiento de su clase
- Disponibilidad de datos de nivel empresarial
- Operaciones de respaldo y recuperación eficientes
- Capacidades de continuidad empresarial holísticas

Información adicional:

- "Opciones de almacenamiento de NetApp"
- "Compatibilidad con vSphere Metro Storage Cluster (vMSC)"
- "Herramientas ONTAP para VMware vSphere"
- "Automatización de VMware con ONTAP"

- "SnapCenter de NetApp"
- "Multicloud híbrida con VMware y NetApp"
- "Seguridad y protección contra ransomware"
- "Migración sencilla de cargas de trabajo de VMware a NetApp"
- "Recuperación ante desastres de BlueXP"
- "Perspectivas de la infraestructura de datos"
- "Recopilador de datos de VM"

Resumen

ONTAP proporciona una plataforma que aborda todos los requisitos de carga de trabajo, ofreciendo soluciones de almacenamiento en bloque personalizadas y ofertas unificadas para permitir resultados más rápidos para máquinas virtuales y aplicaciones de manera confiable y segura. ONTAP incorpora técnicas avanzadas de reducción y movimiento de datos para minimizar el espacio ocupado por el centro de datos, al tiempo que garantiza la disponibilidad a nivel empresarial para mantener las cargas de trabajo críticas en línea. Además, AWS, Azure y Google admiten el almacenamiento externo impulsado por NetApp para mejorar el almacenamiento vSAN en clústeres basados en la nube de VMware como parte de sus ofertas de VMware-in-the-Cloud. En general, las capacidades superiores de NetApp lo convierten en una opción más efectiva para las implementaciones de VMware Cloud Foundation.

Recursos de documentación

Para obtener información detallada sobre las ofertas de NetApp para VMware Cloud Foundation, consulte lo siguiente:

Documentación de VMware Cloud Foundation

- "Documentación de VMware Cloud Foundation"

Serie de blog de cuatro (4) partes sobre VCF con NetApp

- "NetApp y VMware Cloud Foundation simplificados Parte 1: Primeros pasos"
- "NetApp y VMware Cloud Foundation simplificados Parte 2: Almacenamiento principal de VCF y ONTAP"
- "NetApp y VMware Cloud Foundation simplificados Parte 3: Almacenamiento principal de VCF y Element"
- "NetApp y VMware Cloud Foundation simplificados: Parte 4: Herramientas ONTAP para VMware y almacenamiento complementario"

*VMware Cloud Foundation con matrices SAN All-Flash de NetApp *

- "VCF con matrices NetApp ASA : introducción y descripción general de la tecnología"
- "Utilice ONTAP con FC como almacenamiento principal para dominios de administración"
- "Utilice ONTAP con FC como almacenamiento principal para dominios de carga de trabajo de VI"
- "Utilice Ontap Tools para implementar almacenes de datos iSCSI en un dominio de administración de VCF"
- "Utilice Ontap Tools para implementar almacenes de datos FC en un dominio de administración de VCF"
- "Utilice Ontap Tools para implementar almacenes de datos vVols (iSCSI) en un dominio de carga de trabajo VI"

- "Configurar almacenes de datos NVMe sobre TCP para su uso en un dominio de carga de trabajo VI"
- "Implemente y use el SnapCenter Plug-in for VMware vSphere para proteger y restaurar máquinas virtuales en un dominio de carga de trabajo VI"
- "Implemente y use el SnapCenter Plug-in for VMware vSphere para proteger y restaurar máquinas virtuales en un dominio de carga de trabajo VI (almacenes de datos NVMe/TCP)"

*VMware Cloud Foundation con matrices AFF All-Flash de NetApp *

- "VCF con matrices AFF de NetApp : introducción y descripción general de la tecnología"
- "Utilice ONTAP con NFS como almacenamiento principal para dominios de administración"
- "Utilice ONTAP con NFS como almacenamiento principal para dominios de carga de trabajo VI"
- "Utilice las herramientas de ONTAP para implementar almacenes de datos vVols (NFS) en un dominio de carga de trabajo VI"

Soluciones NetApp FlexPod para VMware Cloud Foundation

- "Expansión de la nube híbrida FlexPod con VMware Cloud Foundation"
- "FlexPod como dominio de carga de trabajo para VMware Cloud Foundation"
- "Guía de diseño de FlexPod como dominio de carga de trabajo para VMware Cloud Foundation"

Opciones de diseño con VMware Cloud Foundation y ONTAP

Puede comenzar de nuevo con VCF 9 o reutilizar implementaciones existentes para crear un entorno de nube privada utilizando VCF 9 y ONTAP. Obtenga información sobre los modelos de diseño más populares para VCF 9 y cómo los productos NetApp agregan valor.

Opciones de almacenamiento

VMware Cloud Foundation con ONTAP admite una variedad de configuraciones de almacenamiento para satisfacer diferentes requisitos de rendimiento, escalabilidad y disponibilidad. Las siguientes tablas resumen las opciones de almacenamiento principales y complementarias disponibles para su entorno.

Familia de productos	VMFS en FC	NFSv3
ASA Serie A y Serie C	Sí	No
Serie A y Serie C de AFF	Sí	Sí
FAS	Sí	Sí

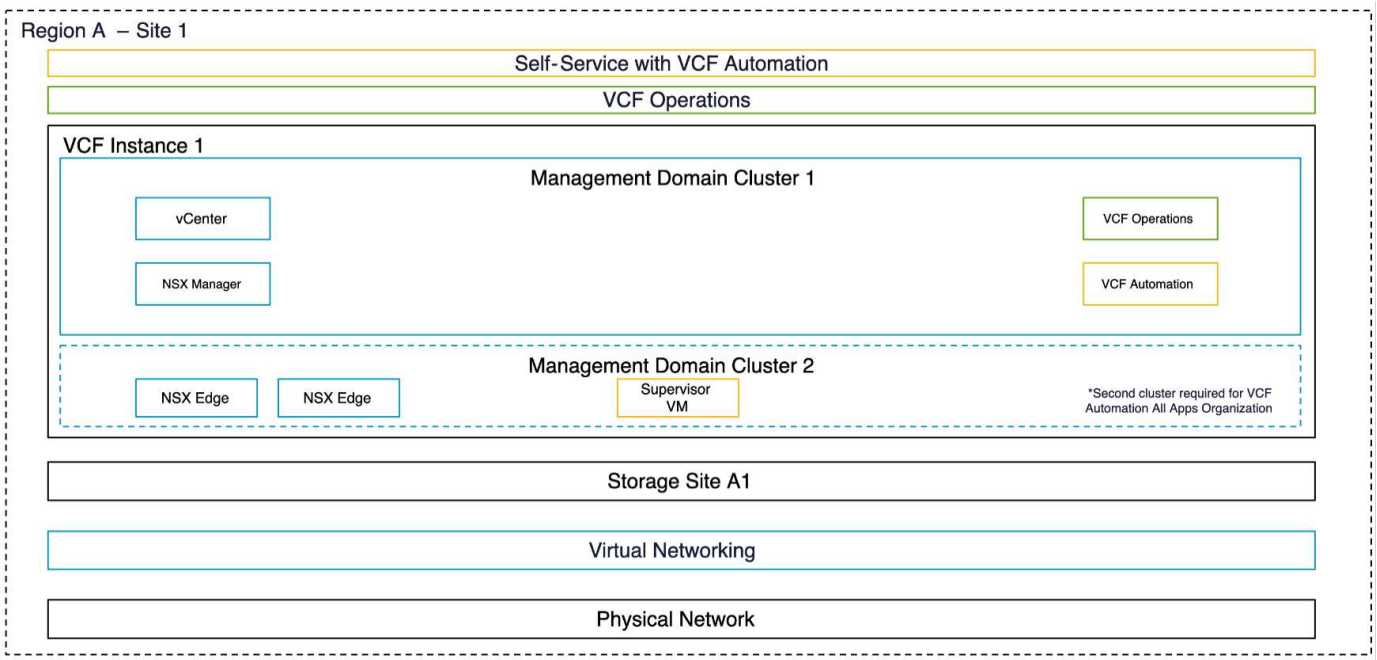
Familia de productos	VMFS en FC	VMFS en iSCSI	VMFS en NVMe-oF	NFSv3	NFSv4.1
ASA Serie A y Serie C	Sí	Sí	Sí	No	No
Serie A y Serie C de AFF	Sí	Sí	Sí	Sí	Sí
FAS	Sí	Sí	Sí	Sí	Sí

Planos

Los siguientes planos ilustran modelos de implementación comunes para VMware Cloud Foundation y ONTAP en varios escenarios de sitios y recursos.

Flota VCF en un solo sitio con un espacio mínimo

Este plan de diseño es para implementar componentes de administración y carga de trabajo en un solo clúster de vSphere con recursos mínimos. Admite almacenes de datos principales VMFS y NFSv3 y una opción de implementación simple con una configuración de dos nodos. Si planea utilizar VCF Automation con el modelo de organización de todas las aplicaciones, necesitará un segundo clúster para implementar los nodos vSphere Supervisor y NSX Edge.



Para minimizar el consumo de recursos, utilice una instancia de herramientas ONTAP existente si es posible. Si no está disponible, es adecuado un solo nodo con un perfil pequeño. El SnapCenter Plug-in for VMware vSphere protege máquinas virtuales y almacenes de datos mediante instantáneas nativas y replicación a otra matriz de almacenamiento ONTAP .

> Si no cuenta con recursos para explorar VCF, muchos proveedores de nube ofrecen VCF como servicio, y ONTAP está disponible como un servicio propio de los proveedores de nube.

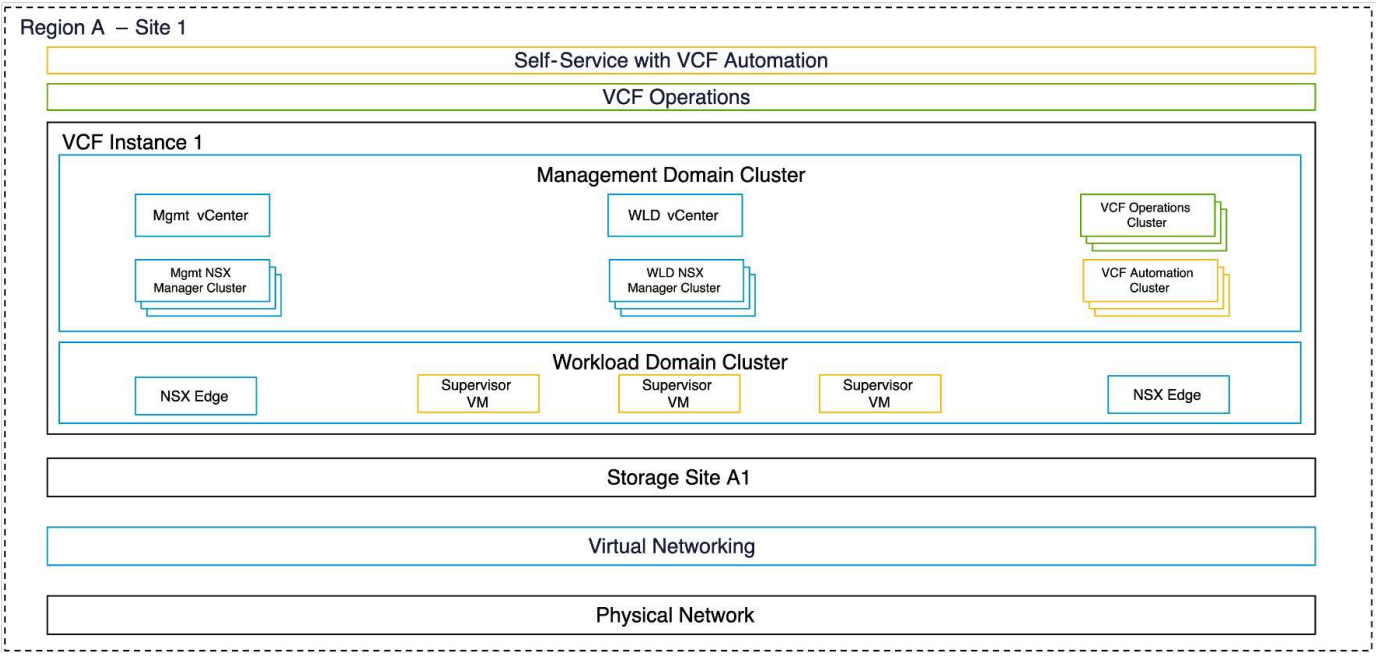
Para obtener más detalles sobre este diseño, consulte la"Documentación técnica de Broadcom sobre la flota VCF en un solo sitio con un espacio mínimo" .

Flota VCF en un solo sitio

Este plan de diseño está dirigido a clientes con un único centro de datos principal que depende de la alta disponibilidad de las aplicaciones. Normalmente se trata de un único entorno VCF. Puede utilizar ASA para cargas de trabajo en bloque y AFF para cargas de trabajo unificadas o de archivos.

El repositorio de contenido comparte plantillas de VM y registros de contenedores entre dominios VCF. Cuando se aloja en FlexGroup Volume, la función FlexCache está disponible para el almacén de datos de suscripción.

No se admite el alojamiento de máquinas virtuales en el almacén de datos FlexCache .



Una sola instancia de herramientas ONTAP en modo HA puede administrar todos los vCenters en la flota de VCF. Consulte la"Límites de configuración de las herramientas ONTAP" Para más información. Las herramientas de ONTAP se integran con VCF SSO y VCF OPS agrupación inteligente para acceso a múltiples vCenter en la misma interfaz de usuario.

Almacén de datos complementario VCF con herramientas ONTAP

Debe implementar el complemento de SnapCenter en cada instancia de vCenter para proteger las máquinas virtuales y los almacenes de datos.

La gestión basada en políticas de almacenamiento se utiliza con vSphere Supervisor para controlar el host de las máquinas virtuales de VKS. Las etiquetas se gestionan de forma centralizada en VCF Ops. NetApp Trident CSI se utiliza con VKS para la protección de copias de seguridad de aplicaciones mediante funciones de matriz nativas. Cuando usa vSphere CSI, los detalles del volumen persistente aparecen en VCF Automation.

Para obtener más detalles sobre este plan, consulte el"Documentación técnica de Broadcom sobre la flota VCF en un solo sitio" .

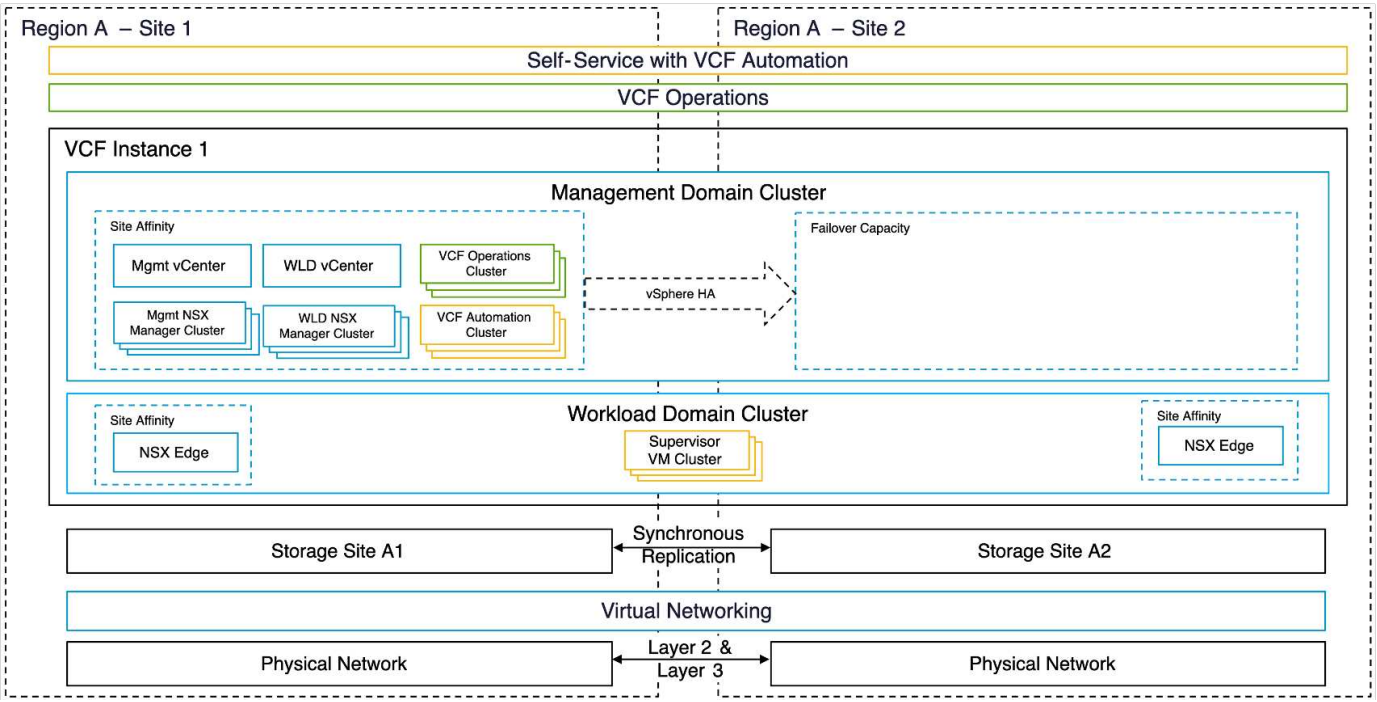
Flota VCF con múltiples sitios en una sola región

Este diseño está destinado a clientes que ofrecen servicios similares a la nube con mayor disponibilidad al distribuir las cargas de trabajo en diferentes dominios de falla.

Para los almacenes de datos VMFS, la sincronización activa de SnapMirror proporciona una unidad de almacenamiento activa-activa para usar con vSphere Metro Storage Cluster. El modo de acceso uniforme ofrece conmutación por error de almacenamiento transparente, mientras que el modo de acceso no uniforme requiere que la máquina virtual se reinicie en caso de falla del dominio de falla.

Para los almacenes de datos NFS, ONTAP MetroCluster con vSphere Metro Storage Cluster garantiza una alta disponibilidad. Un mediador evita escenarios de cerebro dividido y ahora puede alojarse en BlueXP.

Las reglas de ubicación de máquinas virtuales controlan las máquinas virtuales dentro del mismo dominio de falla para los componentes del dominio de administración.



Las herramientas ONTAP proporcionan una interfaz de usuario para configurar las relaciones de sincronización activa de SnapMirror . Los sistemas de almacenamiento de ambos dominios de falla deben estar registrados en las herramientas de ONTAP y en el SnapCenter Plug-in for VMware vSphere.

Puede implementar políticas de respaldo 3-2-1 utilizando BlueXP Backup and Recovery para VM a través de SnapMirror y SnapMirror to Cloud. Puede realizar restauraciones desde cualquiera de las tres ubicaciones.

Trident Protect o BlueXP Backup and Recovery para Kubernetes protegen las aplicaciones del clúster VKS.

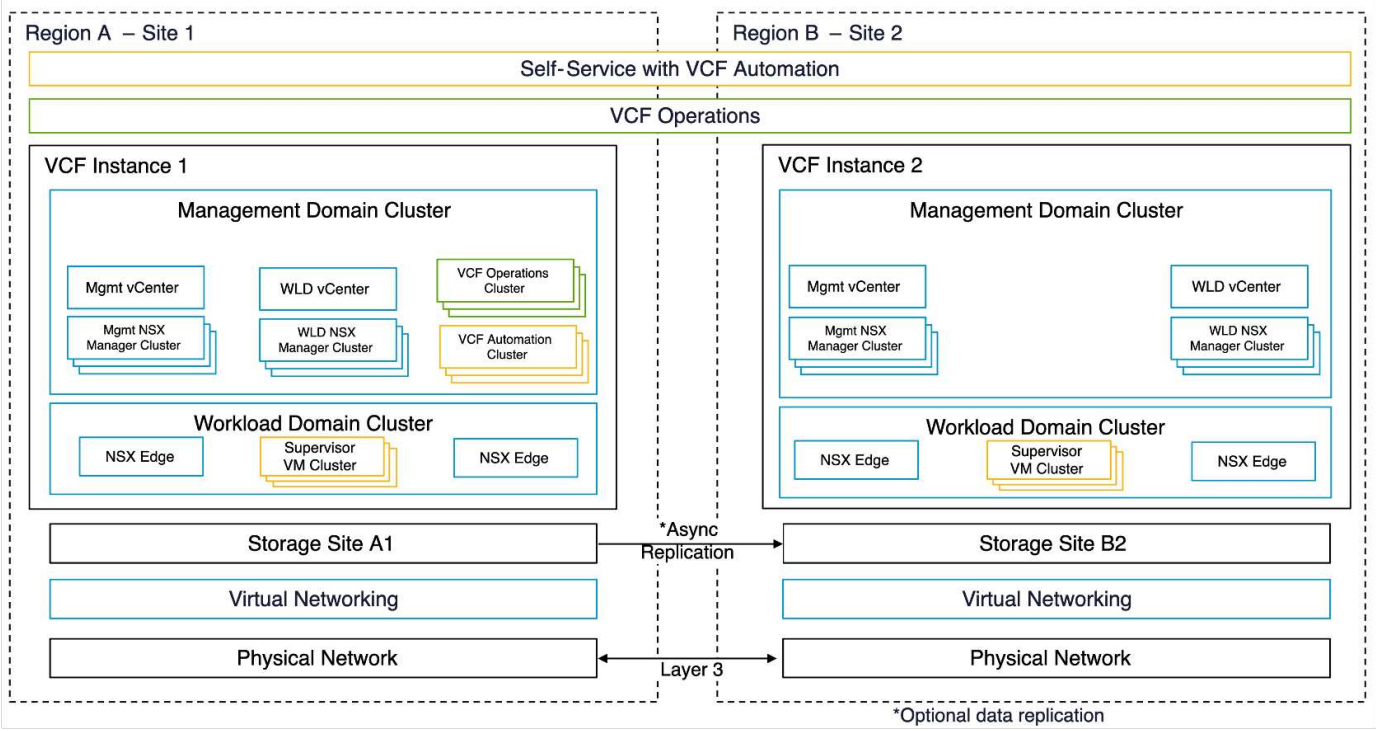
Para más información, consulte la"Documentación técnica de Broadcom sobre la flota VCF con varios sitios en una sola región" .

Flota de VCF con múltiples sitios en varias regiones

Este diseño está dirigido a clientes distribuidos globalmente, que brindan servicios de proximidad y soluciones de recuperación ante desastres.

Puede administrar la recuperación ante desastres de las máquinas virtuales con VMware Live Site Recovery o BlueXP Disaster Recovery como servicio. Las herramientas ONTAP ofrecen el SRA (Adaptador de replicación de almacenamiento) para orquestar las operaciones de almacenamiento con ONTAP.

Familia de productos	Sincronización activa de SnapMirror	MetroCluster
ASA Serie A y Serie C	Sí	Sí
Serie A y Serie C de AFF	Sí	Sí
FAS	No	Sí



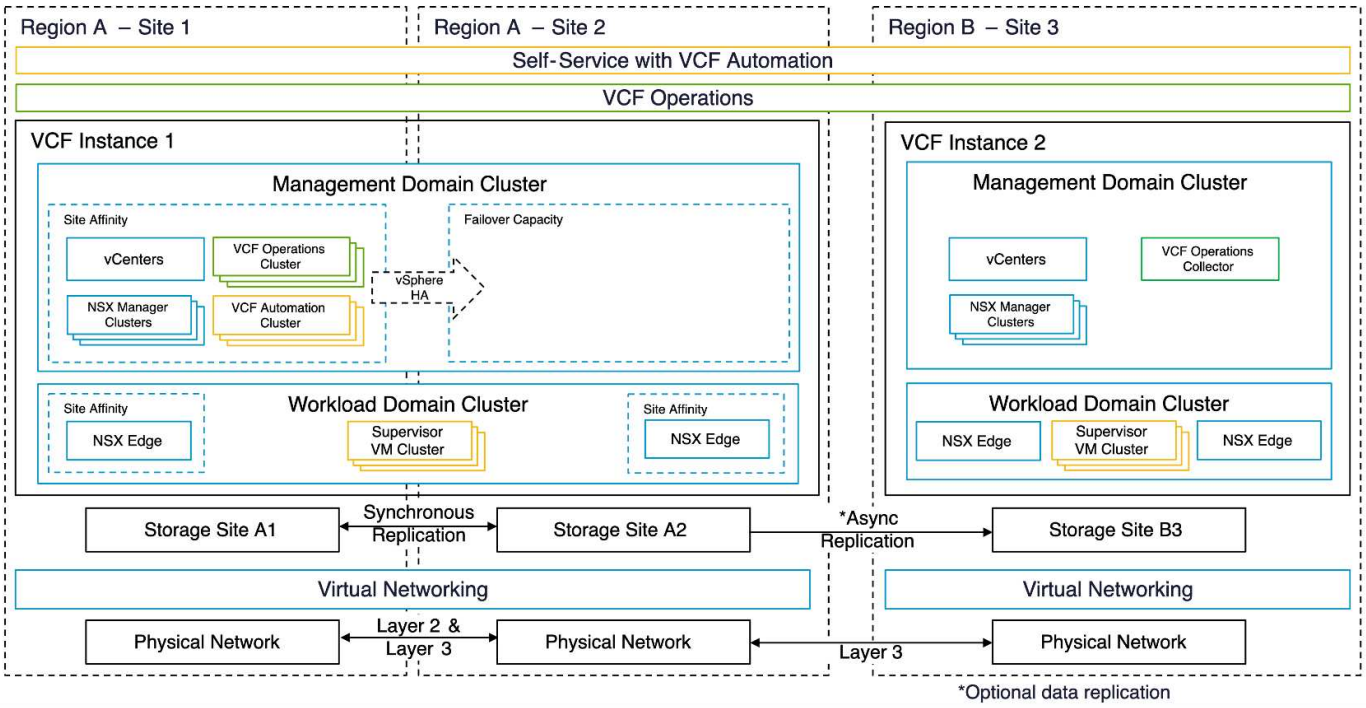
Las herramientas ONTAP proporcionan una interfaz de usuario para la configuración de la replicación del almacén de datos. BlueXP también se puede utilizar para la replicación entre matrices de almacenamiento. El SnapCenter Plug-in for VMware vSphere utiliza las relaciones SnapMirror existentes para SnapShots.

Para más información, consulte la"Documentación técnica de Broadcom sobre la flota VCF con varios sitios en varias regiones" .

Flota VCF con múltiples sitios en una sola región más regiones adicionales

Este diseño aborda tanto la disponibilidad como la recuperación ante desastres de máquinas virtuales y aplicaciones VKS.

ASA, AFF y FAS admiten esta opción de diseño.



Puede utilizar herramientas ONTAP o BlueXP para configurar la relación de replicación.

Para obtener más información, consulte "Documentación técnica de Broadcom sobre la flota VCF con varios sitios en una sola región y regiones adicionales" .

Configurar entornos de nube privada con VMware Cloud Foundation y ONTAP

Implemente, converja o actualice entornos VMware Cloud Foundation 9 con ONTAP. Aprenda a configurar nuevos entornos VCF 9.0, a converger instancias de vCenter existentes y almacenes de datos de ONTAP , y a actualizar implementaciones de VCF anteriores.

Implementar una nueva instancia de VCF 9

Utilice este flujo de trabajo para implementar un entorno VMware Cloud Foundation (VCF) 9.0 limpio. Después de la implementación, puede migrar cargas de trabajo o comenzar a aprovisionar aplicaciones y proporcionar servicios de infraestructura.

Para conocer los pasos de alto nivel, consulte la"Build Journey: instalar una nueva implementación de VMware Cloud Foundation" .

Pasos

1. Sigue el"Pasos de implementación de Broadcom VCF 9" .
2. En el paso de preparación de la implementación, complete las tareas para su opción de almacenamiento principal.

VMFS en FC

1. Recopila los WWPN de todos los hosts ESXi. Puedes correr `esxcli storage san fc list`, utilice el cliente host ESXi o utilice PowerCLI.
2. Configurar la zonificación. Ver "Configuraciones de zonificación FC recomendadas para sistemas ONTAP" .

> Utilice los WWPN de las interfaces lógicas (LIF) de SVM, no los WWPN del adaptador físico.

3. Cree un LUN y asígnelo a los hosts mediante WWPN usando el Administrador del sistema, la CLI de ONTAP o la API.
4. Vuelva a escanear el adaptador de almacenamiento en ESXi y cree el almacén de datos VMFS.

NFSv3

1. Cree una interfaz VMkernel en un host ESXi.
2. Asegúrese de que"SVM tiene NFS habilitado" y"vStorage sobre NFS está habilitado" .
3. Cree un volumen y expórtelo con una política que permita los hosts ESXi.
4. Ajuste los permisos según sea necesario.
5. Implemente el VIB VAAI de ONTAP NFS e inclúyalo en la imagen vLCM. Por ejemplo: `esxcli software vib install -d /NetAppNasPlugin2.0.1.zip`. (Descargue el ZIP del sitio de soporte de NetApp).
6. Monte el volumen NFS en el host donde creó la interfaz VMkernel. Por ejemplo: `esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-cl01-nfs01`.

> El `nConnect` El recuento de sesiones es por host. Actualice otros hosts después de la implementación según sea necesario.

1. Al final de **Verificar resumen de implementación y revisar próximos pasos** en la fase **Implementar flota VCF**, complete lo siguiente:
   a. Implementar herramientas ONTAP
      - "Descargar herramientas ONTAP 10.x"desde el sitio de soporte de NetApp .
      - Cree registros DNS para el administrador de herramientas ONTAP , los nodos y la IP virtual utilizada para la comunicación interna.
      - Implemente el OVA en el servidor vCenter de administración.
      - "Registrar el dominio de administración vCenter"con el administrador de herramientas ONTAP .
      - "Agregar el backend de almacenamiento"utilizando la interfaz de usuario del cliente vSphere.
      - "Crear un almacén de datos complementario"(incluya uno para el registro de contenido).
      - Cree el registro de contenido si planea una implementación de alta disponibilidad.
      - "Habilitar HA"en el Administrador de herramientas de ONTAP .
   b. Implementar el complemento SnapCenter
      - "Implementar el SnapCenter Plug-in for VMware vSphere" .

        - "Agregar el backend de almacenamiento" .
        - "Crear políticas de respaldo" .
        - "Crear grupos de recursos" .
    c. Implementar el conector BlueXP
        - "Revisa lo que puedes hacer sin un Conector" .
        - "Implementar el conector" .
    d. Utilice BlueXP para realizar copias de seguridad y recuperación
        - "Proteja las cargas de trabajo de VM" .
        - "Proteja las cargas de trabajo de VKS" .
2. Después de importar vCenter como un dominio de carga de trabajo en la instancia VCF, complete lo siguiente:
    a. Registrar herramientas ONTAP
        - "Registrar el dominio de carga de trabajo vCenter"con el administrador de herramientas ONTAP .
        - "Agregar el backend de almacenamiento"utilizando la interfaz de usuario del cliente vSphere.
        - "Crear un almacén de datos complementario" .
    b. Implementar el SnapCenter Plug-in for VMware vSphere
        - "Implementar el SnapCenter Plug-in for VMware vSphere" .
        - "Agregar el backend de almacenamiento" .
        - "Crear políticas de respaldo" .
        - "Crear grupos de recursos" .
    c. Utilice BlueXP para realizar copias de seguridad y recuperación
        - "Proteja las cargas de trabajo de VM" .
        - "Proteja las cargas de trabajo de VKS" .

Puede reutilizar estos pasos cada vez que cree un nuevo dominio de carga de trabajo.

Convergir componentes existentes en VCF 9

Es posible que ya tenga algunos componentes de la flota VCF y prefiera reutilizarlos. Cuando se reutiliza una instancia de vCenter, los almacenes de datos frecuentemente se aprovisionan con herramientas ONTAP , que pueden servir como almacenamiento principal para VCF.

Prerrequisitos

- Confirme que las instancias de vCenter existentes sean funcionales.
- Verifique que los almacenes de datos provistos por ONTAP estén disponibles.
- Garantizar el acceso a la"Matriz de interoperabilidad" .

Pasos

1. Revisar el"escenarios admitidos para converger a VCF" .
2. Converja una instancia de vCenter con almacenes de datos aprovisionados por ONTAP como almacenamiento principal.
3. Verifique las versiones compatibles utilizando el"Matriz de interoperabilidad" .

4. Mejora"Herramientas ONTAP" si es necesario.
5. Actualizar el"Complemento de SnapCenter para VMware vSphere" si es necesario.

Actualizar un entorno VCF existente a VCF 9

Actualice una implementación de VCF anterior a la versión 9.0 mediante el proceso de actualización estándar. El resultado es un entorno VCF que ejecuta la versión 9.0 con dominios de gestión y carga de trabajo mejorados.

Prerrequisitos

- Realice una copia de seguridad del dominio de administración y de los dominios de carga de trabajo.
- Verificar la compatibilidad de las herramientas ONTAP y el complemento SnapCenter con VCF 9.0. Sigue el"Matriz de interoperabilidad" a"actualizar las herramientas de ONTAP" y"Complemento de SnapCenter para VMware vSphere" que son compatibles con VCF 9.

Pasos

1. Actualizar el dominio de administración de VCF. Ver"Actualizar el dominio de administración de VCF a VCF 9" para obtener instrucciones.
2. Actualice cualquier dominio de carga de trabajo VCF 5.x. Ver"Actualizar el dominio de carga de trabajo de VCF 5.x a VCF 9" para obtener instrucciones.

Implementación de la recuperación ante desastres con NetApp SnapMirror y BlueXP DRaaS

Solución de recuperación ante desastres VCF para almacén de datos NFS con NetApp SnapMirror y BlueXP DRaaS

La replicación a nivel de bloque desde un sitio de producción a un sitio de recuperación ante desastres (DR) ofrece una estrategia resistente y rentable para proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos, incluidos ataques de ransomware. La replicación SnapMirror de NetApp permite que los dominios de carga de trabajo VMware VCF 9 que se ejecutan en sistemas ONTAP locales (mediante almacenes de datos NFS o VMFS) se repliquen en un sistema ONTAP secundario ubicado en un centro de datos de recuperación designado donde también se implementa VMware.

En esta sección se describe la configuración de BlueXP Disaster Recovery as a Service (DRaaS) para establecer DR para máquinas virtuales VMware locales.

La configuración incluye:

- Creación de una cuenta BlueXP e implementación de un conector BlueXP .
- Agregar matrices ONTAP al lienzo de BlueXP para facilitar la comunicación entre VMware vCenter y el almacenamiento ONTAP .
- Configurar la replicación entre sitios usando SnapMirror.
- Configurar y probar un plan de recuperación para validar la preparación para la conmutación por error.

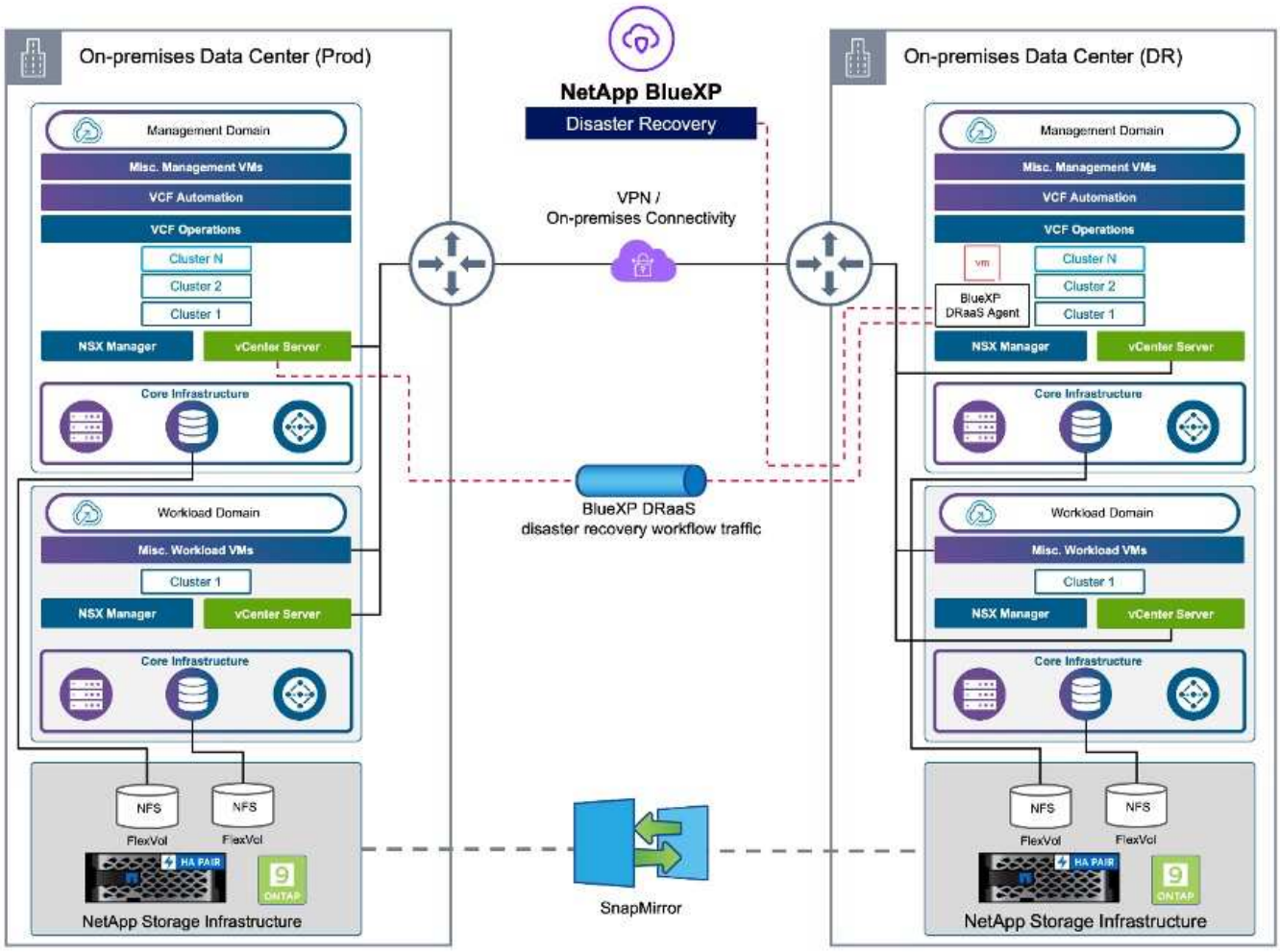
El servicio de BlueXP disaster recovery , integrado en la consola BlueXP de NetApp , permite a las organizaciones descubrir sin problemas sus sistemas de almacenamiento VMware vCenters y ONTAP locales. Una vez descubiertos, los administradores pueden definir agrupaciones de recursos, crear planes de recuperación ante desastres, asociarlos con los recursos adecuados e iniciar o probar operaciones de conmutación por error y recuperación. NetApp SnapMirror proporciona una replicación eficiente a nivel de

bloques, lo que garantiza que el sitio de DR permanezca sincronizado con el entorno de producción a través de actualizaciones incrementales. Esto permite alcanzar un objetivo de punto de recuperación (RPO) de tan solo cinco minutos.

BlueXP DRaaS también admite pruebas de recuperación ante desastres sin interrupciones. Al aprovechar la tecnología FlexClone de ONTAP, crea copias temporales que ahorran espacio del almacén de datos NFS a partir de la instantánea replicada más reciente, sin afectar las cargas de trabajo de producción ni incurrir en costos de almacenamiento adicionales. Después de la prueba, el entorno se puede desmontar fácilmente, preservando la integridad de los datos replicados.

En el caso de una conmutación por error real, BlueXP orquesta el proceso de recuperación, activando automáticamente las máquinas virtuales protegidas en el sitio de recuperación ante desastres designado con una mínima intervención del usuario. Cuando se restaura el sitio principal, el servicio revierte la relación de SnapMirror y replica cualquier cambio en el sitio original, lo que permite una conmutación por error fluida y controlada.

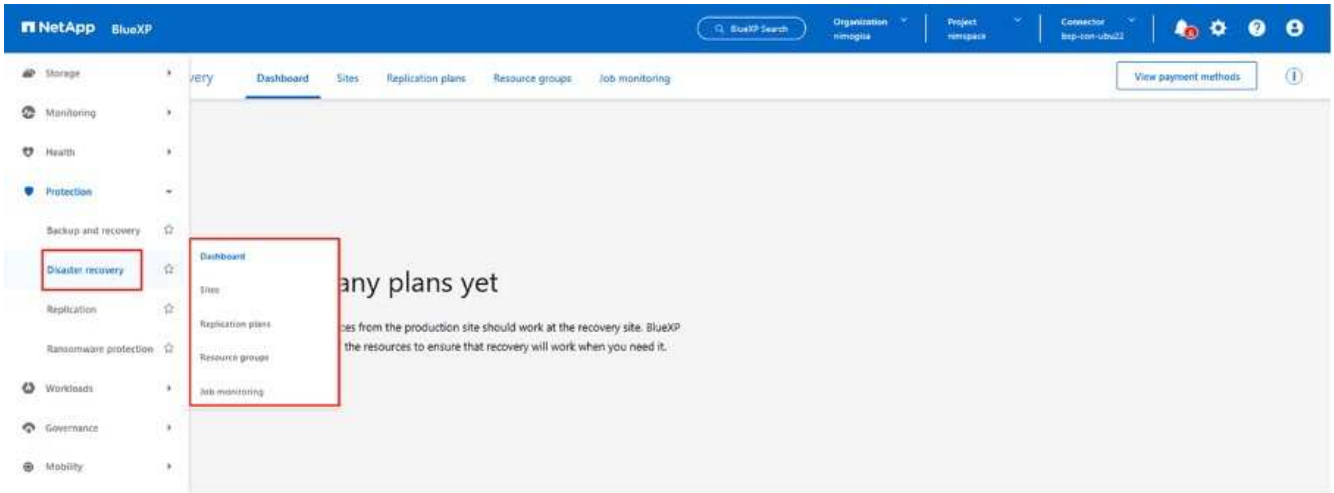
Todas estas capacidades se ofrecen a un coste significativamente menor en comparación con las soluciones tradicionales de recuperación ante desastres.



Empezando

Para comenzar con la BlueXP disaster recovery, utilice la consola de BlueXP y luego acceda al servicio.

1. Inicie sesión en BlueXP.
2. Desde la navegación izquierda de BlueXP , seleccione Protección > Recuperación ante desastres.
3. Aparece el panel de BlueXP disaster recovery .



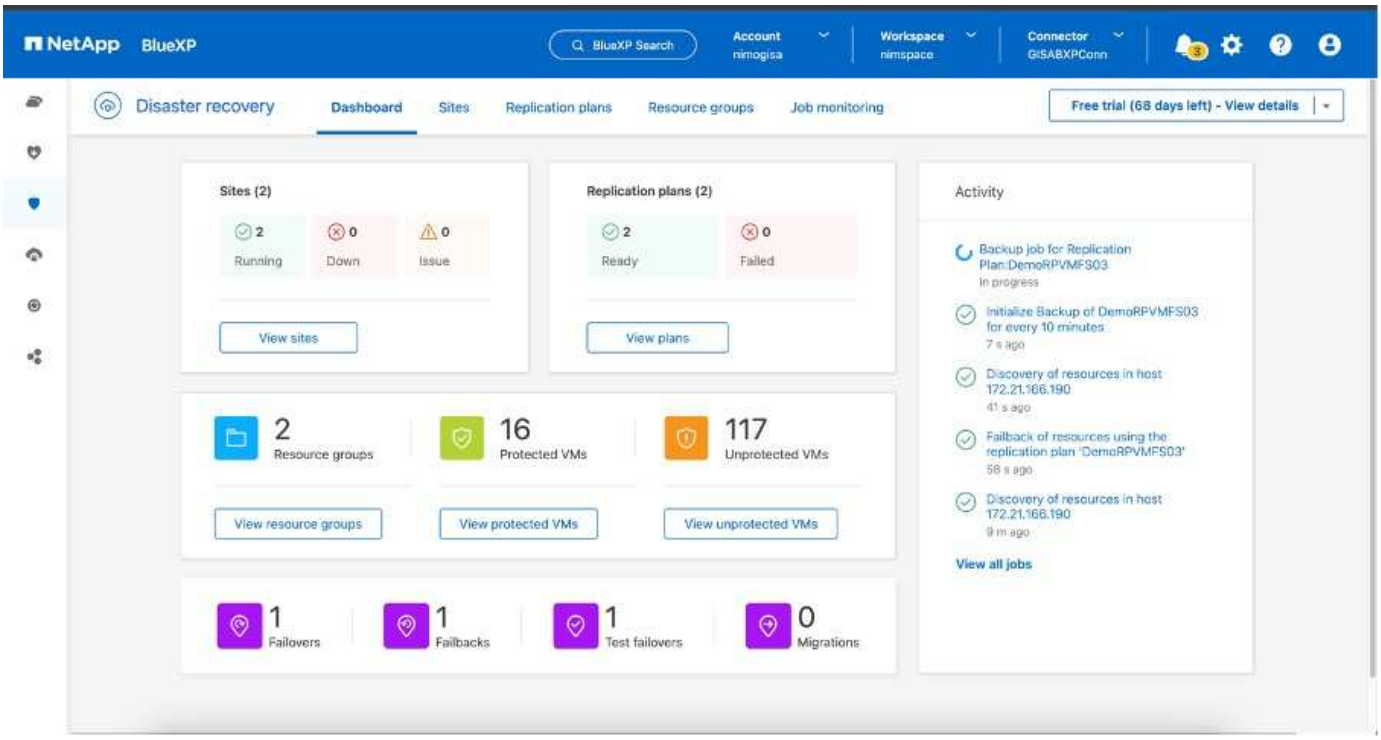
Antes de configurar el plan de recuperación ante desastres, asegúrese de lo siguiente"prerrequisitos" se cumplen:

- El conector BlueXP está configurado en NetApp BlueXP.
- La instancia del conector BlueXP tiene conectividad con el dominio de carga de trabajo de origen y destino vCenter y los sistemas de almacenamiento.
- Clúster NetApp Data ONTAP para proporcionar almacenes de datos NFS o VMFS.
- Los sistemas de almacenamiento NetApp locales que alojan almacenes de datos NFS o VMFS para VMware se agregan en BlueXP.
- La resolución de DNS debe estar vigente cuando se utilizan nombres DNS. De lo contrario, utilice direcciones IP para vCenter.
- La replicación de SnapMirror está configurada para los volúmenes de almacén de datos designados basados en NFS o VMFS.
- Asegúrese de que el entorno tenga versiones compatibles de vCenter Server y servidores ESXi.

Una vez establecida la conectividad entre los sitios de origen y destino, proceda con los pasos de configuración, que deberían tomar un par de clics y entre 3 y 5 minutos.

Nota: NetApp recomienda implementar el conector BlueXP en el sitio de destino o en un tercer sitio, para que el conector BlueXP pueda comunicarse a través de la red con los recursos de origen y destino.

En esta demostración, los dominios de carga de trabajo están configurados con almacenamiento NFS de ONTAP . Los pasos en términos de flujo de trabajo siguen siendo los mismos para los almacenes de datos basados en VMFS.



Configuración de BlueXP disaster recovery

El primer paso para prepararse para la recuperación ante desastres es descubrir y agregar el vCenter de origen y los recursos de almacenamiento a la BlueXP disaster recovery.

Abra la consola BlueXP y seleccione Protección > Recuperación ante desastres en la navegación izquierda. Seleccione Descubrir servidores vCenter o utilice el menú superior, seleccione Sitios > Agregar > Agregar vCenter.

Agregue las siguientes plataformas:

- Dominio de carga de trabajo de origen vCenter
- Dominio de carga de trabajo de destino vCenter.

Una vez que se agregan los vCenters, se activa el descubrimiento automático.

Configuración de la replicación de almacenamiento entre la matriz del sitio de origen y la matriz del sitio de destino

SnapMirror proporciona replicación de datos en un entorno NetApp . Basada en la tecnología NetApp Snapshot®, la replicación de SnapMirror es extremadamente eficiente porque replica solo los bloques que se han modificado o agregado desde la actualización anterior. SnapMirror se configura fácilmente mediante NetApp OnCommand® System Manager o la CLI de ONTAP . BlueXP DRaaS también crea la relación SnapMirror siempre que el peering de clúster y SVM esté configurado de antemano.

Para los casos en los que el almacenamiento principal no se pierde por completo, SnapMirror proporciona un medio eficiente para resincronizar los sitios primarios y de recuperación ante desastres. SnapMirror puede resincronizar los dos sitios, transfiriendo únicamente datos modificados o nuevos al sitio principal desde el sitio de recuperación ante desastres, simplemente invirtiendo las relaciones de SnapMirror . Esto significa que los planes de replicación en BlueXP DRaaS se pueden resincronizar en cualquier dirección después de una conmutación por error sin tener que volver a copiar todo el volumen. Si una relación se vuelve a sincronizar en la dirección inversa, solo los datos nuevos que se escribieron desde la última sincronización exitosa de la

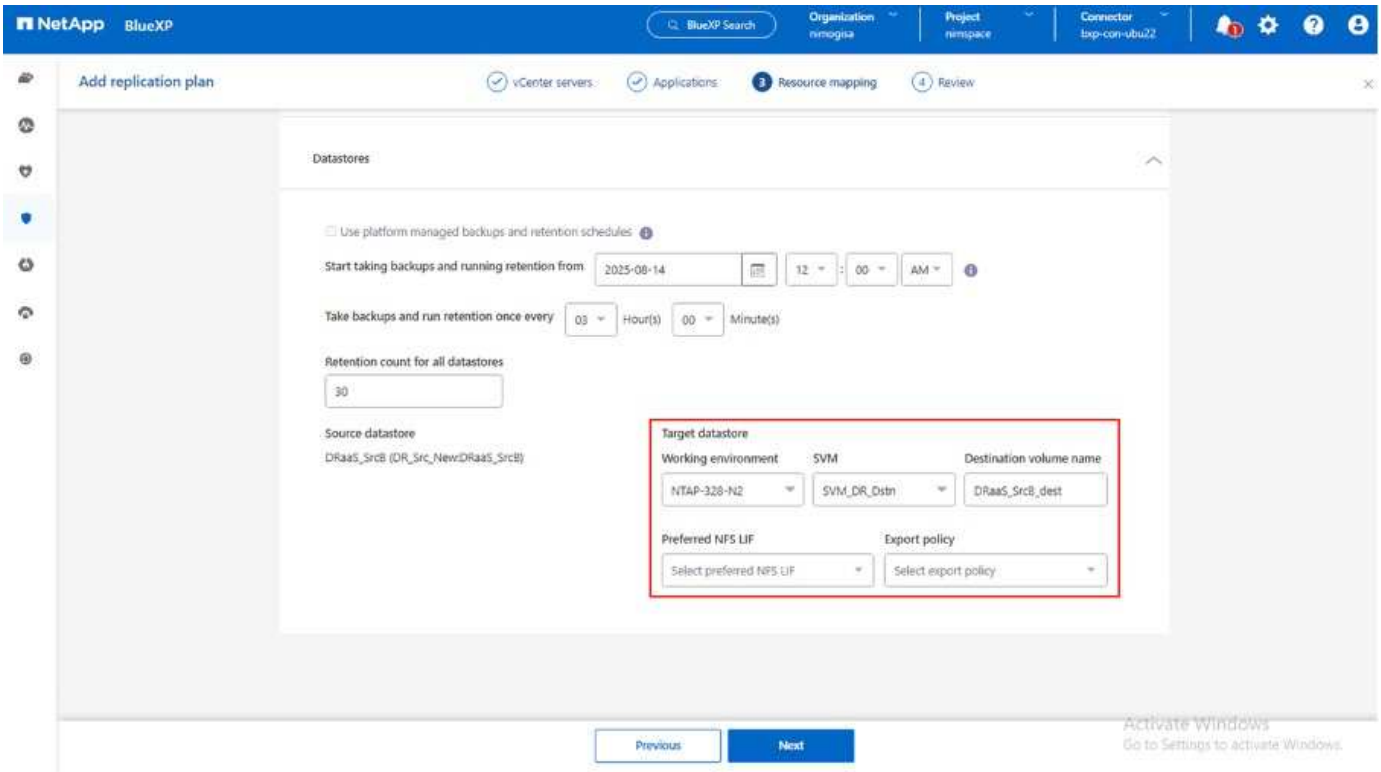
copia de la instantánea se envían de regreso al destino.

> Si la relación SnapMirror ya está configurada para el volumen a través de CLI o el Administrador del sistema, BlueXP DRaaS retoma la relación y continúa con el resto de las operaciones del flujo de trabajo.

Cómo configurarlo para VMware Disaster Recovery

El proceso para crear la replicación de SnapMirror sigue siendo el mismo para cualquier aplicación. El proceso puede ser manual o automatizado. La forma más sencilla es aprovechar BlueXP DRaaS, que automatizará lo mismo siempre que se cumplan los dos criterios siguientes:

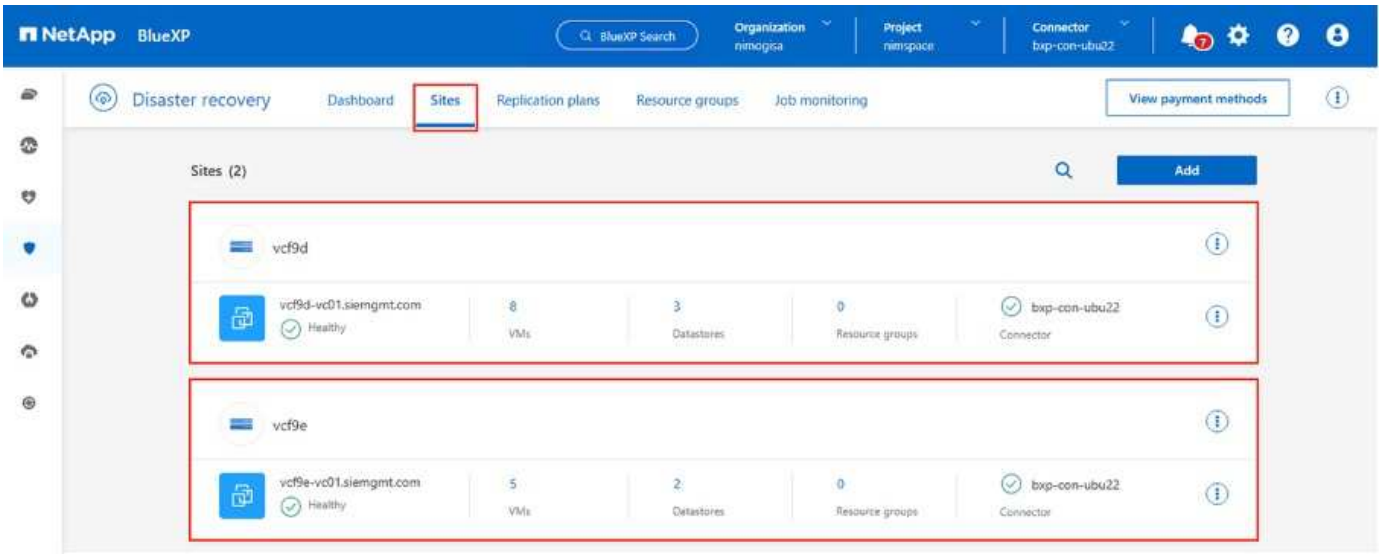
- Los clústeres de origen y destino tienen una relación de pares.
- El SVM de origen y el SVM de destino tienen una relación de pares.



BlueXP también proporciona una opción alternativa para configurar la replicación de SnapMirror mediante un simple arrastrar y soltar del sistema ONTAP de origen en el entorno al destino para activar el asistente que lo guía a través del resto del proceso.

¿Qué puede hacer por usted la BlueXP disaster recovery ?

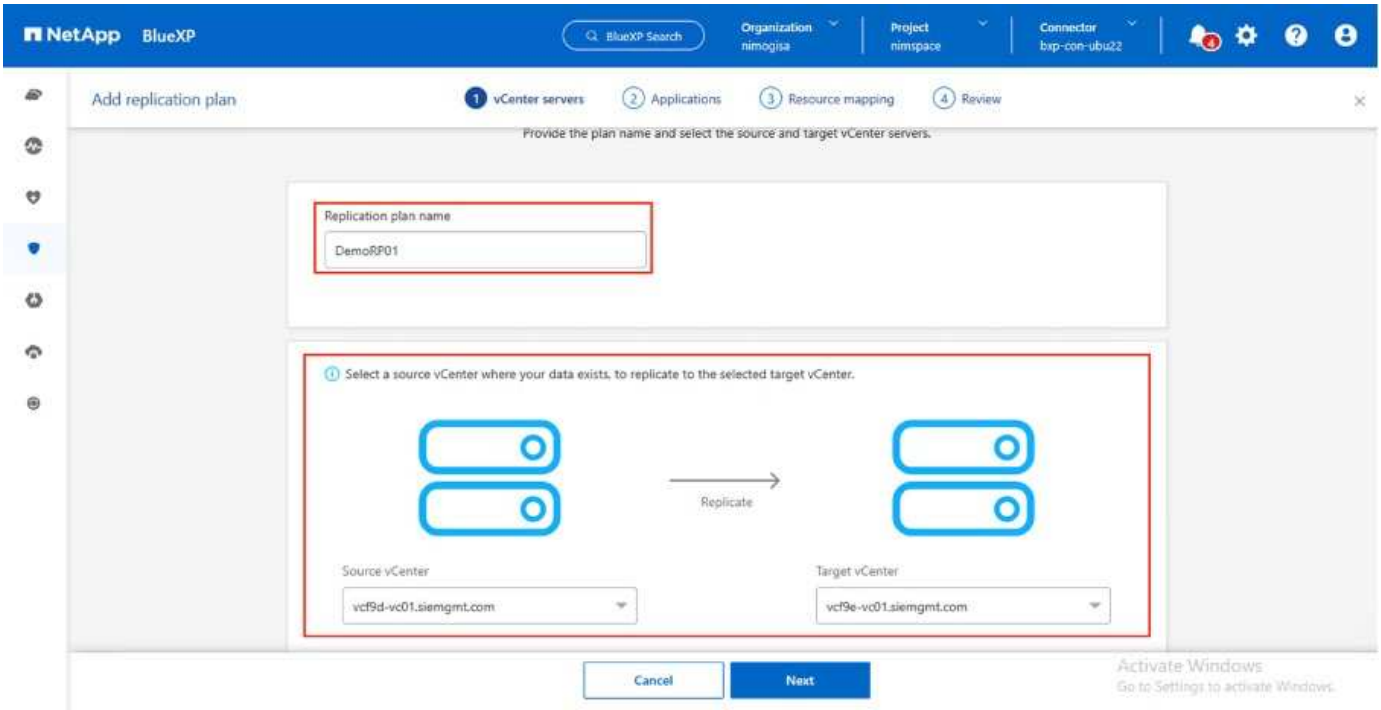
Una vez agregados los sitios de origen y destino, la BlueXP disaster recovery realiza un descubrimiento profundo automático y muestra las máquinas virtuales junto con los metadatos asociados. La BlueXP disaster recovery también detecta automáticamente las redes y los grupos de puertos utilizados por las máquinas virtuales y los completa.



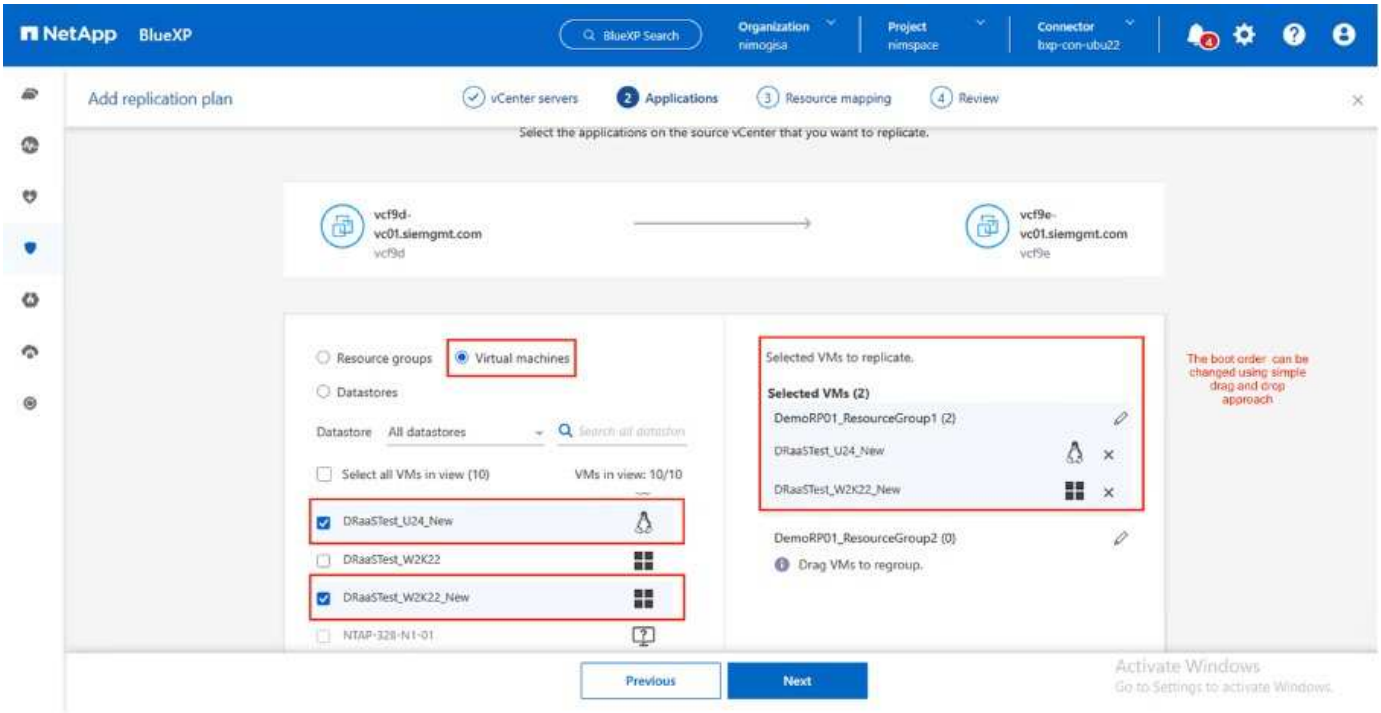
Una vez agregados los sitios, configure el plan de replicación seleccionando las plataformas vCenter de origen y destino del menú desplegable y elija los grupos de recursos que se incluirán en el plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones y el mapeo de clústeres y redes. Para definir el plan de recuperación, navegue a la pestaña **Plan de replicación** y haga clic en **Agregar plan**.

En este paso, las máquinas virtuales se pueden agrupar en grupos de recursos. Los grupos de recursos de BlueXP disaster recovery le permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque y los retrasos de arranque que se pueden ejecutar durante la recuperación. El grupo de recursos también se puede crear utilizando la pestaña Grupo de recursos.

Primero, seleccione el vCenter de origen y luego seleccione el vCenter de destino.



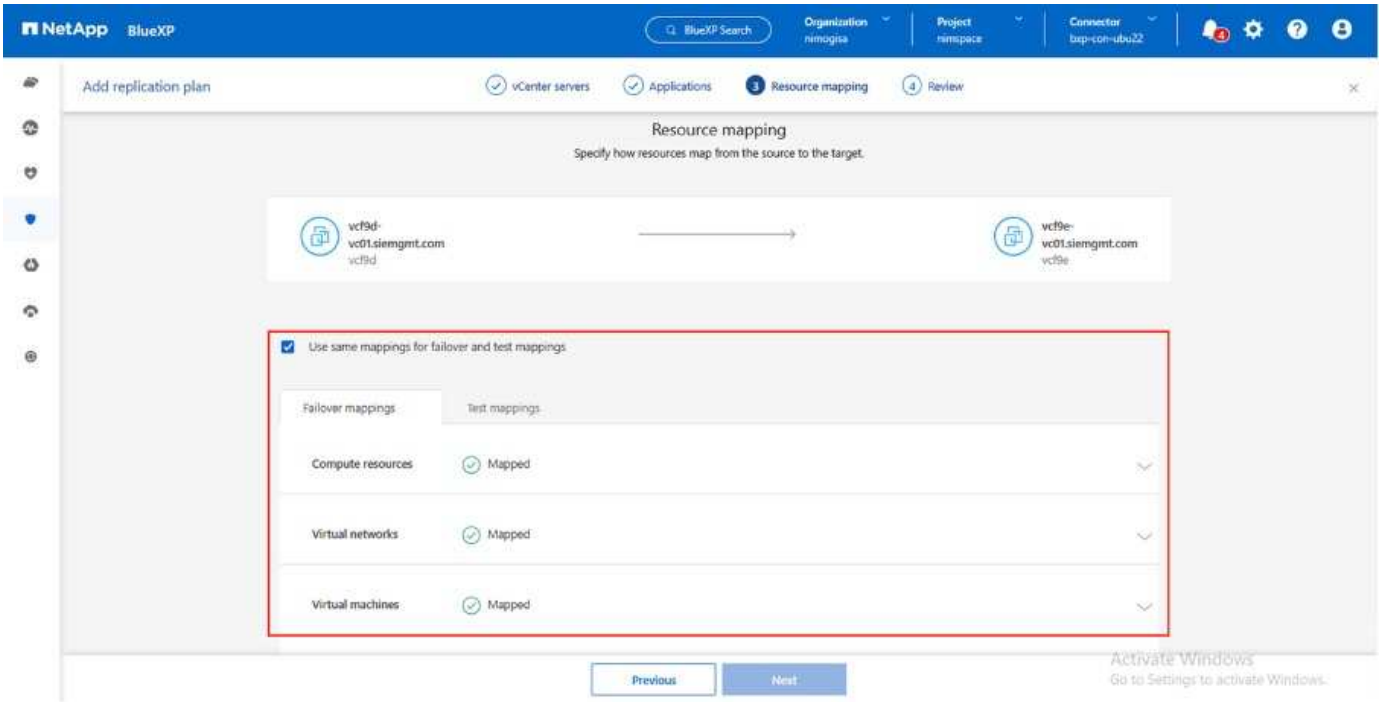
El siguiente paso es seleccionar los grupos de recursos existentes. Si no se crean grupos de recursos, el asistente ayuda a agrupar las máquinas virtuales necesarias (básicamente, crea grupos de recursos funcionales) en función de los objetivos de recuperación. Esto también ayuda a definir la secuencia de operaciones de cómo se deben restaurar las máquinas virtuales de la aplicación.



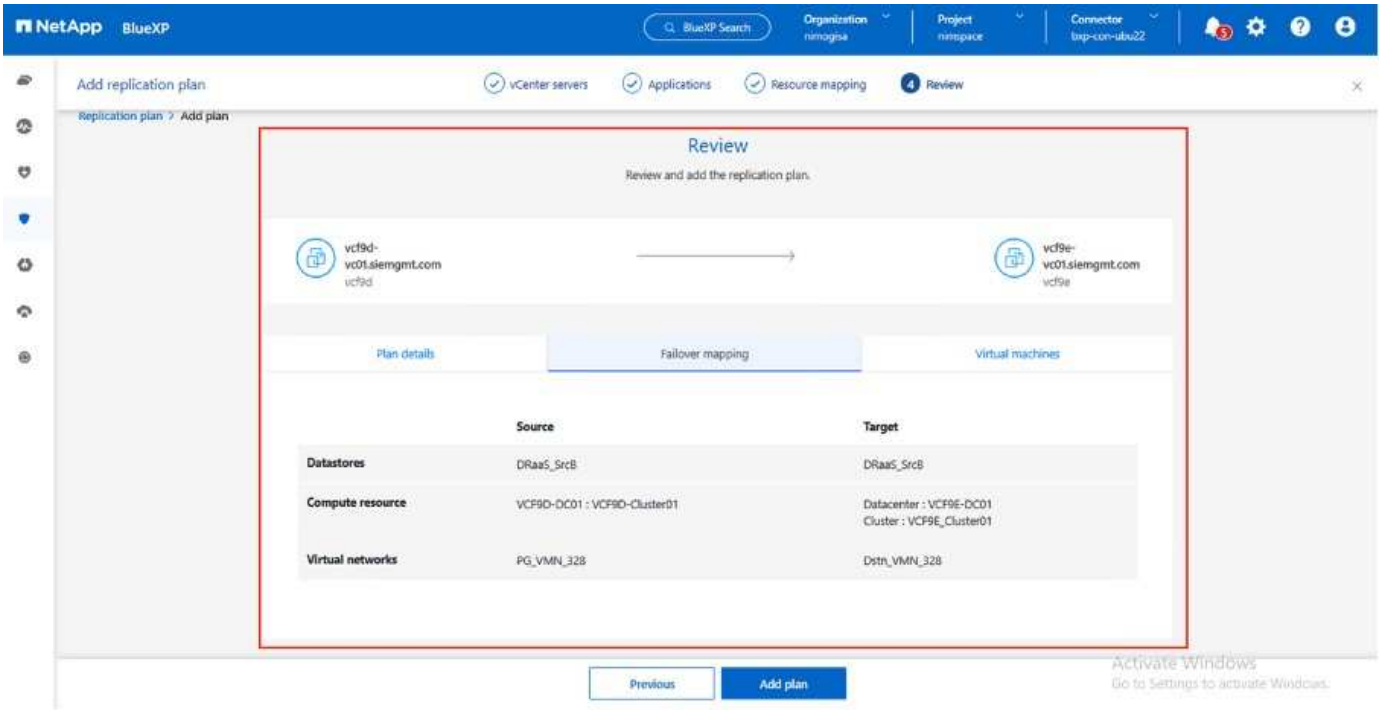
El grupo de recursos permite establecer el orden de arranque mediante la funcionalidad de arrastrar y soltar. Se puede utilizar para modificar fácilmente el orden en que se encenderán las máquinas virtuales durante el proceso de recuperación.

Una vez creados los grupos de recursos a través del plan de replicación, el siguiente paso es seleccionar el plan o una asignación para recuperar máquinas virtuales y aplicaciones en caso de desastre. En este paso, especifique cómo se asignan los recursos del entorno de origen al destino. Esto incluye recursos computacionales, redes virtuales, personalización de IP, scripts previos y posteriores, retrasos de arranque, consistencia de la aplicación, etc. Para obtener información detallada, consulte"Crear un plan de replicación" . Como se menciona en los requisitos previos, la replicación de SnapMirror se puede configurar de antemano o DRaaS puede configurarla utilizando el RPO y el recuento de retención especificados durante la creación del plan de replicación.

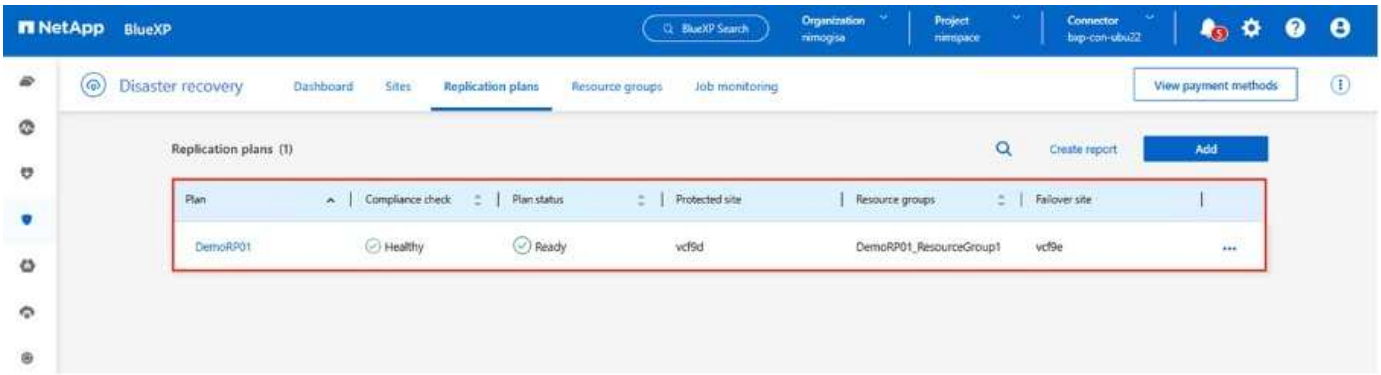
Nota: De forma predeterminada, se utilizan los mismos parámetros de asignación para las operaciones de prueba y de conmutación por error. Para configurar diferentes asignaciones para el entorno de prueba, seleccione la opción Asignación de prueba después de desmarcar la casilla de verificación “Usar las mismas asignaciones para conmutación por error y asignaciones de prueba”. Una vez completado el mapeo de recursos, haga clic en Siguiente.



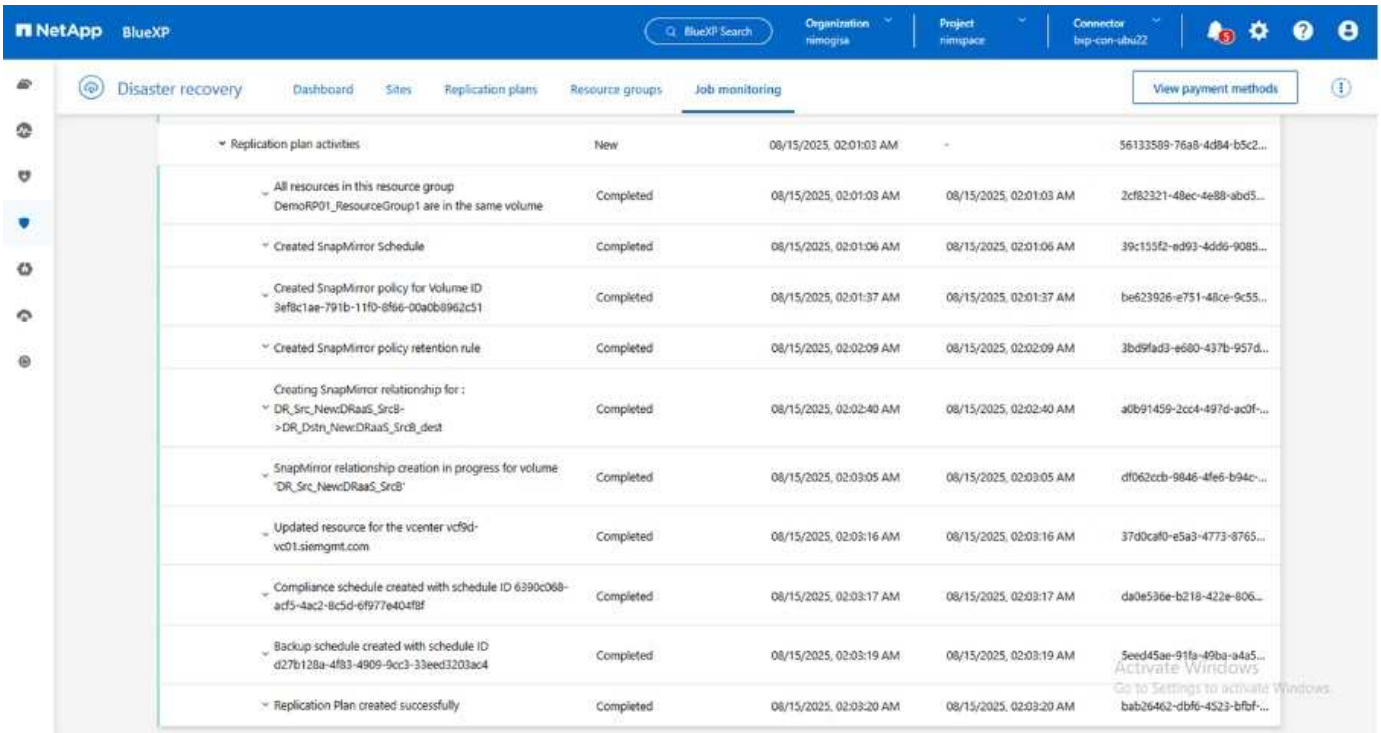
Una vez hecho esto, revise los mapeos creados y luego haga clic en Agregar plan.



Se pueden incluir máquinas virtuales de diferentes volúmenes y SVM en un plan de replicación. Dependiendo de la ubicación de la VM (ya sea en el mismo volumen o en un volumen separado dentro de la misma SVM, volúmenes separados en diferentes SVM), la BlueXP disaster recovery crea una instantánea de grupo de consistencia.

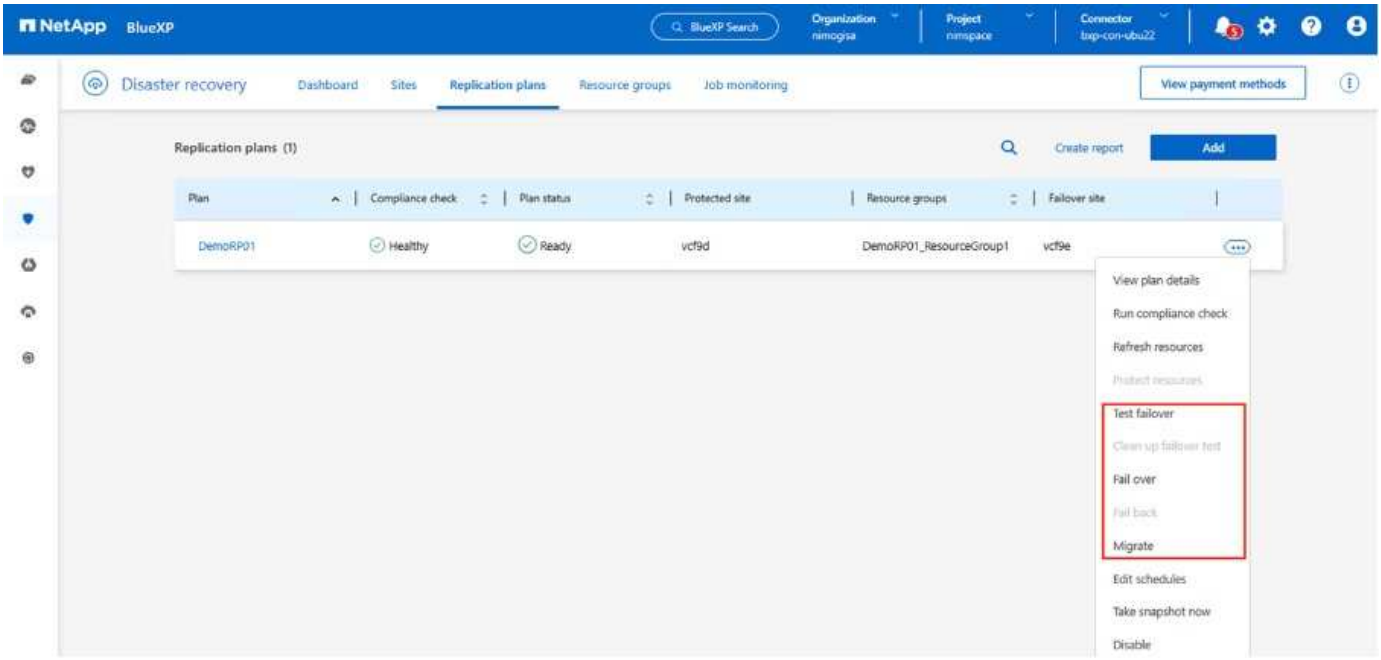


Tan pronto como se crea el plan, se activan una serie de validaciones y se configuran la replicación y las programaciones de SnapMirror según la selección.



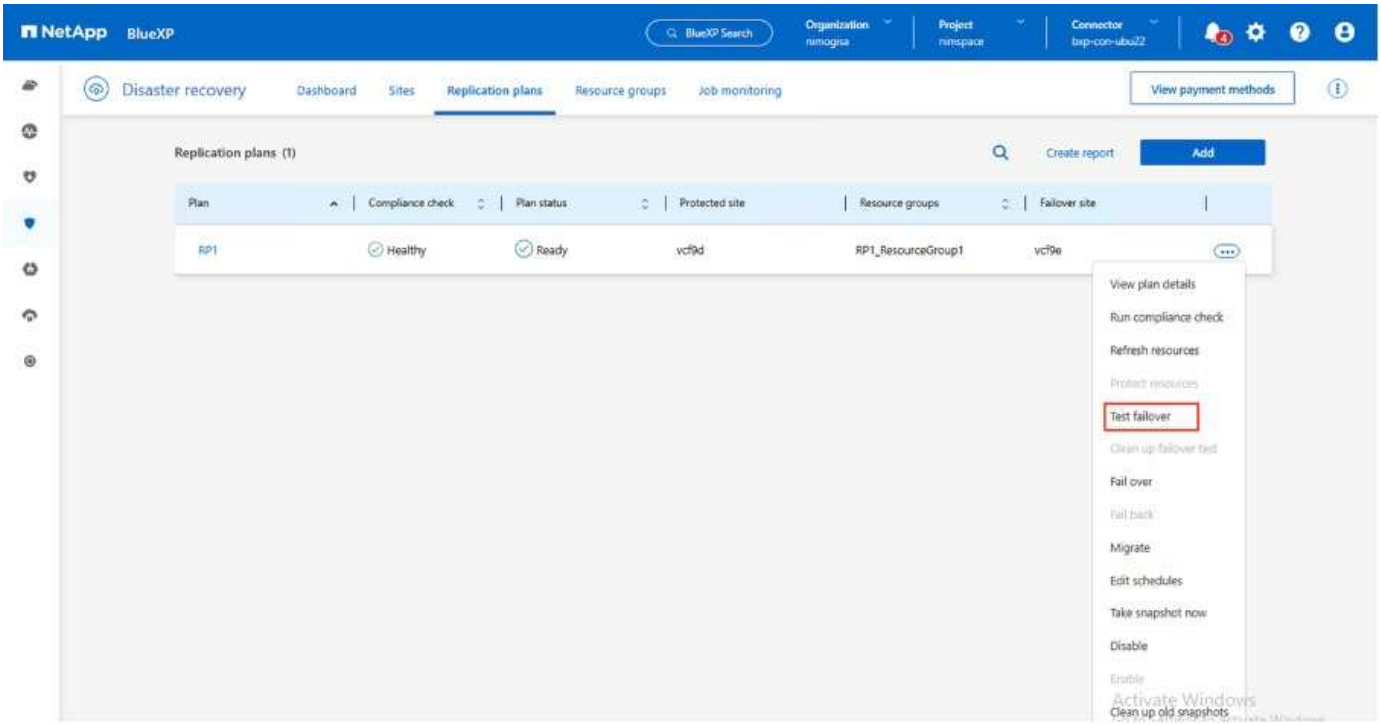
BlueXP DRaaS consta de los siguientes flujos de trabajo:

- Conmutación por error de prueba (incluidas simulaciones automatizadas periódicas)
- Prueba de conmutación por error de limpieza
- Conmutación por error:
  - Migración planificada (ampliar el caso de uso para una conmutación por error única)
  - Recuperación ante desastres
- Recuperación por recuperación

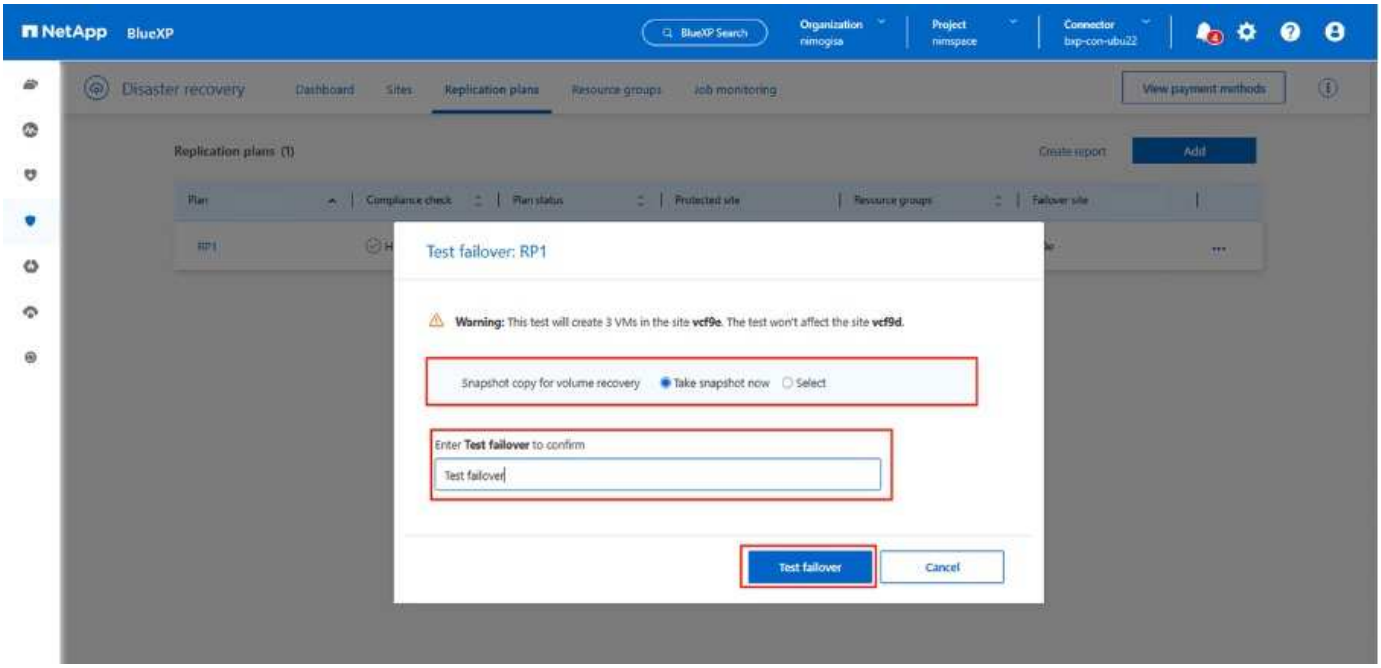


Prueba de conmutación por error

La conmutación por error de prueba en BlueXP DRaaS es un procedimiento operativo que permite a los administradores de VMware validar completamente sus planes de recuperación sin interrumpir sus entornos de producción.

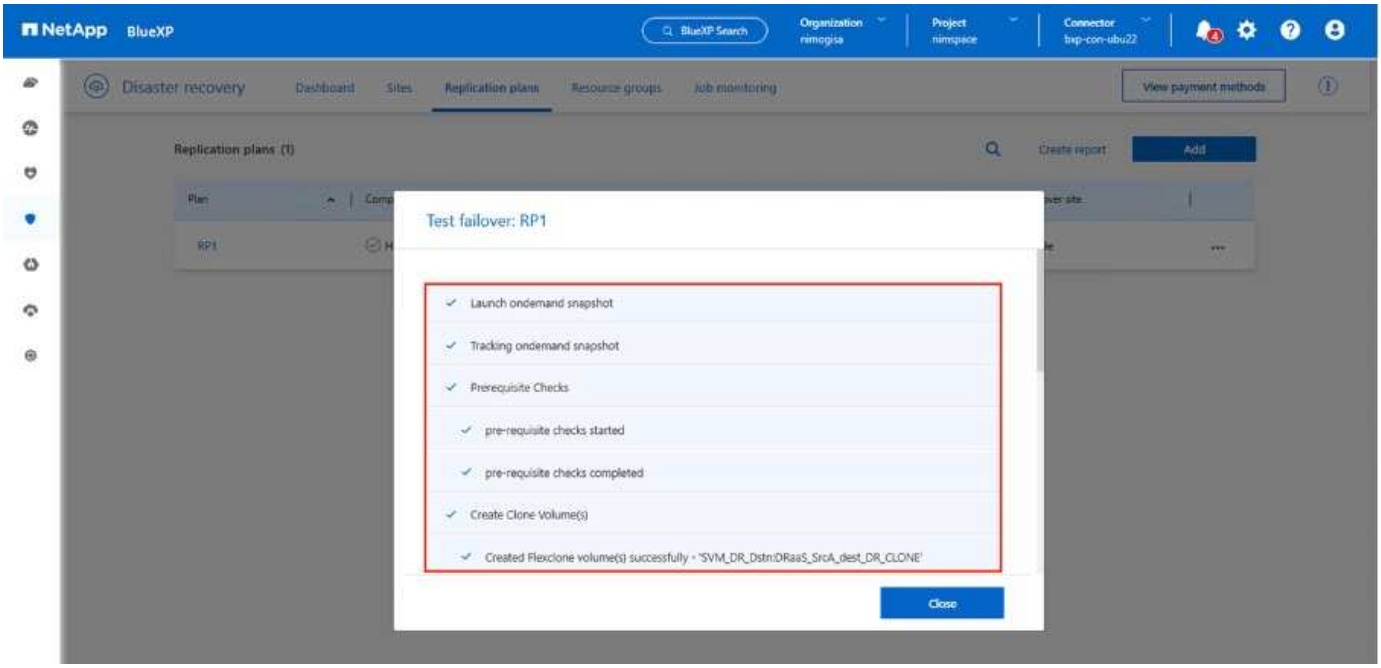


BlueXP DRaaS incorpora la capacidad de seleccionar la instantánea como una capacidad opcional en la operación de conmutación por error de prueba. Esta capacidad permite al administrador de VMware verificar que cualquier cambio realizado recientemente en el entorno se replique en el sitio de destino y, por lo tanto, esté presente durante la prueba. Estos cambios incluyen parches para el sistema operativo invitado de la máquina virtual.



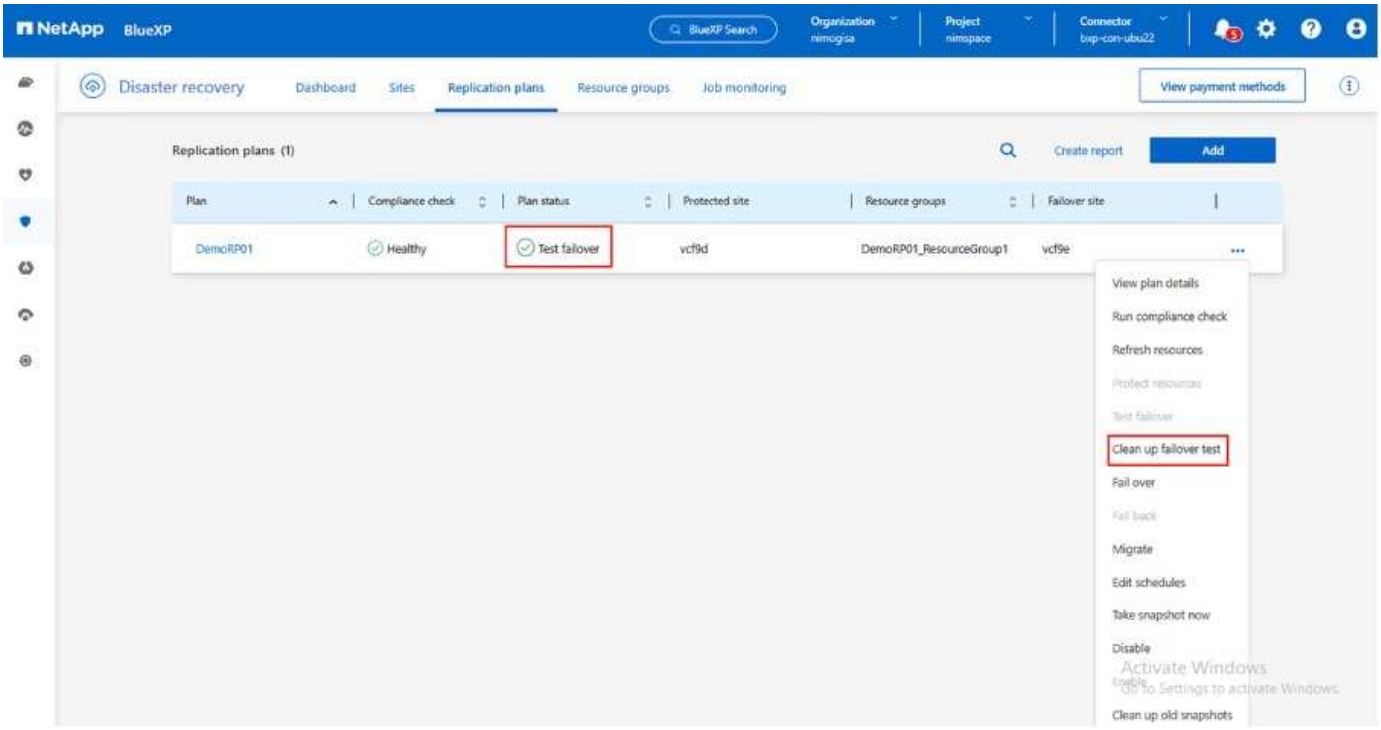
Cuando el administrador de VMware ejecuta una operación de conmutación por error de prueba, BlueXP DRaaS automatiza las siguientes tareas:

- Activar relaciones de SnapMirror para actualizar el almacenamiento en el sitio de destino con cualquier cambio reciente que se haya realizado en el sitio de producción.
- Creación de volúmenes NetApp FlexClone de los volúmenes FlexVol en la matriz de almacenamiento DR.
- Conexión de los almacenes de datos en los volúmenes FlexClone a los hosts ESXi en el sitio de recuperación ante desastres.
- Conectar los adaptadores de red de la máquina virtual a la red de prueba especificada durante la asignación.
- Reconfigurar la configuración de red del sistema operativo invitado de la máquina virtual según lo definido para la red en el sitio de recuperación ante desastres.
- Ejecutar cualquier comando personalizado que se haya almacenado en el plan de replicación.
- Encender las máquinas virtuales en el orden definido en el plan de replicación.



Operación de prueba de conmutación por error de limpieza

La operación de prueba de conmutación por error de limpieza se produce después de que se haya completado la prueba del plan de replicación y el administrador de VMware responda al mensaje de limpieza.

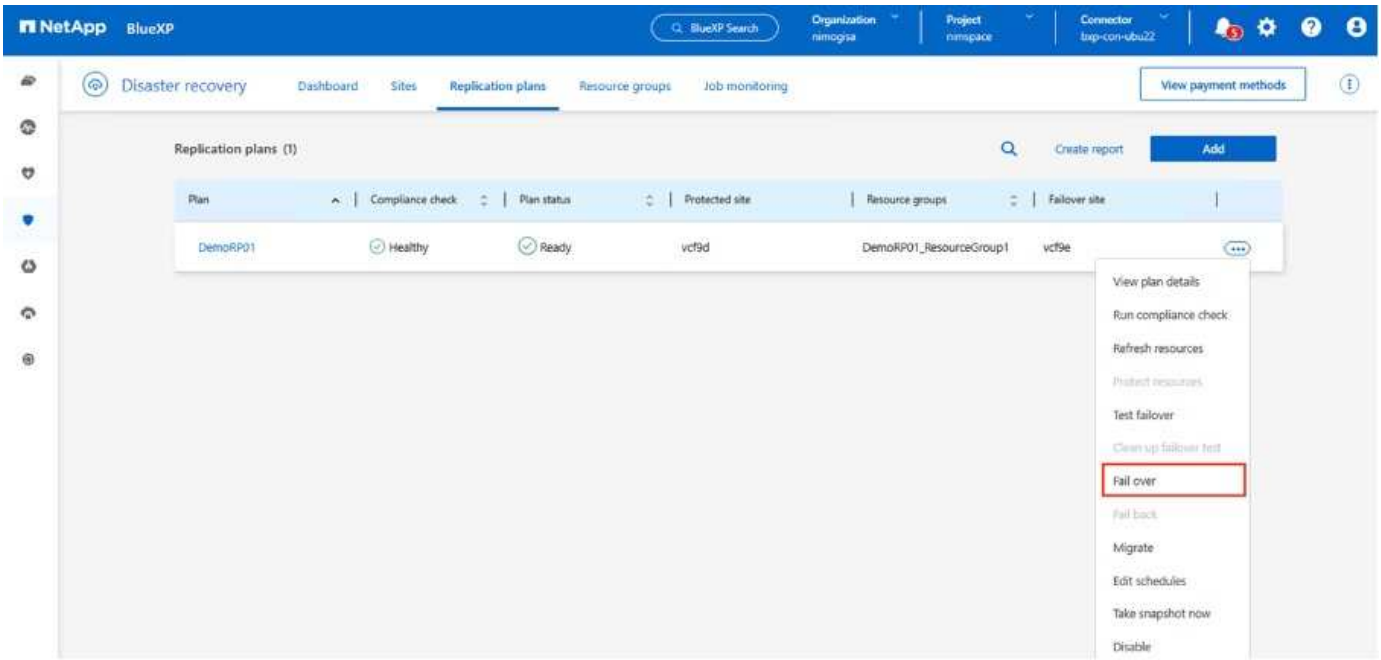


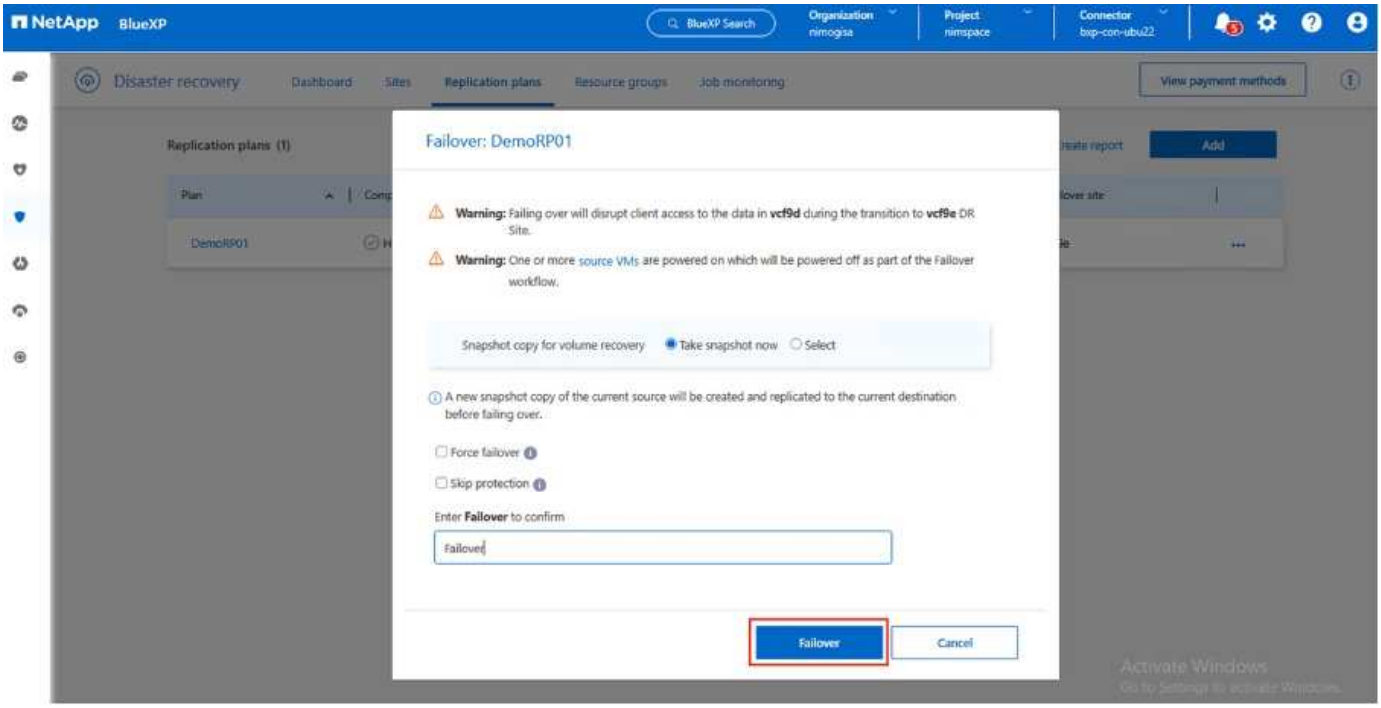
Esta acción restablecerá las máquinas virtuales (VM) y el estado del plan de replicación al estado listo. Cuando el administrador de VMware realiza una operación de recuperación, BlueXP DRaaS completa el siguiente proceso:

1. Apaga cada VM recuperada en la copia FlexClone que se utilizó para la prueba.
2. Elimina el volumen FlexClone que se utilizó para presentar las máquinas virtuales recuperadas durante la prueba.

Migración planificada y conmutación por error

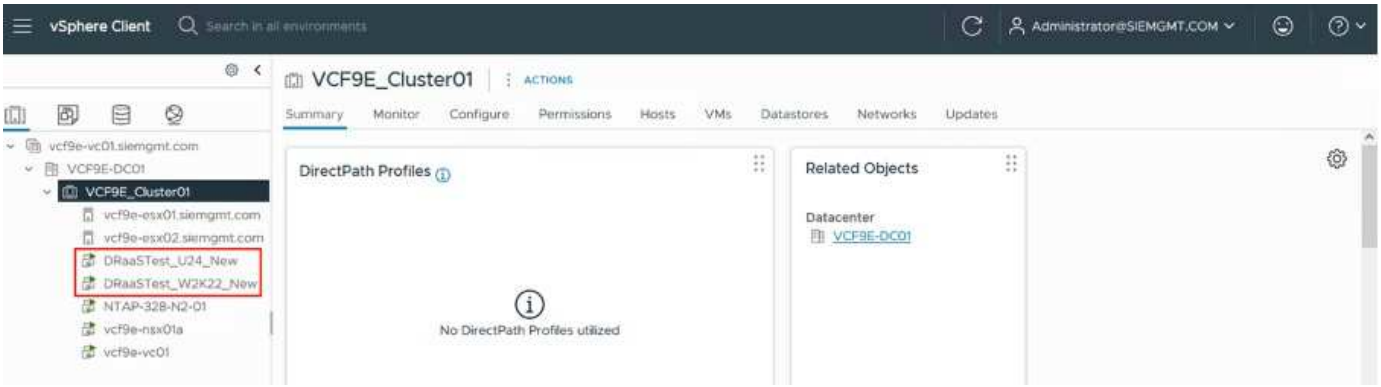
BlueXP DRaaS tiene dos métodos para realizar una conmutación por error real: migración planificada y conmutación por error. El primer método, la migración planificada, incorpora el apagado de la máquina virtual y la sincronización de la replicación del almacenamiento en el proceso para recuperar o mover eficazmente las máquinas virtuales al sitio de destino. La migración planificada requiere acceso al sitio de origen. El segundo método, conmutación por error, es una conmutación por error planificada/no planificada en la que las máquinas virtuales se recuperan en el sitio de destino desde el último intervalo de replicación de almacenamiento que pudo completarse. Dependiendo del RPO que se diseñó en la solución, se puede esperar cierta cantidad de pérdida de datos en el escenario de recuperación ante desastres.





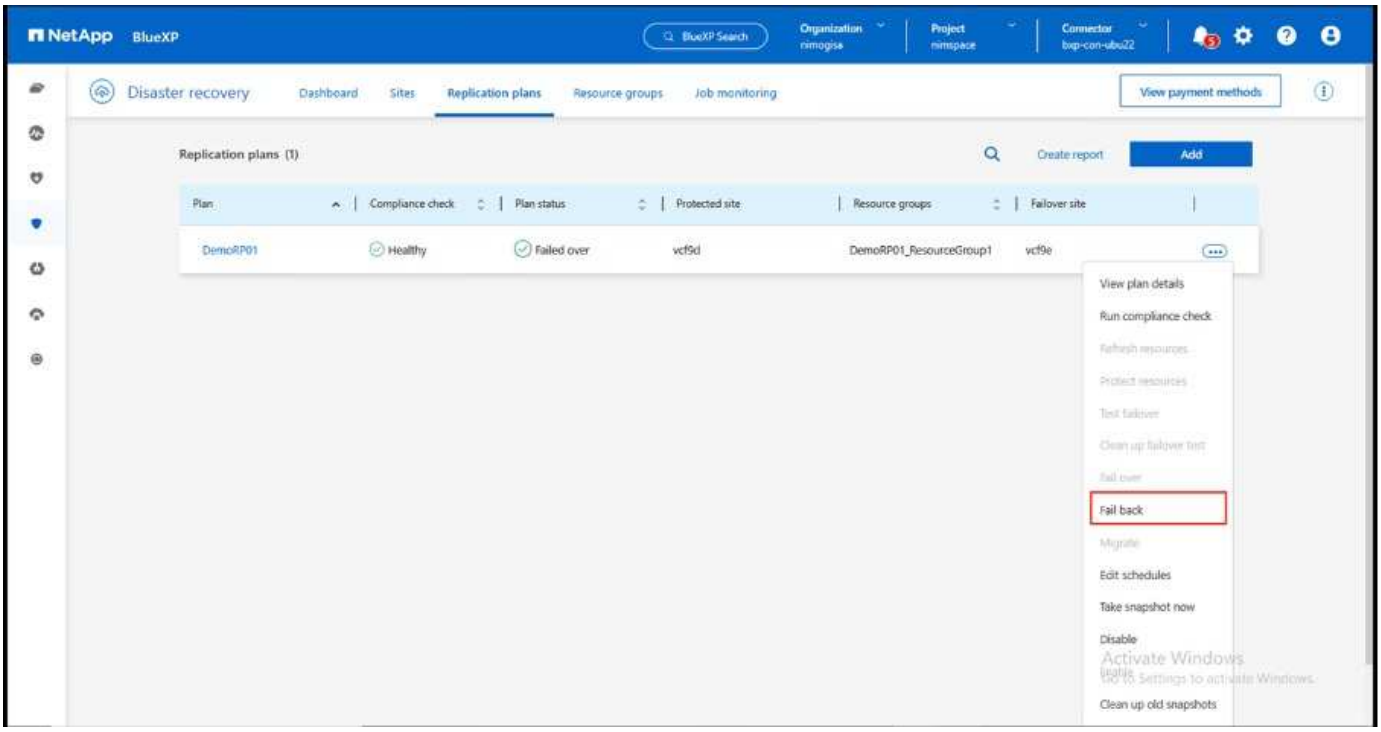
Cuando el administrador de VMware realiza una operación de conmutación por error, BlueXP DRaaS automatiza las siguientes tareas:

- Romper y conmutar por error las relaciones de NetApp SnapMirror .
- Conecte los almacenes de datos replicados a los hosts ESXi en el sitio de recuperación ante desastres.
- Conecte los adaptadores de red de la máquina virtual a la red del sitio de destino apropiado.
- Reconfigure la configuración de red del sistema operativo invitado de la máquina virtual según lo definido para la red en el sitio de destino.
- Ejecute cualquier comando personalizado (si hay alguno) que se haya almacenado en el plan de replicación.
- Encienda las máquinas virtuales en el orden definido en el plan de replicación.



Recuperación por recuperación

Una conmutación por recuperación es un procedimiento opcional que restaura la configuración original de los sitios de origen y destino después de una recuperación.

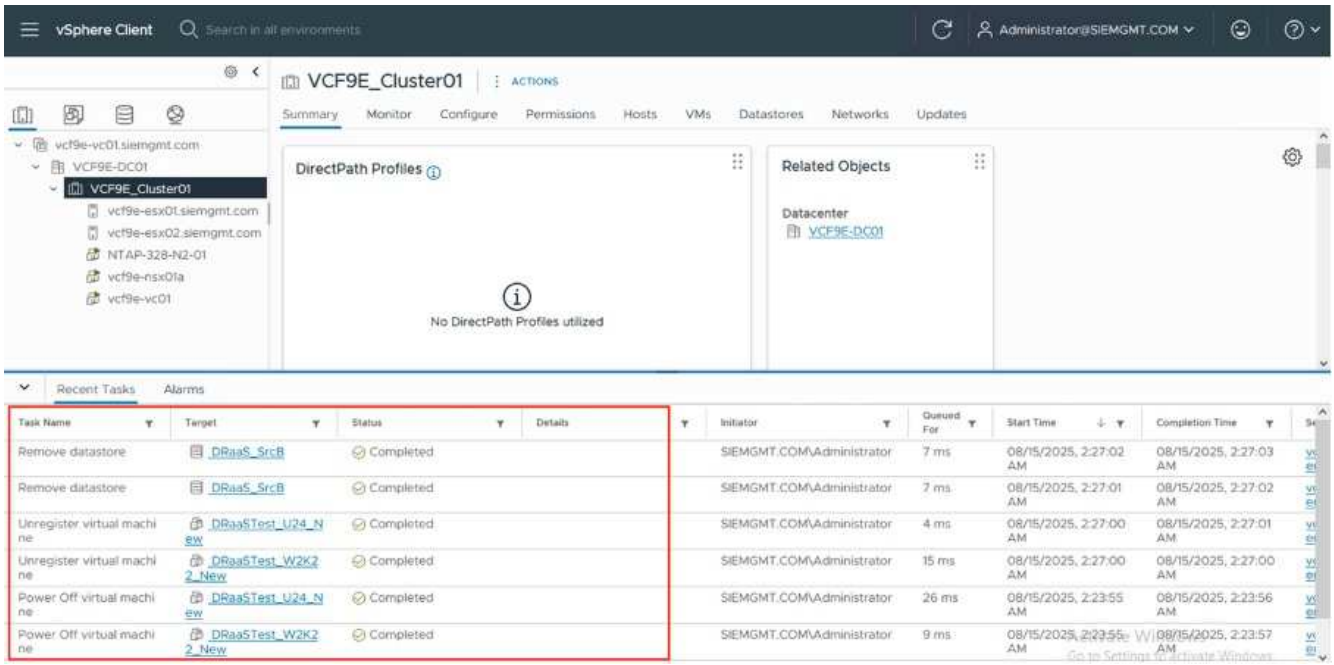


Los administradores de VMware pueden configurar y ejecutar un procedimiento de conmutación por error cuando estén listos para restaurar los servicios en el sitio de origen original.

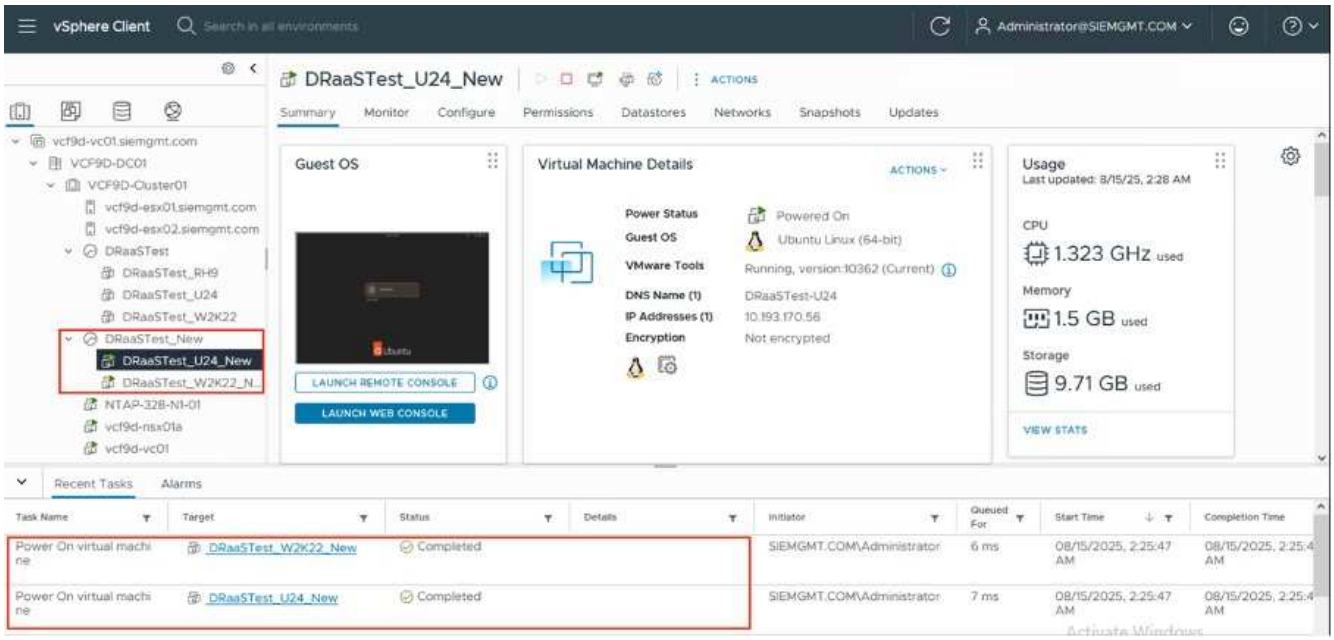
BlueXP DRaaS replica (resincroniza) cualquier cambio en la máquina virtual de origen original antes de revertir la dirección de replicación.

Este proceso comienza a partir de una relación que ha completado la conmutación por error a un destino e implica los siguientes pasos:

- Apague y anule el registro de las máquinas virtuales y los volúmenes en el sitio de destino se desmontan.



- Romper la relación SnapMirror en la fuente original se rompe para hacerla de lectura/escritura.
- Vuelva a sincronizar la relación SnapMirror para revertir la replicación.
- Monte el volumen en la fuente, encienda y registre las máquinas virtuales de origen.

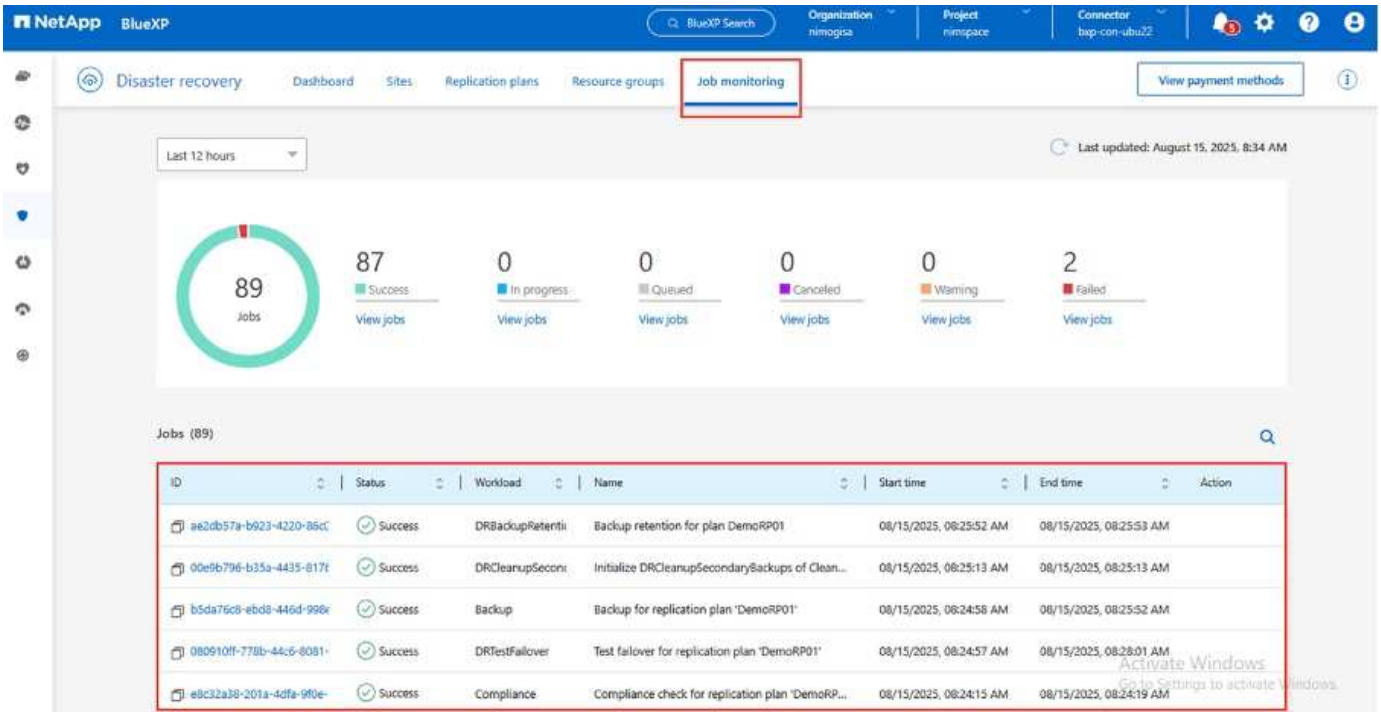


Para obtener más detalles sobre cómo acceder y configurar BlueXP DRaaS, consulte la"Obtenga más

información sobre BlueXP Disaster Recovery para VMware" .

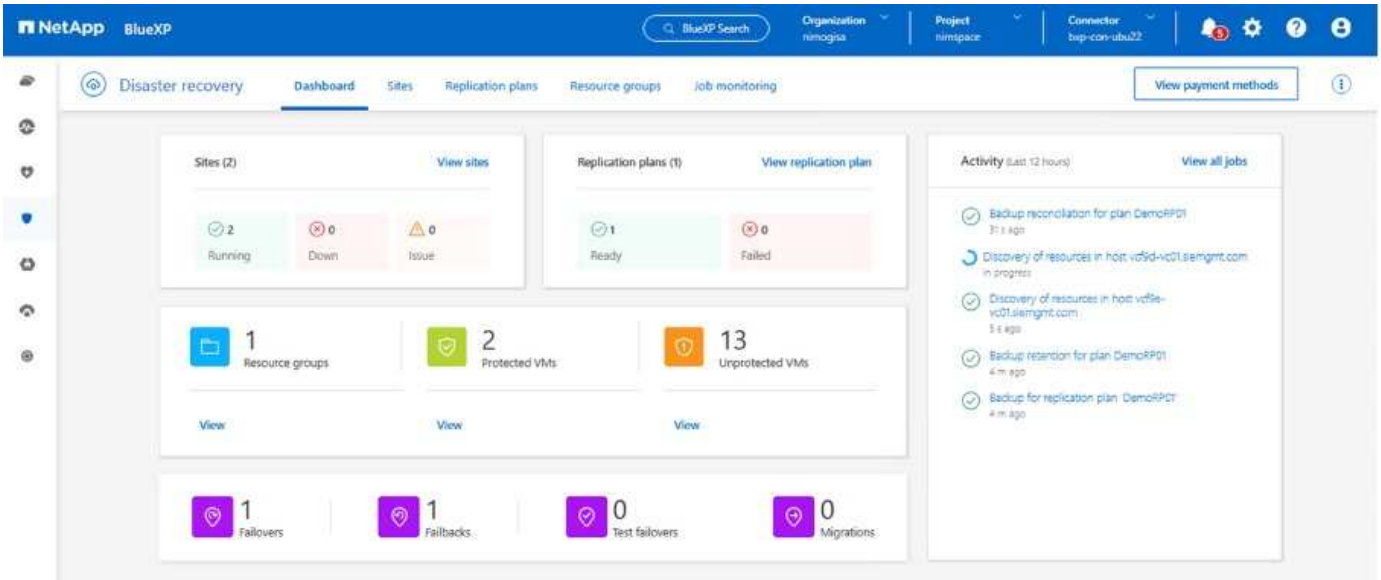
Monitoreo y tablero de control

Desde BlueXP o la CLI de ONTAP , puede supervisar el estado de salud de la replicación para los volúmenes de almacén de datos adecuados, y el estado de una conmutación por error o de una conmutación por error de prueba se puede rastrear a través de la Supervisión de trabajos.



Si un trabajo está actualmente en progreso o en cola y desea detenerlo, existe una opción para cancelarlo.

Con el panel de BlueXP disaster recovery , evalúe con confianza el estado de los sitios de recuperación ante desastres y los planes de replicación. Esto permite a los administradores identificar rápidamente sitios y planes saludables, desconectados o degradados.



Esto proporciona una solución poderosa para gestionar un plan de recuperación ante desastres personalizado y adaptado. La conmutación por error se puede realizar de forma planificada o con solo hacer clic en un botón cuando ocurre un desastre y se toma la decisión de activar el sitio de recuperación ante desastres.

Convertir clústeres de vSphere existentes a VCF

Obtenga información sobre cómo convertir un entorno de vSphere con almacenes de datos existentes a VCF

La conversión de un entorno vSphere con almacenes de datos existentes que se ejecutan en ONTAP en un entorno VMware Cloud Foundation (VCF) implica integrar la infraestructura actual en una arquitectura de nube privada moderna.

Este proceso aprovecha la flexibilidad del almacenamiento ONTAP para lograr un acceso y una gestión de datos sin inconvenientes. Una vez establecido el dominio de administración de VCF, los administradores pueden importar de manera eficiente entornos vSphere adicionales al ecosistema de VCF. Esta integración mejora la utilización de recursos, simplifica la gestión de la nube privada y garantiza una transición fluida con una interrupción mínima de las cargas de trabajo existentes.

Consulte las siguientes soluciones para conocer los detalles técnicos de la conversión de una instancia de vCenter.

- "Convertir una instancia de vCenter existente en un dominio de administración de VCF (NFS)"
- "Convertir una instancia de vCenter (almacén de datos FC) en un dominio de administración de VCF"

Convertir una instancia de servidor vCenter en un dominio de administración VCF (almacén de datos NFS)

Convierta un clúster vSphere 8 existente con almacenes de datos NFS de NetApp ONTAP en un dominio de administración de VMware Cloud Foundation (VCF). Este procedimiento incluye el aprovisionamiento de almacenamiento NFS, la implementación de herramientas ONTAP para VMware y el uso de la herramienta de importación VCF para convertir el clúster para una administración optimizada y una utilización optimizada de los recursos dentro de VCF.

Introducción

La conversión de un clúster con un almacén de datos NFS existente que se ejecuta en ONTAP implica integrar la infraestructura existente en una arquitectura de nube privada moderna. Este proceso se beneficia de la flexibilidad del almacenamiento NFS para garantizar un acceso y una gestión de datos sin inconvenientes. Una vez establecido un dominio de administración de VCF a través del proceso de conversión, los administradores pueden importar de manera eficiente clústeres de vSphere adicionales, incluidos aquellos que usan almacenes de datos NFS, en el ecosistema de VCF. Esta integración no solo mejora la utilización de recursos, sino que también simplifica la gestión de la infraestructura de nube privada, lo que garantiza una transición fluida con una interrupción mínima de las cargas de trabajo existentes.

En esta solución demostraremos cómo un almacén de datos NFS en vSphere 8 se convierte en almacenamiento principal cuando el clúster se convierte en un dominio de administración de VCF.

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Implementar ONTAP tools for VMware vSphere 10.
- Aprovisione un almacén de datos NFS mediante herramientas ONTAP .
- Utilice la herramienta de importación VCF para validar el clúster vSphere.
- Implemente SDDC Manager en el clúster de vSphere.
- Configure un archivo JSON para crear NSX durante la conversión VCF.
- Utilice la herramienta de importación de VCF para convertir el clúster vSphere 8 a VCF 5.2.

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Sistema de almacenamiento NetApp AFF con una máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico NFS.
- Se ha creado una interfaz lógica (LIF) en la red IP que transportará el tráfico NFS y está asociada con la SVM.
- Un clúster vSphere 8 con 4 hosts ESXi y un dispositivo vCenter ubicado en el clúster.
- Grupo de puertos distribuidos configurado para el tráfico de almacenamiento NFS y vMotion en las VLAN o segmentos de red establecidos para este propósito.
- Descargue el software necesario para la conversión VCF.

Las ONTAP tools for VMware vSphere 10 se pueden instalar en configuraciones HA o no HA. Para obtener información completa sobre los requisitos previos para las herramientas ONTAP , consulte "Requisitos previos para las ONTAP tools for VMware vSphere" .

Para conocer el almacenamiento compatible y otras consideraciones para convertir o importar vSphere a VCF 5.2, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

Para el software requerido, vaya a "Portal de soporte de Broadcom" .

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Pasos de implementación

La solución cubre el uso de ONTAP tools for VMware vSphere para aprovisionar almacenes de datos NFS y el proceso de conversión de un clúster vSphere 8 existente a un dominio de administración VCF.

Complete los siguientes pasos:

- Implementar ONTAP tools for VMware vSphere 10.
- Aprovisione un almacén de datos NFS mediante herramientas ONTAP .
- Copie la herramienta de importación VCF al dispositivo vCenter.

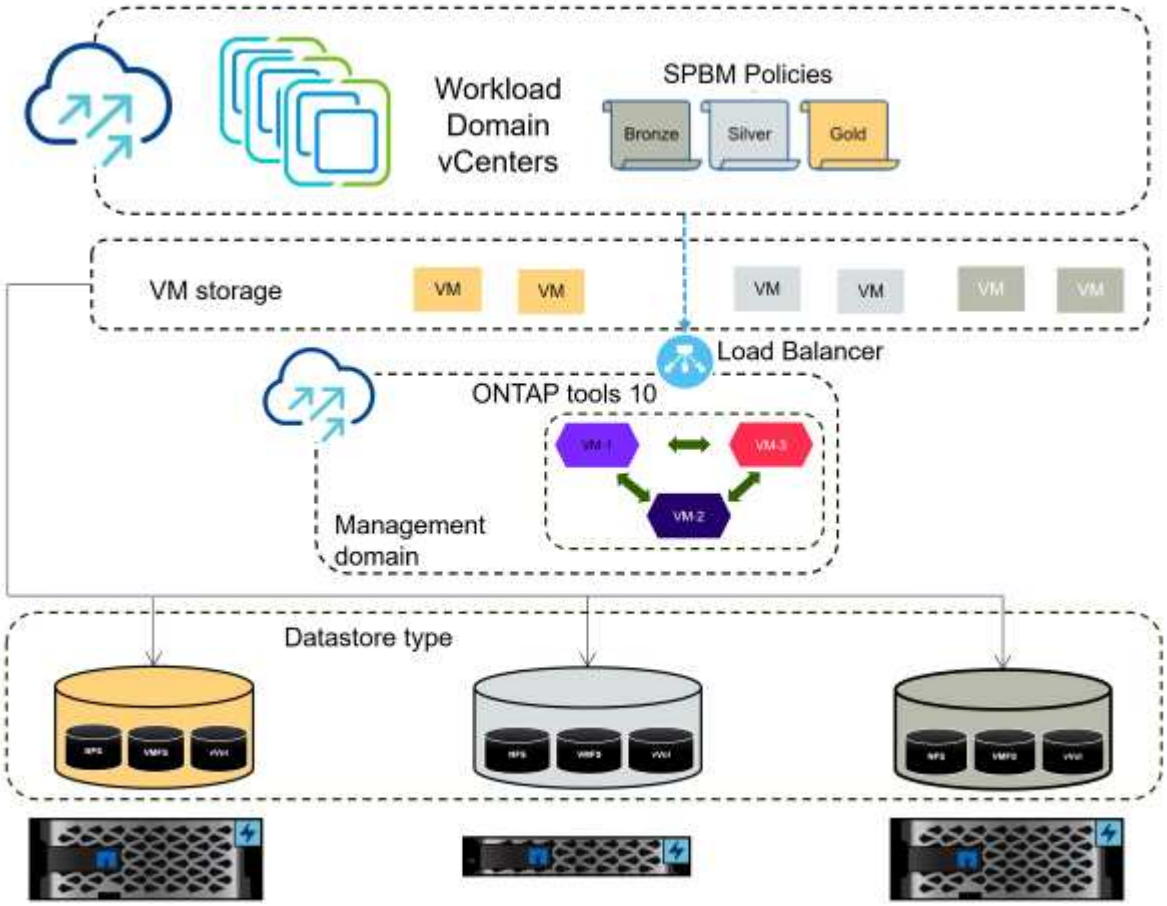
- Ejecute una comprobación previa en el dispositivo vCenter mediante la herramienta de importación VCF.
- Implemente la máquina virtual del administrador de SDDC en el clúster de vCenter.
- Cree un archivo JSON para un clúster NSX que se implementará durante el proceso de conversión.
- Cargue el software requerido en el administrador SDDC.
- Convierta el clúster de vSphere en el inventario del administrador de SDDC.

Para obtener una descripción general del proceso de conversión, consulte "Convertir un entorno de vSphere en un dominio de administración o importar un entorno de vSphere como un dominio de carga de trabajo de VI en VMware Cloud Foundation" .

Implementar herramientas ONTAP y aprovisionar un almacén de datos NFS

La arquitectura de ONTAP Tools 10 está diseñada para integrarse perfectamente con los entornos VMware, aprovechando un marco modular y escalable que incluye los servicios de ONTAP Tools, el complemento vSphere y las API REST para permitir una gestión eficiente del almacenamiento, la automatización y la protección de datos.

Las ONTAP tools for VMware vSphere 10 se pueden instalar en configuraciones HA o no HA.

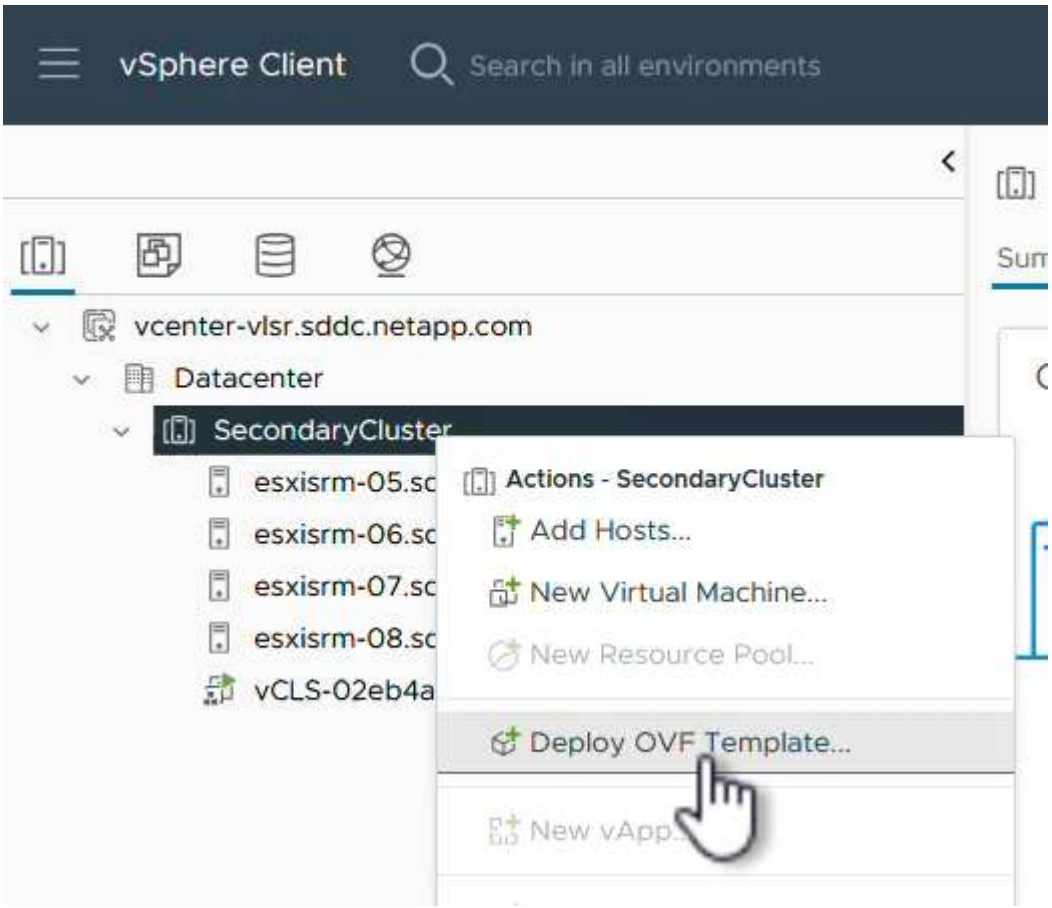


Implementar ONTAP tools for VMware vSphere 10

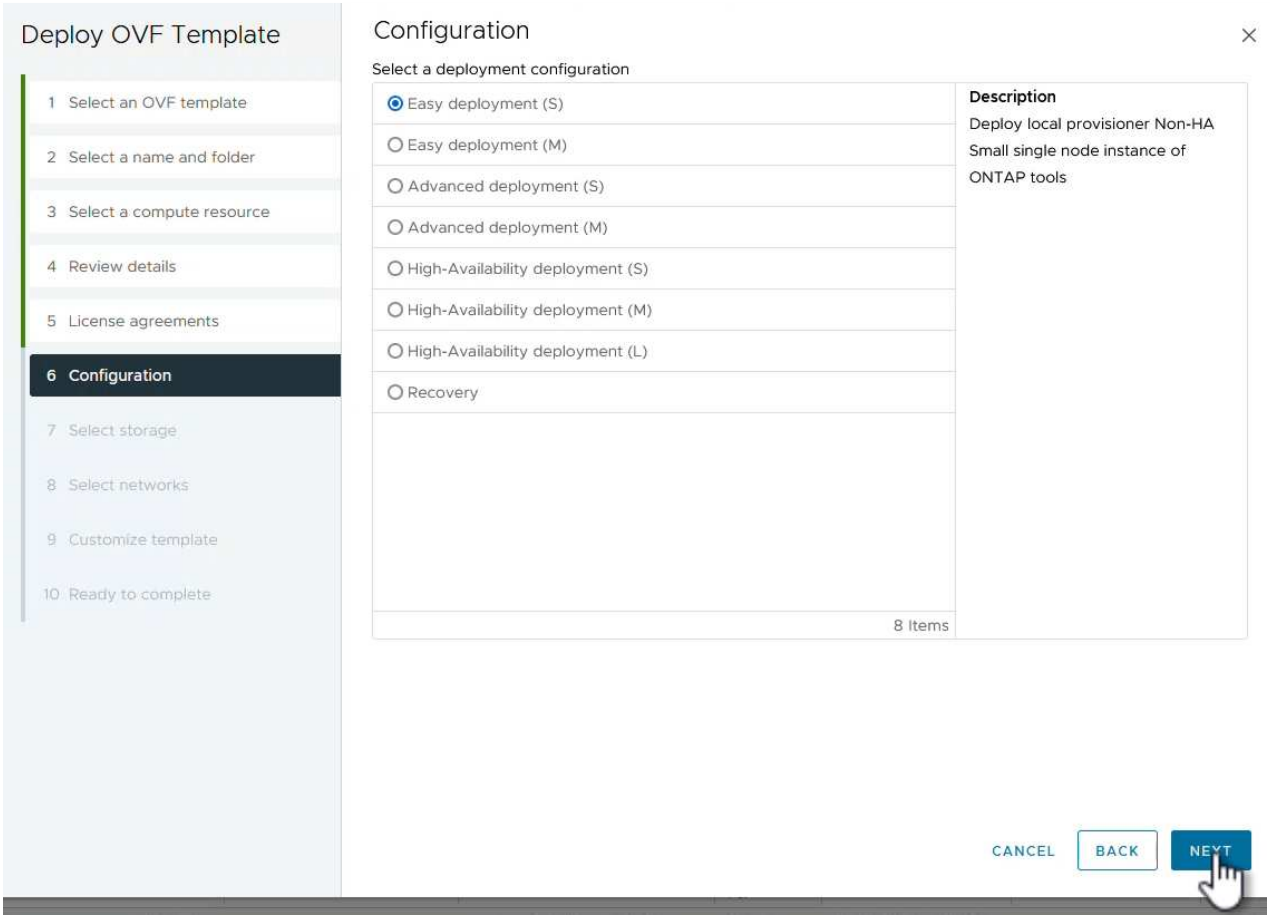
En este paso, se implementa ONTAP tools 10 con una configuración que no es HA.

Para obtener detalles de implementación adicionales sobre configuraciones de alta y baja disponibilidad, consulte "Implementar ONTAP tools for VMware vSphere" .

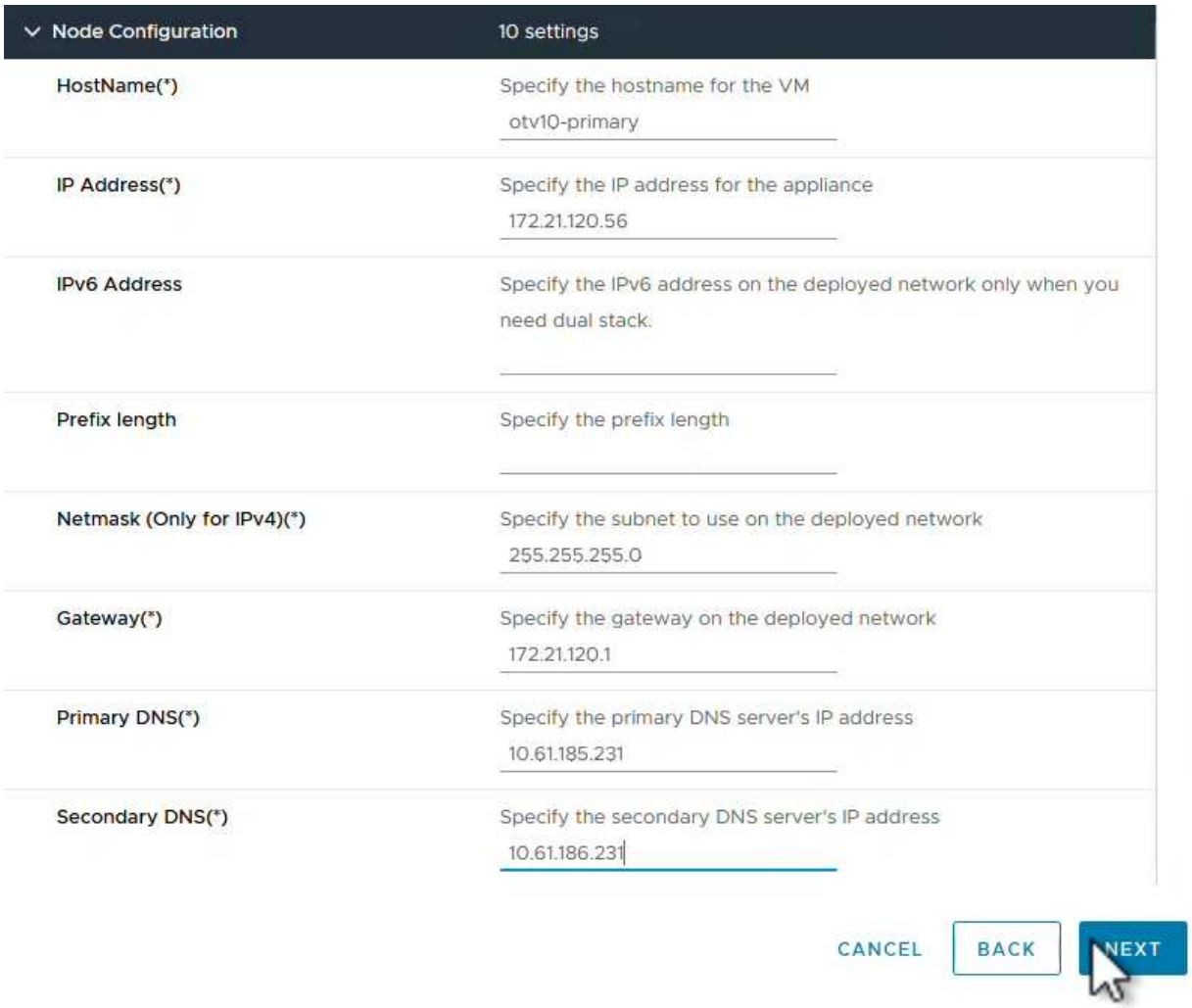
1. Descargue la plantilla OVA de ONTAP tools 10 desde "Sitio de soporte de NetApp" .
2. En el cliente vSphere, haga clic derecho en el clúster y haga clic en **Implementar plantilla OVF**



3. En la **Plantilla OVF de implementación** complete los pasos para:
   - Seleccione una plantilla OVF.
   - Seleccione un nombre y una carpeta.
   - Seleccione un recurso computacional.
   - Detalles de la revisión.
   - Acepte el acuerdo de licencia.
4. En la página **Configuración** de la plantilla, seleccione el tipo de implementación, incluso si desea implementar las herramientas ONTAP en una configuración de alta disponibilidad. Haga clic en **Siguiente** para continuar.



5. En la página **Seleccionar almacenamiento** elija el almacén de datos en el que desea instalar la máquina virtual y haga clic en **Siguiente**.
6. Seleccione la red en la que se comunicará la máquina virtual de herramientas ONTAP . Haga clic en **Siguiente** para continuar.
7. En la ventana "Personalizar plantilla", complete toda la información requerida.
    - Nombre de usuario y contraseña de la aplicación
    - Elija si desea habilitar ASUP (soporte automático), incluida una URL de proxy.
    - Nombre de usuario y contraseña del administrador.
    - Servidores NTP.
    - Nombre de usuario y contraseña de mantenimiento (cuenta de mantenimiento utilizada en la consola).
    - Proporcione las direcciones IP necesarias para la configuración de implementación.
    - Proporciona toda la información de red para la configuración del nodo.

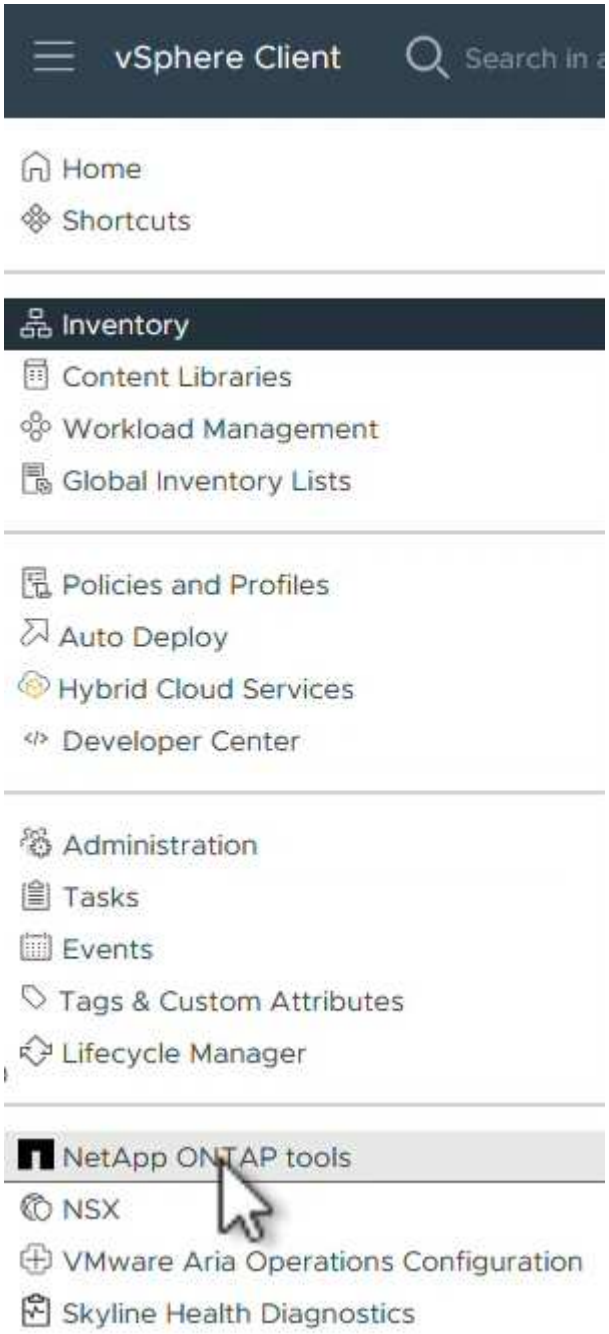


8. Por último, haga clic en **Siguiente** para continuar y luego en **Finalizar** para comenzar la implementación.

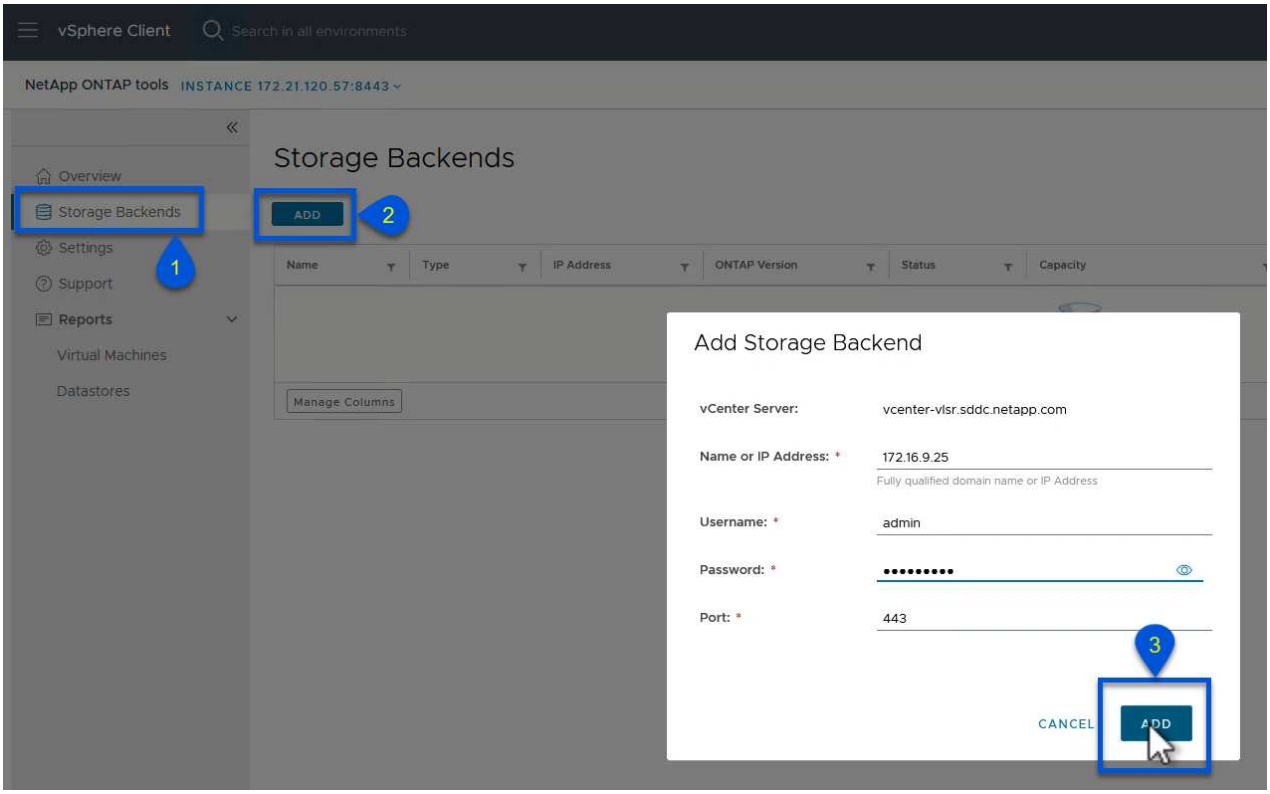
Configurar las herramientas de ONTAP

Una vez instalada y encendida la máquina virtual de herramientas ONTAP , será necesaria alguna configuración básica, como agregar servidores vCenter y sistemas de almacenamiento ONTAP para administrar. Consulte la documentación en "Documentación de ONTAP tools for VMware vSphere" para obtener información detallada.

1. Referirse a "Agregar instancias de vCenter" para configurar las instancias de vCenter que se administrarán con herramientas ONTAP .
2. Para agregar un sistema de almacenamiento ONTAP , inicie sesión en el cliente vSphere y navegue hasta el menú principal a la izquierda. Haga clic en *Herramientas de NetApp ONTAP * para iniciar la interfaz de usuario.



3. Vaya a **Backends de almacenamiento** en el menú de la izquierda y haga clic en **Agregar** para acceder a la ventana **Agregar backend de almacenamiento**.
4. Complete la dirección IP y las credenciales del sistema de almacenamiento ONTAP que se administrará. Haga clic en **Agregar** para finalizar.

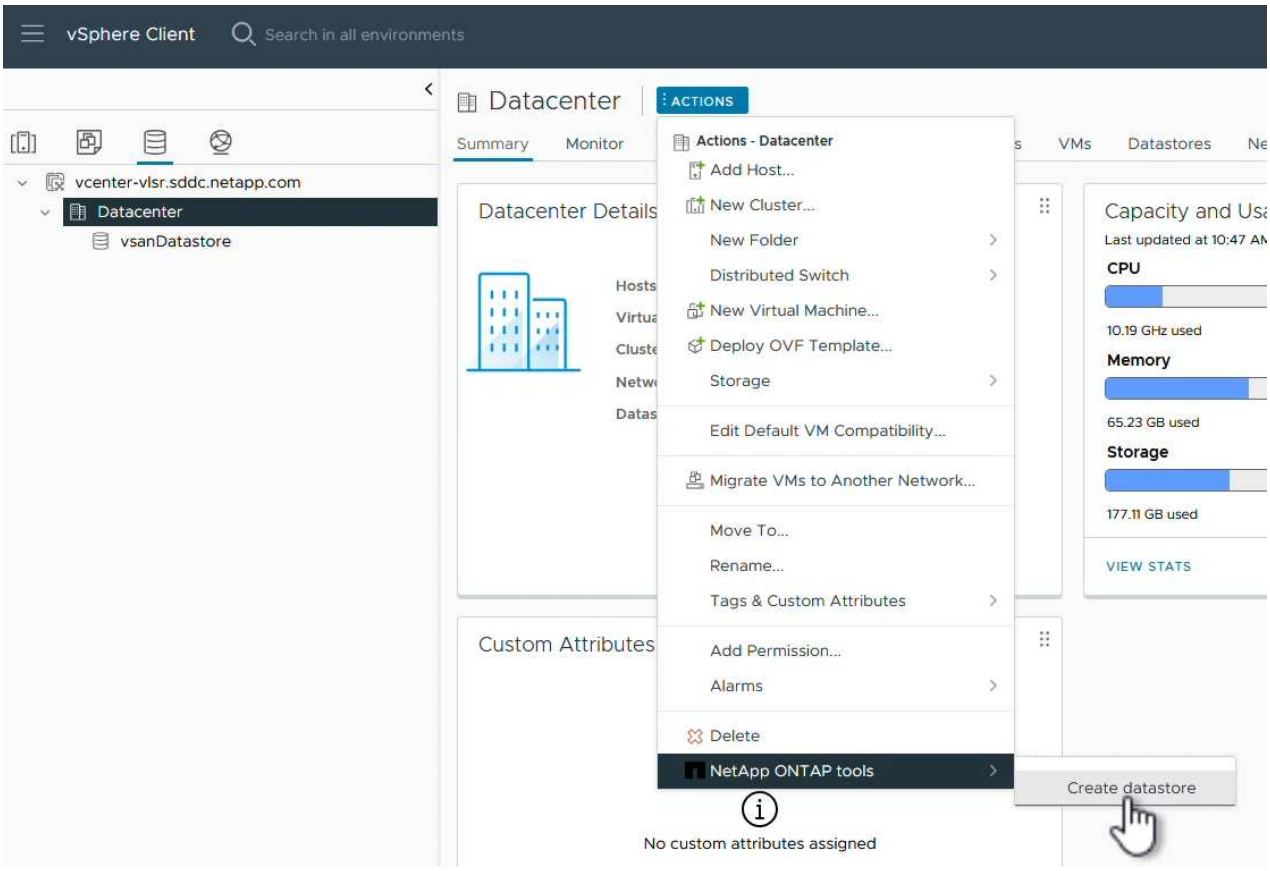


Aquí, el backend de almacenamiento se agrega en la interfaz de usuario del cliente vSphere mediante la dirección IP del clúster. Esto permite la gestión completa de todas las SVM en el sistema de almacenamiento. Alternativamente, el backend de almacenamiento se puede agregar y asociar con una instancia de vCenter mediante el Administrador de herramientas de ONTAP en `https://loadBalanceIP:8443/virtualization/ui/` . Con este método, solo se pueden agregar credenciales de SVM en la interfaz de usuario del cliente vSphere, lo que proporciona un control más granular sobre el acceso al almacenamiento.

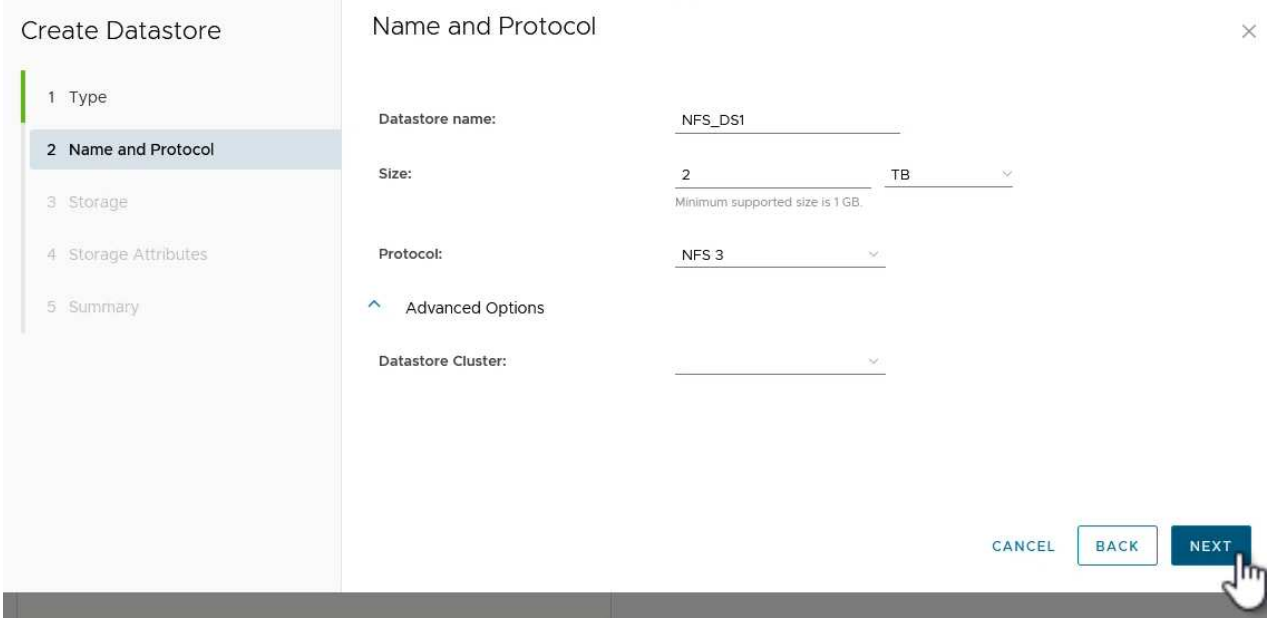
Aprovisionar un almacén de datos NFS con herramientas ONTAP

Las herramientas ONTAP integran funcionalidad en toda la interfaz de usuario del cliente vSphere. En este paso, se aprovisionará un almacén de datos NFS desde la página de inventario de almacenamiento.

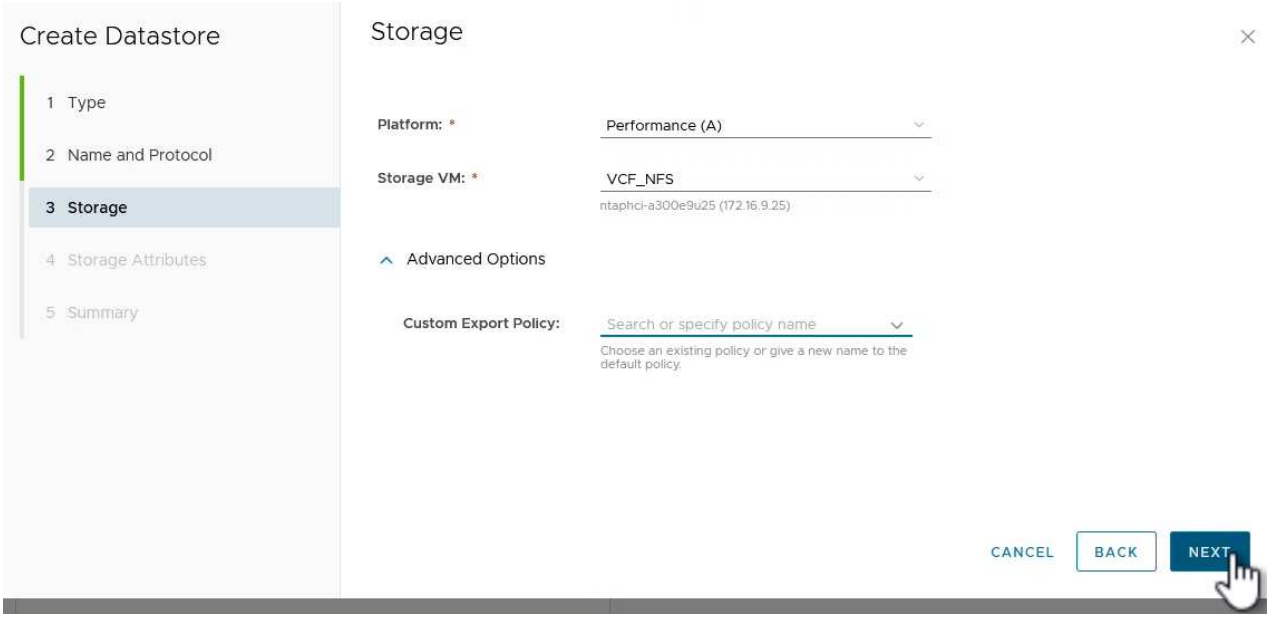
1. En el cliente vSphere, navegue hasta el inventario de almacenamiento.
2. Vaya a **ACCIONES > Herramientas de NetApp ONTAP > Crear almacén de datos**.



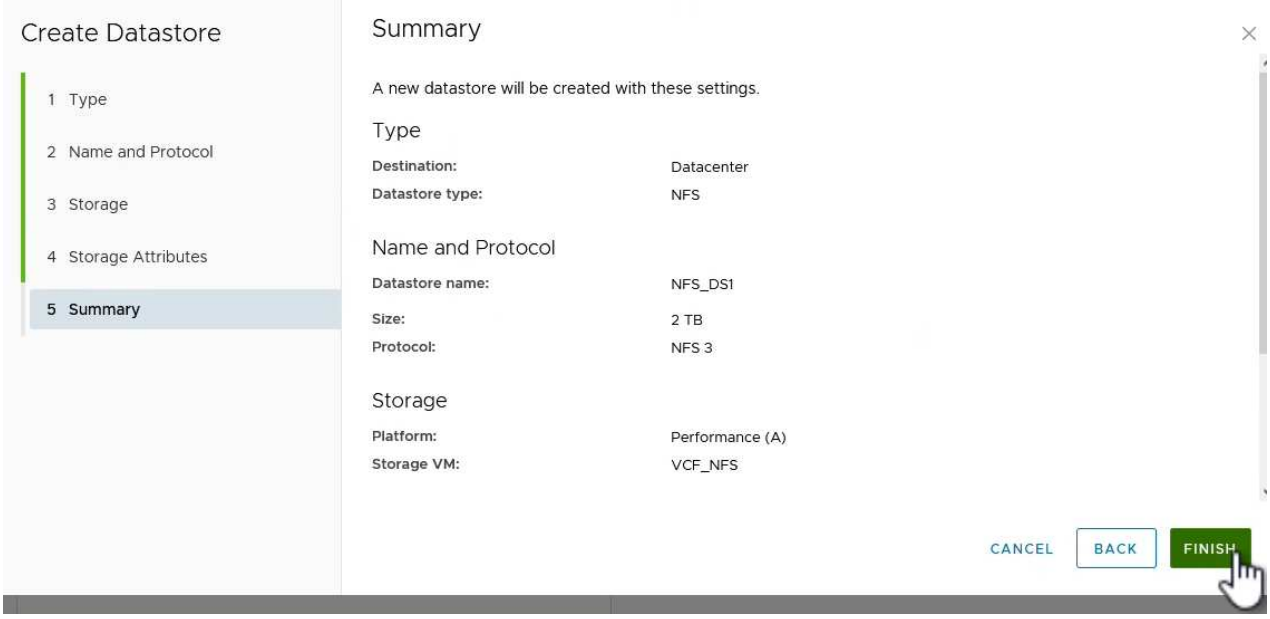
3. En el asistente **Crear almacén de datos**, seleccione el tipo de almacén de datos que desea crear. Las opciones son NFS o VMFS.
4. En la página **Nombre y protocolo**, complete un nombre para el almacén de datos, el tamaño y el protocolo NFS que se utilizará.



5. En la página **Almacenamiento**, seleccione la plataforma de almacenamiento ONTAP y la máquina virtual de almacenamiento (SVM). También puede seleccionar aquí cualquier política de exportación personalizada disponible. Haga clic en **Siguiente** para continuar.



6. En la página **Atributos de almacenamiento**, seleccione el agregado de almacenamiento que se utilizará. Haga clic en **Siguiente** para continuar.
7. En la página **Resumen**, revise la información y haga clic en **Finalizar** para comenzar el proceso de aprovisionamiento. Las herramientas ONTAP crearán un volumen en el sistema de almacenamiento ONTAP y lo montarán como un almacén de datos NFS en todos los hosts ESXi del clúster.



Convertir el clúster de vSphere a VCF 5.2

La siguiente sección cubre los pasos para implementar el administrador SDDC y convertir el clúster vSphere 8 en un dominio de administración VCF 5.2. Cuando corresponda, se consultará la documentación de VMware para obtener detalles adicionales.

La herramienta de importación VCF de VMware by Broadcom es una utilidad que se utiliza tanto en el dispositivo vCenter como en el administrador SDDC para validar configuraciones y proporcionar servicios de conversión e importación para entornos vSphere y VCF.

Para más información, consulte "Opciones y parámetros de la herramienta de importación VCF" .

Copiar y extraer herramienta de importación VCF

Las herramientas de importación de VCF se utilizan en el dispositivo vCenter para validar que el clúster de vSphere se encuentra en un estado correcto para el proceso de importación o conversión de VCF.

Complete los siguientes pasos:

1. Siga los pasos a continuación "Copiar la herramienta de importación de VCF al dispositivo vCenter de destino" en VMware Docs para copiar la herramienta de importación VCF a la ubicación correcta.
2. Extraiga el paquete utilizando el siguiente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar el dispositivo vCenter

Utilice la herramienta de importación VCF para validar el dispositivo vCenter antes de la conversión.

1. Siga los pasos a continuación "Ejecutar una comprobación previa en el vCenter de destino antes de la conversión" para ejecutar la validación.
2. La siguiente salida muestra que el dispositivo vCenter ha pasado la comprobación previa.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Implementar el SDDC Manager

El administrador de SDDC debe estar ubicado en el clúster de vSphere que se convertirá en un dominio de administración de VCF.

Siga las instrucciones de implementación en VMware Docs para completar la implementación.

Referirse a "Implementar el dispositivo SDDC Manager en el vCenter de destino" .

Para más información véase"Anfitriones de la Comisión" en la Guía de administración de VCF.

Crear un archivo JSON para la implementación de NSX

Para implementar NSX Manager al importar o convertir un entorno de vSphere a VMware Cloud Foundation, cree una especificación de implementación de NSX. La implementación de NSX requiere un mínimo de 3 hosts.

> Al implementar un clúster de NSX Manager en una operación de conversión o importación, se utilizan redes NSX-VLAN. Para obtener detalles sobre las limitaciones de la red NSX-VLAN, consulte la sección "Consideraciones antes de convertir o importar entornos vSphere existentes en VMware Cloud Foundation". Para obtener información sobre las limitaciones de la red NSX-VLAN, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

El siguiente es un ejemplo de un archivo JSON para la implementación de NSX:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "NetApp!23456789",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie el archivo JSON a un directorio en el Administrador SDDC.

Subir software a SDDC Manager

Copie la herramienta de importación VCF y el paquete de implementación de NSX al directorio /home/vcf/vcfimport en el Administrador de SDDC.

Ver "Cargue el software necesario en el dispositivo SDDC Manager" para obtener instrucciones detalladas.

Convertir un clúster de vSphere en un dominio de administración de VCF

La herramienta de importación VCF se utiliza para realizar el proceso de conversión. Ejecute el siguiente comando desde el directorio /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset para revisar una impresión de las funciones de la herramienta de importación de VCF:

```
python3 vcf_brownfield.py --help
```

Se ejecuta el siguiente comando para convertir el clúster vSphere en un dominio de administración de VCF e implementar el clúster NSX:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Para obtener instrucciones completas, consulte "Convertir o importar el entorno de vSphere al inventario de SDDC Manager" .

Añadir licencias a VCF

Después de completar la conversión, se debe agregar la licencia al entorno.

1. Inicie sesión en la interfaz de usuario del Administrador de SDDC.
2. Vaya a **Administración > Licencias** en el panel de navegación.
3. Haga clic en **+ Clave de licencia**.
4. Elija un producto del menú desplegable.
5. Introduzca la clave de licencia.
6. Proporcione una descripción de la licencia.
7. Haga clic en **Agregar**.
8. Repita estos pasos para cada licencia.

Demostración en vídeo de las ONTAP tools for VMware vSphere 10

Almacén de datos NFS con ONTAP tools for VMware vSphere 10

Convertir una instancia de servidor vCenter en un dominio de administración VCF (almacén de datos FC)

Convierta un clúster de vSphere 8 que utiliza almacenes de datos de ONTAP Fibre Channel en un dominio de administración de VMware Cloud Foundation. Este procedimiento incluye el aprovisionamiento de almacenamiento FC, la implementación de herramientas ONTAP para VMware y el uso de la herramienta de importación VCF para migrar y administrar el clúster dentro del entorno VCF.

Introducción

La conversión de un entorno vSphere, con un almacén de datos de canal de fibra (FC) existente que se ejecuta en ONTAP, implica integrar la infraestructura existente en una arquitectura de nube privada moderna. Este proceso se beneficia de la robustez del almacenamiento FC, para garantizar un acceso y una gestión de datos sin inconvenientes. Una vez establecido un dominio de administración de VCF a través del proceso de conversión, los administradores pueden importar de manera eficiente entornos vSphere adicionales, incluidos aquellos que utilizan almacenes de datos FC, en el ecosistema VCF. Esta integración no solo mejora la utilización de recursos, sino que también simplifica la gestión de la infraestructura de nube privada, lo que garantiza una transición fluida con una interrupción mínima de las cargas de trabajo existentes.

En esta solución demostraremos cómo un almacén de datos FC en vSphere 8 se convierte en almacenamiento principal cuando el clúster se convierte en un dominio de administración de VCF.

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Implementar ONTAP tools for VMware vSphere 10.
- Aprovisione un almacén de datos FC mediante herramientas ONTAP .
- Utilice la herramienta de importación VCF para validar el clúster vSphere.
- Implemente SDDC Manager en el clúster de vSphere.
- Configure un archivo JSON para crear NSX durante la conversión VCF.
- Utilice la herramienta de importación de VCF para convertir el clúster de vSphere 8 a VCF 5.2.1

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Sistema de almacenamiento NetApp ASA R2/ ASA/ AFF con una máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico de canal de fibra (FC).
- Se ha creado una interfaz lógica (LIF) para transportar tráfico FC y está asociada con la SVM.
- La zonificación FC se ha configurado en los conmutadores designados para transportar tráfico FC.
- Un clúster vSphere 8 con 4 hosts ESXi y un dispositivo vCenter ubicado en el clúster.
- Grupo de puertos distribuidos configurado para vMotion en las VLAN o segmentos de red establecidos para este propósito.
- Descargue el software necesario para la conversión VCF.

Las ONTAP tools for VMware vSphere 10 se pueden instalar en configuraciones HA o no HA. Para obtener información completa sobre los requisitos previos para las herramientas ONTAP , consulte "Requisitos previos

para las ONTAP tools for VMware vSphere" .

Para conocer el almacenamiento compatible y otras consideraciones para convertir o importar vSphere a VCF 5.2, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

Para el software necesario, consulte "Descargar software para convertir o importar entornos vSphere existentes" .

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation 5.2" .

Pasos de implementación

La solución cubre el uso de ONTAP tools for VMware vSphere para aprovisionar almacenes de datos FC y el proceso de conversión de un clúster vSphere 8 existente a un dominio de administración VCF.

Complete los siguientes pasos:

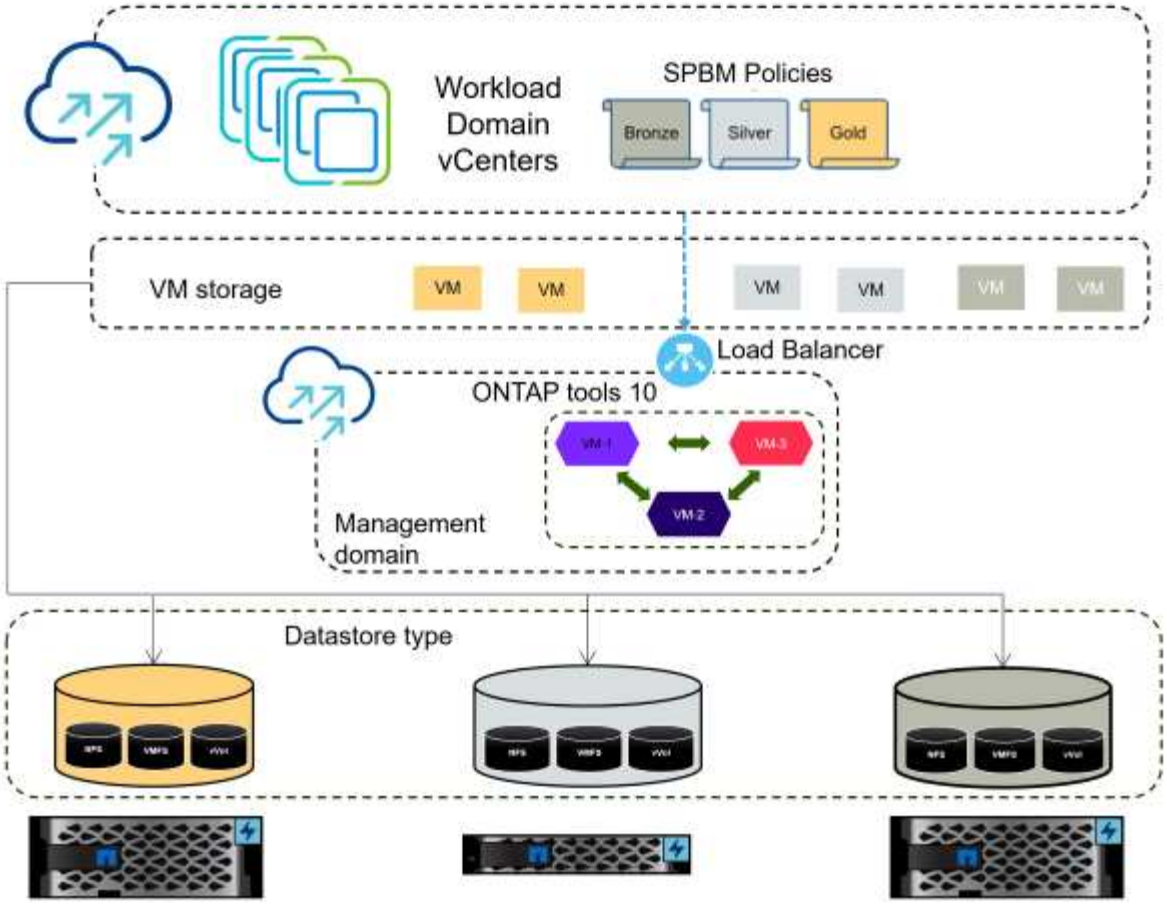
- Implementar ONTAP tools for VMware vSphere 10.
- Aprovisione un almacén de datos FC mediante herramientas ONTAP .
- Copie la herramienta de importación VCF al dispositivo vCenter.
- Ejecute una comprobación previa en el dispositivo vCenter mediante la herramienta de importación VCF.
- Implemente la máquina virtual del administrador de SDDC en el clúster de vCenter.
- Cree un archivo JSON para un clúster NSX que se implementará durante el proceso de conversión.
- Cargue el software requerido en el administrador SDDC.
- Convierta el clúster de vSphere en el inventario del administrador de SDDC.

Para obtener una descripción general del proceso de conversión, consulte "Convertir un entorno de vSphere en un dominio de administración o importar un entorno de vSphere como un dominio de carga de trabajo de VI en VMware Cloud Foundation" .

Implementar herramientas ONTAP y aprovisionar un almacén de datos FC

La arquitectura de ONTAP Tools 10 está diseñada para integrarse perfectamente con los entornos VMware, aprovechando un marco modular y escalable que incluye los servicios de ONTAP Tools, el complemento vSphere y las API REST para permitir una gestión eficiente del almacenamiento, la automatización y la protección de datos.

Las ONTAP tools for VMware vSphere 10 se pueden instalar en configuraciones HA o no HA.

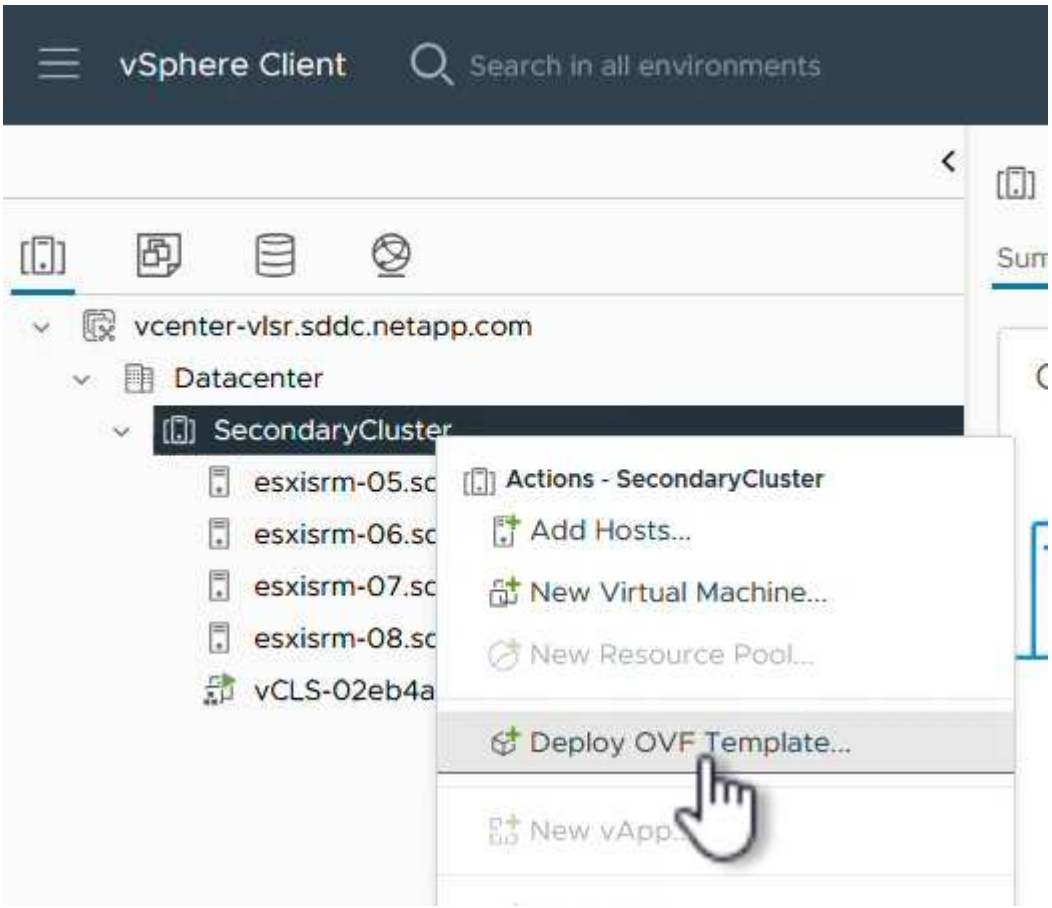

Workload
Domain
vCenters
SPBM Policies
Bronze
Silver
Gold
VM storage
VM
VM
VM
VM
VM
VM
Load Balancer
ONTAP tools 10
VM-1
VM-3
VM-2
Management
domain
Datastore type

Implementar ONTAP tools for VMware vSphere 10

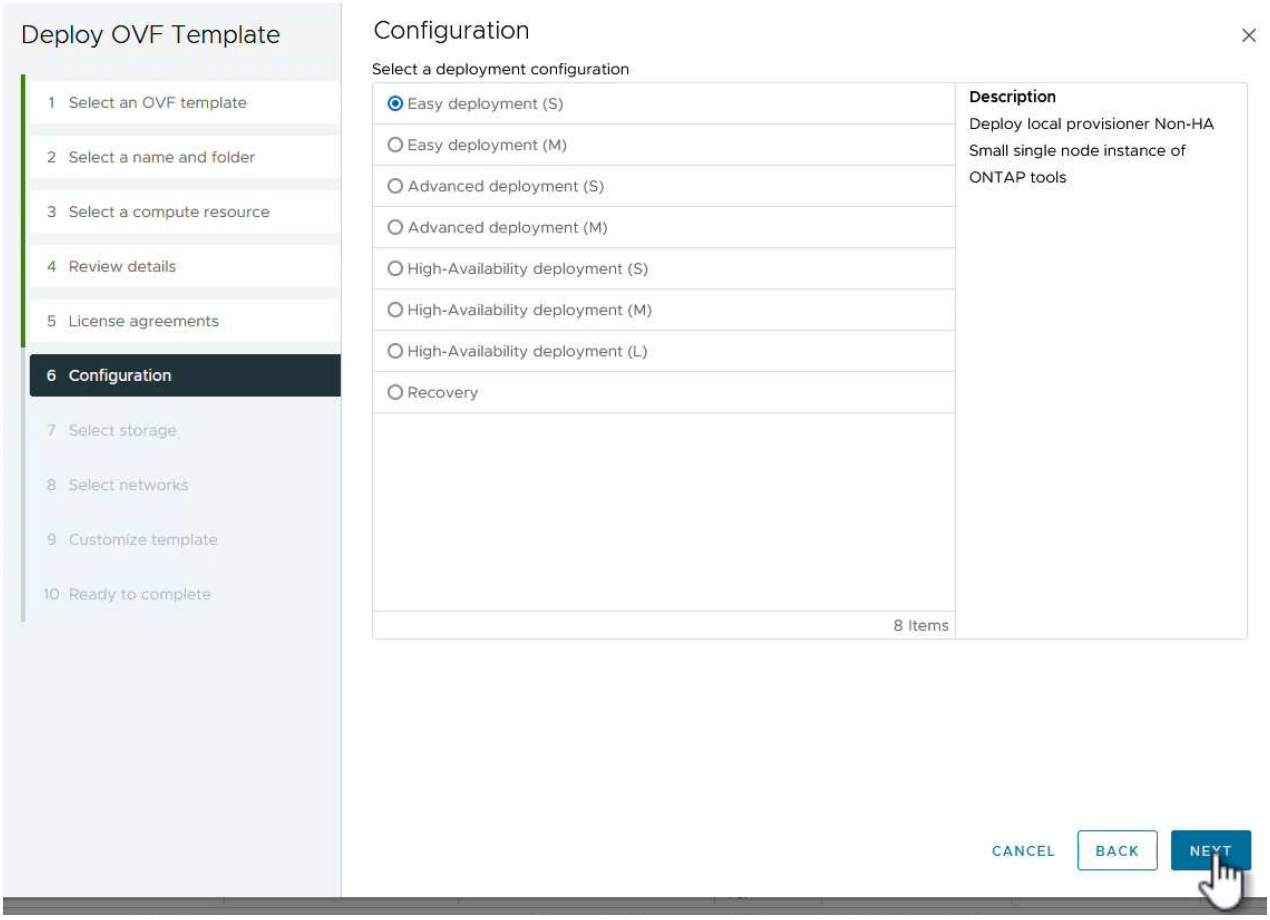
En este paso, se implementa ONTAP tools 10 con una configuración que no es HA.

Para obtener detalles de implementación adicionales sobre configuraciones de alta y baja disponibilidad, consulte "Implementar ONTAP tools for VMware vSphere" .

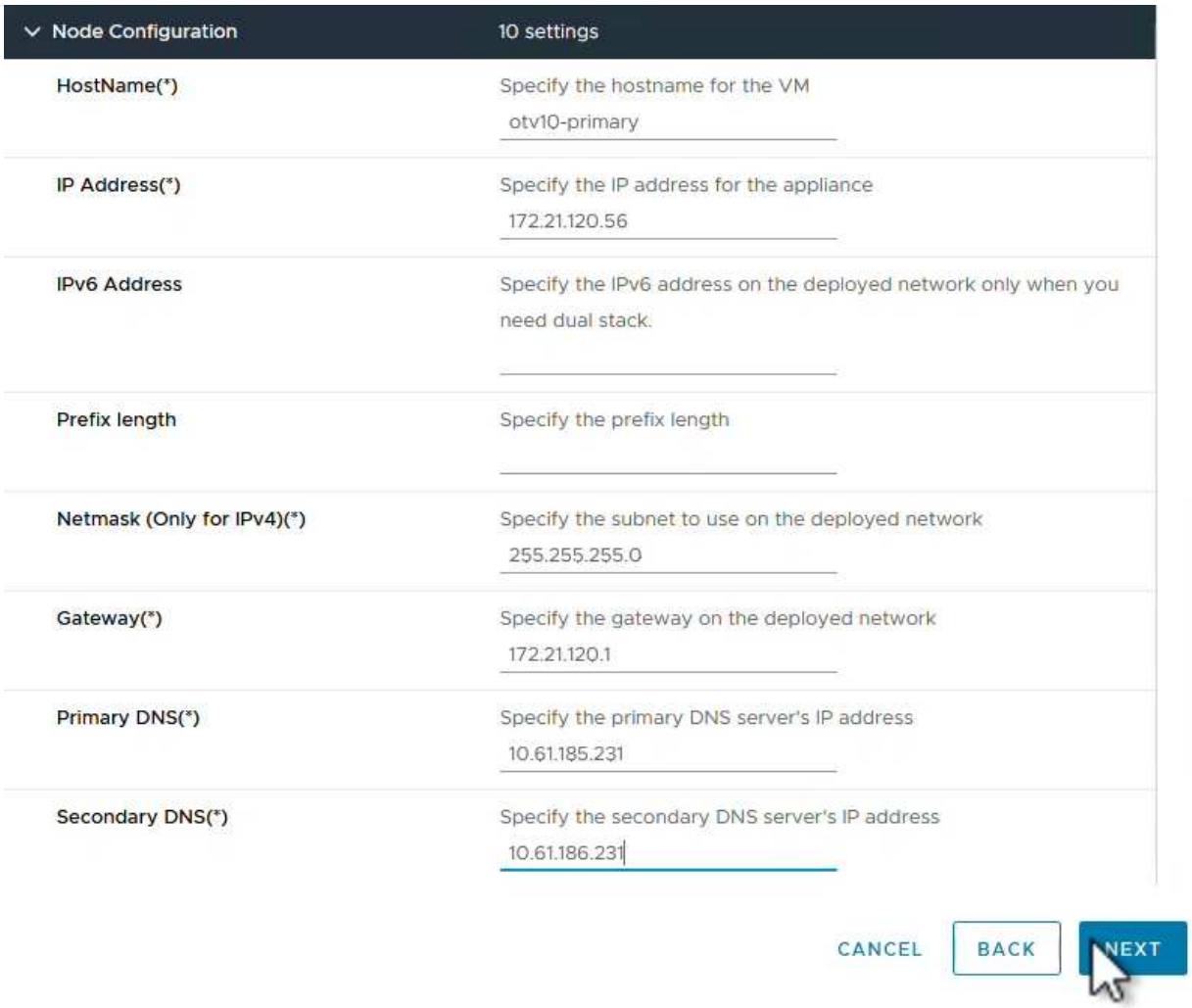
1. Descargue la plantilla OVA de ONTAP tools 10 desde "Sitio de soporte de NetApp" .
2. En el cliente vSphere, haga clic derecho en el clúster y haga clic en **Implementar plantilla OVF**



3. En la **Plantilla OVF de implementación** complete los pasos para:
   - Seleccione una plantilla OVF.
   - Seleccione un nombre y una carpeta.
   - Seleccione un recurso computacional.
   - Detalles de la revisión.
   - Acepte el acuerdo de licencia.
4. En la página **Configuración** de la plantilla, seleccione el tipo de implementación, incluso si desea implementar las herramientas ONTAP en una configuración de alta disponibilidad. Haga clic en **Siguiente** para continuar.



5. En la página **Seleccionar almacenamiento** elija el almacén de datos en el que desea instalar la máquina virtual y haga clic en **Siguiente**.
6. Seleccione la red en la que se comunicará la máquina virtual de herramientas ONTAP . Haga clic en **Siguiente** para continuar.
7. En la ventana "Personalizar plantilla", complete toda la información requerida.
    - Nombre de usuario y contraseña de la aplicación
    - Elija si desea habilitar ASUP (soporte automático), incluida una URL de proxy.
    - Nombre de usuario y contraseña del administrador.
    - Servidores NTP.
    - Nombre de usuario y contraseña de mantenimiento (cuenta de mantenimiento utilizada en la consola).
    - Proporcione las direcciones IP necesarias para la configuración de implementación.
    - Proporciona toda la información de red para la configuración del nodo.

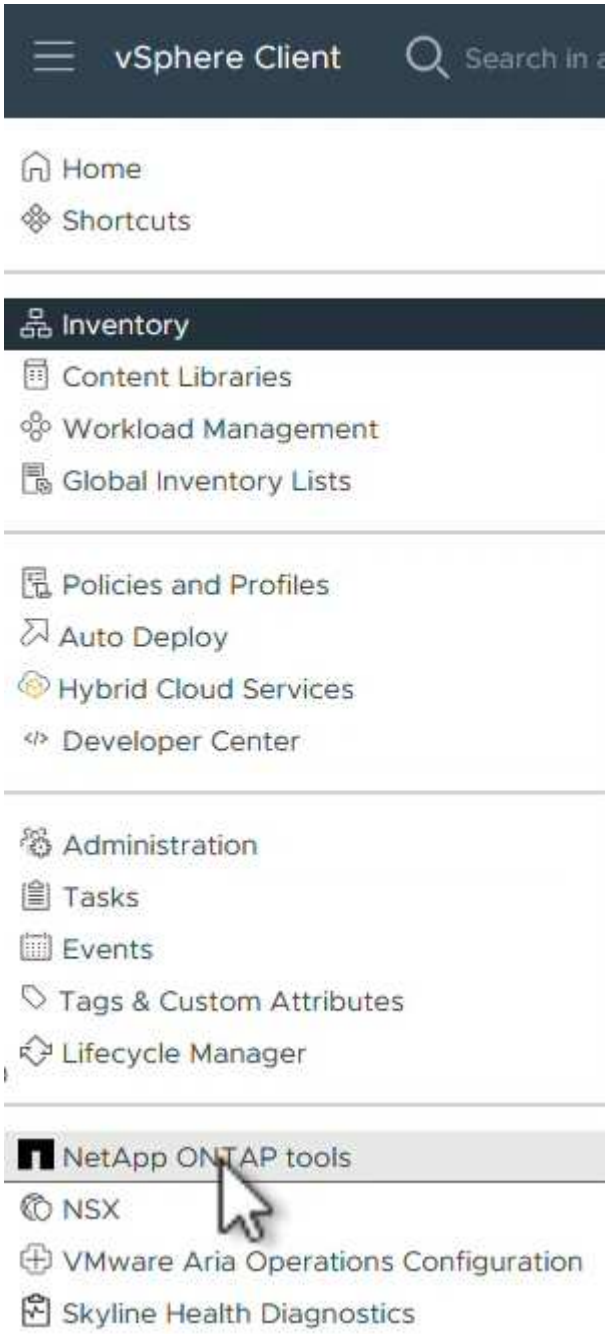


8. Por último, haga clic en **Siguiente** para continuar y luego en **Finalizar** para comenzar la implementación.

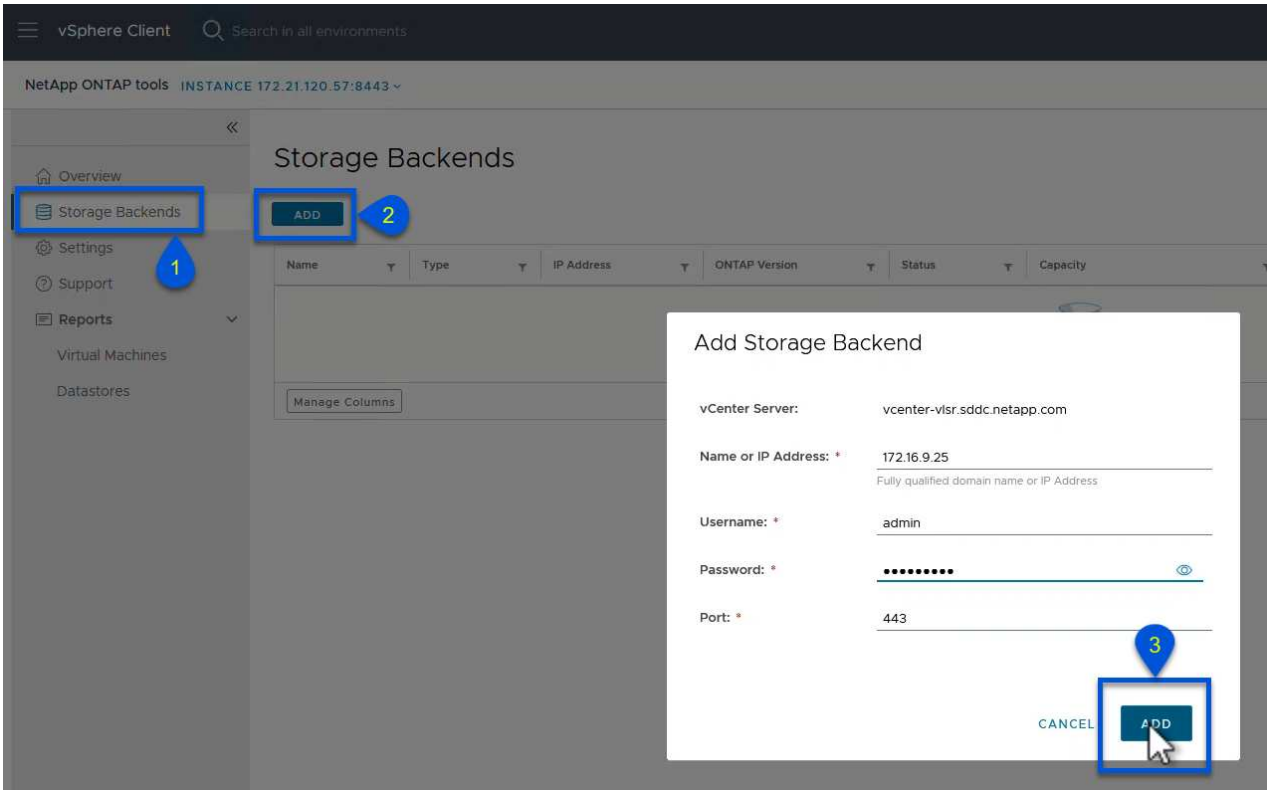
Configurar las herramientas de ONTAP

Una vez instalada y encendida la máquina virtual de herramientas ONTAP , será necesaria alguna configuración básica, como agregar servidores vCenter y sistemas de almacenamiento ONTAP para administrar. Consulte la documentación en "Documentación de ONTAP tools for VMware vSphere" para obtener información detallada.

1. Referirse a "Agregar instancias de vCenter" para configurar las instancias de vCenter que se administrarán con herramientas ONTAP .
2. Para agregar un sistema de almacenamiento ONTAP , inicie sesión en el cliente vSphere y navegue hasta el menú principal a la izquierda. Haga clic en *Herramientas de NetApp ONTAP * para iniciar la interfaz de usuario.



3. Vaya a **Backends de almacenamiento** en el menú de la izquierda y haga clic en **Agregar** para acceder a la ventana **Agregar backend de almacenamiento**.
4. Complete la dirección IP y las credenciales del sistema de almacenamiento ONTAP que se administrará. Haga clic en **Agregar** para finalizar.

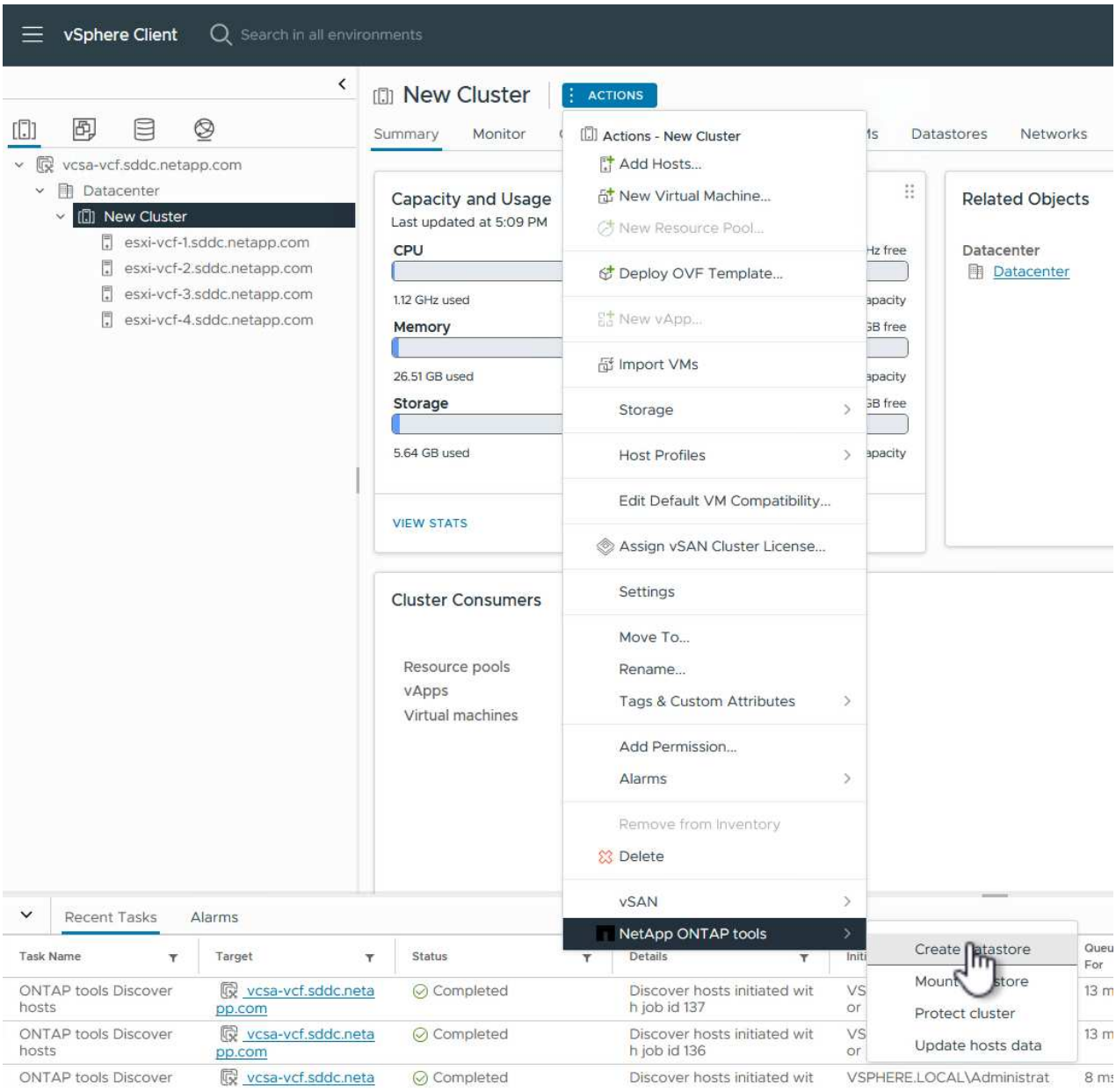


Aquí, el backend de almacenamiento se agrega en la interfaz de usuario del cliente vSphere mediante la dirección IP del clúster. Esto permite la gestión completa de todas las SVM en el sistema de almacenamiento. Alternativamente, el backend de almacenamiento se puede agregar y asociar con una instancia de vCenter mediante el Administrador de herramientas de ONTAP en `https://loadBalanceIP:8443/virtualization/ui/` . Con este método, solo se pueden agregar credenciales de SVM en la interfaz de usuario del cliente vSphere, lo que proporciona un control más granular sobre el acceso al almacenamiento.

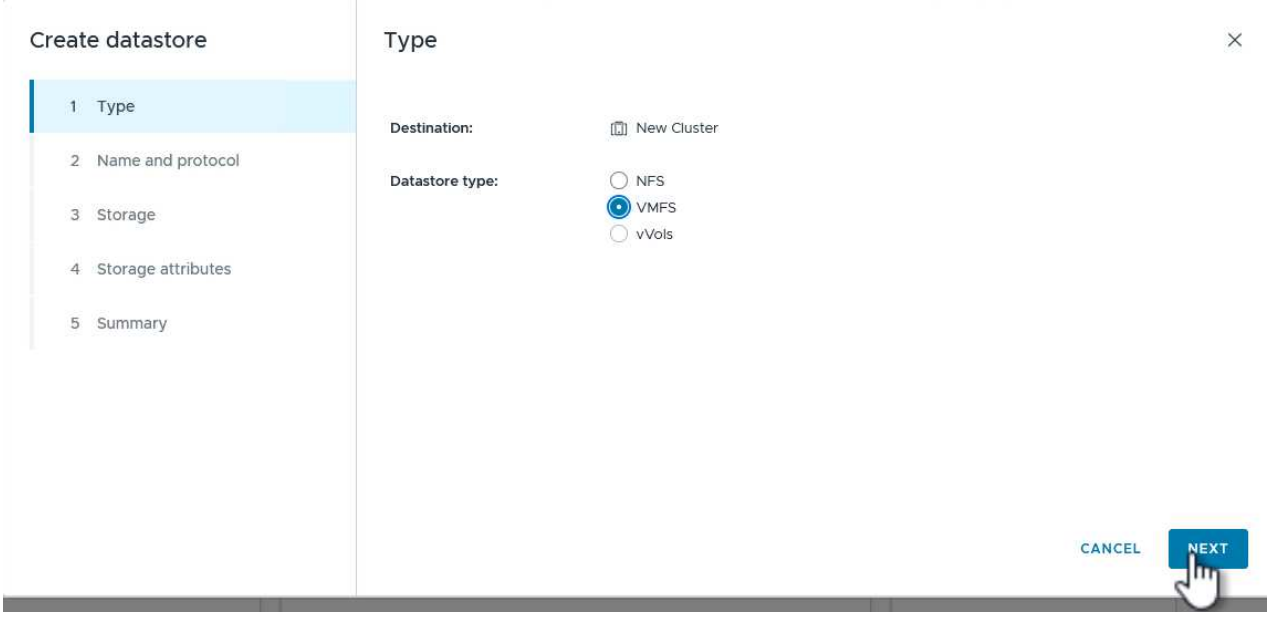
Aprovisionar un almacén de datos FC con herramientas ONTAP

Las herramientas ONTAP integran funcionalidad en toda la interfaz de usuario del cliente vSphere. En este paso se aprovisionará un almacén de datos FC desde la página de inventario de hosts.

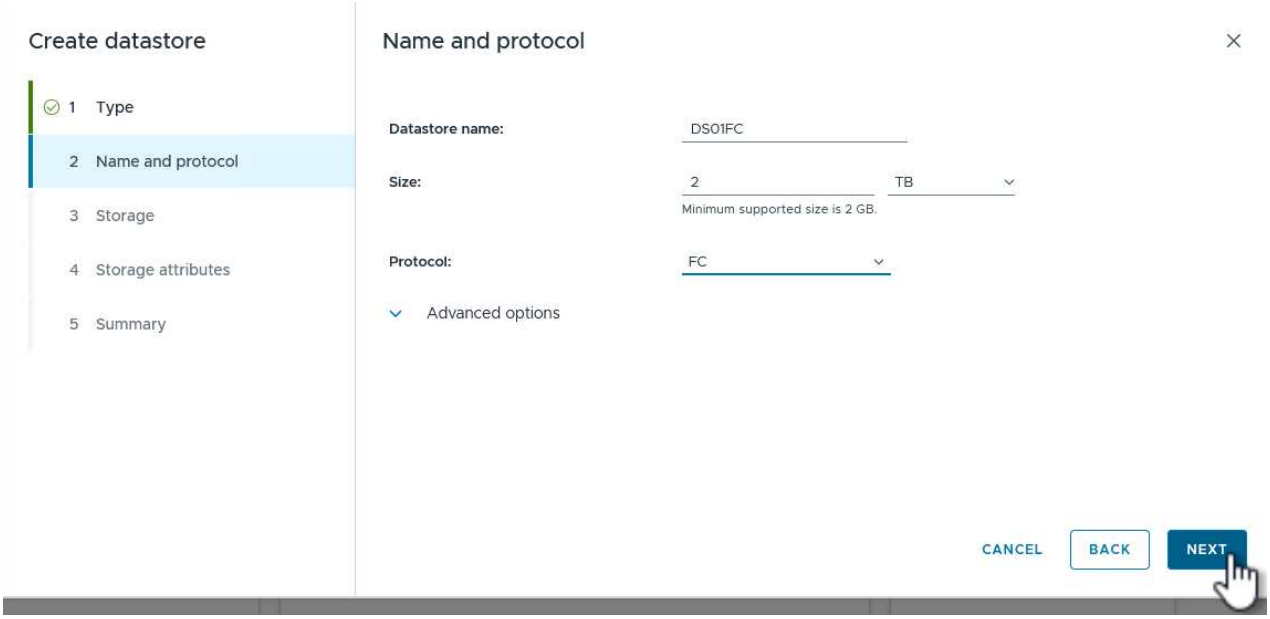
1. En el cliente vSphere, navegue hasta el inventario de hosts (o almacenamiento).
2. Vaya a **ACCIONES > Herramientas de NetApp ONTAP > Crear almacén de datos**.



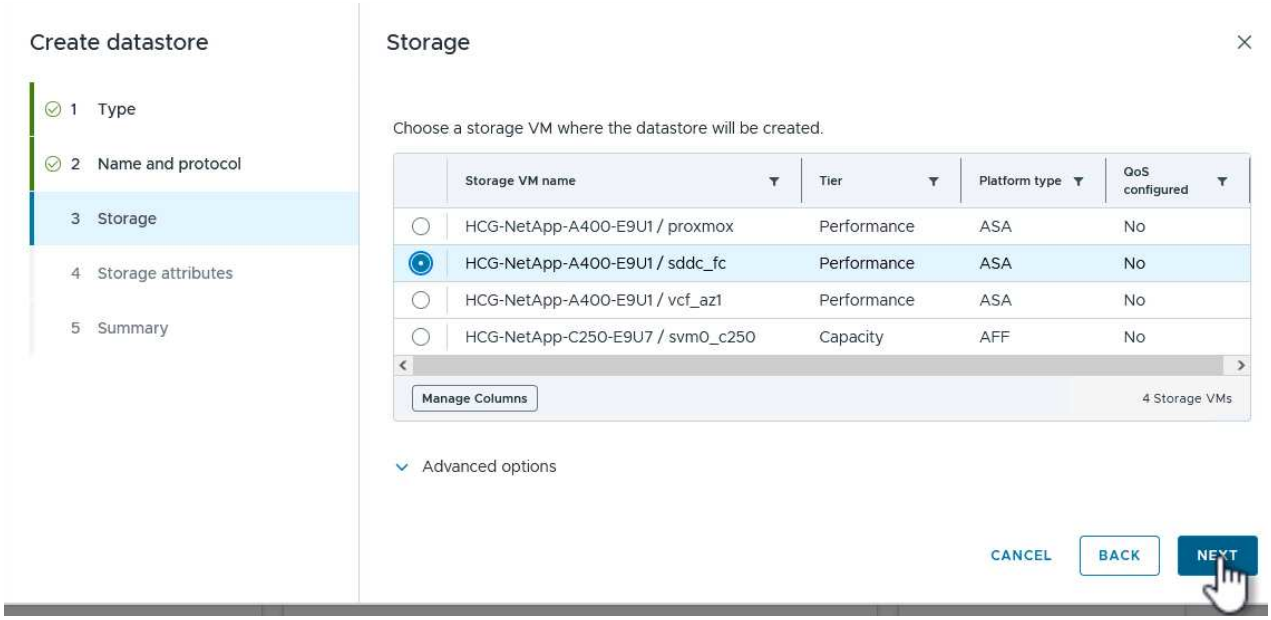
3. En el asistente **Crear almacén de datos**, seleccione VMFS para el tipo de almacén de datos que desea crear.



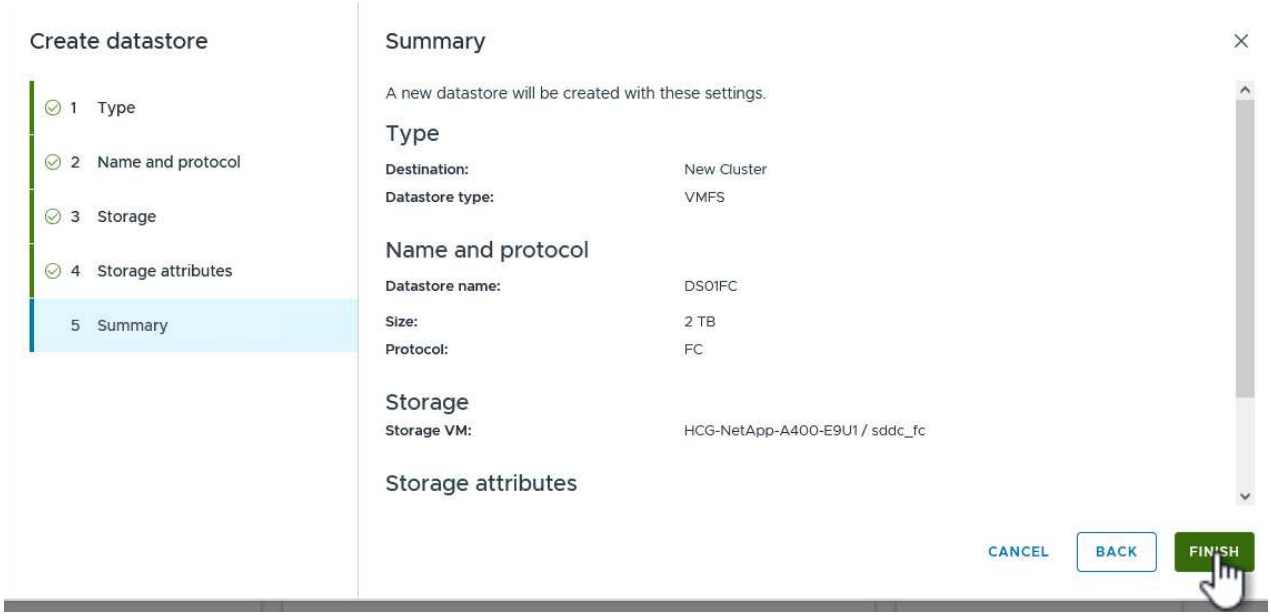
4. En la página **Nombre y protocolo**, complete un nombre para el almacén de datos, el tamaño y el protocolo FC que se utilizará.



5. En la página **Almacenamiento**, seleccione la plataforma de almacenamiento ONTAP y la máquina virtual de almacenamiento (SVM). También puede seleccionar aquí cualquier política de exportación personalizada disponible. Haga clic en **Siguiente** para continuar.



6. En la página **Atributos de almacenamiento**, seleccione el agregado de almacenamiento que se utilizará. Haga clic en **Siguiente** para continuar.
7. En la página **Resumen**, revise la información y haga clic en **Finalizar** para comenzar el proceso de aprovisionamiento. Las herramientas ONTAP crearán un volumen en el sistema de almacenamiento ONTAP y lo montarán como un almacén de datos FC en todos los hosts ESXi del clúster.



Convertir el entorno de vSphere a VCF 5.2

La siguiente sección cubre los pasos para implementar el administrador SDDC y convertir el clúster vSphere 8 en un dominio de administración VCF 5.2. Cuando corresponda, se consultará la documentación de VMware para obtener detalles adicionales.

La herramienta de importación VCF de VMware by Broadcom es una utilidad que se utiliza tanto en el

dispositivo vCenter como en el administrador SDDC para validar configuraciones y proporcionar servicios de conversión e importación para entornos vSphere y VCF.

Para más información, consulte "Opciones y parámetros de la herramienta de importación VCF" .

Copiar y extraer herramienta de importación VCF

Las herramientas de importación de VCF se utilizan en el dispositivo vCenter para validar que el clúster de vSphere se encuentra en un estado correcto para el proceso de importación o conversión de VCF.

Complete los siguientes pasos:

1. Siga los pasos a continuación "Copiar la herramienta de importación de VCF al dispositivo vCenter de destino" en VMware Docs para copiar la herramienta de importación VCF a la ubicación correcta.
2. Extraiga el paquete utilizando el siguiente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar el dispositivo vCenter

Utilice la herramienta de importación VCF para validar el dispositivo vCenter antes de la conversión.

1. Siga los pasos a continuación "Ejecutar una comprobación previa en el vCenter de destino antes de la conversión" para ejecutar la validación.
2. La siguiente salida muestra que el dispositivo vCenter ha pasado la comprobación previa.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Implementar el SDDC Manager

El administrador de SDDC debe estar ubicado en el clúster de vSphere que se convertirá en un dominio de administración de VCF.

Siga las instrucciones de implementación en VMware Docs para completar la implementación.

Referirse a "Implementar el dispositivo SDDC Manager en el vCenter de destino" .

Para más información véase"Anfitriones de la Comisión" en la Guía de administración de VCF.

Crear un archivo JSON para la implementación de NSX

Para implementar NSX Manager al importar o convertir un entorno de vSphere a VMware Cloud Foundation, cree una especificación de implementación de NSX. La implementación de NSX requiere un mínimo de 3 hosts.

Para obtener información completa, consulte "Generar una especificación de implementación de NSX para convertir o importar entornos vSphere existentes" .

> Al implementar un clúster de NSX Manager en una operación de conversión o importación, se utilizan redes NSX-VLAN. Para obtener detalles sobre las limitaciones de la red NSX-VLAN, consulte la sección "Consideraciones antes de convertir o importar entornos vSphere existentes en VMware Cloud Foundation". Para obtener información sobre las limitaciones de la red NSX-VLAN, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

El siguiente es un ejemplo de un archivo JSON para la implementación de NSX:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "************************",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie el archivo JSON a un directorio en el Administrador SDDC.

Subir software a SDDC Manager

Copie la herramienta de importación VCF y el paquete de implementación de NSX al directorio /home/vcf/vcfimport en el Administrador de SDDC.

Ver "Cargue el software necesario en el dispositivo SDDC Manager" para obtener instrucciones detalladas.

Convertir un clúster de vSphere en un dominio de administración de VCF

La herramienta de importación VCF se utiliza para realizar el proceso de conversión. Ejecute el siguiente comando desde el directorio /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset para revisar una impresión de las funciones de la herramienta de importación de VCF:

```
python3 vcf_brownfield.py --help
```

Se ejecuta el siguiente comando para convertir el clúster vSphere en un dominio de administración de VCF e implementar el clúster NSX:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Para obtener instrucciones completas, consulte "Convertir o importar el entorno de vSphere al inventario de SDDC Manager" .

Añadir licencias a VCF

Después de completar la conversión, se debe agregar la licencia al entorno.

1. Inicie sesión en la interfaz de usuario del Administrador de SDDC.
2. Vaya a **Administración > Licencias** en el panel de navegación.
3. Haga clic en **+ Clave de licencia**.
4. Elija un producto del menú desplegable.
5. Introduzca la clave de licencia.
6. Proporcione una descripción de la licencia.
7. Haga clic en **Agregar**.
8. Repita estos pasos para cada licencia.

Demostración en vídeo de las ONTAP tools for VMware vSphere 10

Almacén de datos NFS con ONTAP tools for VMware vSphere 10

Aprovisionar VCF con almacenamiento principal

Proporcionar un entorno VCF con ONTAP como solución de almacenamiento principal

El almacenamiento NetApp ONTAP es una solución de almacenamiento principal ideal para la administración de VMware Cloud Foundation (VCF) y los dominios de carga de trabajo de infraestructura virtual (VI). ONTAP ofrece alto rendimiento, escalabilidad, gestión de datos avanzada e integración perfecta para mejorar la eficiencia operativa y la protección de datos.

Consulte las siguientes soluciones para conocer los detalles técnicos sobre cómo aprovisionar un entorno VCF en el dominio apropiado y con el protocolo apropiado.

- "Dominio de gestión con FC"
- "Dominio de gestión con NFS"
- "Dominio de carga de trabajo de infraestructura virtual con FC"
- "Dominio de carga de trabajo de infraestructura virtual con NFS"

Utilice un almacén de datos VMFS basado en FC en ONTAP como almacenamiento principal para el dominio de administración de VCF

En este caso de uso, describimos el procedimiento para utilizar un almacén de datos VMFS basado en FC existente en ONTAP como almacenamiento principal para los dominios de administración de VMware Cloud Foundation (VCF). Este procedimiento resume los componentes, las configuraciones y los pasos de implementación necesarios.

Introducción

Cuando sea apropiado, haremos referencia a la documentación externa para conocer los pasos que se deben realizar en el Administrador SDDC de VCF y haremos referencia a aquellos pasos que son específicos de la parte de configuración de almacenamiento.

Para obtener información sobre cómo convertir un entorno vSphere basado en FC existente con ONTAP, consulte"Convertir el entorno de vSphere (almacén de datos FC) en un dominio de administración de VCF" .

> La versión 5.2 de VCF introdujo la capacidad de convertir un entorno vSphere 8 existente en un dominio de administración de VCF o importarlo como dominios de carga de trabajo de VCF VI. Antes de esta versión, VMware vSAN era la única opción de almacenamiento principal para el dominio de administración de VCF.

> Esta solución es aplicable a las plataformas ONTAP compatibles con almacenamiento FC, incluidos NetApp ASA, AFF y FAS.

Prerrequisitos

En este escenario se utilizan los siguientes componentes y configuraciones:

- Sistema de almacenamiento NetApp con una máquina virtual de almacenamiento (SVM) configurada para permitir tráfico FC.
- Se han creado interfaces lógicas (LIF) en la estructura FC que transportará el tráfico FC y está asociada con la SVM.
- La zonificación se ha configurado para utilizar una única zonificación de iniciador-destino en conmutadores FC para HBA de host y destinos de almacenamiento.

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Pasos de implementación

Dominio de administración - Clúster predeterminado

El almacenamiento principal de FC en el clúster inicial solo es compatible con la herramienta de importación brownfield de VCF. Si VCF se implementa con la herramienta Cloud Builder (antes de la versión de lanzamiento 5.2.x), solo se admite vSAN.

Para obtener más información sobre el uso de un entorno vSphere existente, consulte "Conversión del entorno vSphere existente a un dominio de administración" Para más información.

Dominio de administración - Clúster adicional

El clúster vSphere adicional en el dominio de administración se puede implementar con las siguientes opciones:

- Tenga un clúster adicional en el entorno de vSphere y utilice la herramienta de importación brownfield de VCF para convertir el entorno de vSphere en un dominio de administración. "ONTAP tools for VMware vSphere" "Administrador del sistema o API de ONTAP" Se puede utilizar para implementar el almacén de datos VMFS en el clúster vSphere.
- Utilice la API de SDDC para implementar un clúster adicional. Los hosts de vSphere deben tener el almacén de datos VMFS configurado. Usar "Administrador del sistema o API de ONTAP" para implementar LUN en hosts vSphere.
- Utilice la interfaz de usuario de SDDC Manager para implementar un clúster adicional. Pero esta opción solo crea un almacén de datos VSAN hasta la versión 5.2.x.

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Utilice un almacén de datos NFS en ONTAP como almacenamiento principal para el dominio de administración de VCF

En este caso de uso, describimos el procedimiento para utilizar un almacén de datos NFS existente en ONTAP como almacenamiento principal para los dominios de administración de VMware Cloud Foundation (VCF). Este procedimiento resume los componentes necesarios, los pasos de configuración y el proceso de implementación.

Introducción

Cuando sea apropiado, haremos referencia a la documentación externa para conocer los pasos que se deben realizar en el Administrador SDDC de VCF y haremos referencia a aquellos pasos que son específicos de la parte de configuración de almacenamiento.

Para obtener información sobre cómo convertir un entorno vSphere basado en NFS existente con ONTAP, consulte"Convertir el entorno de vSphere (almacén de datos NFS) en un dominio de administración de VCF" .

> La versión 5.2 de VCF introdujo la capacidad de convertir un entorno vSphere 8 existente en un dominio de administración de VCF o importarlo como dominios de carga de trabajo de VCF VI. Antes de esta versión, VMware vSAN era la única opción de almacenamiento principal para el dominio de administración de VCF.

> Esta solución es aplicable a las plataformas ONTAP compatibles con almacenamiento NFS, incluidos NetApp AFF y FAS.

Prerrequisitos

En este escenario se utilizan los siguientes componentes y configuraciones:

- Sistema de almacenamiento NetApp con una máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico NFS.
- Se ha creado una interfaz lógica (LIF) en la red IP que transportará el tráfico NFS y está asociada con la SVM.
- Un clúster vSphere 8 con 4 hosts ESXi y un dispositivo vCenter ubicado en el clúster.
- Grupo de puertos distribuidos configurado para el tráfico de almacenamiento NFS y vMotion en las VLAN o segmentos de red establecidos para este propósito.
- Descargue el software necesario para la conversión VCF.

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Pasos de implementación

Dominio de administración - Clúster predeterminado

El almacenamiento principal NFS en el clúster inicial solo es compatible con la herramienta de importación brownfield VCF. Si VCF se implementa con la herramienta Cloud Builder (hasta la versión 5.2.x), solo se admite VSAN.

Para obtener más información sobre el uso de un entorno vSphere existente, consulte "Conversión del entorno vSphere existente a un dominio de administración" Para más información.

Dominio de administración - Clúster adicional

El clúster vSphere adicional en el dominio de administración se puede implementar con las siguientes opciones:

- Tenga un clúster adicional en el entorno de vSphere y utilice la herramienta de importación brownfield de VCF para convertir el entorno de vSphere en un dominio de administración. "ONTAP tools for VMware vSphere" "Administrador del sistema o API de ONTAP" Se puede utilizar para implementar el almacén de datos NFS en el clúster vSphere.
- Utilice la API de SDDC para implementar un clúster adicional. Los hosts de vSphere deben tener el almacén de datos NFS configurado. Usar "Administrador del sistema o API de ONTAP" para implementar LUN en hosts vSphere.
- Utilice la interfaz de usuario de SDDC Manager para implementar un clúster adicional. Pero esta opción solo crea un almacén de datos vSAN con versiones anteriores a 5.2.x.

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Utilice un almacén de datos VMFS basado en FC en ONTAP como almacenamiento principal para un dominio de carga de trabajo VI

En este caso de uso, describimos el procedimiento para configurar un almacén de datos VMFS de canal de fibra (FC) en ONTAP como la solución de almacenamiento principal para un dominio de carga de trabajo de infraestructura virtual (VI) de VMware Cloud Foundation (VCF). Este procedimiento resume los componentes necesarios, los pasos de configuración y el proceso de implementación.

Beneficios del canal de fibra

Alto rendimiento: FC proporciona velocidades de transferencia de datos de alta velocidad, lo que lo hace ideal para aplicaciones que requieren acceso rápido y confiable a grandes cantidades de datos.

Baja latencia: Latencia muy baja, lo cual es crucial para aplicaciones sensibles al rendimiento, como bases de datos y entornos virtualizados.

Confiabilidad: Las redes FC son conocidas por su robustez y confiabilidad, con características como redundancia incorporada y corrección de errores.

Ancho de banda dedicado: FC proporciona ancho de banda dedicado para el tráfico de almacenamiento, lo que reduce el riesgo de congestión de la red.

Para obtener más información sobre el uso de Fibre Channel con sistemas de almacenamiento NetApp , consulte "Aprovisionamiento de SAN con FC" .

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico FC.
- Recopile información WWPN de los hosts que se implementarán y cree grupos de iniciadores correspondientes en el sistema de almacenamiento ONTAP .
- Cree un volumen FC en el sistema de almacenamiento ONTAP .
- Asignar grupos de iniciadores para crear un volumen FC
- Utilice la zonificación de iniciador-destino único en los conmutadores FC. Cree una zona para cada iniciador (zona de iniciador único).
  - Para cada zona, incluya un destino que sea la interfaz lógica ONTAP FC (WWPN) para las SVM. Debe haber al menos dos interfaces lógicas por nodo por SVM. No utilice el WWPN de los puertos físicos.
- Cree un grupo de redes para el tráfico de vMotion en SDDC Manager.
- La comisión aloja servidores en VCF para su uso en un dominio de carga de trabajo VI.
- Implemente un dominio de carga de trabajo VI en VCF utilizando un almacén de datos FC como almacenamiento principal.

> Esta solución es aplicable a las plataformas ONTAP compatibles con almacenamiento NFS, incluidos NetApp AFF y FAS.

Prerrequisitos

En este escenario se utilizan los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP AFF o ASA con puertos FC conectados a conmutadores FC.
- SVM creado con FC lifs.
- vSphere con HBA FC conectados a conmutadores FC.
- La zonificación de iniciador-destino único está configurada en los conmutadores FC.

> NetApp recomienda múltiples rutas para LUN FC.

Pasos de implementación

Dominio de administración - Clúster predeterminado

El almacenamiento principal de FC en el clúster inicial solo es compatible con la herramienta de importación brownfield de VCF. Si VCF se implementa con la herramienta CloudBuilder (hasta la versión 5.2.x), solo se admite VSAN. Referirse "Conversión del entorno vSphere existente a un dominio de administración" Para más información.

Dominio de administración - Clúster adicional

El clúster vSphere adicional en el dominio de administración se puede implementar con las siguientes opciones: * Tener un clúster adicional en el entorno vSphere y usar la herramienta de importación brownfield VCF para convertir el entorno vSphere al dominio de administración. "ONTAP tools for VMware vSphere" , "Administrador del sistema o API de ONTAP" Se puede utilizar para implementar el almacén de datos VMFS en el clúster vSphere. * Utilice la API de SDDC para implementar un clúster adicional. Los hosts de vSphere deben tener el almacén de datos VMFS configurado. Usar "Administrador del sistema o API de ONTAP" para

implementar LUN en hosts vSphere. * Utilice la interfaz de usuario de SDDC Manager para implementar un clúster adicional. Pero esta opción solo crea un almacén de datos VSAN hasta la versión 5.2.x.

Dominio de carga de trabajo VI: clúster predeterminado

Una vez que el dominio de administración esté en funcionamiento, se puede crear el dominio de carga de trabajo de VI:

- Uso de la interfaz de usuario del administrador SDDC. Los hosts de vSphere deben tener el almacén de datos VMFS configurado. Utilice el Administrador del sistema o la API de ONTAP para implementar LUN en hosts vSphere.
- Importar un entorno vSphere existente como nuevo dominio de carga de trabajo VI. Se pueden usar las ONTAP tools for VMware vSphere, System Manager o ONTAP API para implementar el almacén de datos VMFS en el clúster vSphere.

Dominio de carga de trabajo VI - Clúster adicional

Una vez que la carga de trabajo de VI esté en funcionamiento, se pueden implementar clústeres adicionales con VMFS en FC LUN utilizando las siguientes opciones.

- Clústeres adicionales en el entorno de vSphere importados mediante la herramienta de importación brownfield de VCF. Se pueden usar las ONTAP tools for VMware vSphere, System Manager o ONTAP API para implementar el almacén de datos VMFS en el clúster vSphere.
- Usar la interfaz de usuario o la API de SDDC Manager para implementar un clúster adicional. Los hosts de vSphere deben tener el almacén de datos VMFS configurado. Utilice el Administrador del sistema o la API de ONTAP para implementar LUN en hosts vSphere.

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Utilice un almacén de datos NFS en ONTAP como almacenamiento principal para un dominio de carga de trabajo VI

En este caso de uso, describimos el procedimiento para configurar un almacén de datos NFS en ONTAP como la solución de almacenamiento principal para un dominio de carga de trabajo de infraestructura virtual (VI) de VMware Cloud Foundation (VCF). Este procedimiento resume los componentes necesarios, los pasos de configuración y el proceso de implementación.

Beneficios de NFS

Simplicidad y facilidad de uso: NFS es fácil de configurar y administrar, lo que lo convierte en una excelente opción para entornos que requieren compartir archivos de manera rápida y sencilla.

Escalabilidad: La arquitectura de ONTAP permite que NFS escale de manera eficiente, soportando las crecientes necesidades de datos sin cambios significativos en la infraestructura.

Flexibilidad: NFS admite una amplia gama de aplicaciones y cargas de trabajo, lo que lo hace versátil para

diversos casos de uso, incluidos entornos virtualizados.

Para obtener más información, consulte la Guía de referencia de NFS v3 para vSphere 8.

Para obtener más información sobre el uso de Fibre Channel con sistemas de almacenamiento NetApp , consulte"Guía de referencia de NFS v3 para vSphere 8" .

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Cree una máquina virtual de almacenamiento (SVM) con interfaz lógica (LIF) para el tráfico NFS
- Verifique la red para la máquina virtual de almacenamiento ONTAP (SVM) y que haya una interfaz lógica (LIF) presente para transportar tráfico NFS.
- Cree una política de exportación para permitir que los hosts ESXi accedan al volumen NFS.
- Cree un volumen NFS en el sistema de almacenamiento ONTAP .
- Cree un grupo de redes para el tráfico NFS y vMotion en SDDC Manager.
- La comisión aloja servidores en VCF para su uso en un dominio de carga de trabajo VI.
- Implemente un dominio de carga de trabajo VI en VCF utilizando un almacén de datos NFS como almacenamiento principal.
- Instalar el complemento NFS de NetApp para VMware VAAI

> Esta solución es aplicable a las plataformas ONTAP compatibles con almacenamiento NFS, incluidos NetApp AFF y FAS.

Prerrequisitos

En este escenario se utilizan los siguientes componentes y configuraciones:

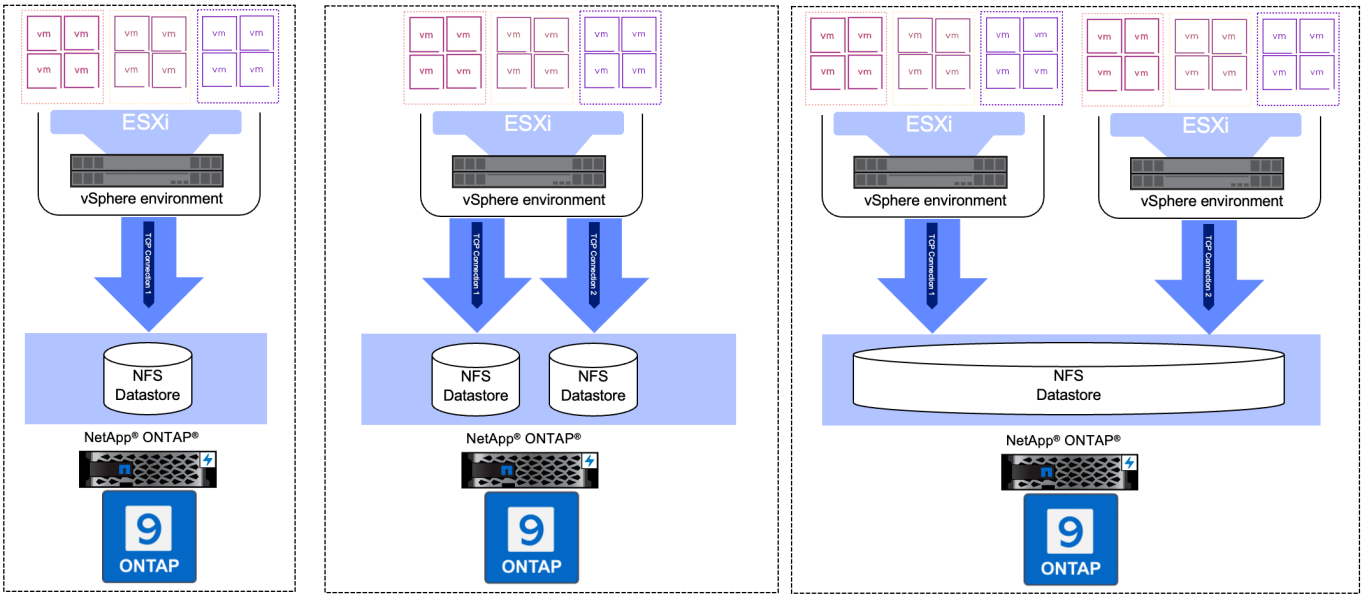
- Sistema de almacenamiento NetApp AFF con una máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico NFS.
- Se ha creado una interfaz lógica (LIF) en la red IP que transportará el tráfico NFS y está asociada con la SVM.
- La implementación del dominio de administración de VCF está completa y se puede acceder a la interfaz del Administrador de SDDC.
- 4 hosts ESXi configurados para la comunicación en la red de administración de VCF.
- Direcciones IP reservadas para el tráfico de almacenamiento vMotion y NFS en la VLAN o segmento de red establecido para este propósito.

> Al implementar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se hace utilizando el adaptador de administración en los hosts ESXi antes de agregar cualquier adaptador vmkernel adicional con la dirección IP NFS. Por lo tanto, es necesario garantizar que 1) la red de administración sea enrutable al servidor NFS o 2) se haya agregado un LIF para la red de administración al SVM que aloja el volumen del almacén de datos NFS, para garantizar que la validación pueda continuar.

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Para obtener más información sobre el uso de NFS con clústeres de vSphere, consulte la"Guía de referencia de NFS v3 para vSphere 8" .



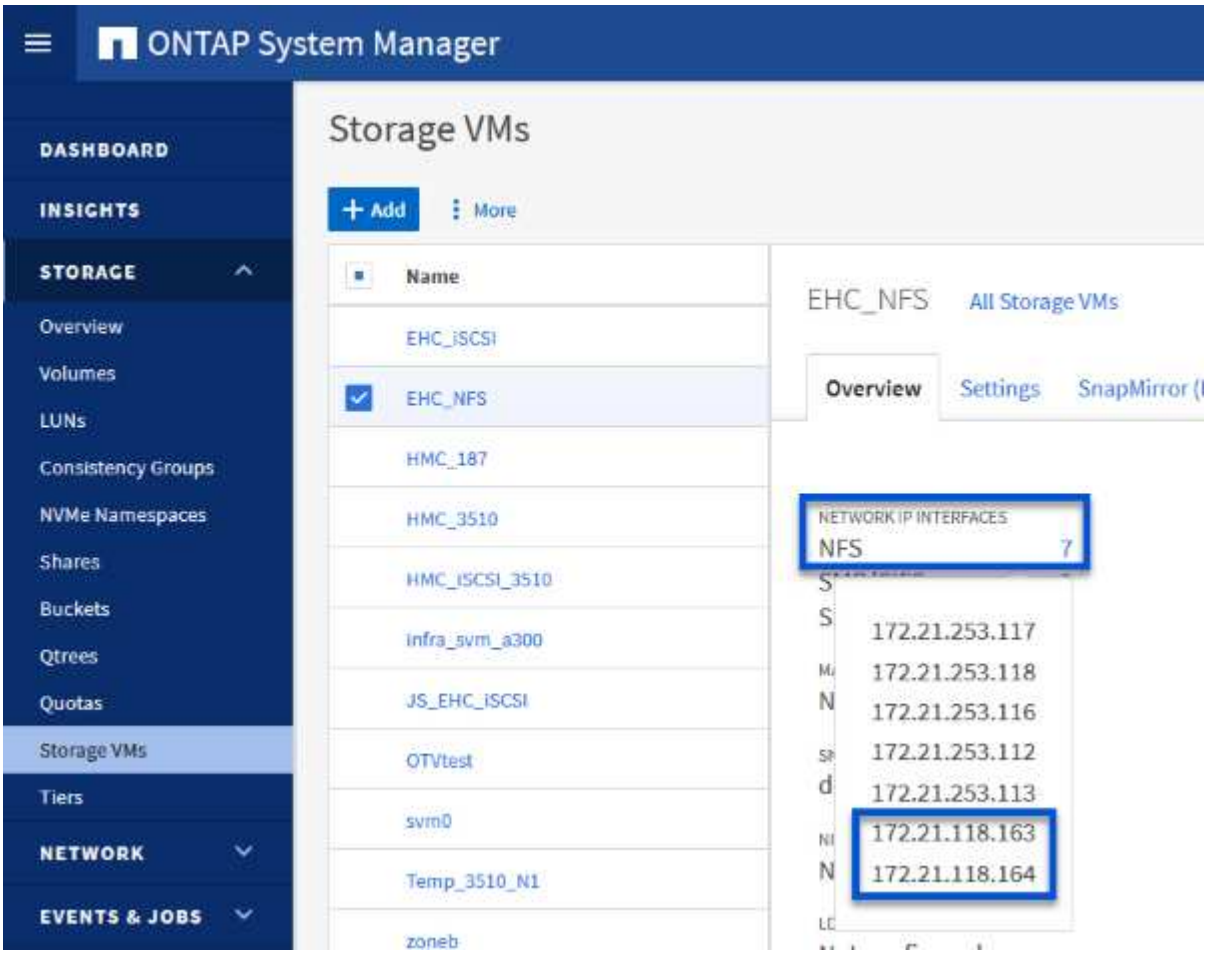
Pasos de implementación

Para implementar un dominio de carga de trabajo VI con un almacén de datos NFS como almacenamiento principal, complete los siguientes pasos:

Verificar la red para ONTAP SVM

Verifique que se hayan establecido las interfaces lógicas necesarias para la red que transportará el tráfico NFS entre el clúster de almacenamiento ONTAP y el dominio de carga de trabajo VI.

1. Desde el Administrador del sistema ONTAP , navegue hasta **Máquinas virtuales de almacenamiento** en el menú de la izquierda y haga clic en la SVM que se utilizará para el tráfico NFS. En la pestaña **Descripción general**, en **INTERFACES IP DE RED**, haga clic en el número a la derecha de **NFS**. En la lista, verifique que se incluyan las direcciones IP LIF requeridas.



Como alternativa, verifique los LIF asociados con una SVM desde la CLI de ONTAP con el siguiente comando:

```
network interface show -vserver <SVM_NAME>
```

1. Verifique que los hosts ESXi puedan comunicarse con el servidor NFS de ONTAP . Inicie sesión en el host ESXi a través de SSH y haga ping al LIF de SVM:

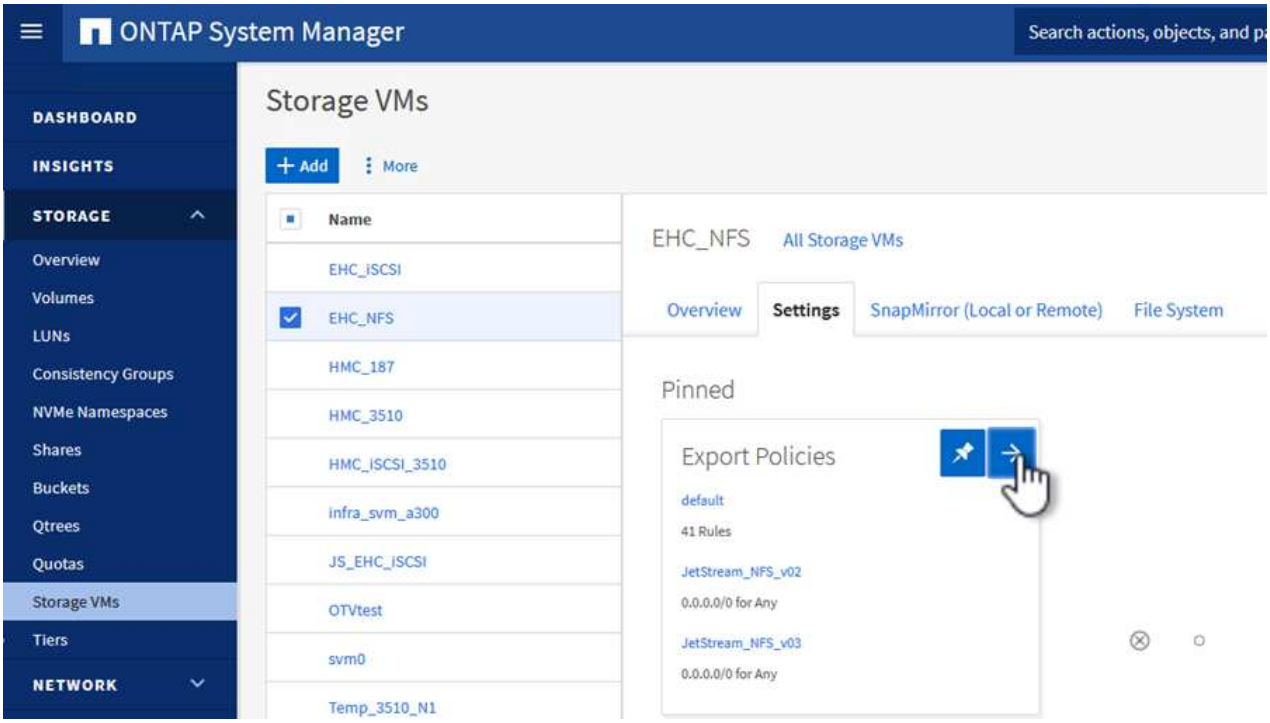
```
vmkping <IP Address>
```

Al implementar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se hace utilizando el adaptador de administración en los hosts ESXi antes de agregar cualquier adaptador vmkernel adicional con la dirección IP NFS. Por lo tanto, es necesario garantizar que 1) la red de administración sea enrutable al servidor NFS o 2) se haya agregado un LIF para la red de administración al SVM que aloja el volumen del almacén de datos NFS, para garantizar que la validación pueda continuar.

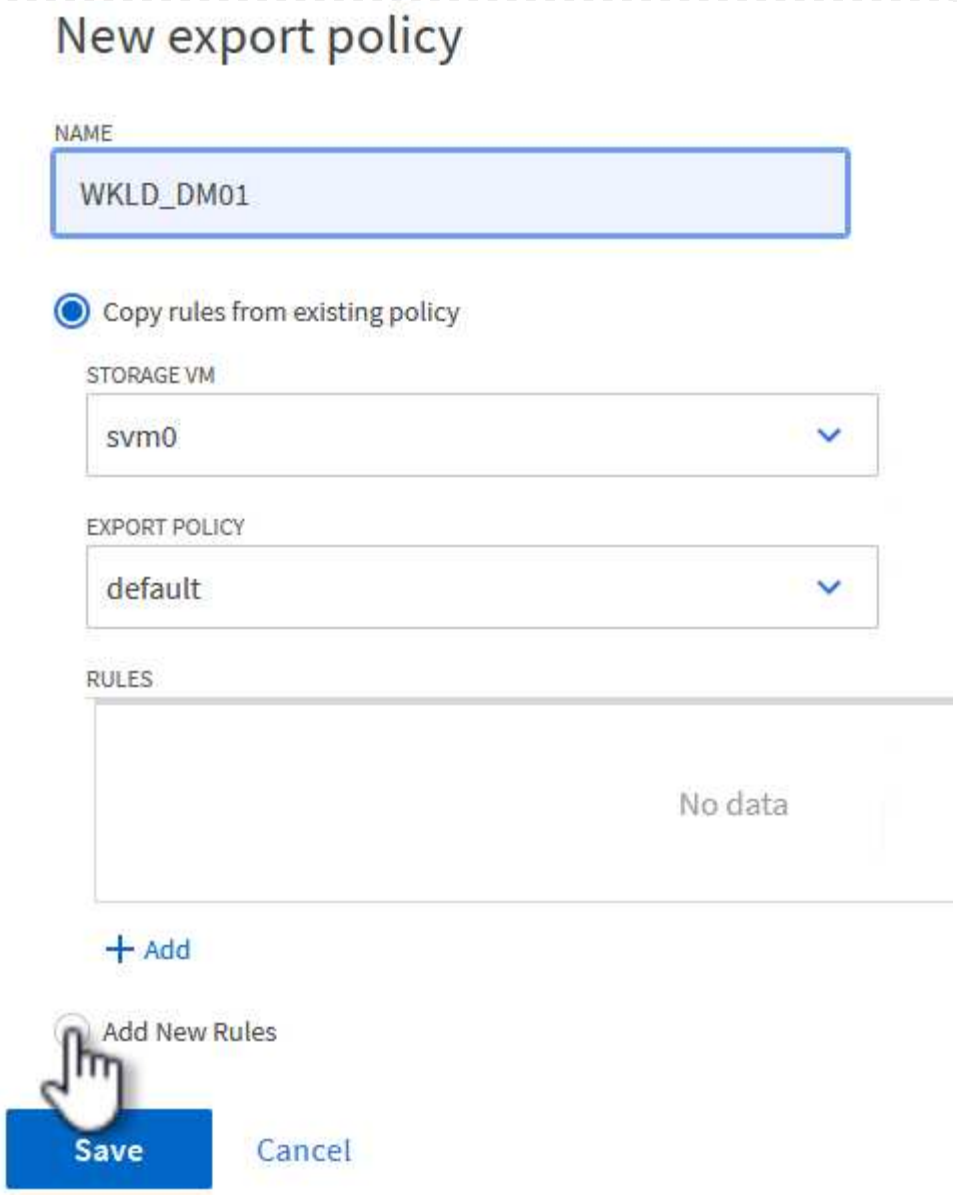
Crear una política de exportación para compartir un volumen NFS

Cree una política de exportación en ONTAP System Manager para definir el control de acceso para volúmenes NFS.

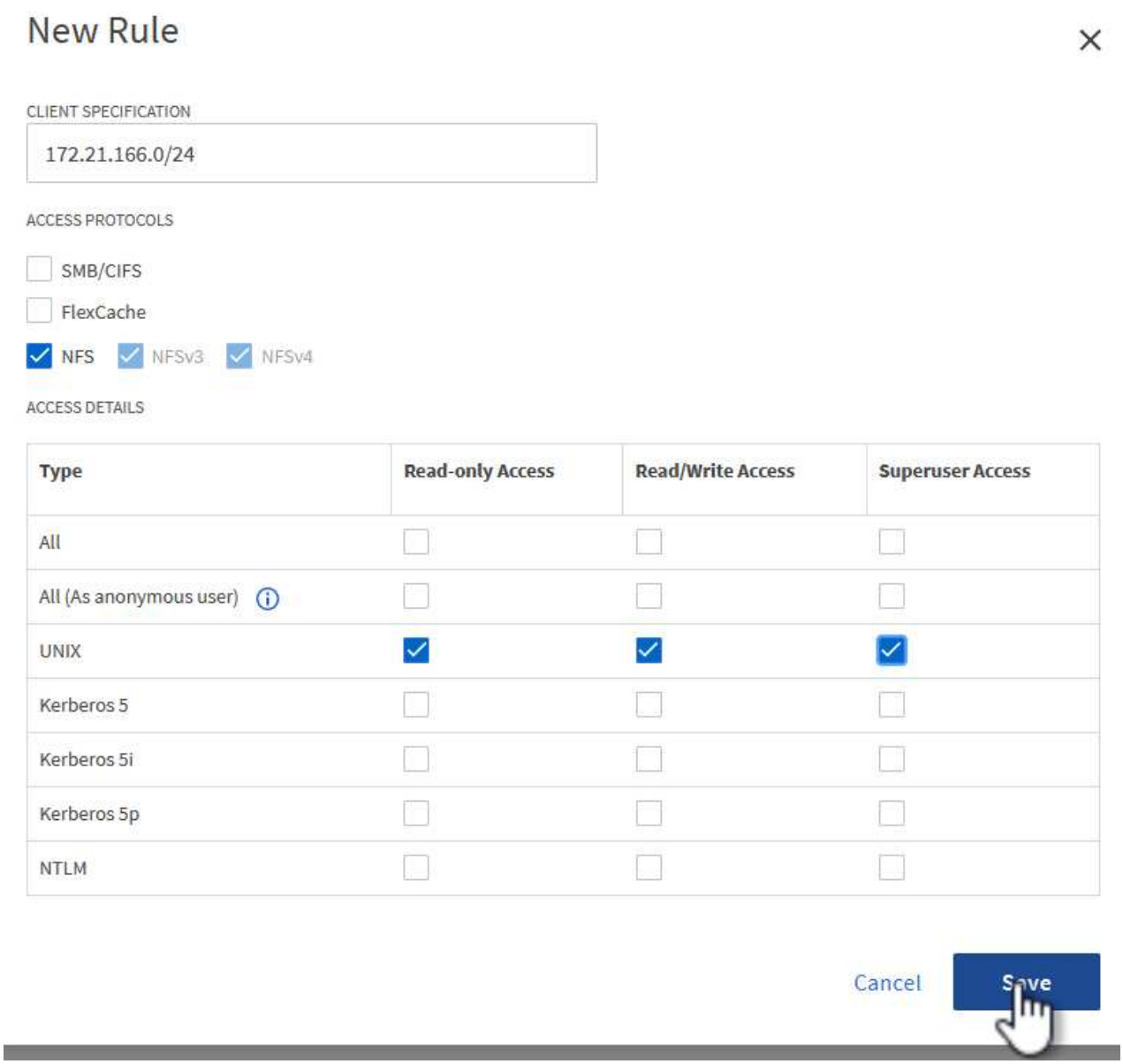
1. En el Administrador del sistema ONTAP , haga clic en **Máquinas virtuales de almacenamiento** en el menú de la izquierda y seleccione una SVM de la lista.
2. En la pestaña **Configuración**, busque **Políticas de exportación** y haga clic en la flecha para acceder.



3. En la ventana **Nueva política de exportación** agregue un nombre para la política, haga clic en el botón **Agregar nuevas reglas** y luego en el botón **+Agregar** para comenzar a agregar una nueva regla.



4. Complete las direcciones IP, el rango de direcciones IP o la red que desea incluir en la regla. Desmarque las casillas **SMB/Cifs** y * FlexCache* y realice selecciones para los detalles de acceso a continuación. Seleccionar las casillas UNIX es suficiente para acceder al host ESXi.



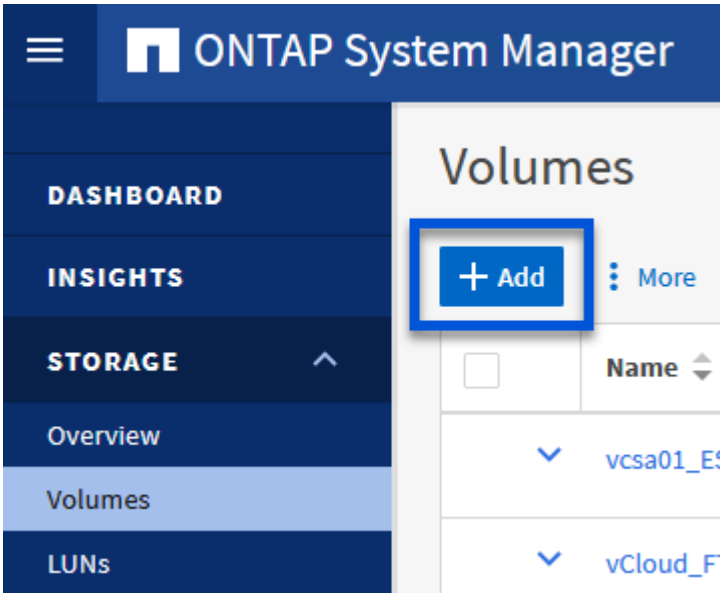
> Al implementar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se hace utilizando el adaptador de administración en los hosts ESXi antes de agregar cualquier adaptador vmkernel adicional con la dirección IP NFS. Por lo tanto, es necesario garantizar que la política de exportación incluya la red de gestión del VCF para permitir que se lleve a cabo la validación.

5. Una vez ingresadas todas las reglas, haga clic en el botón **Guardar** para guardar la nueva Política de exportación.
6. Alternativamente, puede crear políticas y reglas de exportación en la CLI de ONTAP . Consulte los pasos para crear una política de exportación y agregar reglas en la documentación de ONTAP .
   - Utilice la CLI de ONTAP para"Crear una política de exportación" .
   - Utilice la CLI de ONTAP para"Agregar una regla a una política de exportación" .

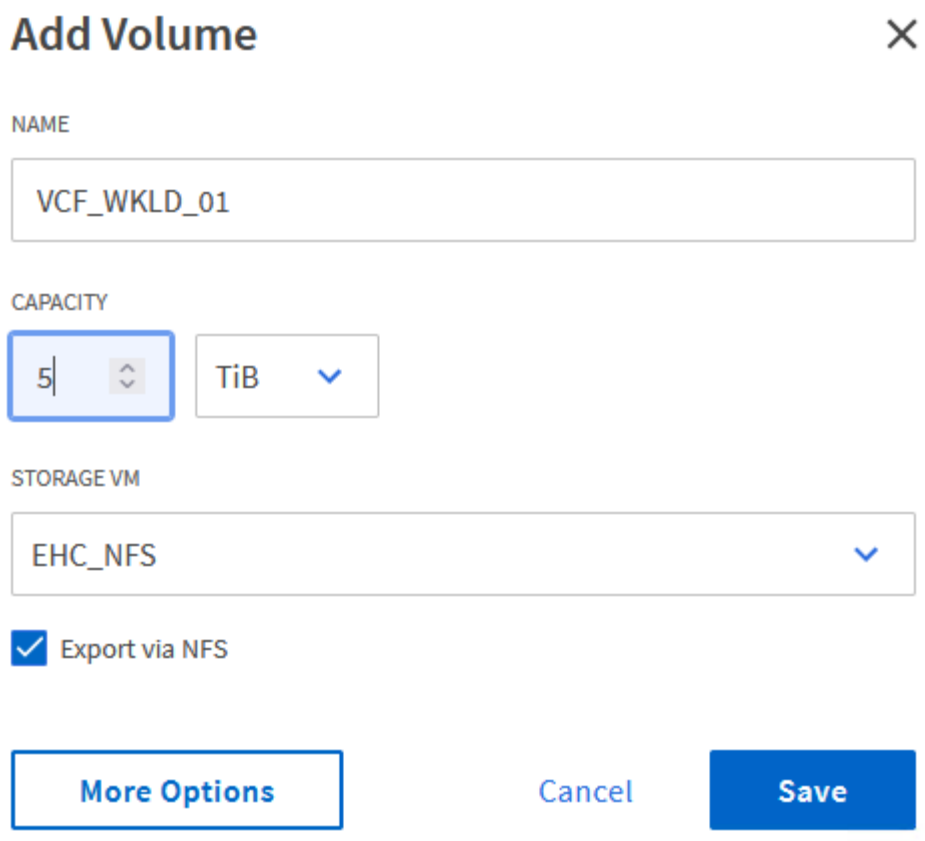
Crear volumen NFS

Cree un volumen NFS en el sistema de almacenamiento ONTAP para usarlo como almacén de datos en la implementación del dominio de carga de trabajo.

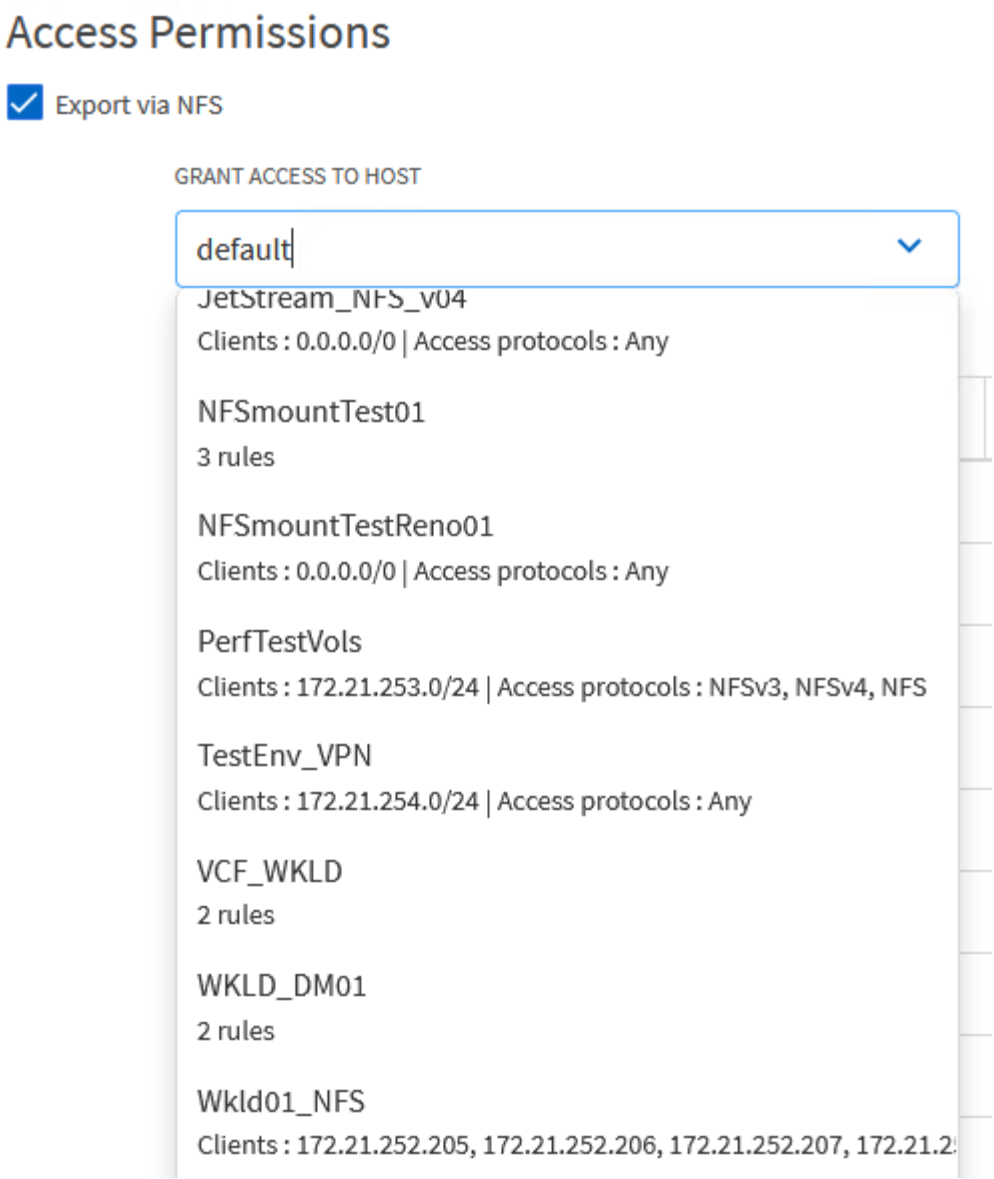
1. Desde el Administrador del sistema ONTAP , navegue a **Almacenamiento > Volúmenes** en el menú de la izquierda y haga clic en **+Agregar** para crear un nuevo volumen.



2. Agregue un nombre para el volumen, complete la capacidad deseada y seleccione la máquina virtual de almacenamiento que alojará el volumen. Haga clic en **Más opciones** para continuar.



3. En Permisos de acceso, seleccione la Política de exportación que incluye la red de administración de VCF o la dirección IP y las direcciones IP de la red NFS que se utilizarán tanto para la validación del servidor NFS como para el tráfico NFS.



+

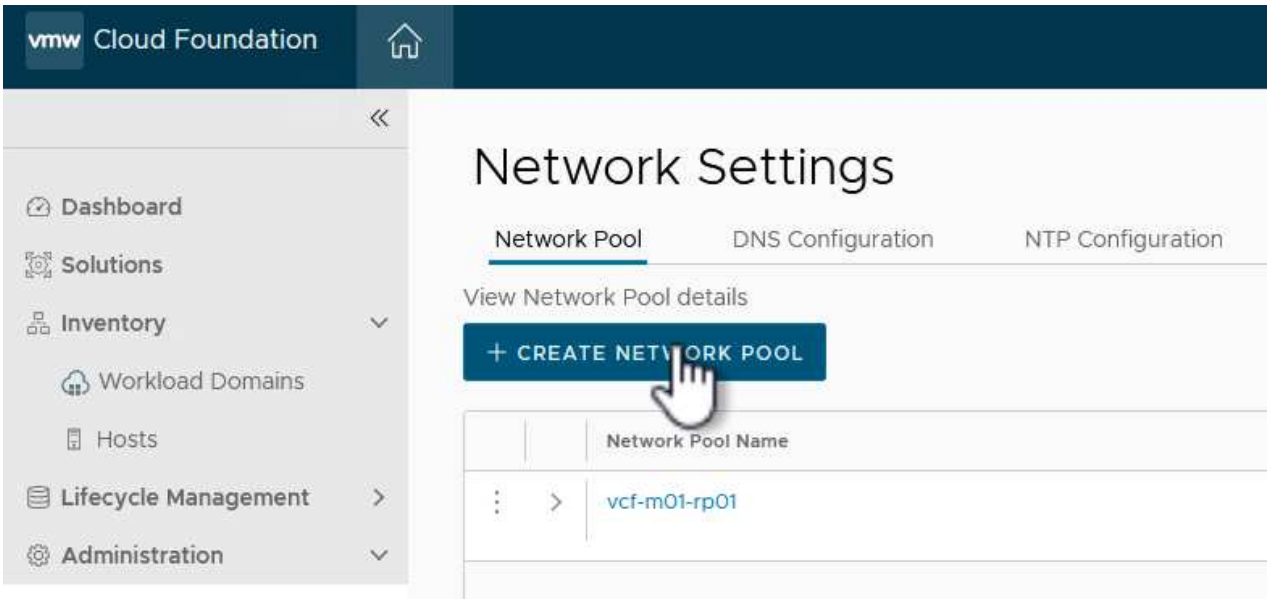
> Al implementar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se hace utilizando el adaptador de administración en los hosts ESXi antes de agregar cualquier adaptador vmkernel adicional con la dirección IP NFS. Por lo tanto, es necesario garantizar que 1) la red de administración sea enrutable al servidor NFS o 2) se haya agregado un LIF para la red de administración al SVM que aloja el volumen del almacén de datos NFS, para garantizar que la validación pueda continuar.

4. Alternativamente, los volúmenes ONTAP se pueden crear en la CLI de ONTAP . Para obtener más información, consulte la"lun crear" Comando en la documentación de comandos de ONTAP .

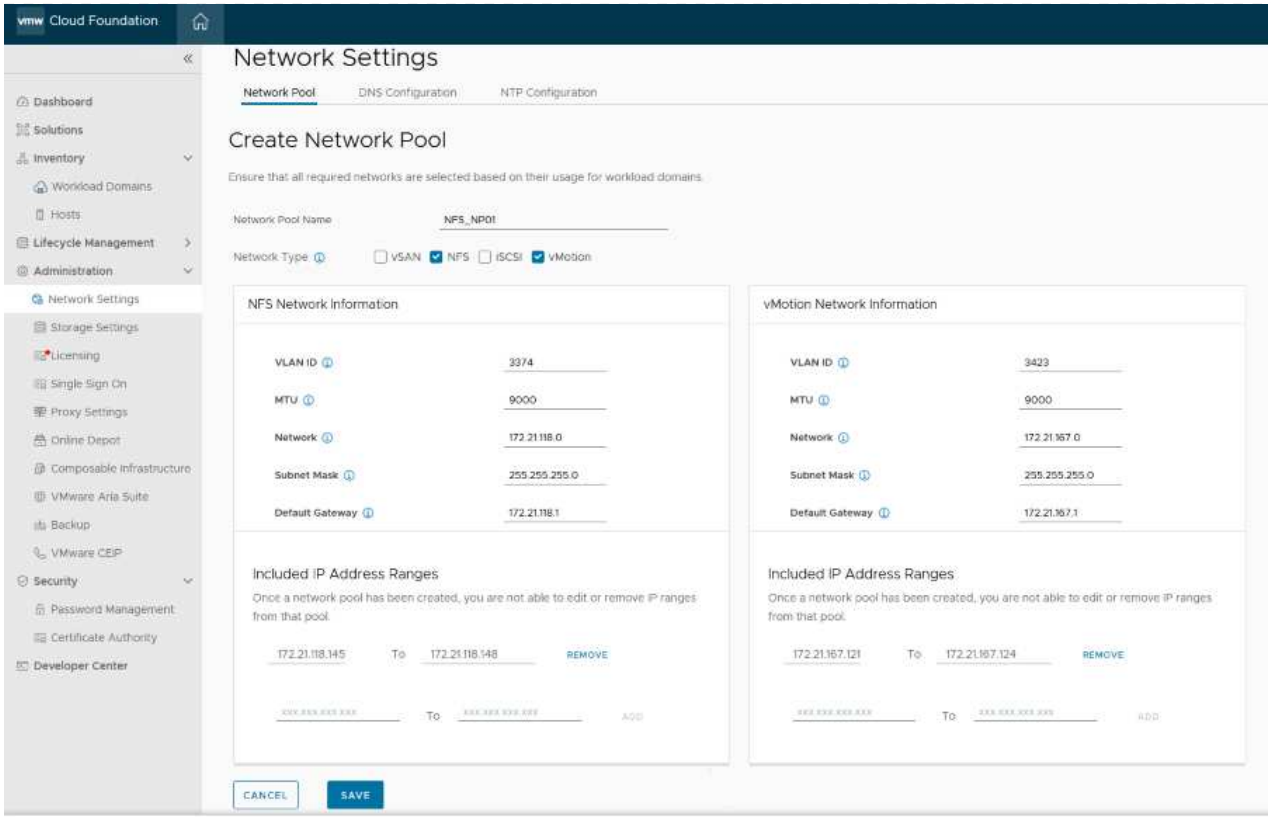
Crear un grupo de redes en SDDC Manager

Se debe crear un grupo de redes en SDDC Manager antes de poner en funcionamiento los hosts ESXi, como preparación para implementarlos en un dominio de carga de trabajo VI. El grupo de redes debe incluir la información de red y los rangos de direcciones IP para que los adaptadores VMkernel se utilicen para la comunicación con el servidor NFS.

1. Desde la interfaz web de SDDC Manager, navegue a **Configuración de red** en el menú de la izquierda y haga clic en el botón **+ Crear grupo de redes**.



2. Complete un nombre para el grupo de redes, seleccione la casilla de verificación para NFS y complete todos los detalles de la red. Repita esto para la información de la red vMotion.



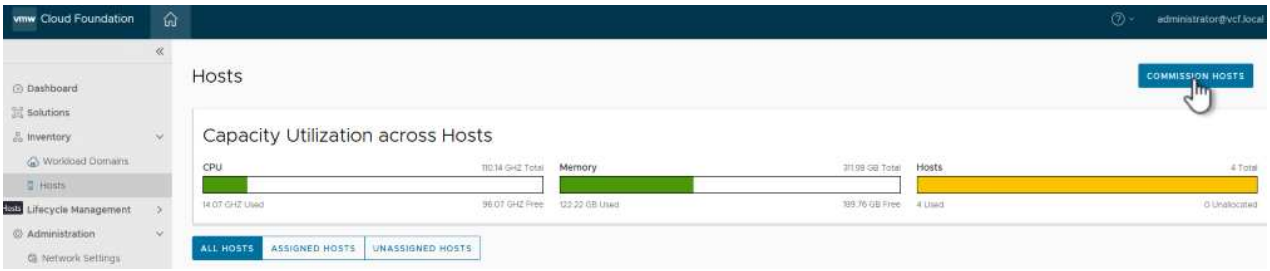
3. Haga clic en el botón **Guardar** para completar la creación del grupo de redes.

Anfitriones de la Comisión

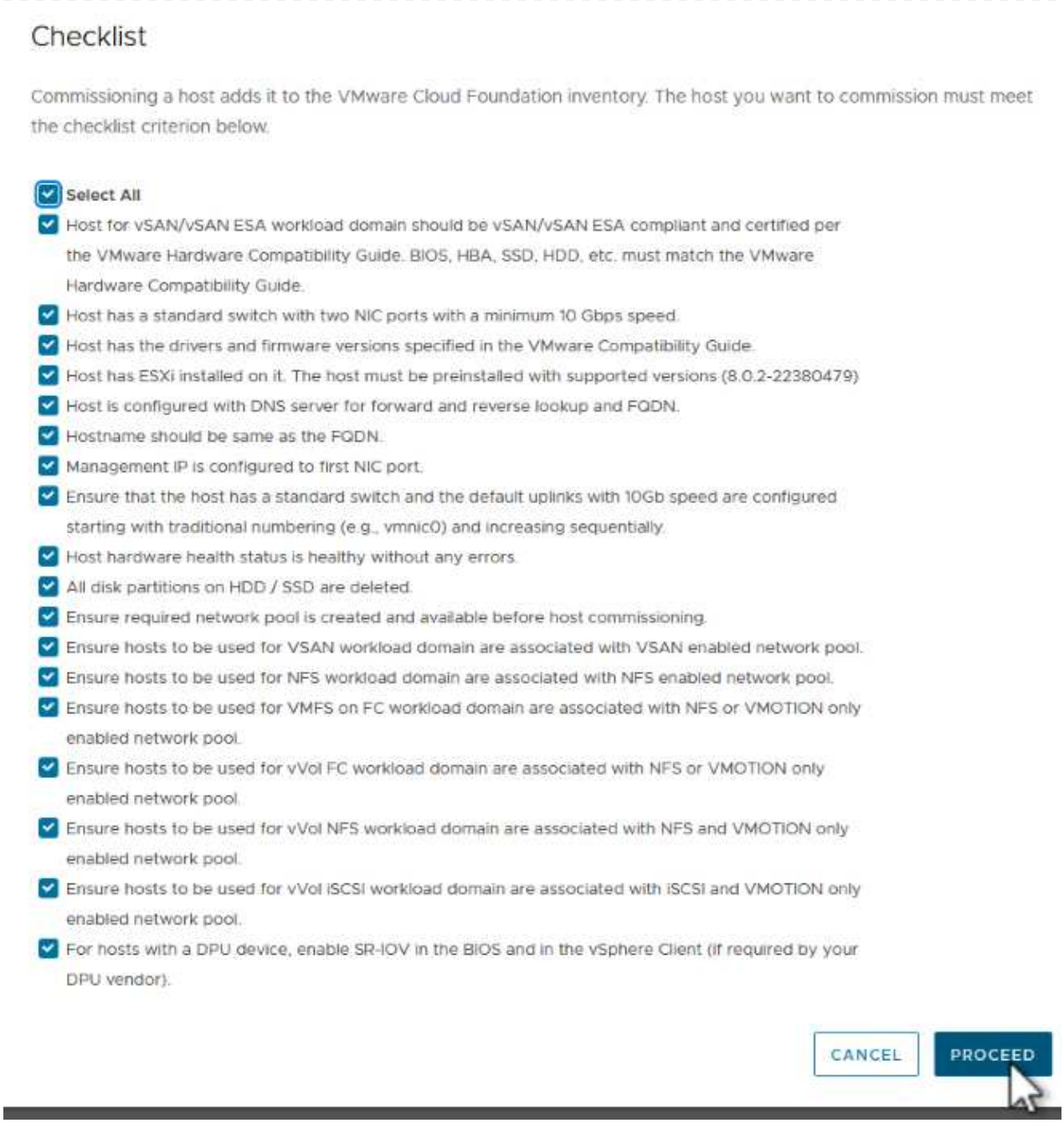
Antes de que los hosts ESXi se puedan implementar como un dominio de carga de trabajo, se deben agregar al inventario de SDDC Manager. Esto implica proporcionar la información requerida, pasar la validación e iniciar el proceso de puesta en servicio.

Para más información véase"Anfitriones de la Comisión" en la Guía de administración de VCF.

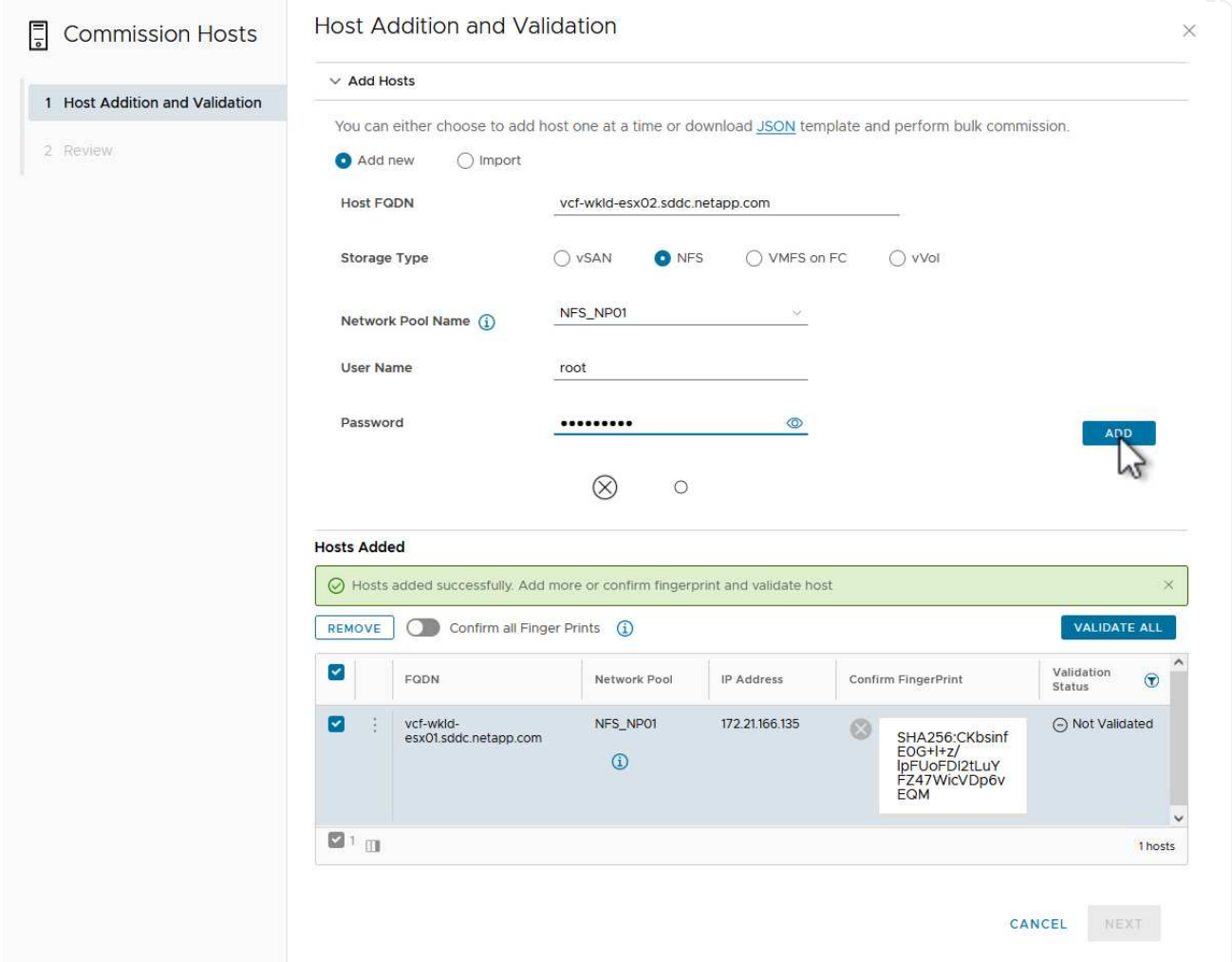
1. Desde la interfaz del Administrador de SDDC, navegue hasta **Hosts** en el menú de la izquierda y haga clic en el botón **Comisionar Hosts**.



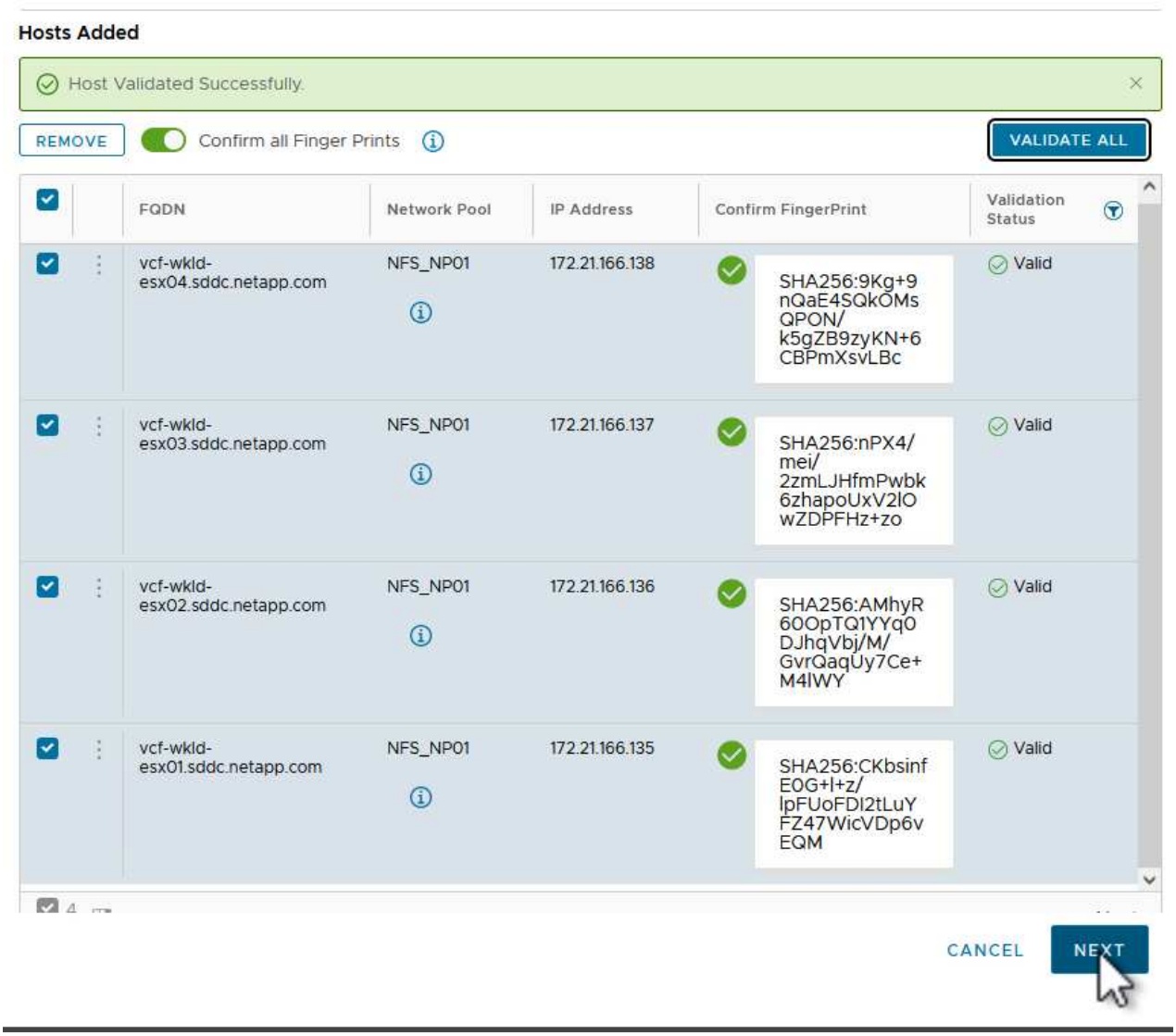
2. La primera página es una lista de verificación de requisitos previos. Verifique todos los requisitos previos y seleccione todas las casillas de verificación para continuar.



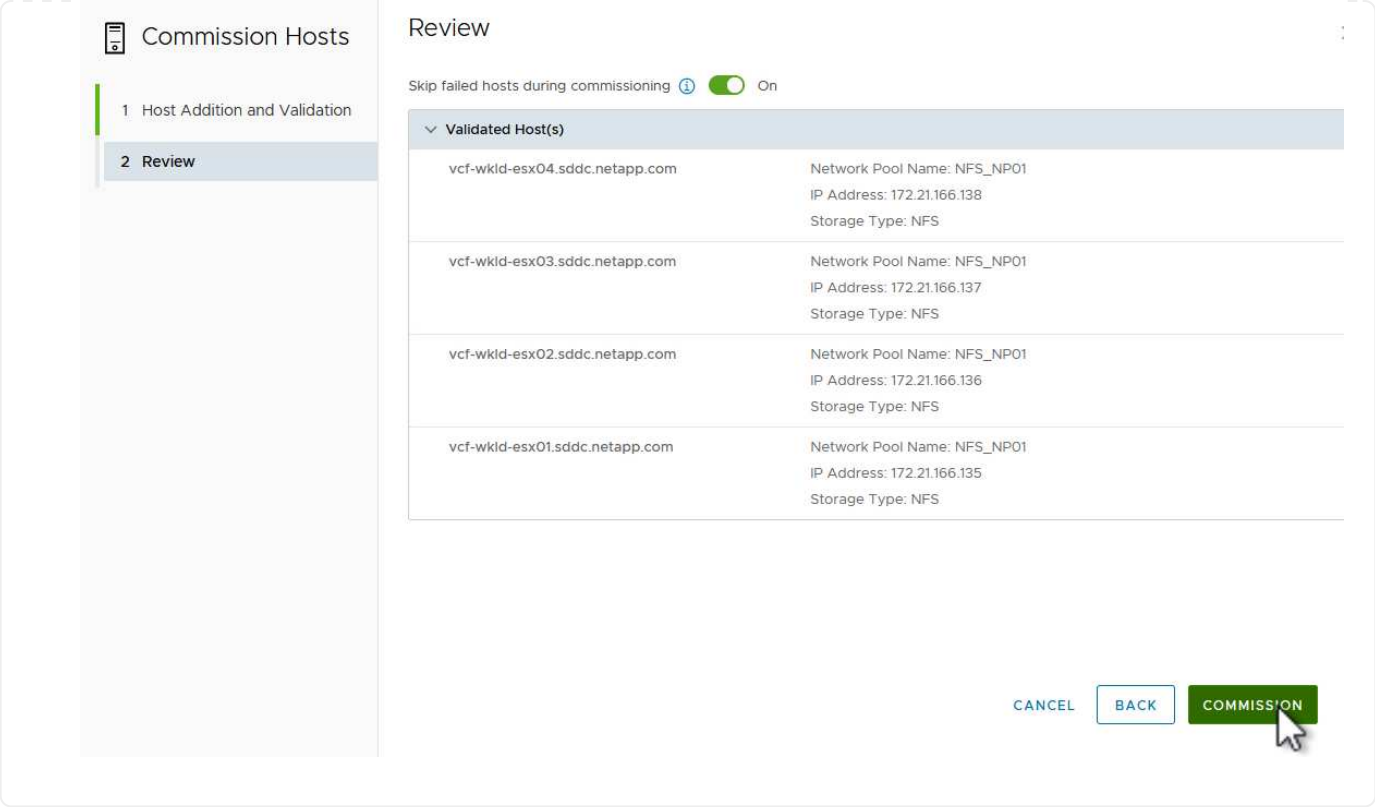
3. En la ventana **Adición y validación de host**, complete el **FQDN del host**, el **Tipo de almacenamiento**, el nombre del **Grupo de red** que incluye las direcciones IP de almacenamiento NFS y vMotion que se usarán para el dominio de carga de trabajo y las credenciales para acceder al host ESXi. Haga clic en **Agregar** para agregar el host al grupo de hosts que se validará.



4. Una vez que se hayan agregado todos los hosts que se validarán, haga clic en el botón **Validar todo** para continuar.
5. Suponiendo que todos los hosts estén validados, haga clic en **Siguiente** para continuar.



6. Revise la lista de hosts que serán comisionados y haga clic en el botón **Comisión** para iniciar el proceso. Supervise el proceso de puesta en servicio desde el panel de tareas en el administrador de SDDC.

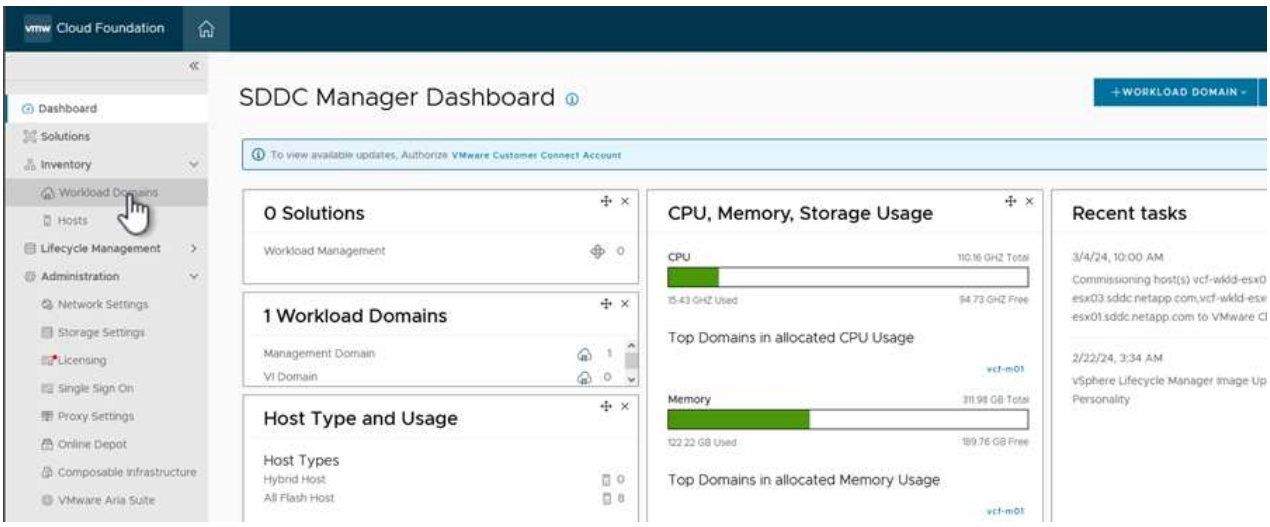

Commission Hosts
1 Host Addition and Validation
2 Review
Review
Skip failed hosts during commissioning
On
Validated Host(s)
vcf-wkld-esx04.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.138
Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.137
Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.136
Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.135
Storage Type: NFS
CANCEL
BACK
COMMISSION

Implementar el dominio de carga de trabajo de VI

La implementación de dominios de carga de trabajo VI se logra mediante la interfaz de VCF Cloud Manager. Aquí solo se presentarán los pasos relacionados con la configuración del almacenamiento.

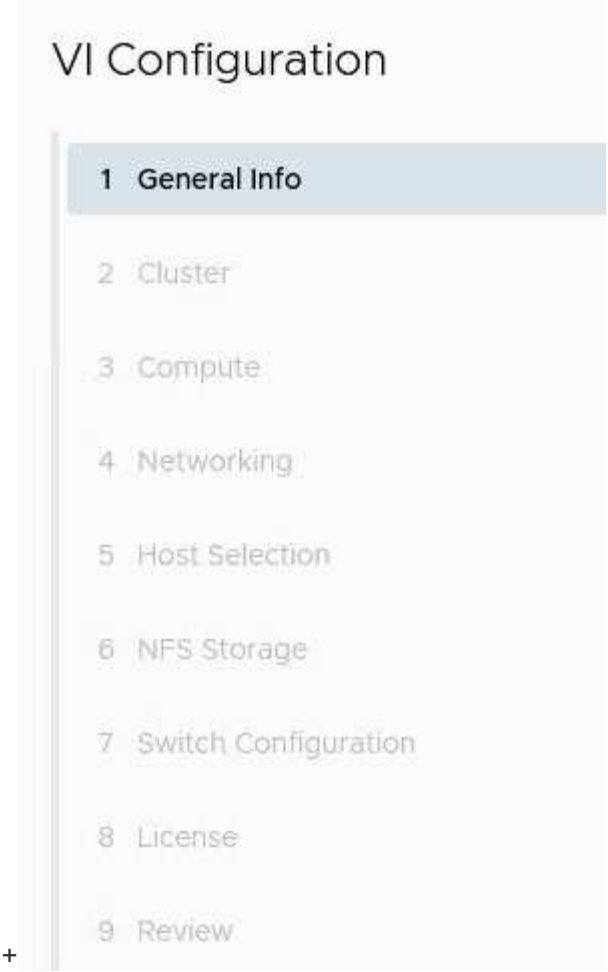
Para obtener instrucciones paso a paso sobre cómo implementar un dominio de carga de trabajo VI, consulte"Implementar un dominio de carga de trabajo de VI mediante la interfaz de usuario del administrador de SDDC" .

1. Desde el panel de control de SDDC Manager, haga clic en **+ Dominio de carga de trabajo** en la esquina superior derecha para crear un nuevo dominio de carga de trabajo.



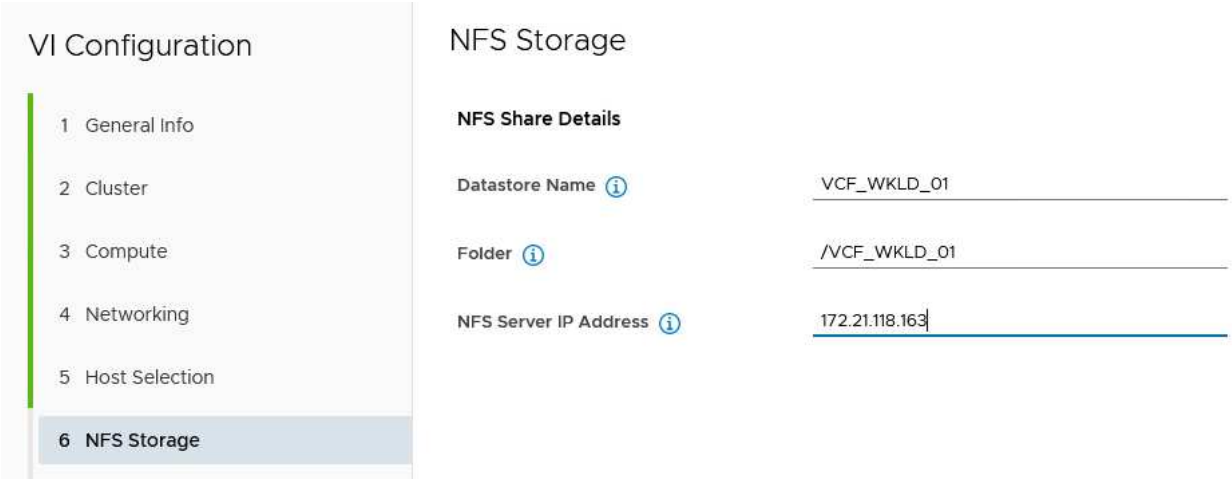
2. En el asistente de configuración de VI, complete las secciones de **Información general, Clúster, Computación, Redes** y **Selección de host** según sea necesario.

Para obtener información sobre cómo completar la información requerida en el asistente de configuración de VI, consulte"Implementar un dominio de carga de trabajo de VI mediante la interfaz de usuario del administrador de SDDC" .

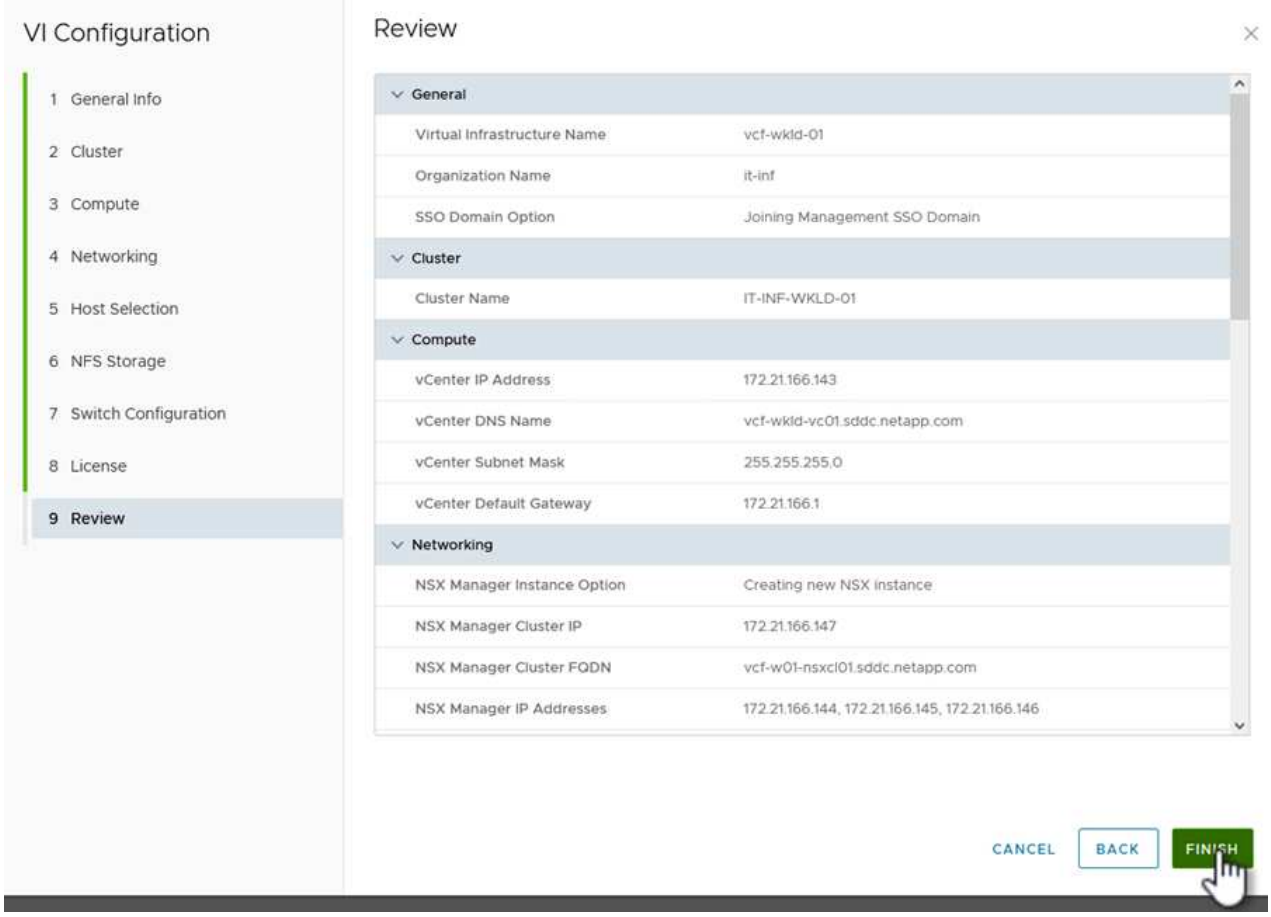


+

1. En la sección Almacenamiento NFS, complete el nombre del almacén de datos, el punto de montaje de la carpeta del volumen NFS y la dirección IP del LIF de la máquina virtual de almacenamiento NFS de ONTAP .



2. En el asistente de configuración de VI, complete los pasos de Configuración del conmutador y Licencia y, a continuación, haga clic en **Finalizar** para iniciar el proceso de creación del Dominio de carga de trabajo.



3. Supervisar el proceso y resolver cualquier problema de validación que surja durante el proceso.

Instalar el complemento NFS de NetApp para VMware VAAI

El complemento NFS de NetApp para VMware VAAI integra las bibliotecas de discos virtuales de VMware instaladas en el host ESXi y proporciona operaciones de clonación de mayor rendimiento que finalizan más rápido. Este es un procedimiento recomendado cuando se utilizan sistemas de almacenamiento ONTAP con VMware vSphere.

Para obtener instrucciones paso a paso sobre cómo implementar el complemento NFS de NetApp para VMware VAAI, siga las instrucciones en"Instalar el complemento NFS de NetApp para VMware VAAI" .

Demostración en vídeo de esta solución

Almacenes de datos NFS como almacenamiento principal para dominios de carga de trabajo VCF

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Ampliar VCF con almacenamiento complementario

Obtenga información sobre cómo ampliar el almacenamiento para un entorno VCF mediante almacenamiento complementario

VMware Cloud Foundation (VCF) admite una amplia gama de opciones de almacenamiento complementario para expandir el almacenamiento en dominios de administración de VCF y dominios de carga de trabajo de infraestructura virtual (VI).

Las herramientas ONTAP de NetApp para VMware vSphere proporcionan una solución eficiente para esta expansión al integrar perfectamente el almacenamiento de NetApp en el entorno VCF. Las herramientas de ONTAP simplifican la configuración y la administración de almacenes de datos, lo que permite a los administradores aprovisionar y administrar el almacenamiento directamente desde vSphere Client. Las funciones avanzadas de ONTAP, como instantáneas, clonación y protección de datos, mejoran el rendimiento, la eficiencia y la escalabilidad del almacenamiento dentro del entorno VCF.

Consulte las siguientes soluciones para obtener detalles técnicos para ampliar el entorno VCF.

- "Dominio de gestión con iSCSI"
- "Dominio de gestión con FC"
- "Dominio de carga de trabajo de infraestructura virtual con vVols (iSCSI)"
- "Dominio de carga de trabajo de infraestructura virtual con vVols (NFS)"
- "Dominio de carga de trabajo de infraestructura virtual con NVMe/TCP"
- "Dominio de carga de trabajo de infraestructura virtual con FC"

Agregue un almacén de datos iSCSI como almacenamiento complementario para un dominio de administración mediante ONTAP tools for VMware vSphere

En este caso de uso, describimos el procedimiento para agregar un almacén de datos iSCSI como almacenamiento complementario para un dominio de administración de VMware Cloud Foundation (VCF). Este procedimiento resume la configuración de una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para iSCSI, la configuración de redes iSCSI en hosts ESXi, la implementación de herramientas ONTAP para VMware vSphere y la creación de un almacén de datos VMFS.

Beneficios de iSCSI

Alto rendimiento: Ofrece un alto rendimiento para brindar velocidades de transferencia de datos rápidas y eficientes y baja latencia. Ideal para aplicaciones empresariales exigentes y entornos virtualizados.

Facilidad de administración: Simplifica la gestión del almacenamiento mediante el uso de herramientas y protocolos familiares basados en IP.

Rentable: Utiliza la infraestructura Ethernet existente, lo que reduce la necesidad de hardware especializado y permite a las organizaciones lograr soluciones de almacenamiento confiables y escalables.

Para obtener más información sobre el uso de iSCSI con sistemas de almacenamiento NetApp , consulte "Aprovisionamiento de SAN con iSCSI" .

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

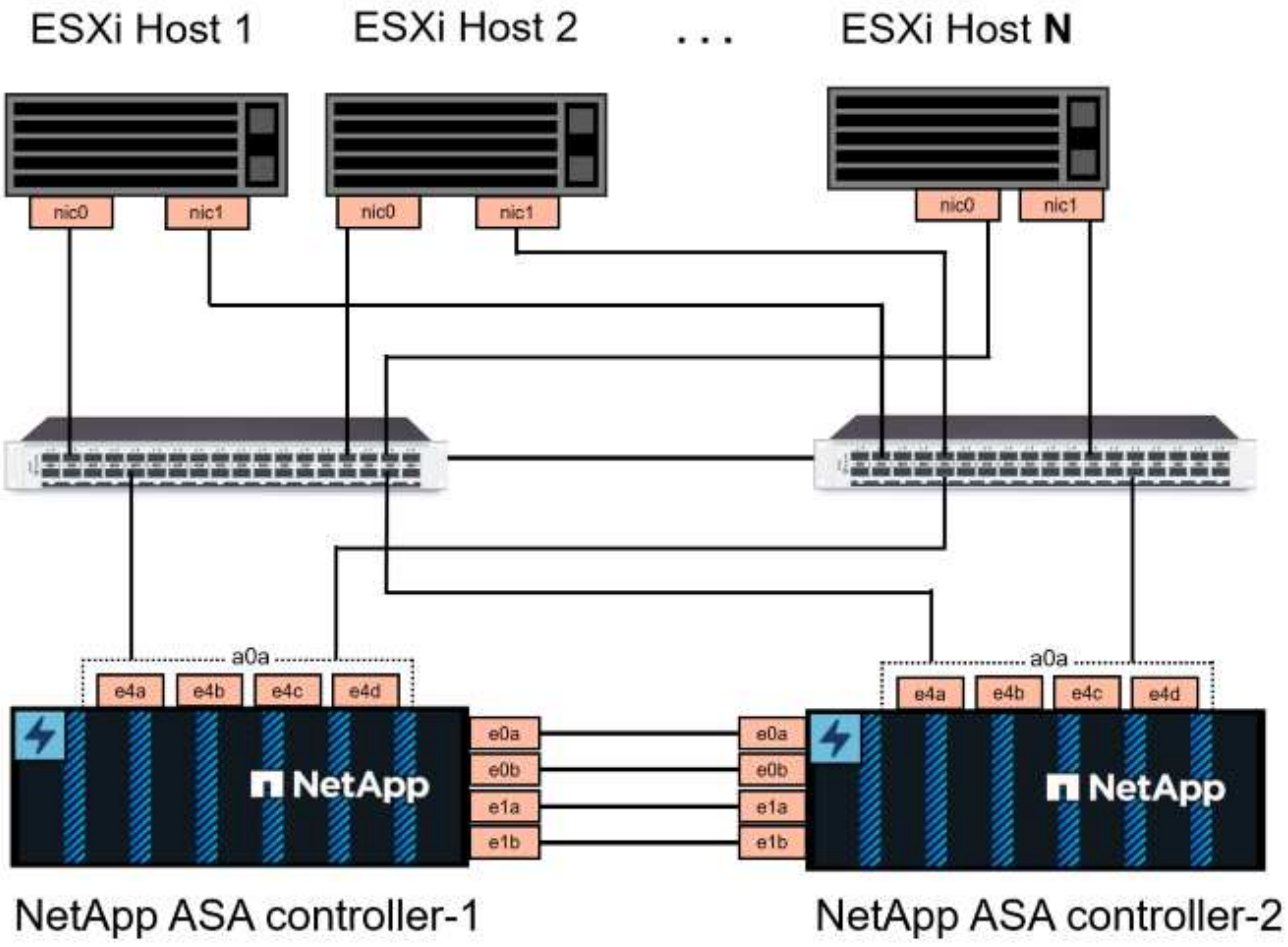
- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico iSCSI.
- Cree grupos de puertos distribuidos para redes iSCSI en el dominio de administración de VCF.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de administración de VCF.
- Implementar herramientas ONTAP en el dominio de administración de VCF.
- Cree un nuevo almacén de datos VMFS en el dominio de administración de VCF.

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP AFF o ASA con puertos de datos físicos en conmutadores Ethernet dedicados al tráfico de almacenamiento.
- La implementación del dominio de administración de VCF está completa y el cliente vSphere es accesible.

NetApp recomienda diseños de red totalmente redundantes para iSCSI. El siguiente diagrama ilustra un ejemplo de una configuración redundante, que proporciona tolerancia a fallas para sistemas de almacenamiento, conmutadores, adaptadores de red y sistemas host. Consulte NetApp"Referencia de configuración de SAN" Para obtener información adicional.



Para rutas múltiples y conmutación por error en múltiples rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet separadas para todas las SVM en configuraciones iSCSI.

Esta documentación demuestra el proceso de creación de una nueva SVM y la especificación de la información de la dirección IP para crear múltiples LIF para el tráfico iSCSI. Para agregar nuevos LIF a un SVM existente, consulte"Crear una LIF (interfaz de red)" .

Para obtener información adicional sobre el uso de almacenes de datos iSCSI VMFS con VMware, consulte"vSphere VMFS Datastore: backend de almacenamiento iSCSI con ONTAP" .

> En situaciones donde se configuran varios adaptadores VMkernel en la misma red IP, se recomienda utilizar la vinculación de puertos iSCSI de software en los hosts ESXi para garantizar que se produzca un equilibrio de carga entre los adaptadores. Consulte el artículo de Knowledge Base"Consideraciones para el uso de la vinculación de puertos iSCSI de software en ESX/ESXi (2038869)" .

Pasos de implementación

Para implementar ONTAP Tools y usarlo para crear un almacén de datos VMFS en el dominio de administración de VCF, complete los siguientes pasos:

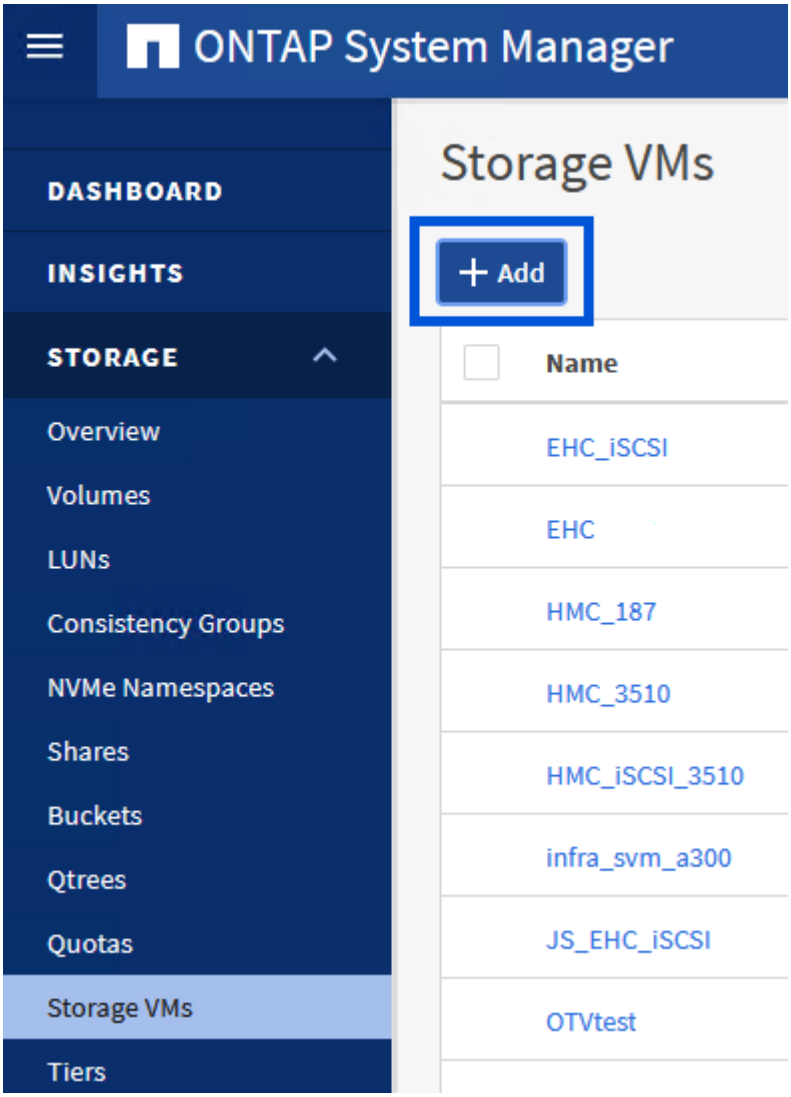
Crear SVM y LIF en el sistema de almacenamiento ONTAP

El siguiente paso se realiza en ONTAP System Manager.

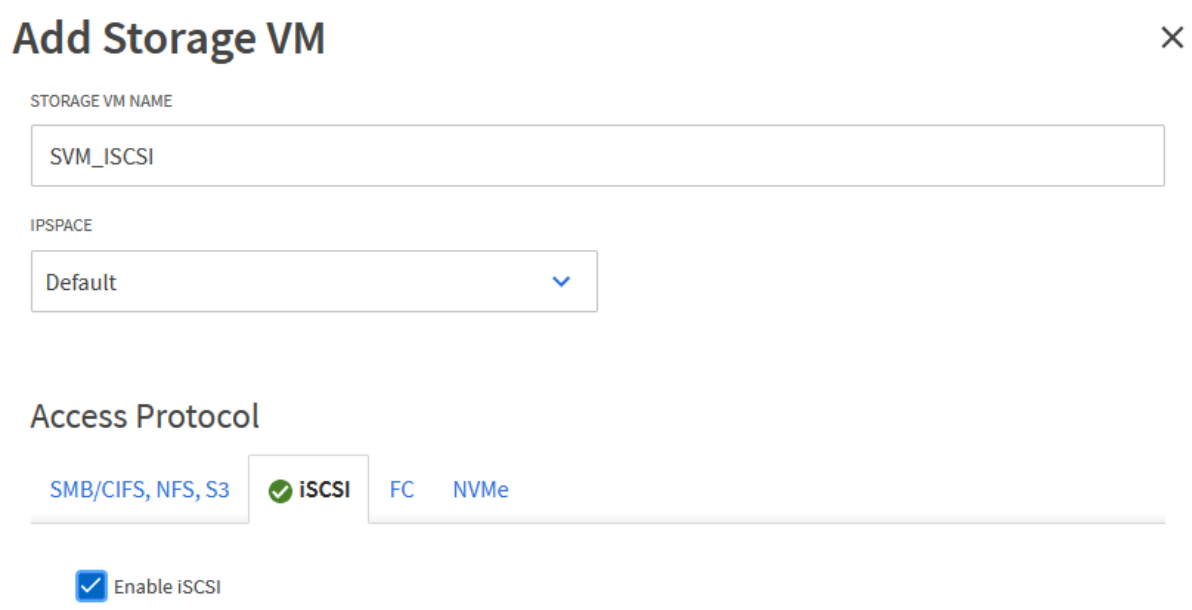
Cree la máquina virtual de almacenamiento y los LIF

Complete los siguientes pasos para crear una SVM junto con múltiples LIF para el tráfico iSCSI.

1. Desde el Administrador del sistema ONTAP , navegue hasta **Máquinas virtuales de almacenamiento** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.

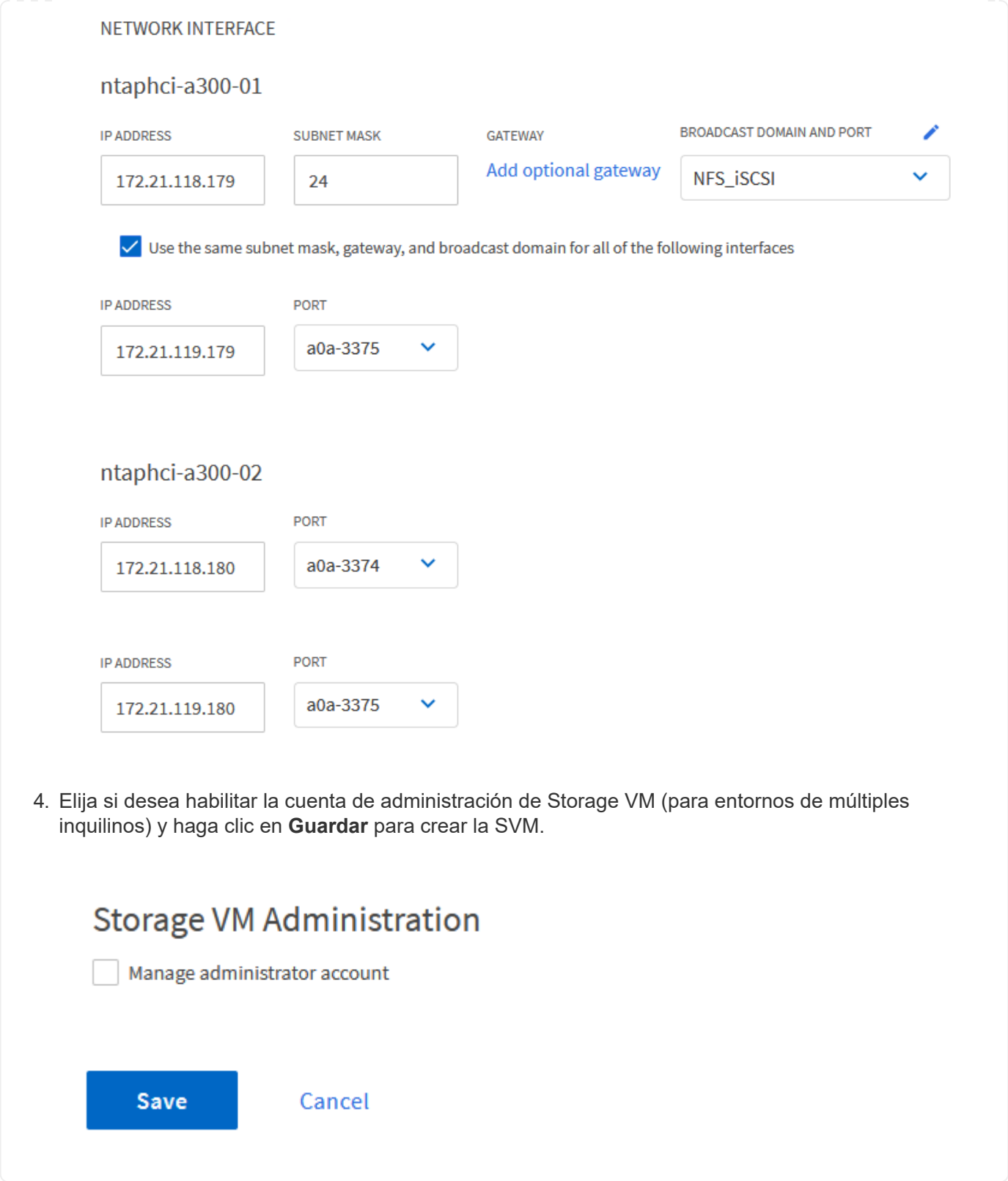


2. En el asistente **Agregar VM de almacenamiento**, proporcione un **Nombre** para la SVM, seleccione el **Espacio IP** y luego, en **Protocolo de acceso, haga clic en la pestaña *iSCSI** y marque la casilla para **Habilitar iSCSI**.



3. En la sección **Interfaz de red**, complete la **Dirección IP**, la **Máscara de subred** y el **Dominio de transmisión y puerto** para el primer LIF. Para los LIF posteriores, la casilla de verificación se puede habilitar para utilizar configuraciones comunes en todos los LIF restantes o utilizar configuraciones separadas.

> Para rutas múltiples y conmutación por error en múltiples rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet separadas para todas las SVM en configuraciones iSCSI.



4. Elija si desea habilitar la cuenta de administración de Storage VM (para entornos de múltiples inquilinos) y haga clic en **Guardar** para crear la SVM.

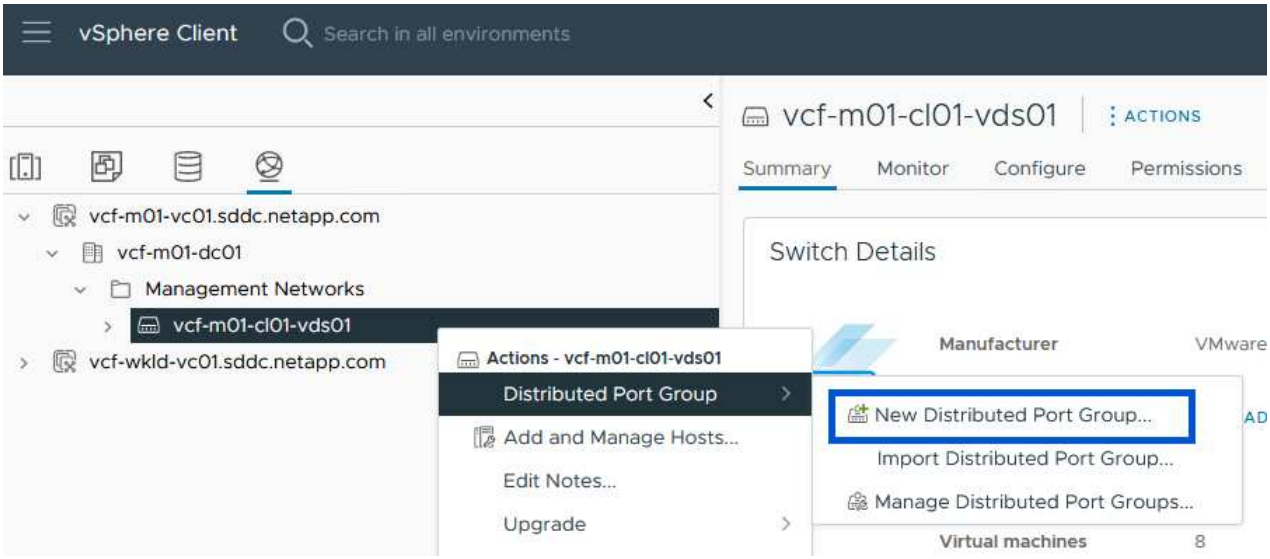
Configurar la red para iSCSI en hosts ESXi

Los siguientes pasos se realizan en el clúster de dominio de administración de VCF mediante el cliente vSphere.

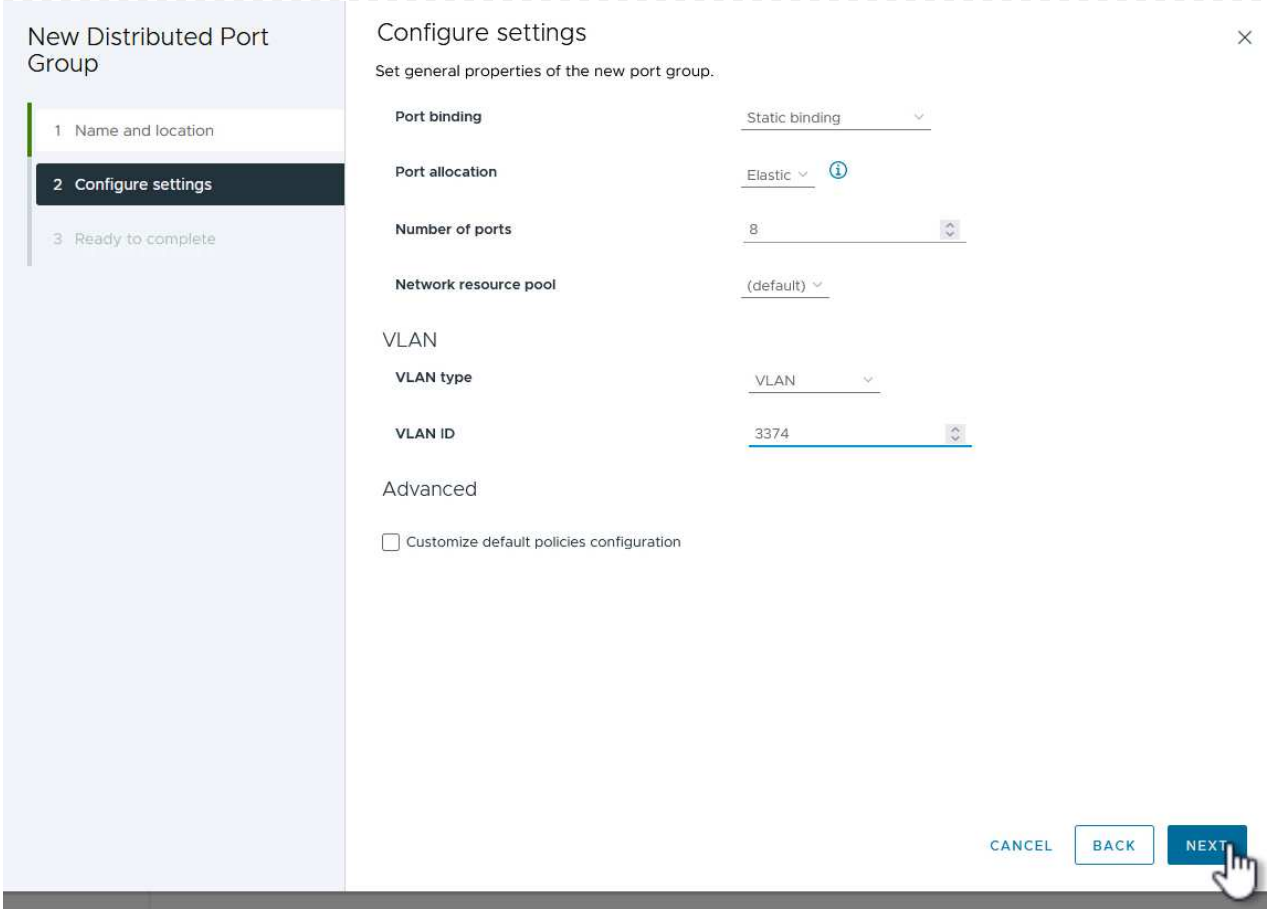
Crear grupos de puertos distribuidos para el tráfico iSCSI

Complete lo siguiente para crear un nuevo grupo de puertos distribuidos para cada red iSCSI:

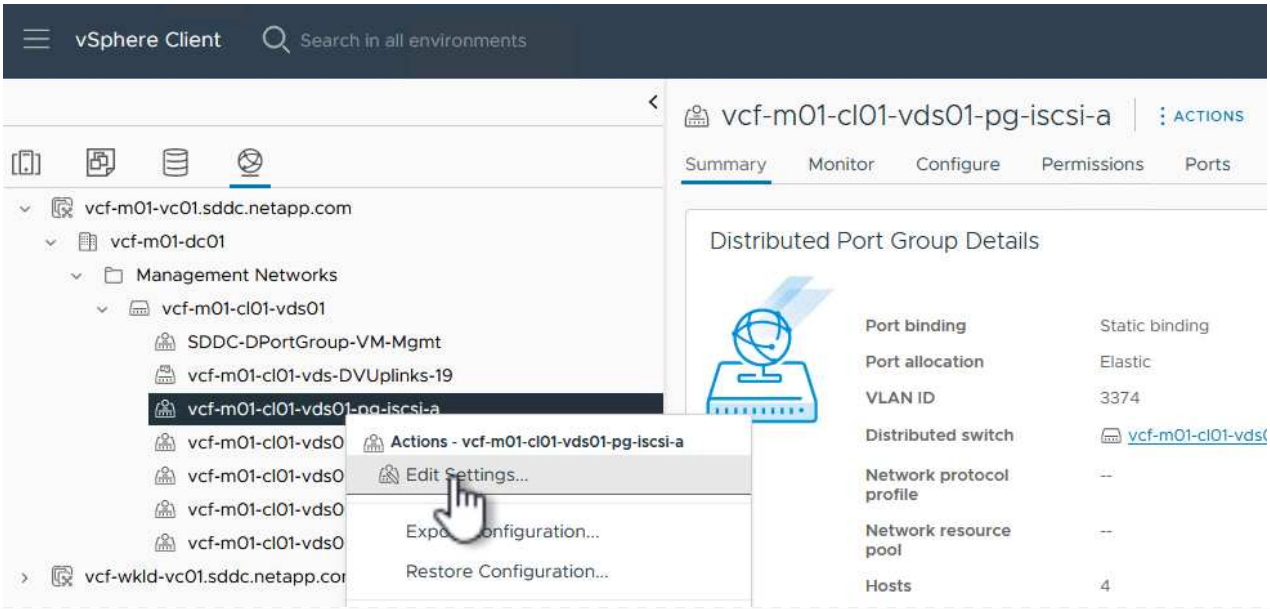
1. Desde el cliente vSphere del clúster del dominio de administración, navegue a **Inventario > Redes**. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos…**.



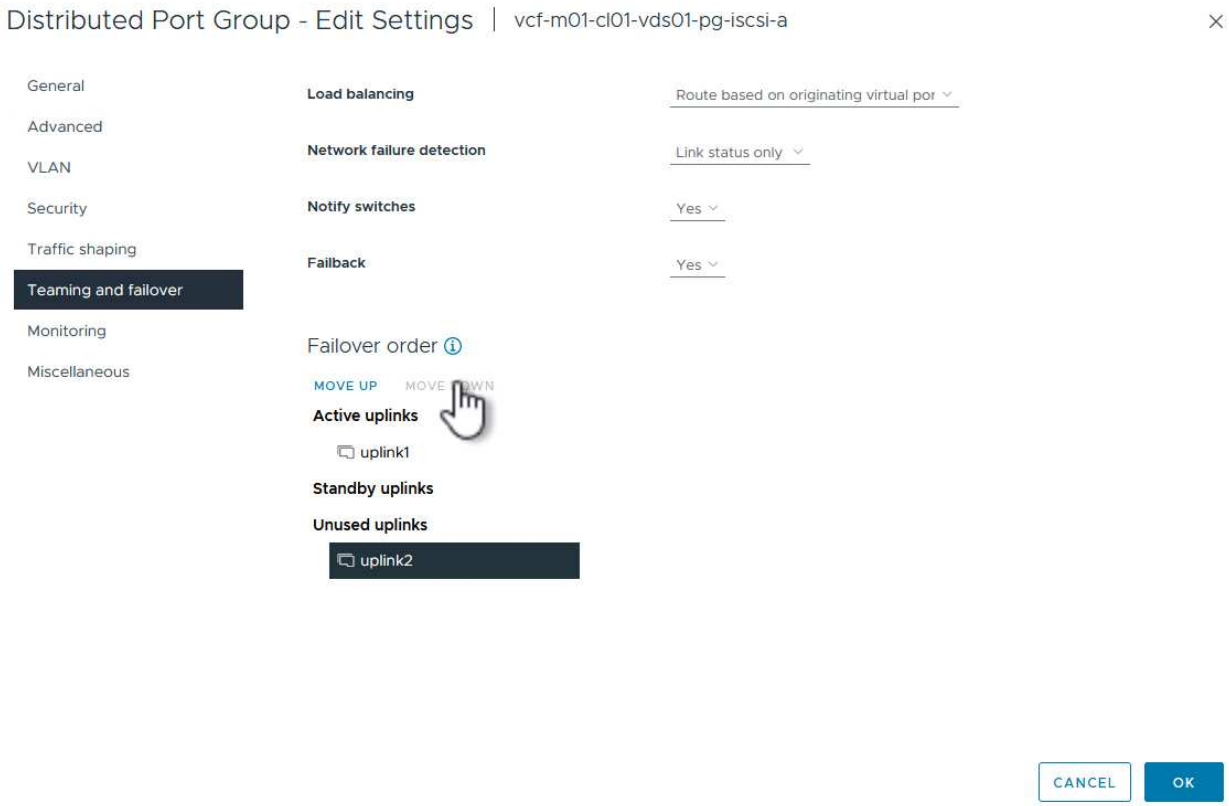
2. En el asistente **Nuevo grupo de puertos distribuidos**, complete un nombre para el nuevo grupo de puertos y haga clic en **Siguiente** para continuar.
3. En la página **Configurar ajustes** complete todas las configuraciones. Si se utilizan VLAN, asegúrese de proporcionar la ID de VLAN correcta. Haga clic en **Siguiente** para continuar.



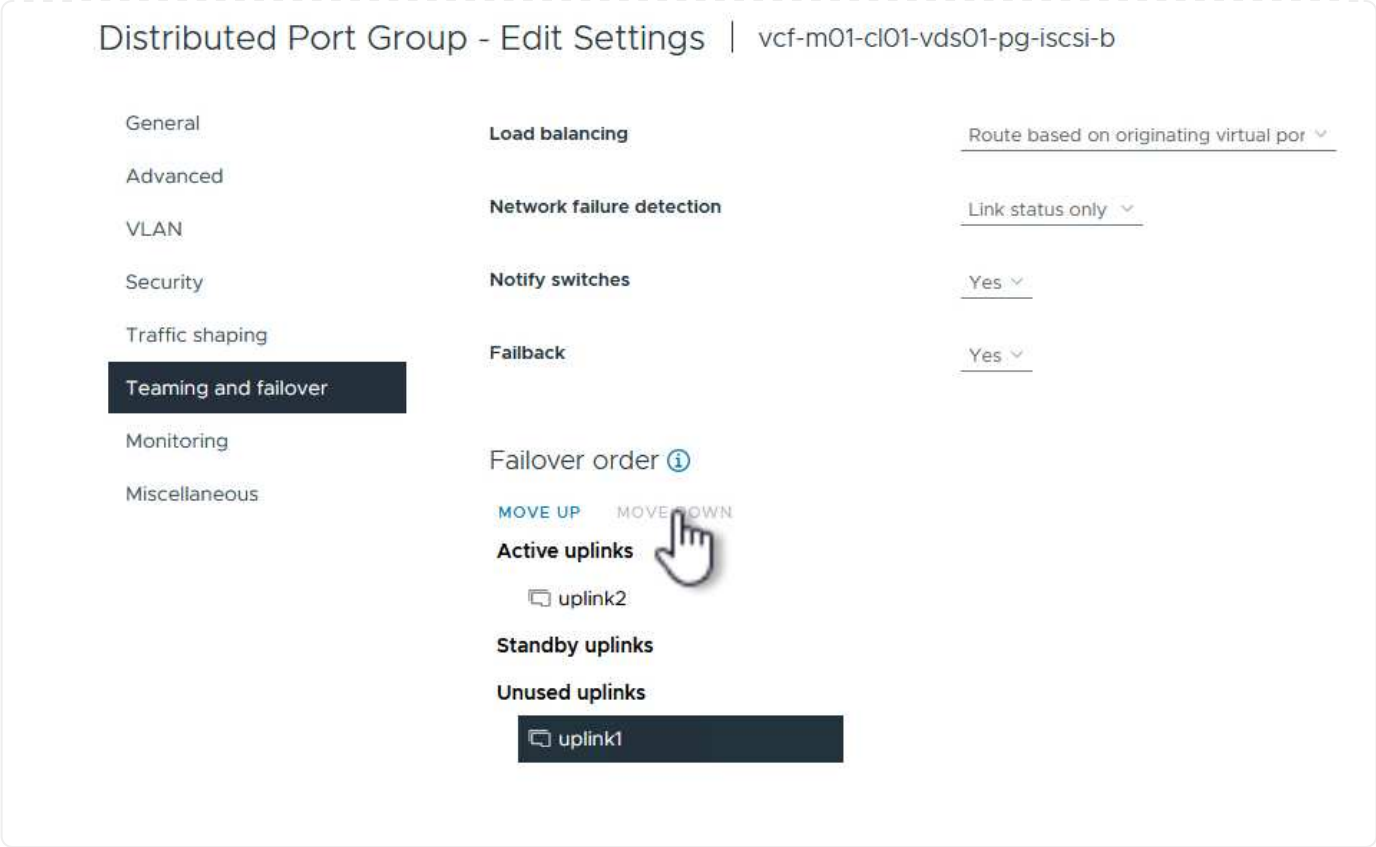
4. En la página **Listo para completar**, revise los cambios y haga clic en **Finalizar** para crear el nuevo grupo de puertos distribuidos.
5. Repita este proceso para crear un grupo de puertos distribuidos para la segunda red iSCSI que se esté utilizando y asegúrese de haber ingresado el **VLAN ID** correcto.
6. Una vez que se hayan creado ambos grupos de puertos, navegue hasta el primer grupo de puertos y seleccione la acción **Editar configuración…**.



7. En la página **Grupo de puertos distribuidos - Editar configuración**, navegue a **Equipo y conmutación por error** en el menú de la izquierda y haga clic en **uplink2** para moverlo hacia abajo a **Enlaces ascendentes no utilizados**.



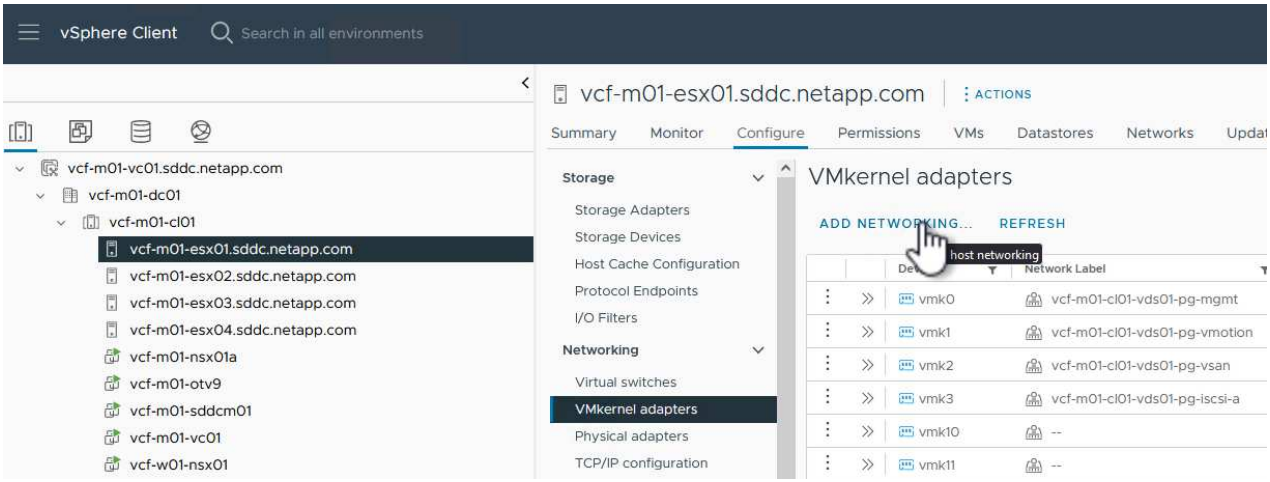
8. Repita este paso para el segundo grupo de puertos iSCSI. Sin embargo, esta vez mueva **uplink1** a **Unused uplinks**.


Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b
General
Advanced
VLAN
Security
Traffic shaping
Teaming and failover
Monitoring
Miscellaneous
Load balancing
Route based on originating virtual por
Network failure detection
Link status only
Notify switches
Yes
Failback
Yes
Failover order
MOVE UP
MOVE DOWN
Active uplinks
uplink2
Standby uplinks
Unused uplinks
uplink1

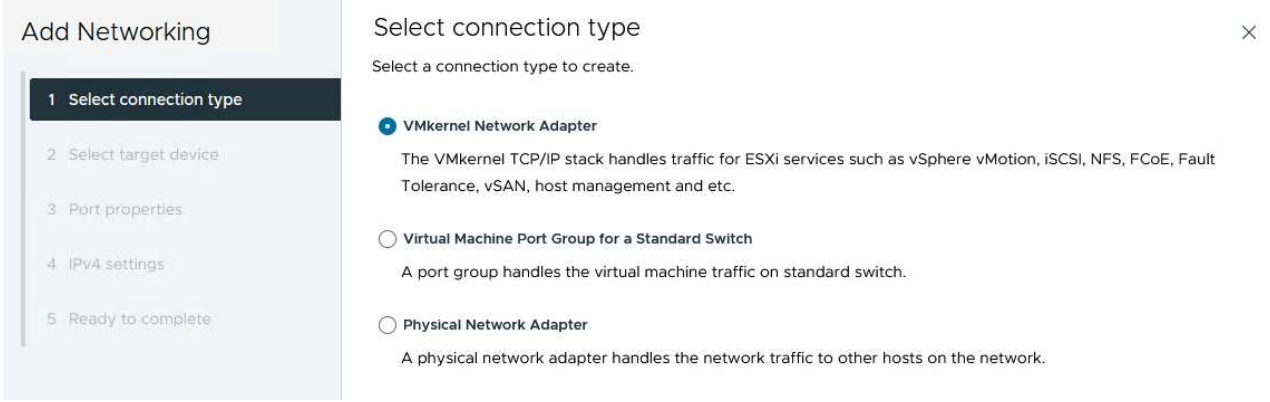
Cree adaptadores VMkernel en cada host ESXi

Repita este proceso en cada host ESXi en el dominio de administración.

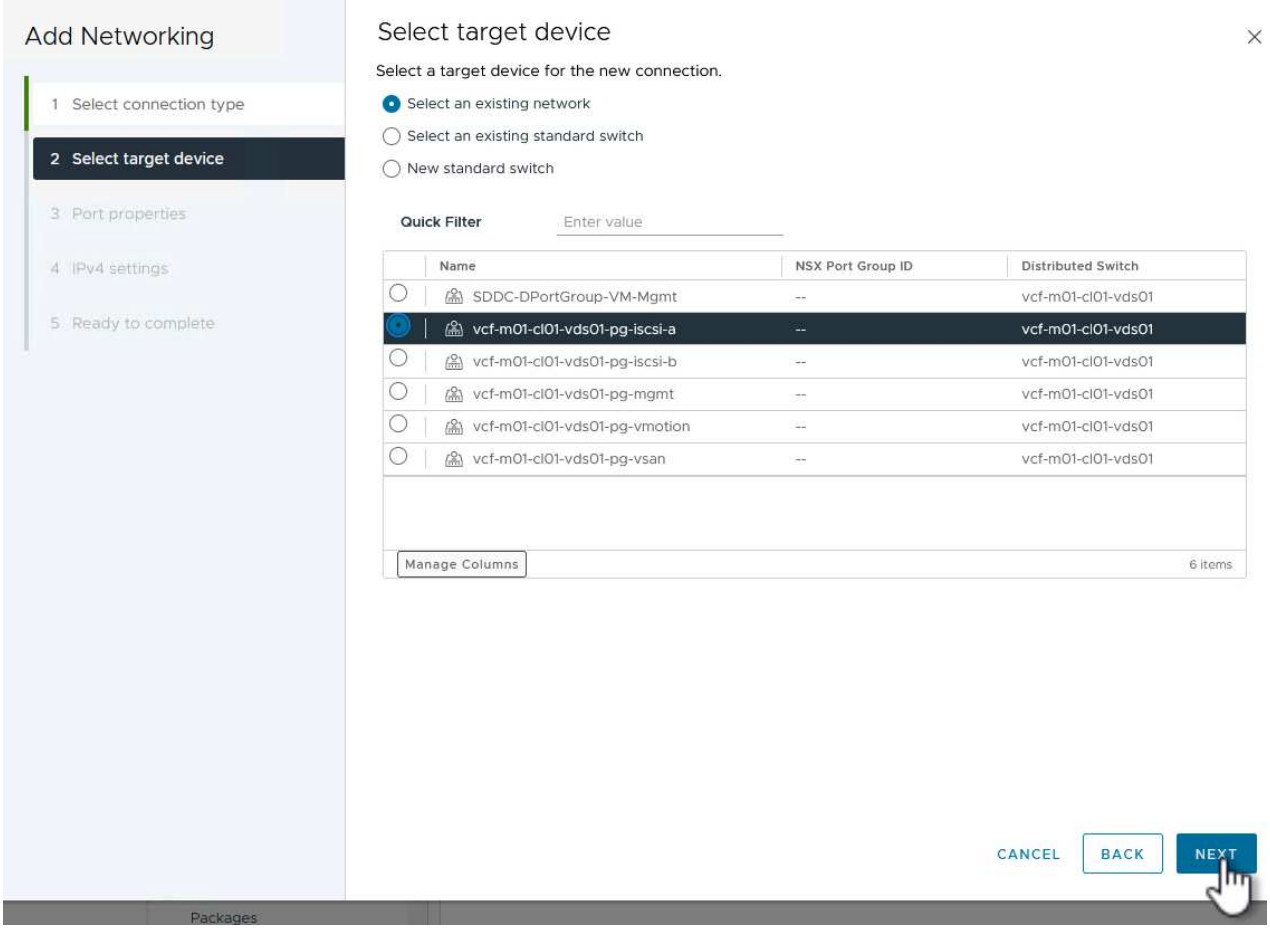
1. Desde el cliente vSphere, navegue a uno de los hosts ESXi en el inventario del dominio de administración. Desde la pestaña **Configurar** seleccione **Adaptadores VMkernel** y haga clic en **Agregar red…** para comenzar.



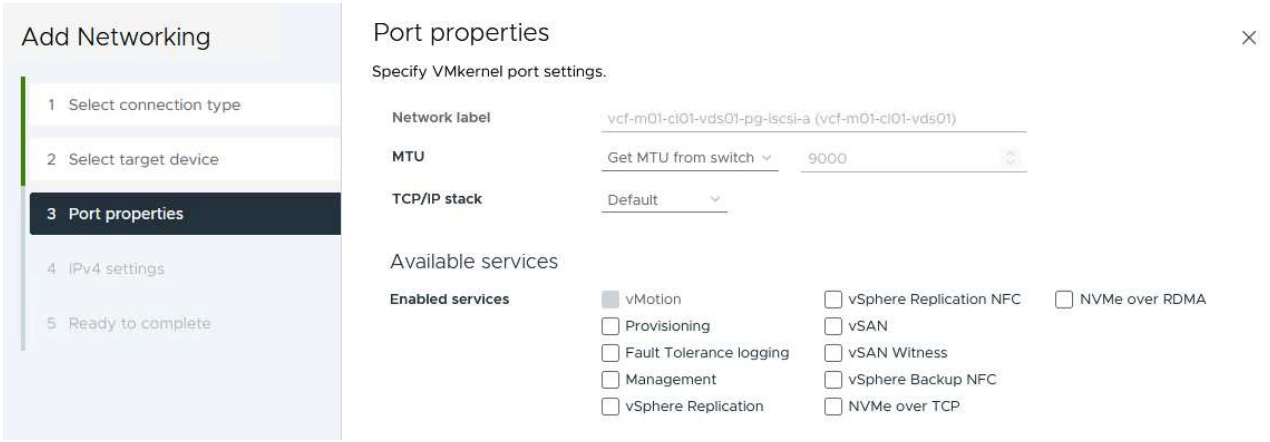
2. En la ventana **Seleccionar tipo de conexión** elija **Adaptador de red VMkernel** y haga clic en **Siguiente** para continuar.



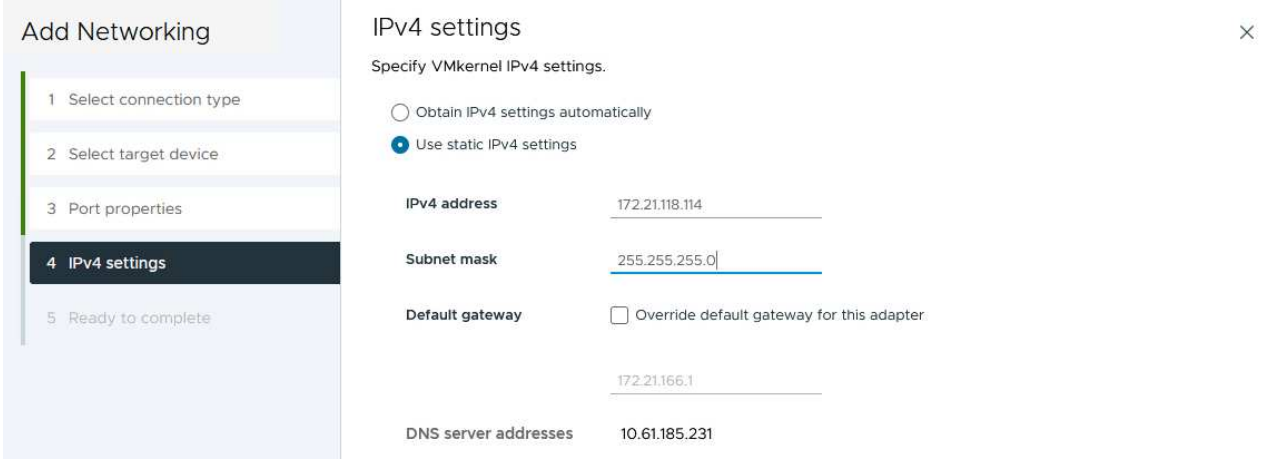
3. En la página **Seleccionar dispositivo de destino**, elija uno de los grupos de puertos distribuidos para iSCSI que se crearon anteriormente.



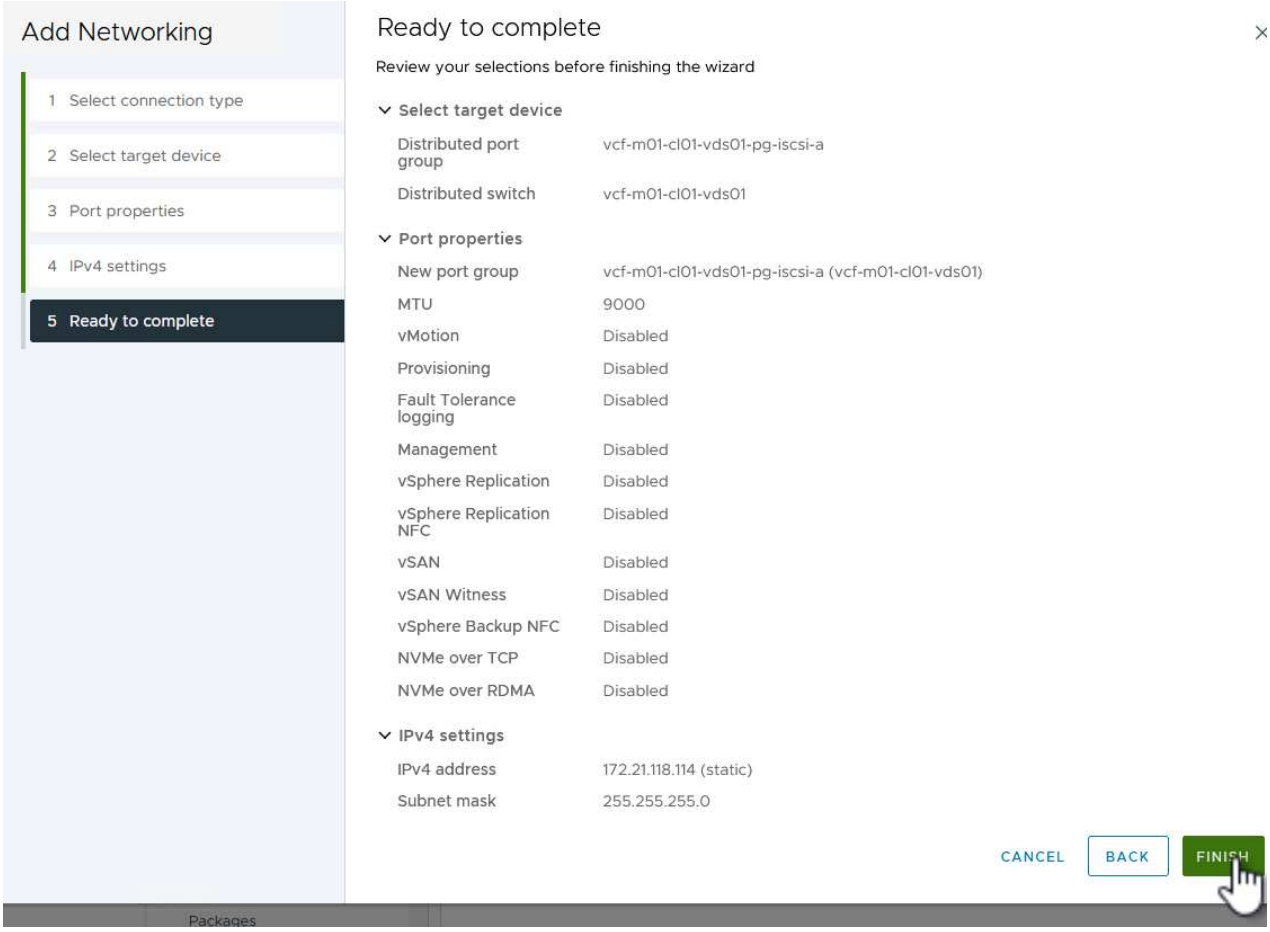
4. En la página **Propiedades del puerto** mantenga los valores predeterminados y haga clic en **Siguiente** para continuar.



5. En la página de **Configuración de IPv4**, complete la **dirección IP**, la **Máscara de subred** y proporcione una nueva dirección IP de puerta de enlace (solo si es necesario). Haga clic en **Siguiente** para continuar.



6. Revise sus selecciones en la página **Listo para completar** y haga clic en **Finalizar** para crear el adaptador VMkernel.



7. Repita este proceso para crear un adaptador VMkernel para la segunda red iSCSI.

Implementar y usar herramientas ONTAP para configurar el almacenamiento

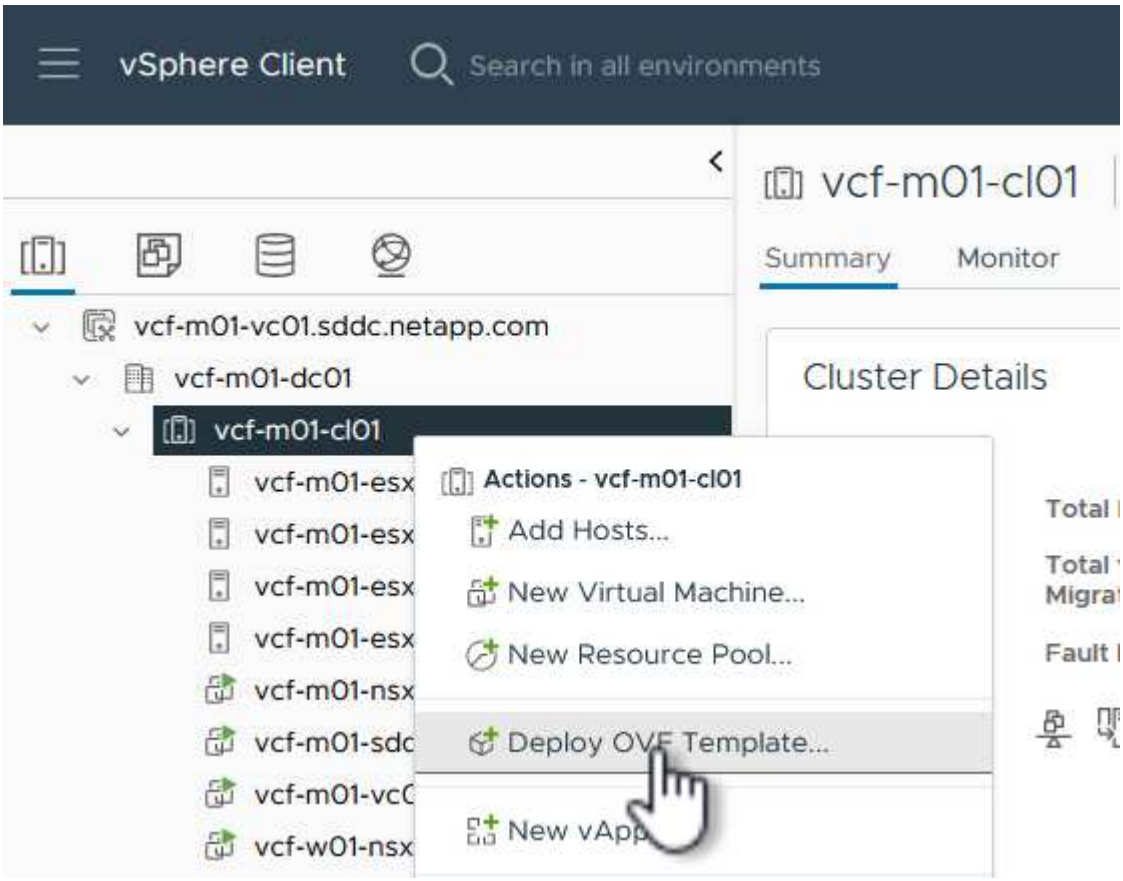
Los siguientes pasos se realizan en el clúster de dominio de administración de VCF mediante el cliente vSphere e implican la implementación de OTV, la creación de un almacén de datos iSCSI VMFS y la migración de las máquinas virtuales de administración al nuevo almacén de datos.

Implementar ONTAP tools for VMware vSphere

Las ONTAP tools for VMware vSphere (OTV) se implementan como un dispositivo de VM y proporcionan una interfaz de usuario vCenter integrada para administrar el almacenamiento de ONTAP .

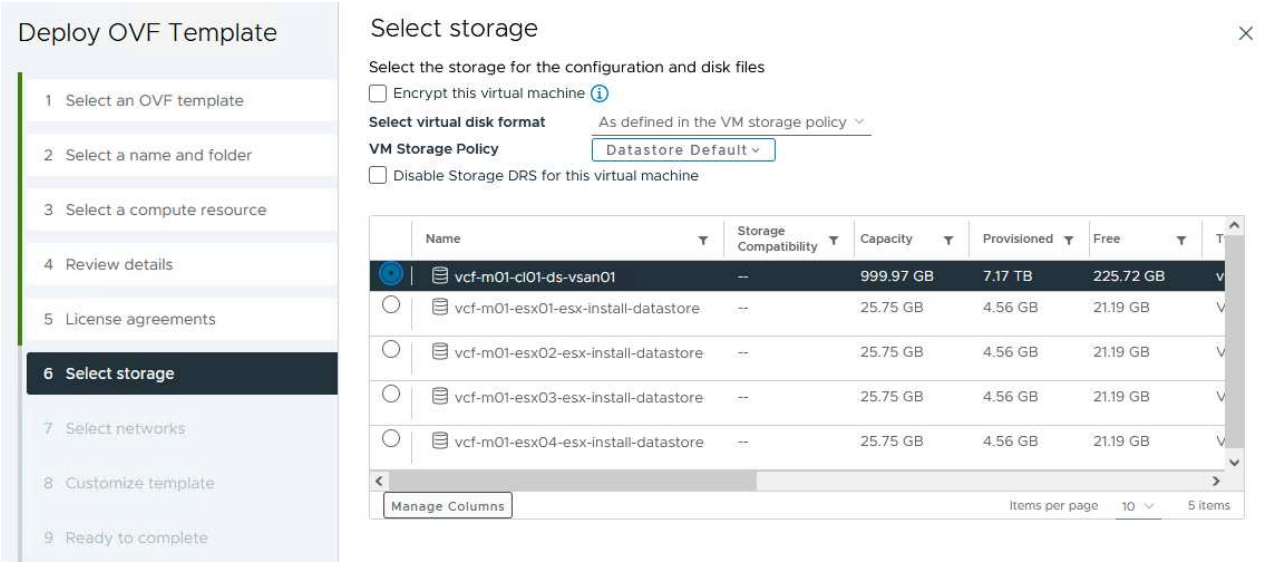
Complete lo siguiente para implementar ONTAP tools for VMware vSphere:

1. Obtenga la imagen OVA de las herramientas ONTAP desde"Sitio de soporte de NetApp" y descargar a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de administración de VCF.
3. Desde la interfaz del dispositivo vCenter, haga clic con el botón derecho en el clúster de administración y seleccione **Implementar plantilla OVF…**

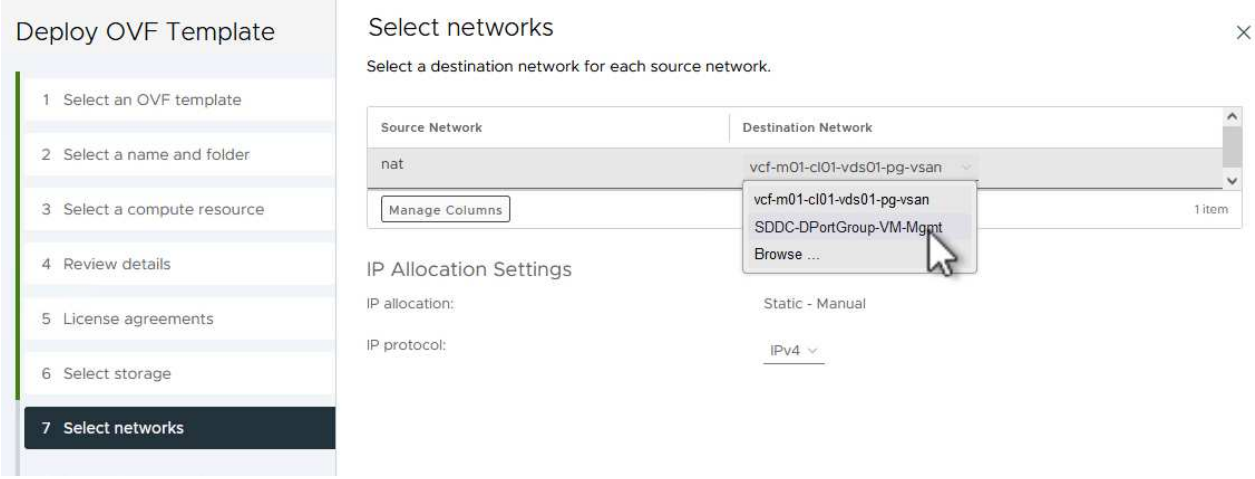


4. En el asistente **Implementar plantilla OVF**, haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de las herramientas ONTAP descargado en el paso anterior.

5. Para los pasos 2 a 5 del asistente, seleccione un nombre y una carpeta para la máquina virtual, seleccione el recurso computacional, revise los detalles y acepte el acuerdo de licencia.
6. Para la ubicación de almacenamiento de los archivos de configuración y de disco, seleccione el almacén de datos vSAN del clúster de dominio de administración de VCF.

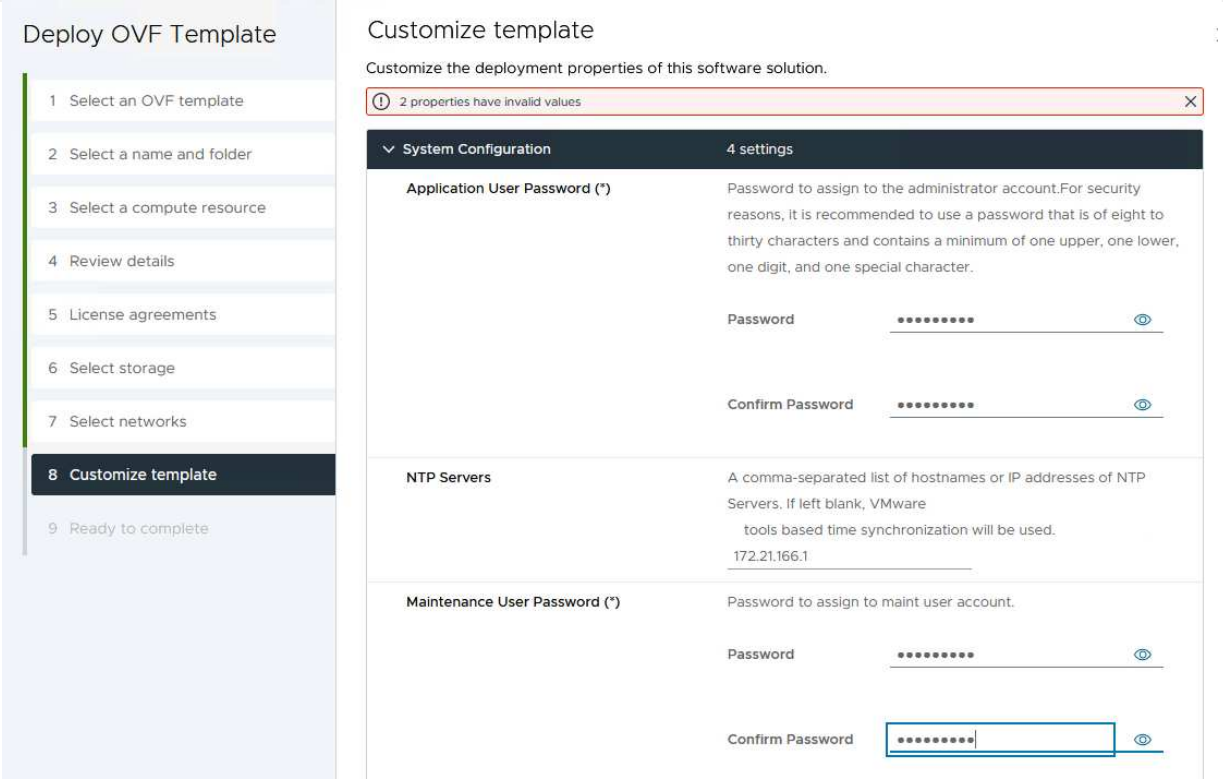


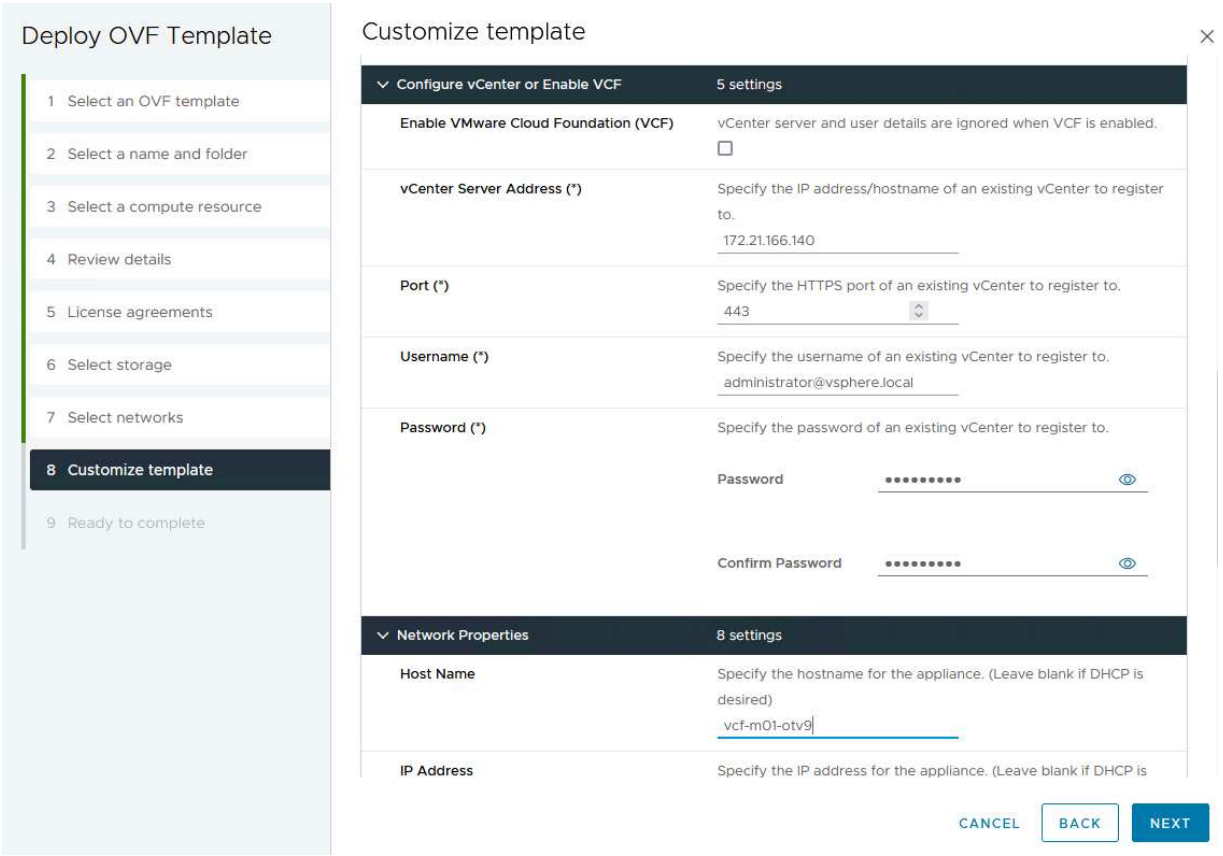
7. En la página Seleccionar red, seleccione la red utilizada para administrar el tráfico.



8. En la página Personalizar plantilla, complete toda la información requerida:
   - Contraseña que se utilizará para el acceso administrativo a OTV.
   - Dirección IP del servidor NTP.
   - Contraseña de la cuenta de mantenimiento de OTV.
   - Contraseña de OTV Derby DB.
   - No marque la casilla para **Habilitar VMware Cloud Foundation (VCF)**. El modo VCF no es necesario para implementar almacenamiento complementario.
   - FQDN o dirección IP del dispositivo vCenter y proporcione credenciales para vCenter.
   - Proporcione los campos de propiedades de red requeridos.

     Haga clic en **Siguiente** para continuar.



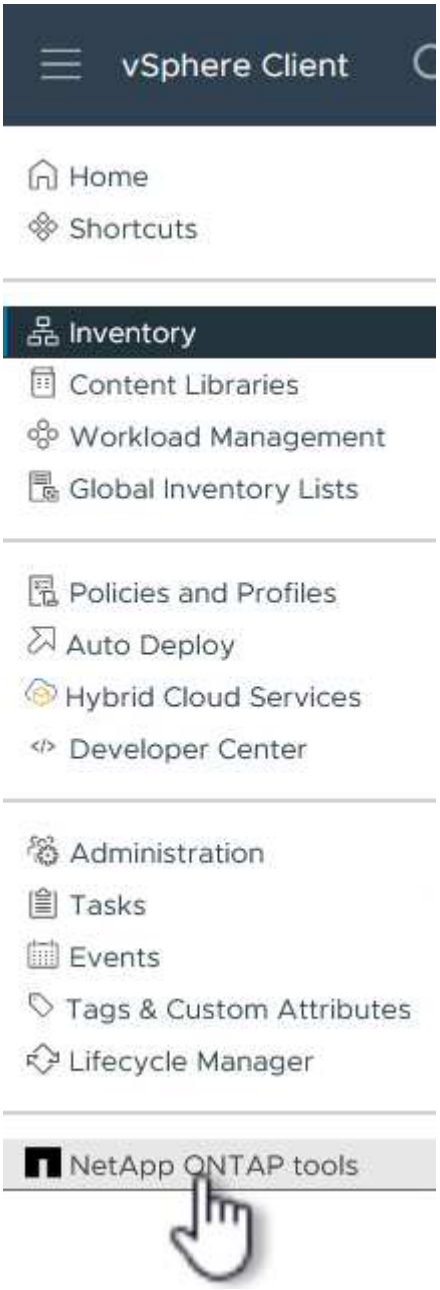


9. Revise toda la información en la página Listo para completar y haga clic en Finalizar para comenzar a implementar el dispositivo OTV.

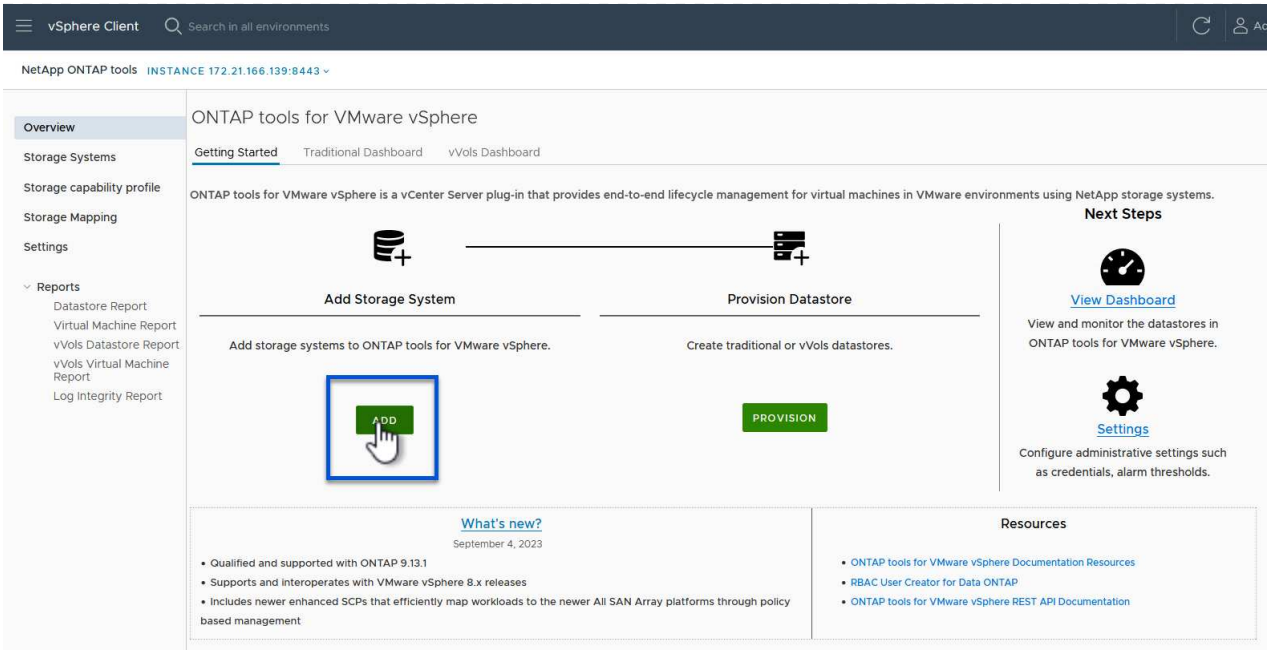
Configurar un almacén de datos iSCSI VMFS en el dominio de administración mediante OTV

Complete lo siguiente para usar OTV para configurar un almacén de datos iSCSI VMFS como almacenamiento complementario en el dominio de administración:

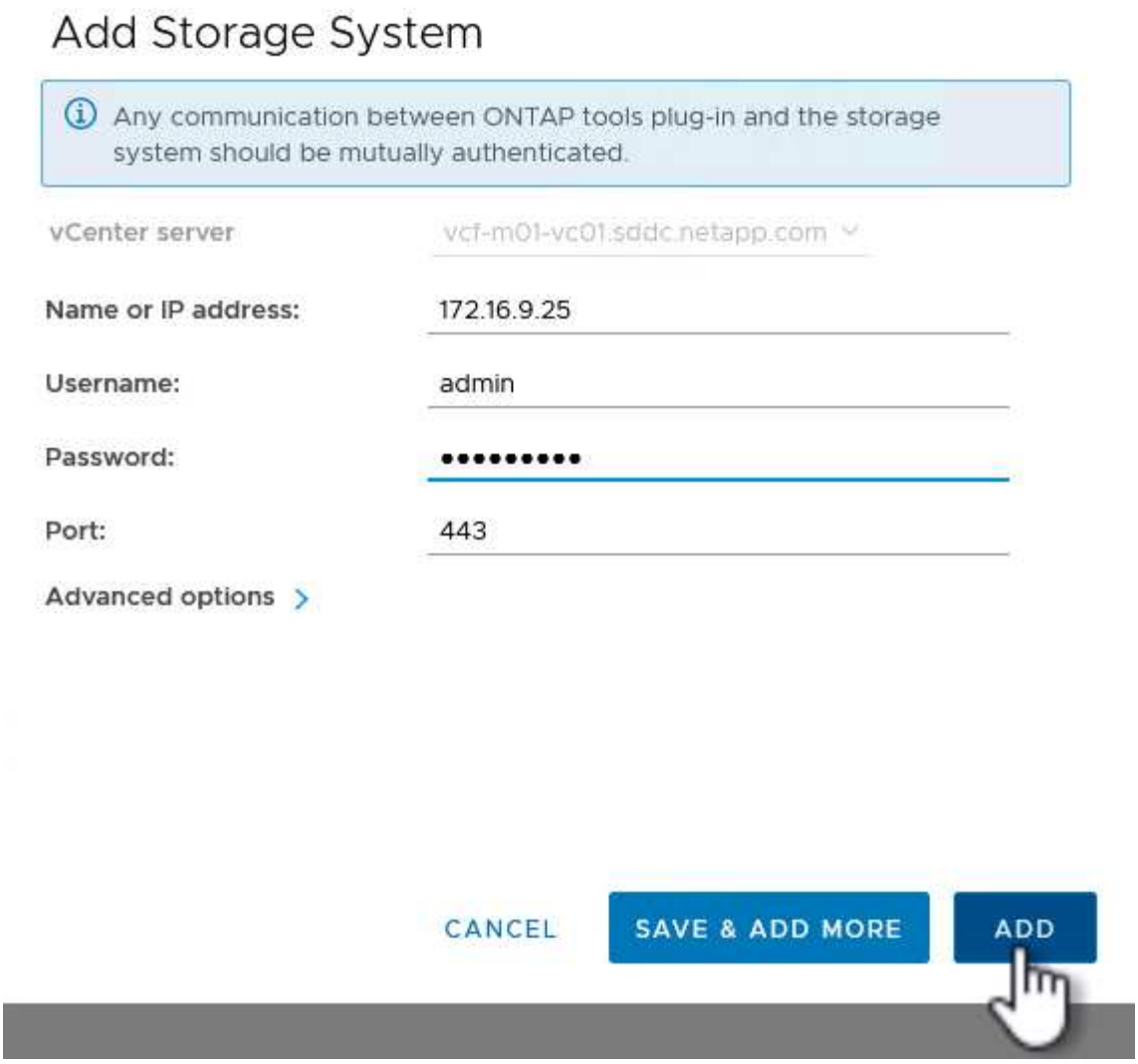
1. En el cliente vSphere, navegue al menú principal y seleccione *Herramientas de NetApp ONTAP *.



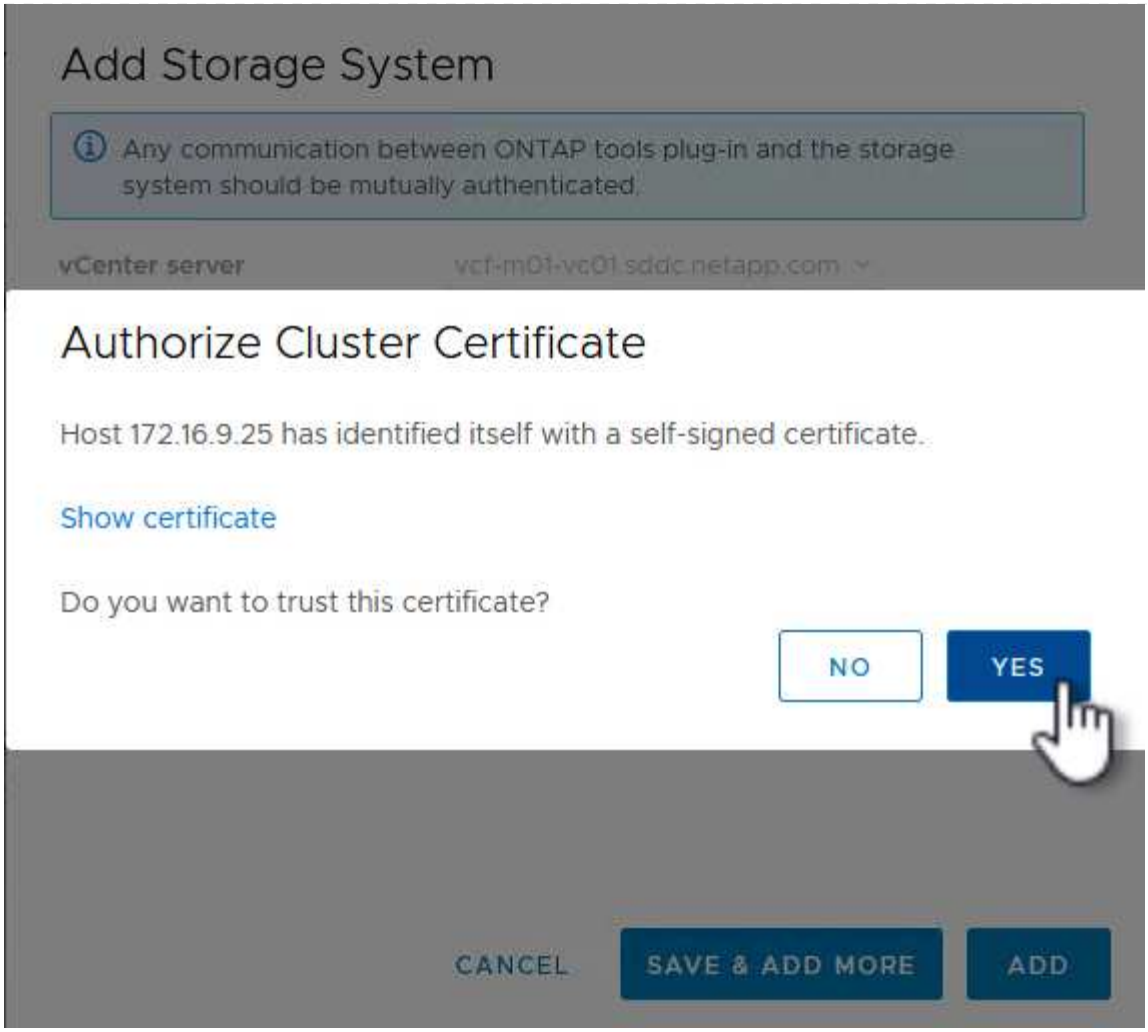
2. Una vez en * ONTAP Tools*, desde la página de Primeros pasos (o desde **Sistemas de almacenamiento**), haga clic en **Agregar** para agregar un nuevo sistema de almacenamiento.



3. Proporcione la dirección IP y las credenciales del sistema de almacenamiento ONTAP y haga clic en **Agregar**.



4. Haga clic en **Sí** para autorizar el certificado del clúster y agregar el sistema de almacenamiento.

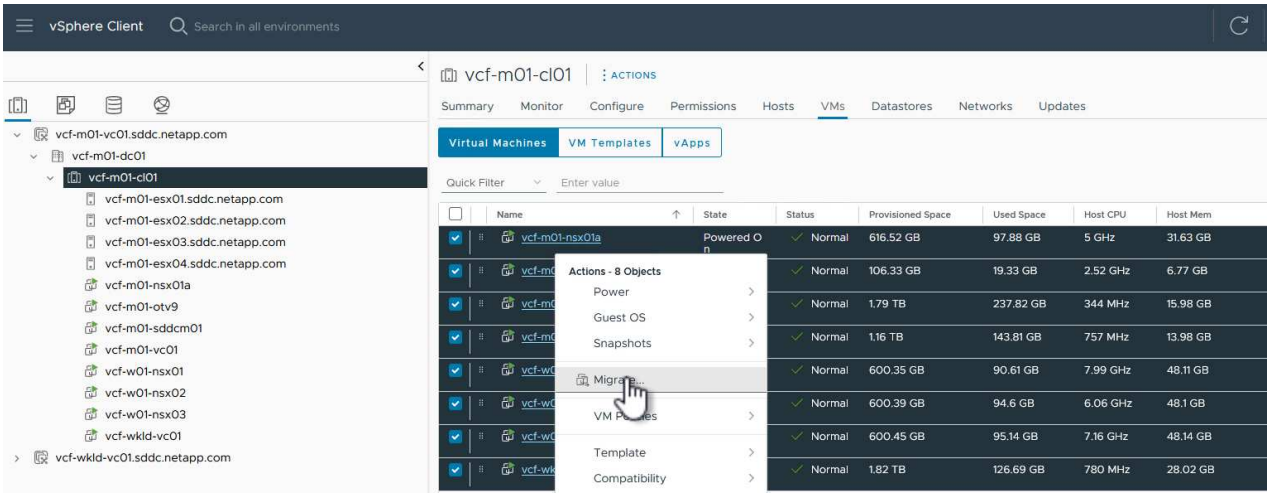

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Authorize Cluster Certificate
Host 172.16.9.25 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
SAVE & ADD MORE
ADD

Migrar máquinas virtuales de administración a un almacén de datos iSCSI

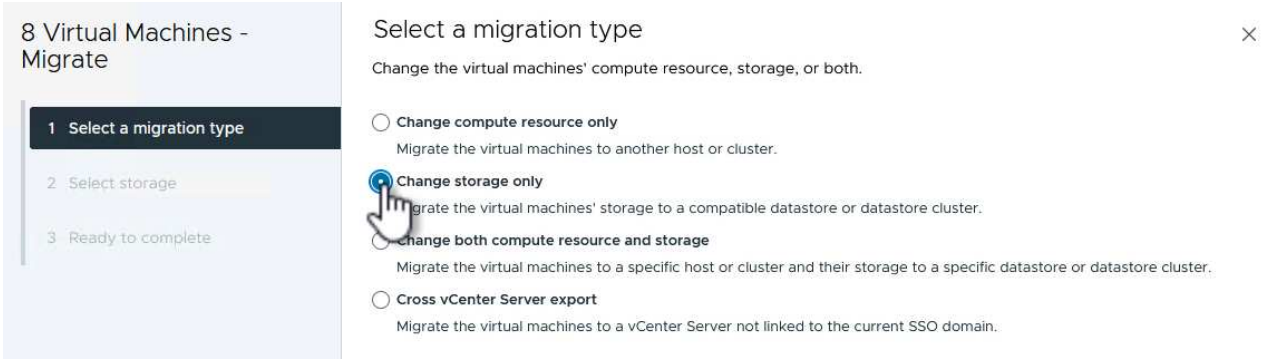
En los casos en los que se prefiere utilizar el almacenamiento ONTAP para proteger las máquinas virtuales administradas por VCF, se puede utilizar vMotion para migrar las máquinas virtuales al almacén de datos iSCSI recién creado.

Complete los siguientes pasos para migrar las máquinas virtuales de administración de VCF al almacén de datos iSCSI.

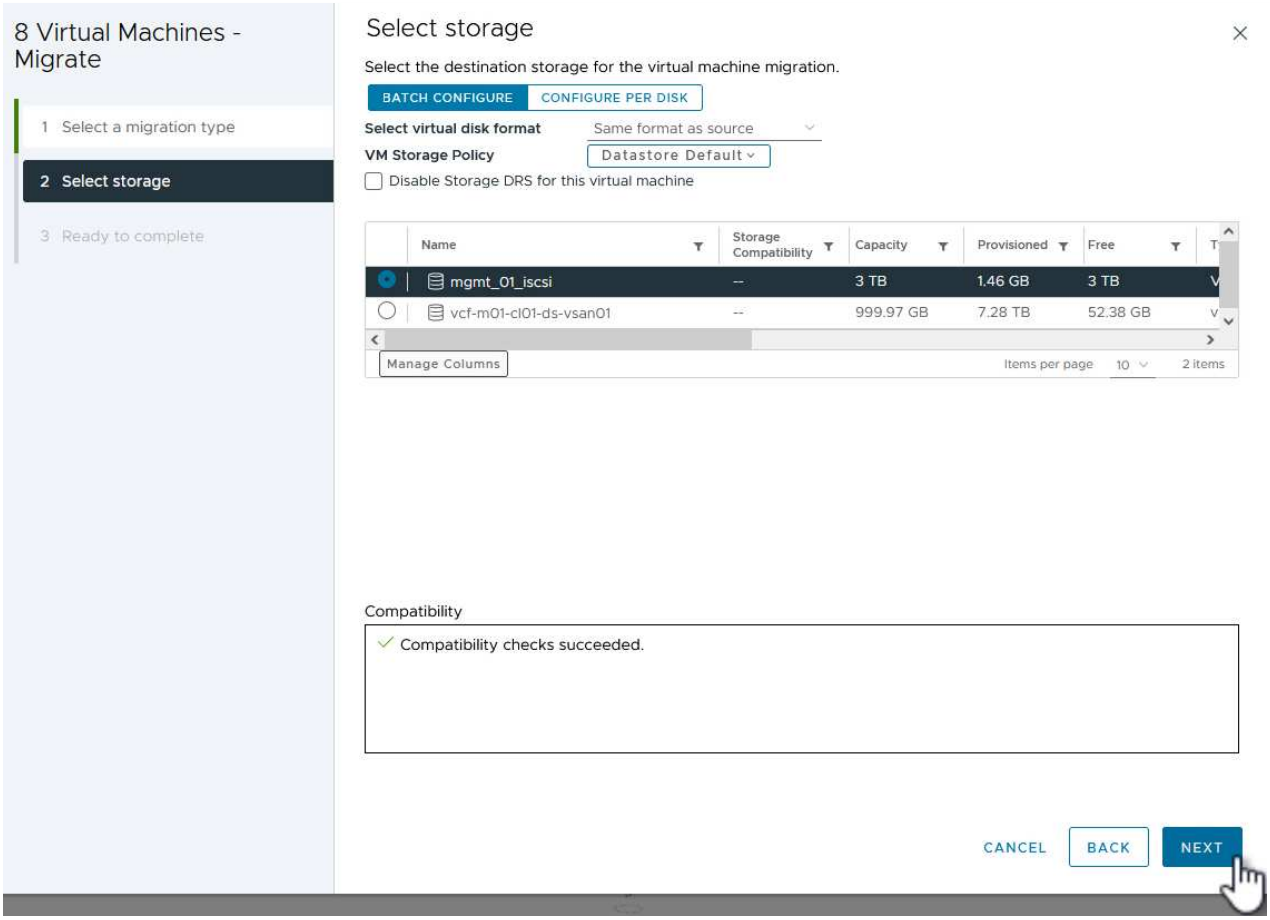
1. Desde vSphere Client, navegue hasta el clúster del dominio de administración y haga clic en la pestaña **VMs**.
2. Seleccione las máquinas virtuales que se migrarán al almacén de datos iSCSI, haga clic con el botón derecho y seleccione **Migrar…**.



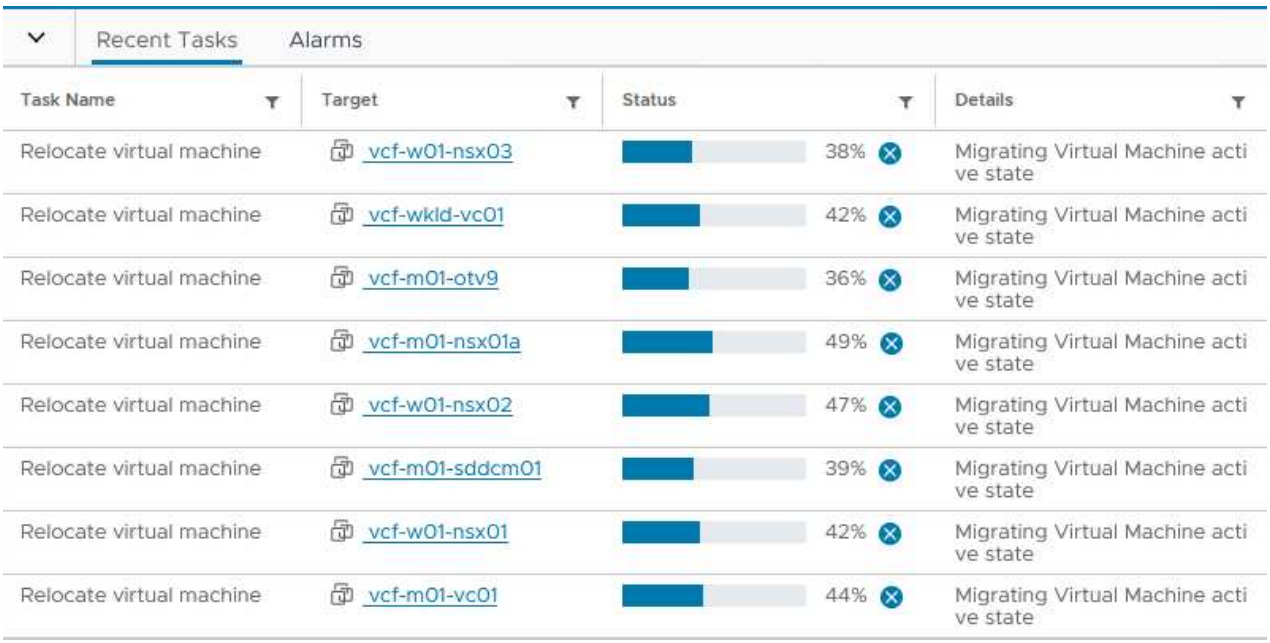
3. En el asistente **Máquinas virtuales - Migrar**, seleccione **Cambiar solo almacenamiento** como tipo de migración y haga clic en **Siguiente** para continuar.



4. En la página **Seleccionar almacenamiento**, seleccione el almacén de datos iSCSi y seleccione **Siguiente** para continuar.



5. Revise las selecciones y haga clic en **Finalizar** para iniciar la migración.
6. El estado de la reubicación se puede ver desde el panel **Tareas recientes**.



Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Demostración en vídeo de esta solución

Almacenes de datos iSCSI como almacenamiento complementario para dominios de administración de VCF

Agregue un almacén de datos VMFS basado en FC como almacenamiento complementario para un dominio de administración mediante ONTAP tools for VMware vSphere

En este caso de uso, describimos el procedimiento para utilizar ONTAP Tools for VMware para configurar un almacén de datos VMFS mediante Fibre Channel (FC) como almacenamiento complementario para el dominio de administración de VMware Cloud Foundation (VCF). Este procedimiento resume la implementación de ONTAP Tools para VMware vSphere, el registro de servidores vCenter, la definición del backend de almacenamiento y el aprovisionamiento del almacén de datos FC.

Beneficios del canal de fibra

Alto rendimiento: FC proporciona velocidades de transferencia de datos de alta velocidad, lo que lo hace ideal para aplicaciones que requieren acceso rápido y confiable a grandes cantidades de datos.

Baja latencia: Latencia muy baja, lo cual es crucial para aplicaciones sensibles al rendimiento, como bases de datos y entornos virtualizados.

Confiabilidad: Las redes FC son conocidas por su robustez y confiabilidad, con características como redundancia incorporada y corrección de errores.

Ancho de banda dedicado: FC proporciona ancho de banda dedicado para el tráfico de almacenamiento, lo que reduce el riesgo de congestión de la red.

Para obtener más información sobre el uso de Fibre Channel con sistemas de almacenamiento NetApp , consulte "Aprovisionamiento de SAN con FC" .

Descripción general del escenario

El almacén de datos complementario VCF se aprovisiona como parte de las operaciones del día 2 mediante vCenter. Este escenario cubre los siguientes pasos de alto nivel:

- Implementación de herramientas ONTAP en el dominio de gestión
- Registrar servidores vCenter de carga de trabajo VI en las herramientas ONTAP
- Definir el backend de almacenamiento en el complemento de herramientas ONTAP para VMware vSphere
- Aprovisionar VMFS en el transporte FC

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP con puertos FC conectados a conmutadores FC.
- SVM creado con FC lifs.
- vSphere con HBA FC conectados a conmutadores FC.
- La zonificación de iniciador-destino único está configurada en los conmutadores FC.

> Utilice la interfaz lógica SVM FC en la configuración de zona en lugar de puertos FC físicos en los sistemas ONTAP .

NetApp recomienda múltiples rutas para LUN FC.

Para obtener información completa sobre la configuración del canal de fibra en los sistemas de almacenamiento ONTAP , consulte "Gestión de almacenamiento SAN" en la documentación de ONTAP 9.

Para obtener más información sobre el uso de VMFS con sistemas de almacenamiento ONTAP , consulte la"Guía de implementación para VMFS" .

Pasos de implementación para el dominio de administración

Para implementar ONTAP Tools y usarlo para crear un almacén de datos VMFS en el dominio de administración de VCF, complete los siguientes pasos:

- "Implementar herramientas ONTAP en el dominio de administración"
- "Definir el backend de almacenamiento mediante la interfaz del cliente vSphere"
- "Aprovisionar VMFS en FC"

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Demostración en vídeo de esta solución

Almacén de datos VMFS(FC) como almacenamiento complementario para el dominio de administración de VCF

Agregue vVols como almacenamiento complementario a los dominios de carga de trabajo VI mediante ONTAP tools for VMware vSphere

En este caso de uso, describimos el procedimiento para configurar un almacén de datos vVols con iSCSI para almacenamiento complementario en un dominio de carga de trabajo de infraestructura virtual (VI) de VMware Cloud Foundation (VCF). Este procedimiento resume la configuración de la red iSCSI, la implementación de ONTAP Tools para VMware vSphere y el aprovisionamiento del almacén de datos vVols .

iSCSI se utiliza como protocolo de almacenamiento para el almacén de datos vVols .

Beneficios de iSCSI

Alto rendimiento: Ofrece un alto rendimiento para brindar velocidades de transferencia de datos rápidas y eficientes y baja latencia. Ideal para aplicaciones empresariales exigentes y entornos virtualizados.

Facilidad de administración: Simplifica la gestión del almacenamiento mediante el uso de herramientas y protocolos familiares basados en IP.

Rentable: Utiliza la infraestructura Ethernet existente, lo que reduce la necesidad de hardware especializado y permite a las organizaciones lograr soluciones de almacenamiento confiables y escalables.

Para obtener más información sobre el uso de iSCSI con sistemas de almacenamiento NetApp , consulte "Aprovisionamiento de SAN con iSCSI" .

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

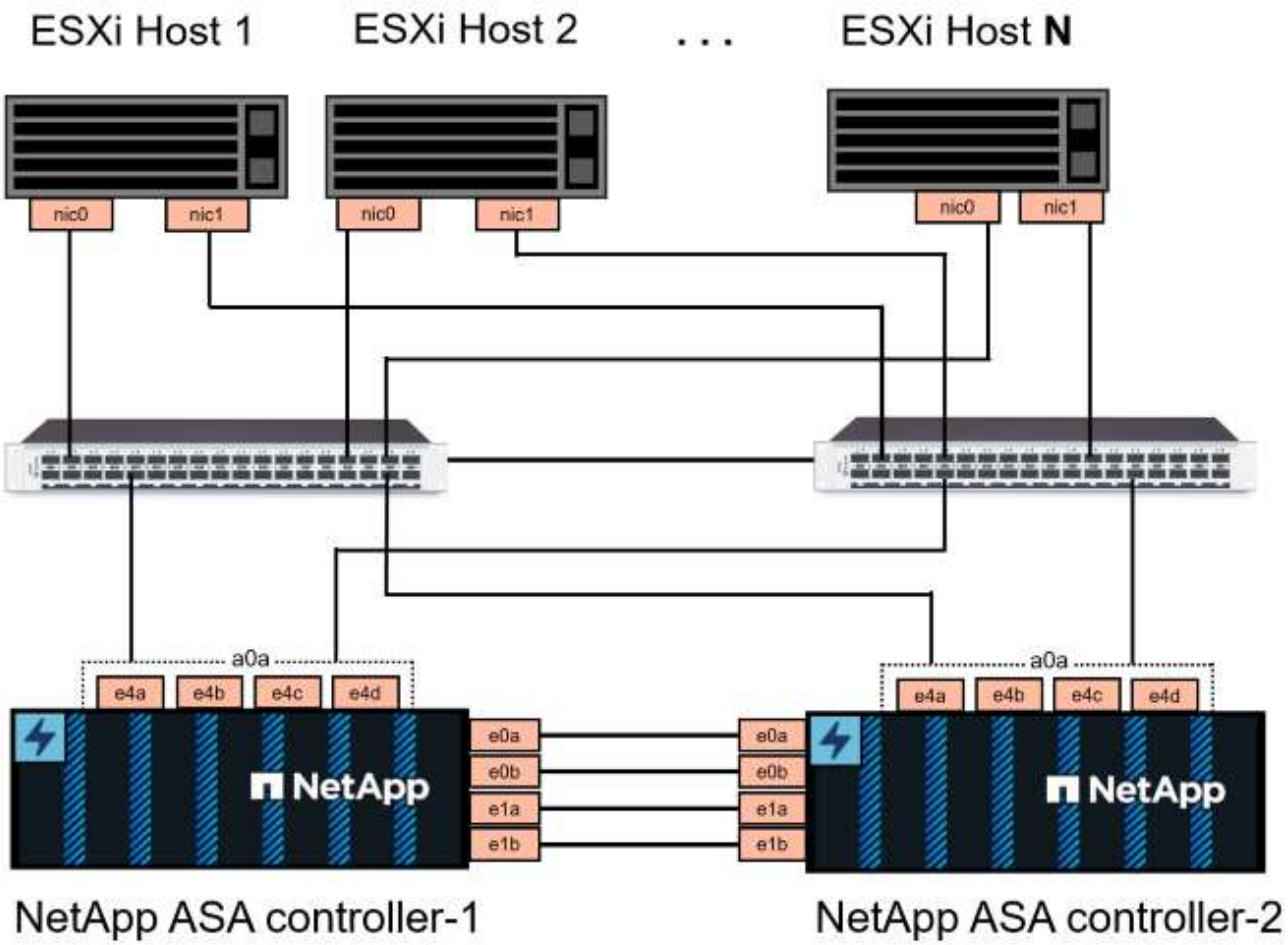
- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico iSCSI.
- Cree grupos de puertos distribuidos para redes iSCSI en el dominio de carga de trabajo VI.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de carga de trabajo VI.
- Implementar herramientas ONTAP en el dominio de carga de trabajo VI.
- Cree un nuevo almacén de datos vVols en el dominio de carga de trabajo VI.

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP AFF o ASA con puertos de datos físicos en conmutadores Ethernet dedicados al tráfico de almacenamiento.
- La implementación del dominio de administración de VCF está completa y el cliente vSphere es accesible.
- Previamente se ha implementado un dominio de carga de trabajo VI.

NetApp recomienda diseños de red totalmente redundantes para iSCSI. El siguiente diagrama ilustra un ejemplo de una configuración redundante, que proporciona tolerancia a fallas para sistemas de almacenamiento, conmutadores, adaptadores de red y sistemas host. Consulte NetApp"Referencia de configuración de SAN" Para obtener información adicional.



Para rutas múltiples y conmutación por error en múltiples rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet separadas para todas las SVM en configuraciones iSCSI.

Esta documentación demuestra el proceso de creación de una nueva SVM y la especificación de la información de la dirección IP para crear múltiples LIF para el tráfico iSCSI. Para agregar nuevos LIF a un SVM existente, consulte"Crear una LIF (interfaz de red)" .

> En situaciones donde se configuran varios adaptadores VMkernel en la misma red IP, se recomienda utilizar la vinculación de puertos iSCSI de software en los hosts ESXi para garantizar que se produzca un equilibrio de carga entre los adaptadores. Consulte el artículo de Knowledge Base"Consideraciones para el uso de la vinculación de puertos iSCSI de software en ESX/ESXi (2038869)" .

Para obtener información adicional sobre el uso de almacenes de datos iSCSI VMFS con VMware, consulte"vSphere VMFS Datastore: backend de almacenamiento iSCSI con ONTAP" .

Pasos de implementación

Para implementar ONTAP Tools y usarlo para crear un almacén de datos vVols en el dominio de administración de VCF, complete los siguientes pasos:

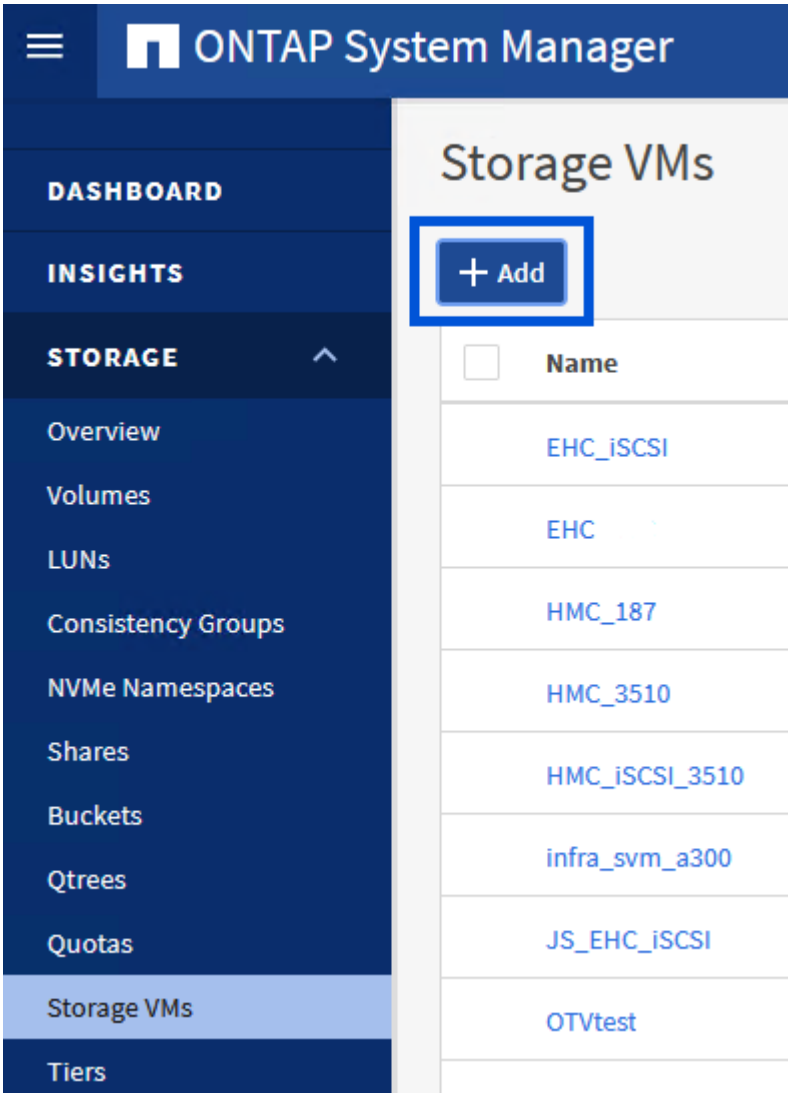
Crear SVM y LIF en el sistema de almacenamiento ONTAP

El siguiente paso se realiza en ONTAP System Manager.

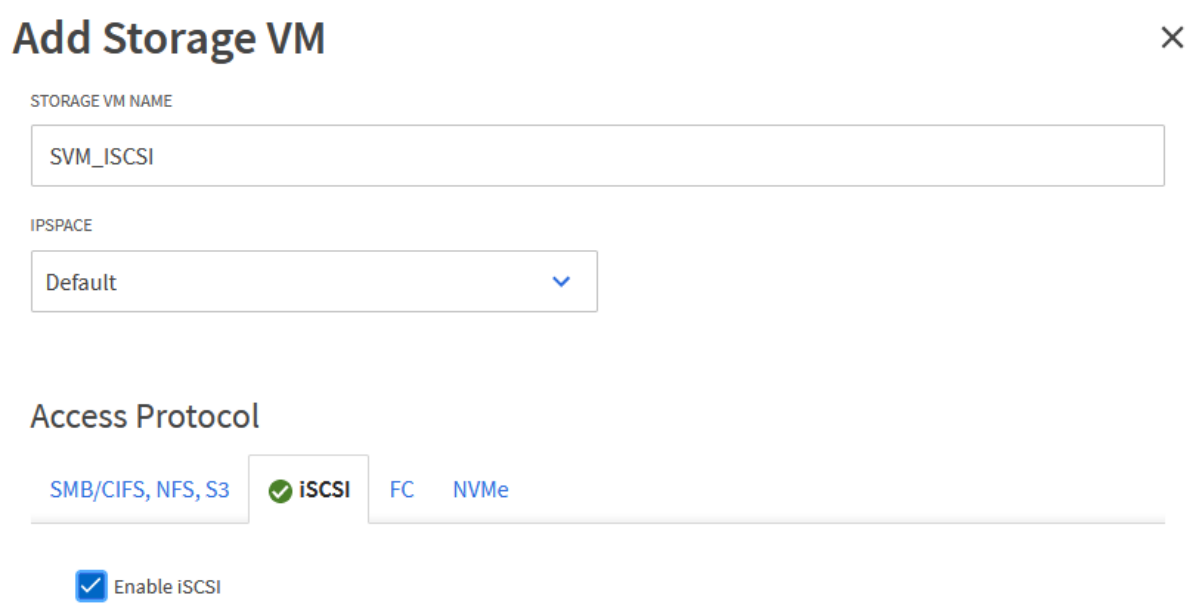
Cree la máquina virtual de almacenamiento y los LIF

Complete los siguientes pasos para crear una SVM junto con múltiples LIF para el tráfico iSCSI.

1. Desde el Administrador del sistema ONTAP , navegue hasta **Máquinas virtuales de almacenamiento** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.

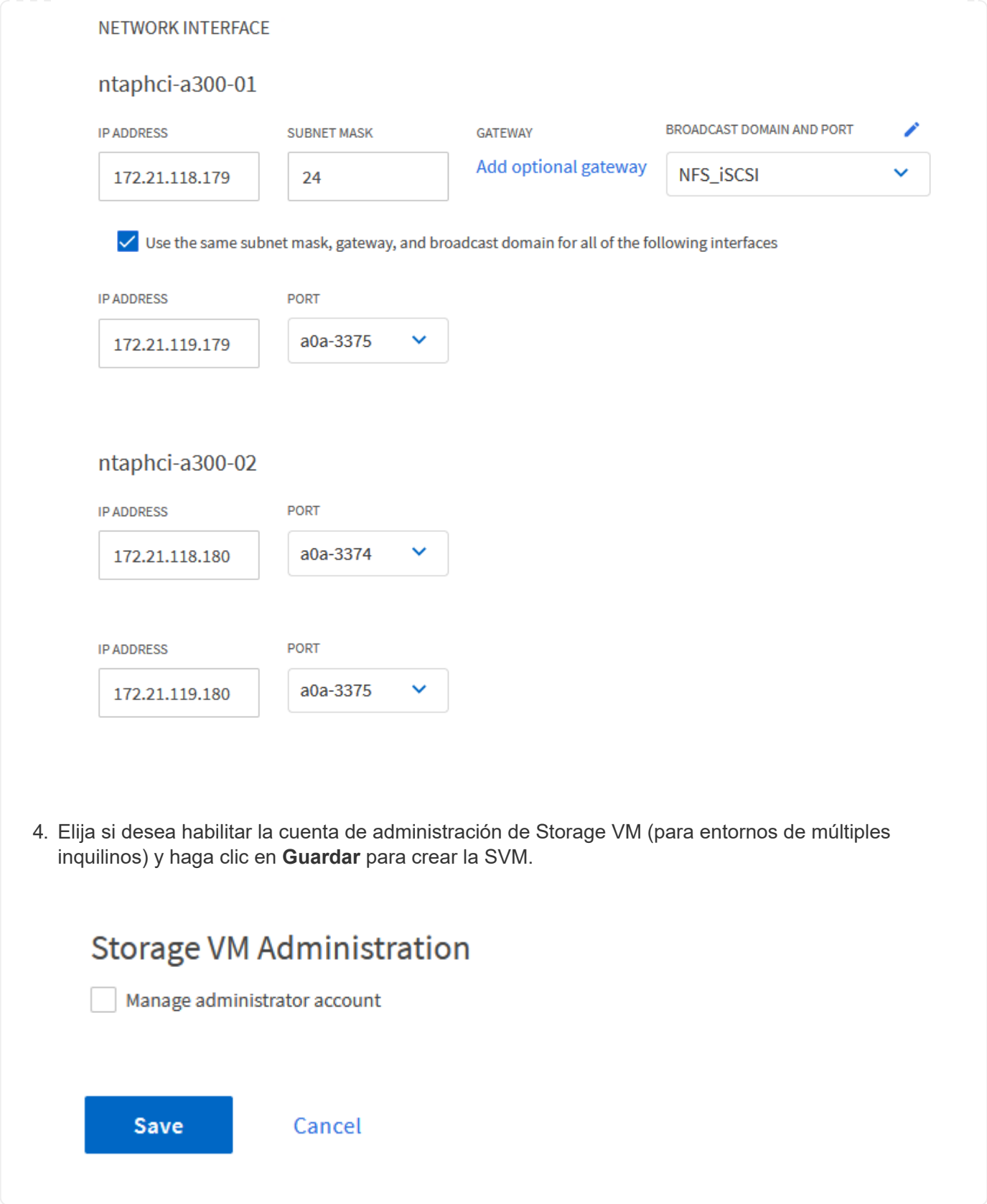


2. En el asistente **Agregar VM de almacenamiento**, proporcione un **Nombre** para la SVM, seleccione el **Espacio IP** y luego, en **Protocolo de acceso**, haga clic en la pestaña **iSCSI** y marque la casilla para **Habilitar iSCSI**.



3. En la sección **Interfaz de red**, complete la **Dirección IP**, la **Máscara de subred** y el **Dominio de transmisión y puerto** para el primer LIF. Para los LIF posteriores, la casilla de verificación se puede habilitar para utilizar configuraciones comunes en todos los LIF restantes o utilizar configuraciones separadas.

> Para rutas múltiples y conmutación por error en múltiples rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet separadas para todas las SVM en configuraciones iSCSI.



4. Elija si desea habilitar la cuenta de administración de Storage VM (para entornos de múltiples inquilinos) y haga clic en **Guardar** para crear la SVM.

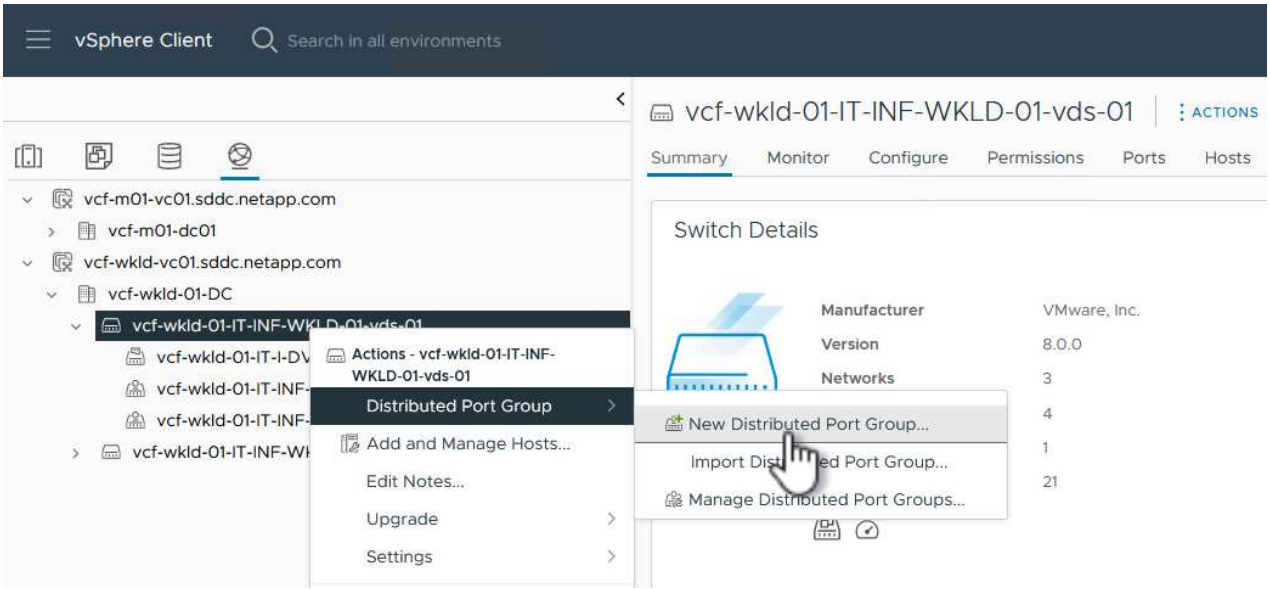
Configurar la red para iSCSI en hosts ESXi

Los siguientes pasos se realizan en el clúster de dominio de carga de trabajo VI mediante el cliente vSphere. En este caso, se utiliza vCenter Single Sign-On para que el cliente vSphere sea común en los dominios de administración y carga de trabajo.

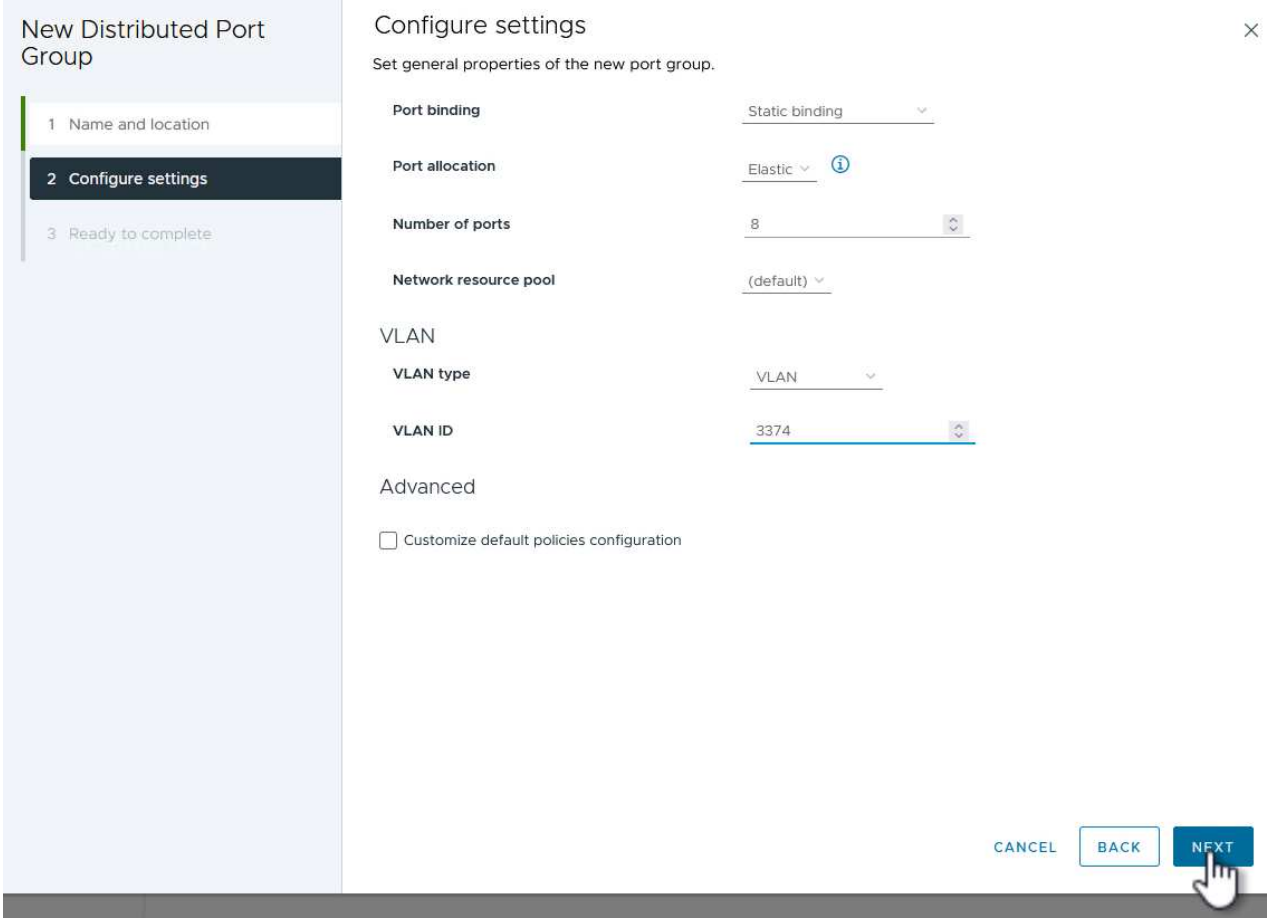
Crear grupos de puertos distribuidos para el tráfico iSCSI

Complete lo siguiente para crear un nuevo grupo de puertos distribuidos para cada red iSCSI:

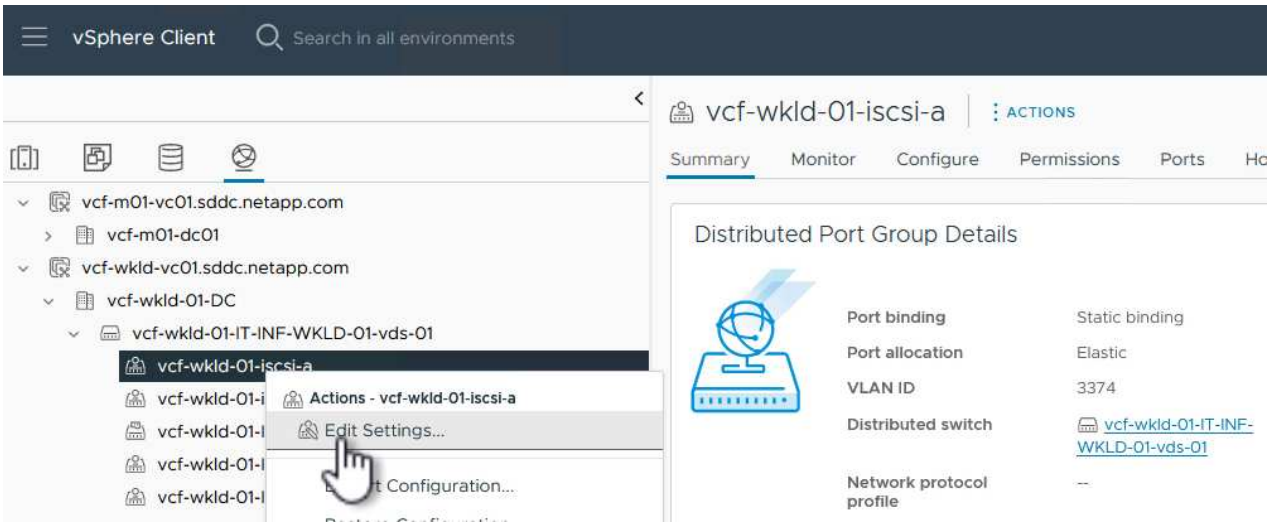
1. Desde el cliente vSphere, navegue a **Inventario > Redes** para el dominio de carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos…**.



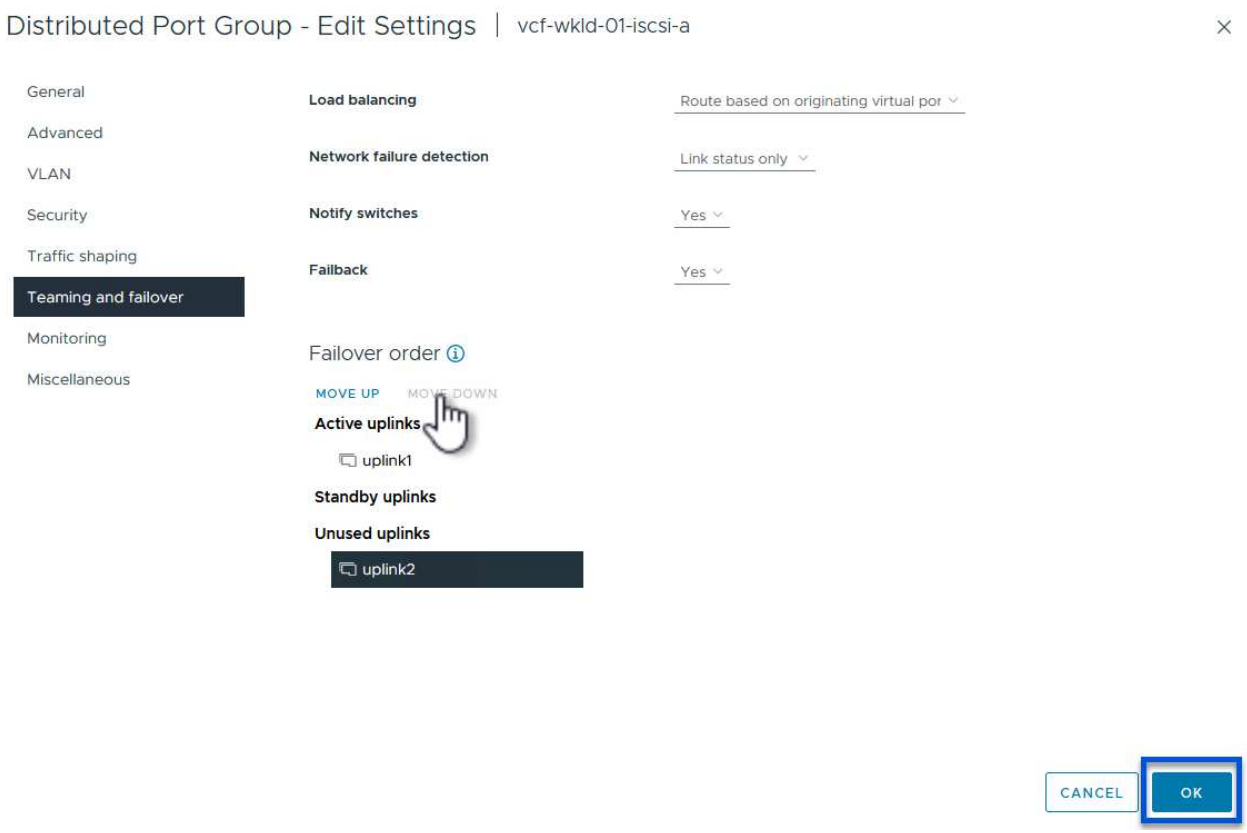
2. En el asistente **Nuevo grupo de puertos distribuidos**, complete un nombre para el nuevo grupo de puertos y haga clic en **Siguiente** para continuar.
3. En la página **Configurar ajustes** complete todas las configuraciones. Si se utilizan VLAN, asegúrese de proporcionar la ID de VLAN correcta. Haga clic en **Siguiente** para continuar.



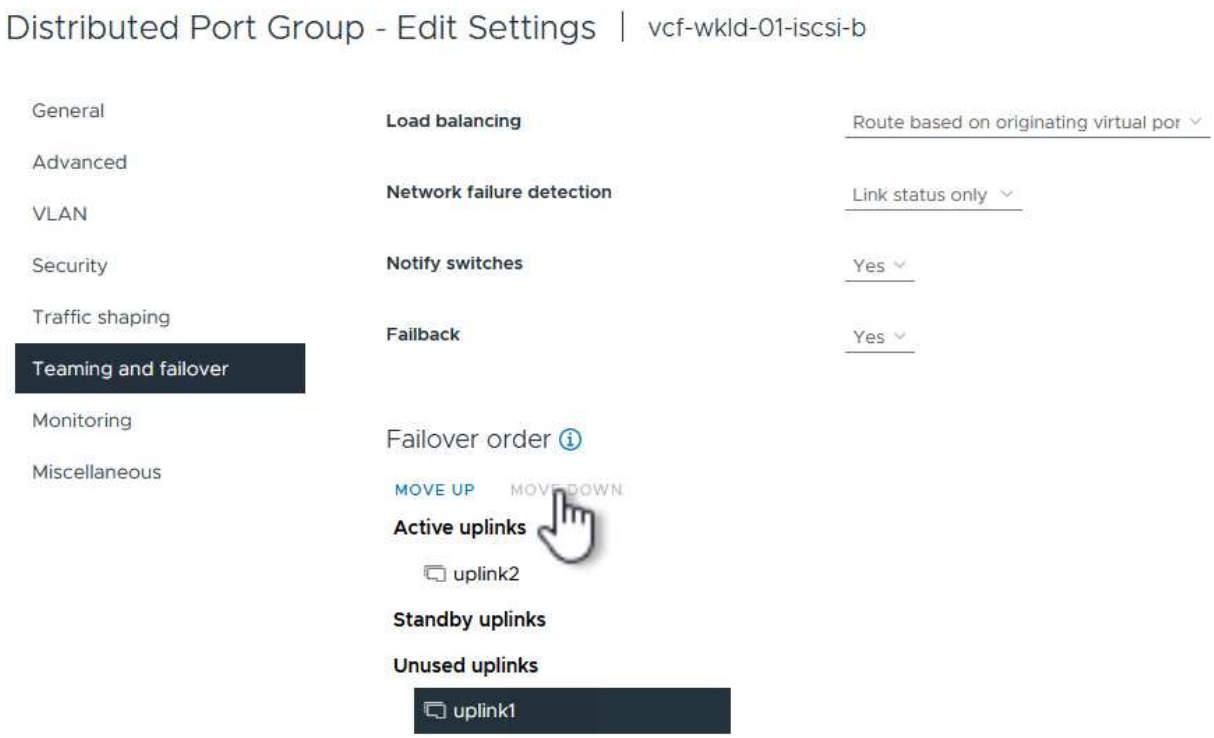
4. En la página **Listo para completar**, revise los cambios y haga clic en **Finalizar** para crear el nuevo grupo de puertos distribuidos.
5. Repita este proceso para crear un grupo de puertos distribuidos para la segunda red iSCSI que se esté utilizando y asegúrese de haber ingresado el **VLAN ID** correcto.
6. Una vez que se hayan creado ambos grupos de puertos, navegue hasta el primer grupo de puertos y seleccione la acción **Editar configuración…**.



7. En la página **Grupo de puertos distribuidos - Editar configuración**, navegue a **Equipo y conmutación por error** en el menú de la izquierda y haga clic en **uplink2** para moverlo hacia abajo a **Enlaces ascendentes no utilizados**.



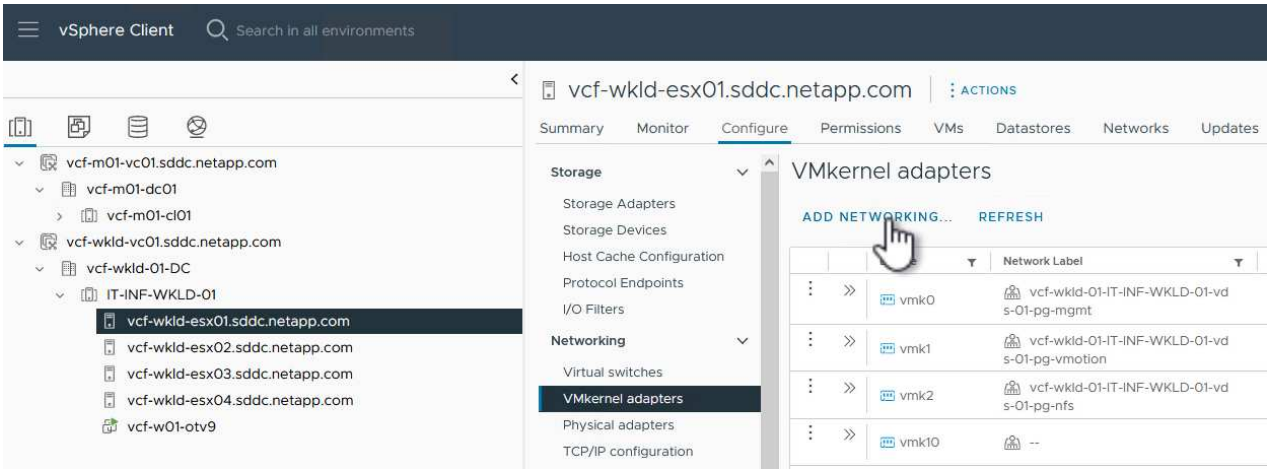
8. Repita este paso para el segundo grupo de puertos iSCSI. Sin embargo, esta vez mueva **uplink1** a **Unused uplinks**.



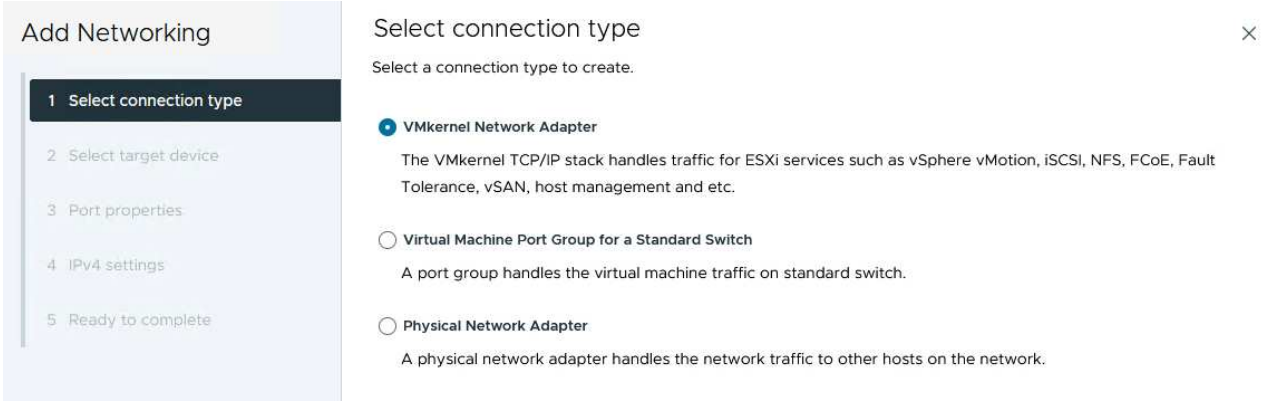
Cree adaptadores VMkernel en cada host ESXi

Repita este proceso en cada host ESXi en el dominio de carga de trabajo.

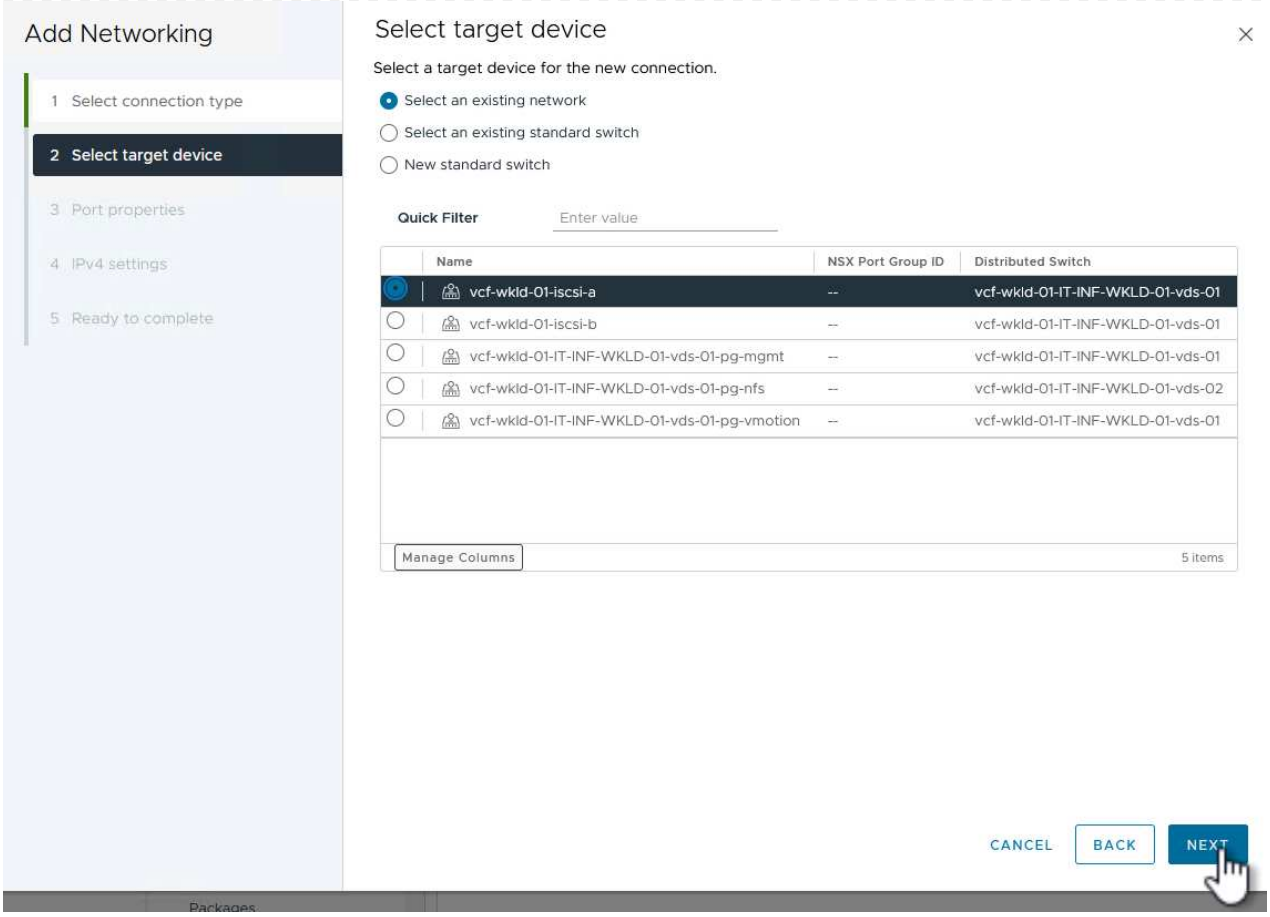
1. Desde el cliente vSphere, navegue a uno de los hosts ESXi en el inventario del dominio de carga de trabajo. Desde la pestaña **Configurar** seleccione **Adaptadores VMkernel** y haga clic en **Agregar red…** para comenzar.



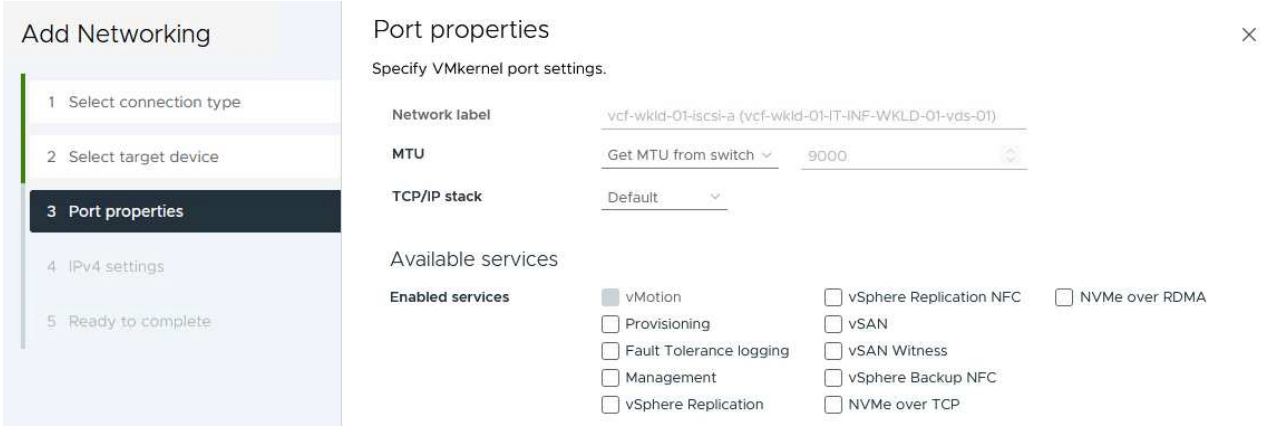
2. En la ventana **Seleccionar tipo de conexión** elija **Adaptador de red VMkernel** y haga clic en **Siguiente** para continuar.



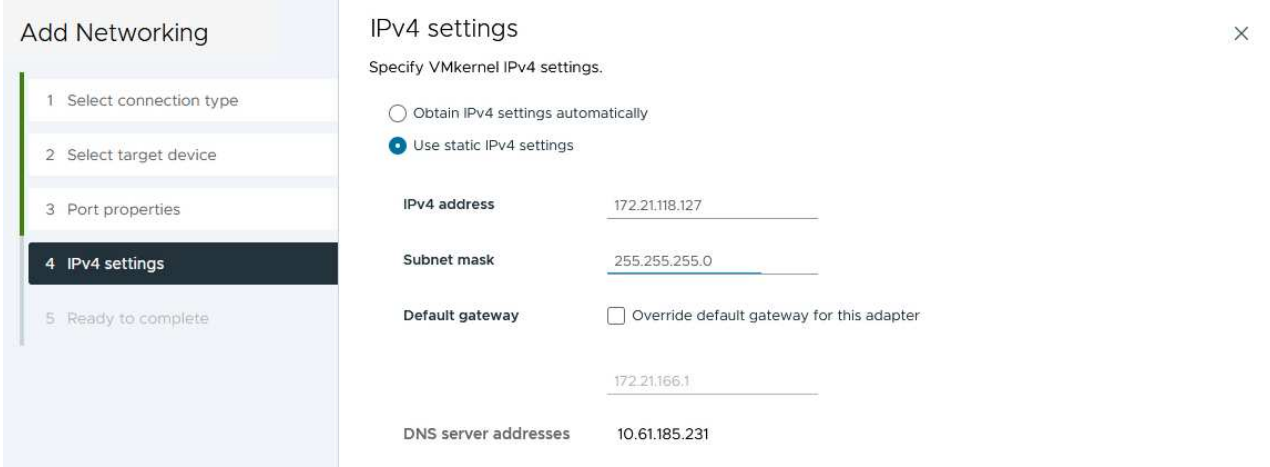
3. En la página **Seleccionar dispositivo de destino**, elija uno de los grupos de puertos distribuidos para iSCSI que se crearon anteriormente.



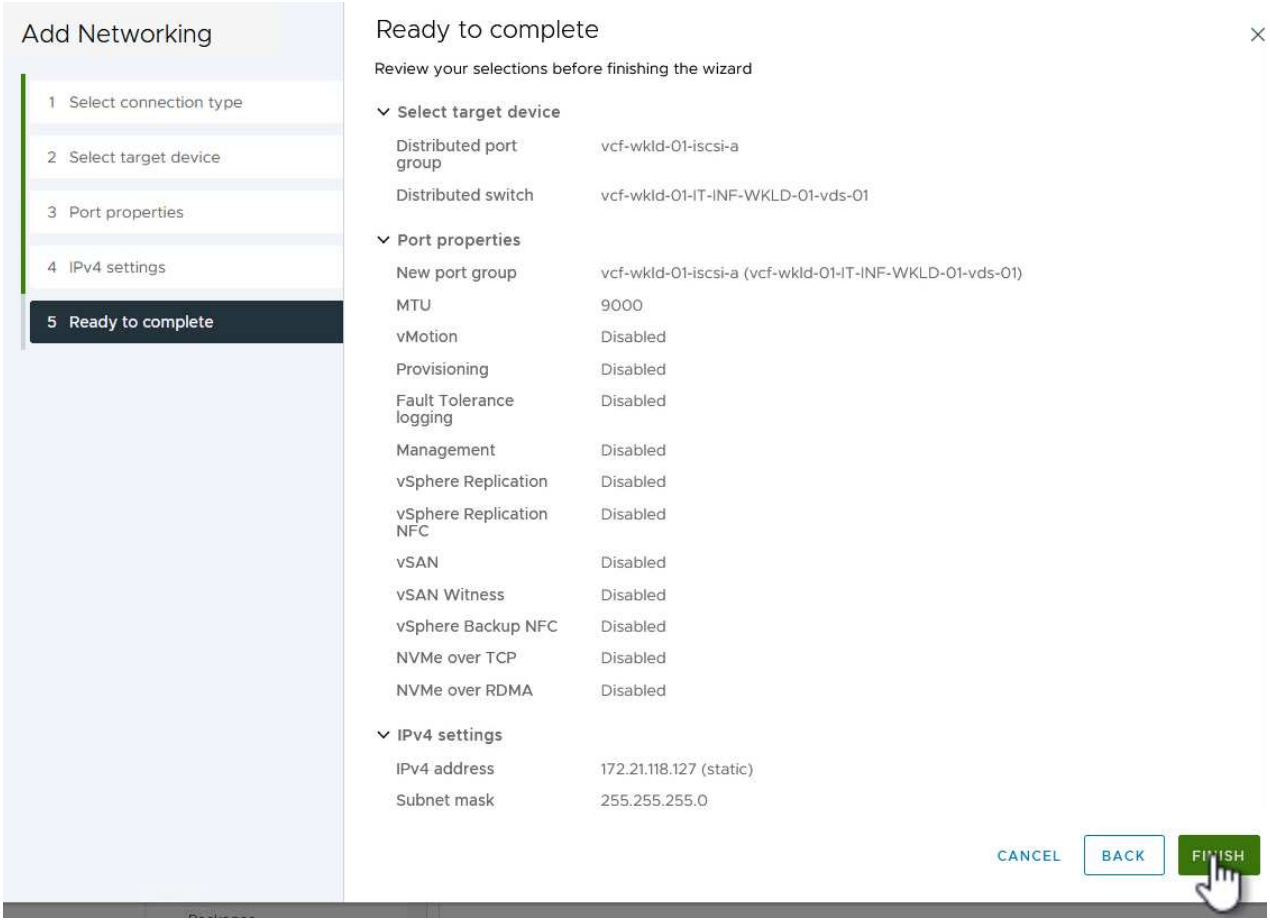
4. En la página **Propiedades del puerto** mantenga los valores predeterminados y haga clic en **Siguiente** para continuar.



5. En la página de **Configuración de IPv4**, complete la **dirección IP**, la **Máscara de subred** y proporcione una nueva dirección IP de puerta de enlace (solo si es necesario). Haga clic en **Siguiente** para continuar.



6. Revise sus selecciones en la página **Listo para completar** y haga clic en **Finalizar** para crear el adaptador VMkernel.



7. Repita este proceso para crear un adaptador VMkernel para la segunda red iSCSI.

Implementar y usar herramientas ONTAP para configurar el almacenamiento

Los siguientes pasos se realizan en el clúster de dominio de administración de VCF mediante el cliente vSphere e implican la implementación de ONTAP Tools, la creación de un almacén de datos iSCSI de vVols y la migración de las máquinas virtuales de administración al nuevo almacén de datos.

Para los dominios de carga de trabajo VI, ONTAP Tools se instala en el clúster de administración de VCF, pero se registra en el vCenter asociado con el dominio de carga de trabajo VI.

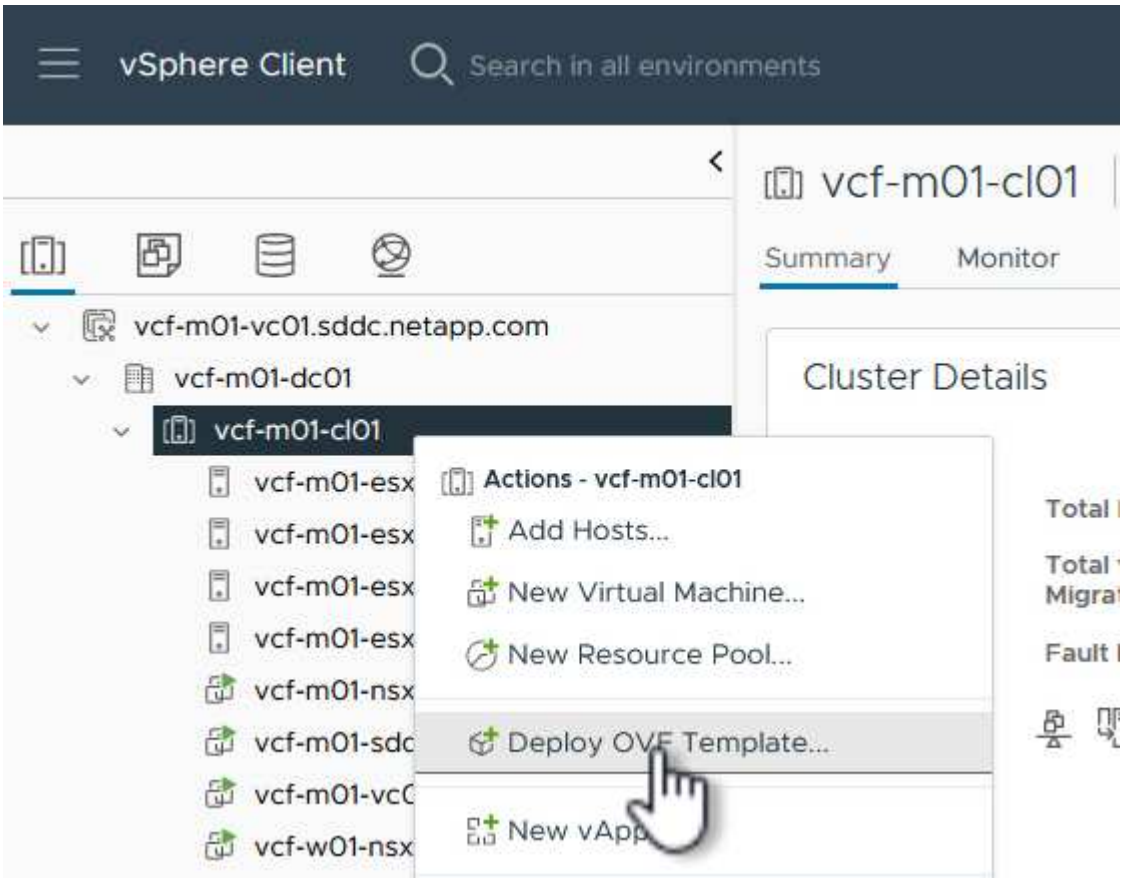
Para obtener información adicional sobre la implementación y el uso de herramientas ONTAP en un entorno de varios vCenter, consulte"Requisitos para registrar herramientas ONTAP en entornos de múltiples servidores vCenter" .

Implementar ONTAP tools for VMware vSphere

Las ONTAP tools for VMware vSphere se implementan como un dispositivo de VM y proporcionan una interfaz de usuario vCenter integrada para administrar el almacenamiento de ONTAP .

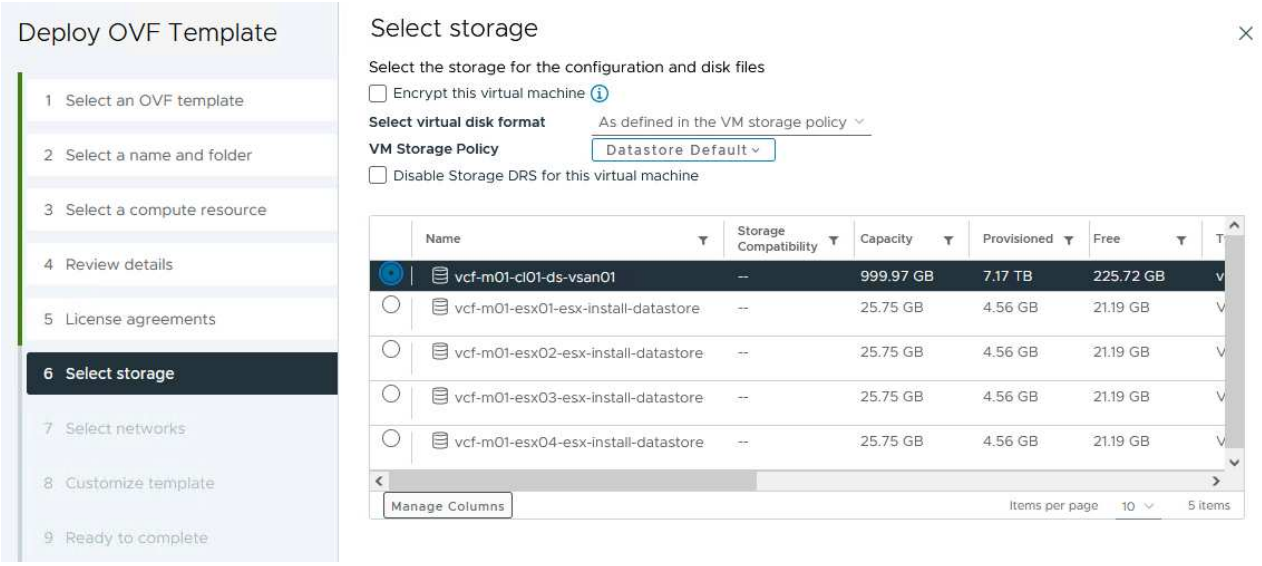
Complete lo siguiente para implementar ONTAP tools for VMware vSphere:

1. Obtenga la imagen OVA de las herramientas ONTAP desde"Sitio de soporte de NetApp" y descargar a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de administración de VCF.
3. Desde la interfaz del dispositivo vCenter, haga clic con el botón derecho en el clúster de administración y seleccione **Implementar plantilla OVF…**

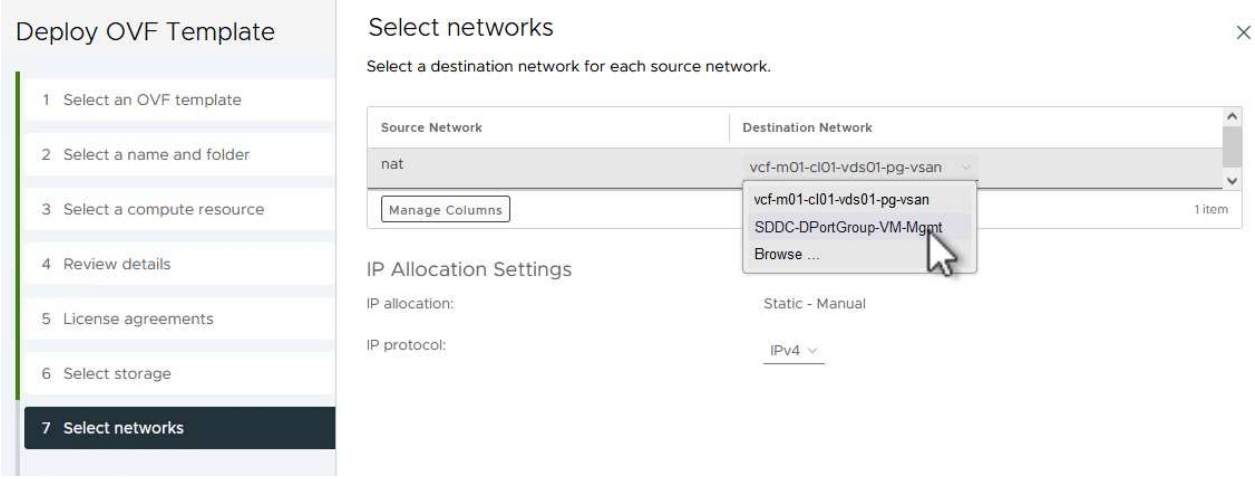


4. En el asistente **Implementar plantilla OVF**, haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de las herramientas ONTAP descargado en el paso anterior.

5. Para los pasos 2 a 5 del asistente, seleccione un nombre y una carpeta para la máquina virtual, seleccione el recurso computacional, revise los detalles y acepte el acuerdo de licencia.
6. Para la ubicación de almacenamiento de los archivos de configuración y de disco, seleccione el almacén de datos vSAN del clúster de dominio de administración de VCF.

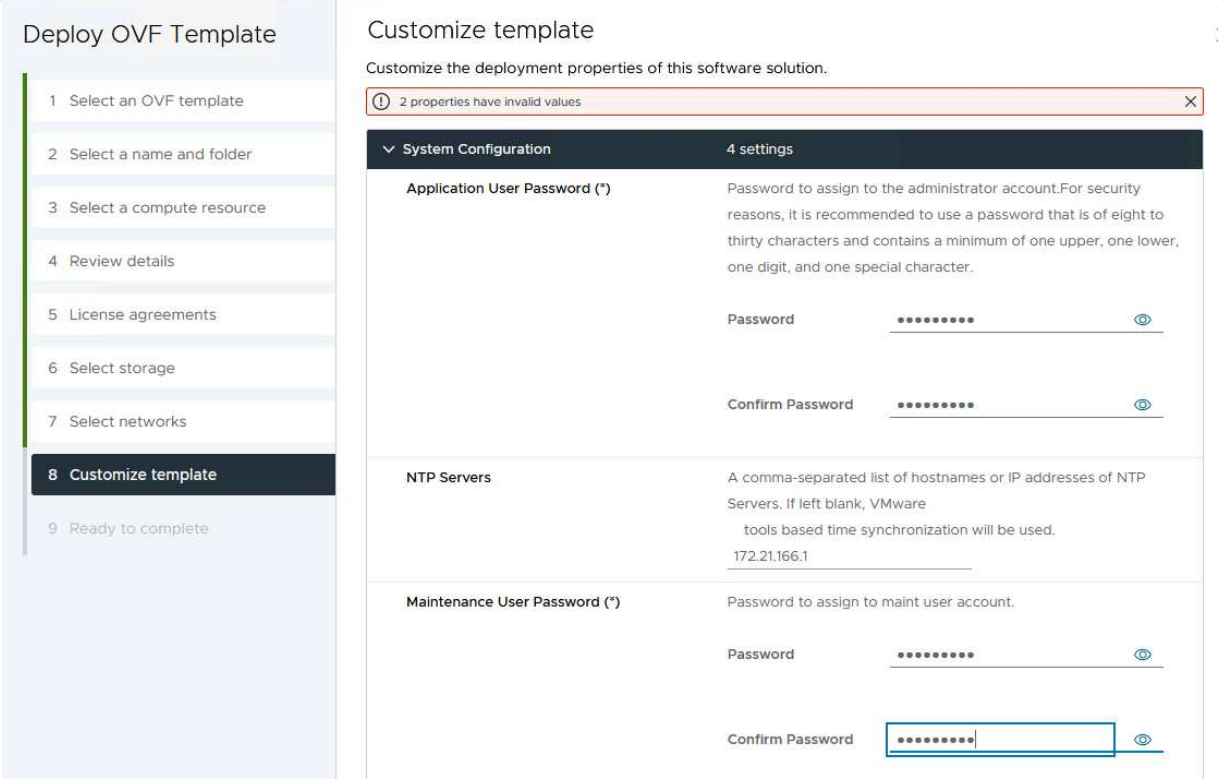


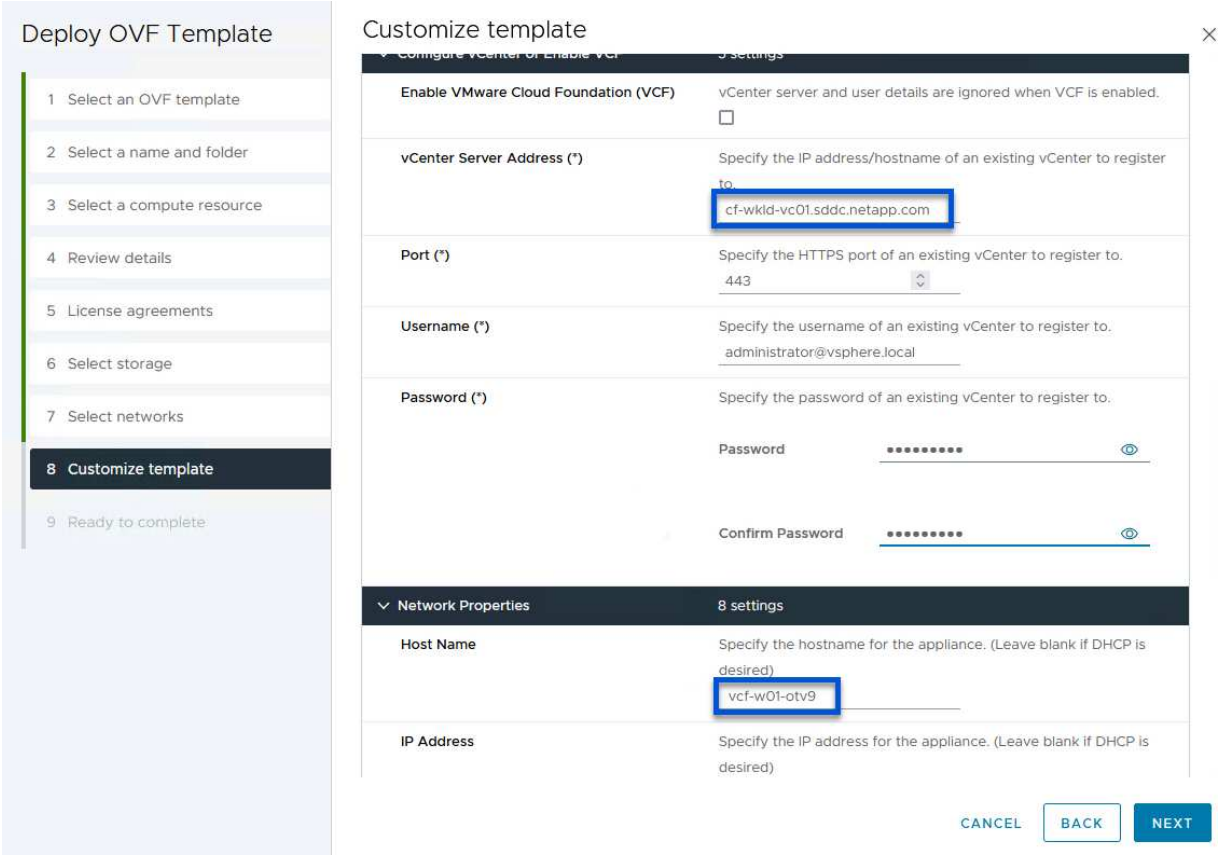
7. En la página Seleccionar red, seleccione la red utilizada para administrar el tráfico.



8. En la página Personalizar plantilla, complete toda la información requerida:
   - Contraseña que se utilizará para el acceso administrativo a las herramientas ONTAP .
   - Dirección IP del servidor NTP.
   - Contraseña de la cuenta de mantenimiento de ONTAP Tools.
   - Contraseña de base de datos Derby de herramientas ONTAP .
   - No marque la casilla para **Habilitar VMware Cloud Foundation (VCF)**. El modo VCF no es necesario para implementar almacenamiento complementario.
   - FQDN o dirección IP del dispositivo vCenter para el **VI Workload Domain**
   - Credenciales para el dispositivo vCenter del **VI Workload Domain**
   - Proporcione los campos de propiedades de red requeridos.

     Haga clic en **Siguiente** para continuar.

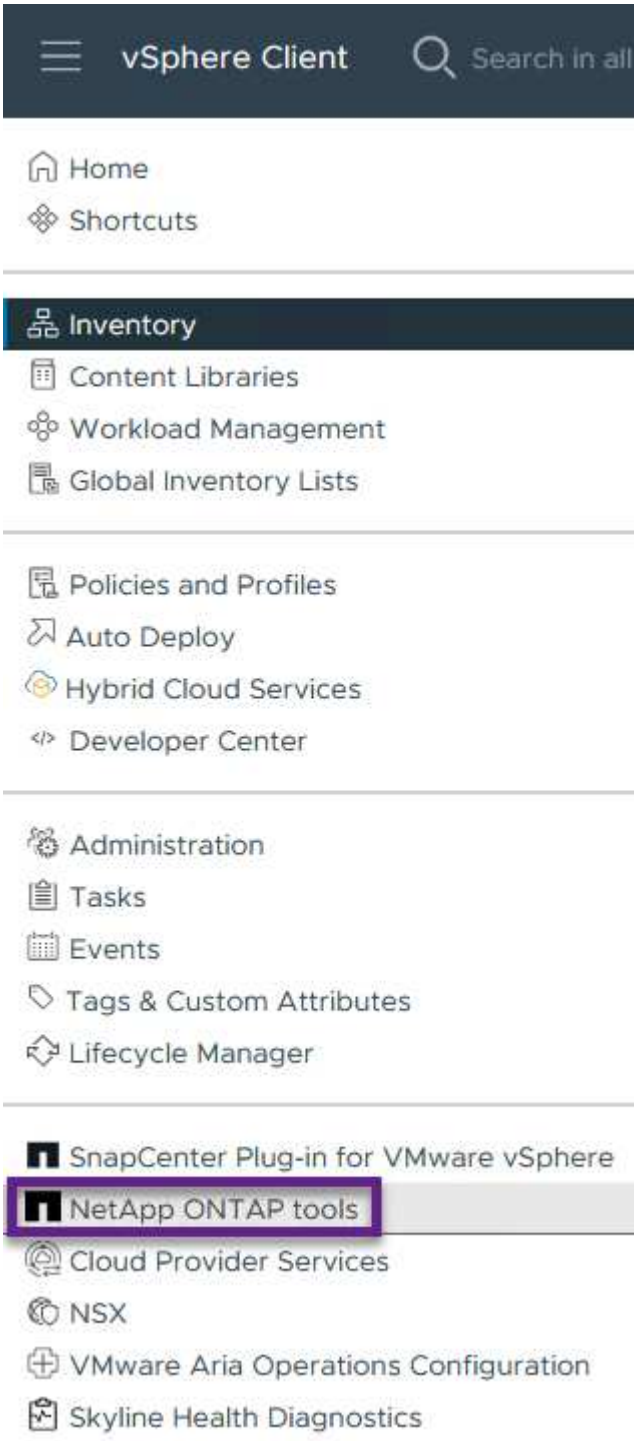




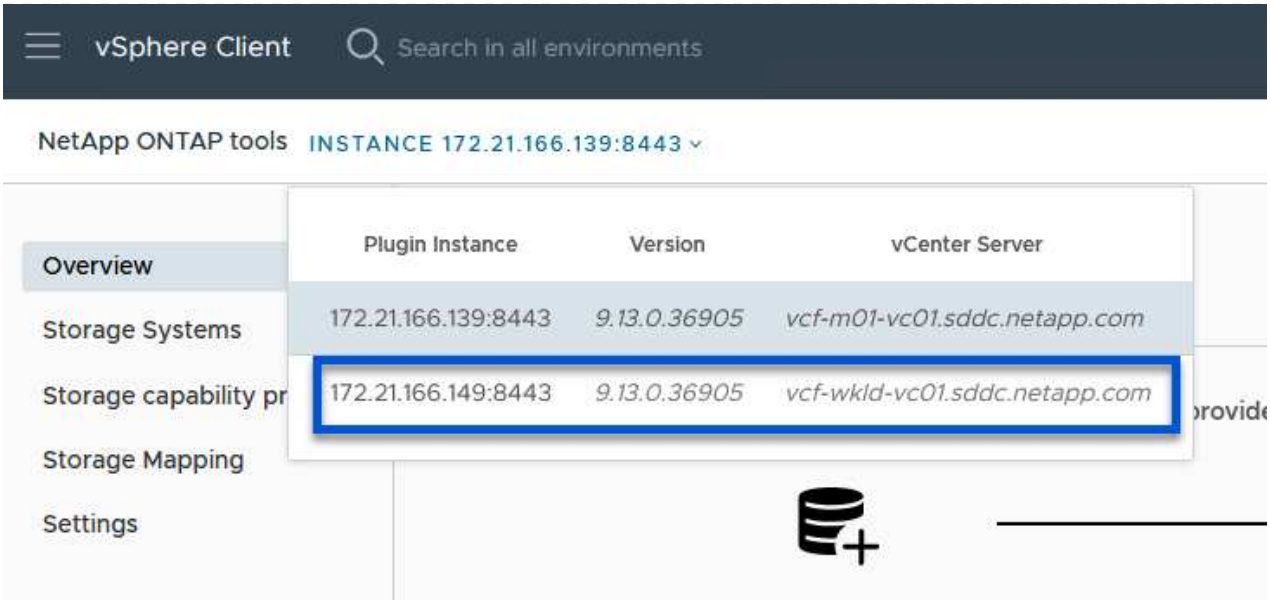
9. Revise toda la información en la página Listo para completar y haga clic en Finalizar para comenzar a implementar el dispositivo ONTAP Tools.

Agregue un sistema de almacenamiento a ONTAP Tools.

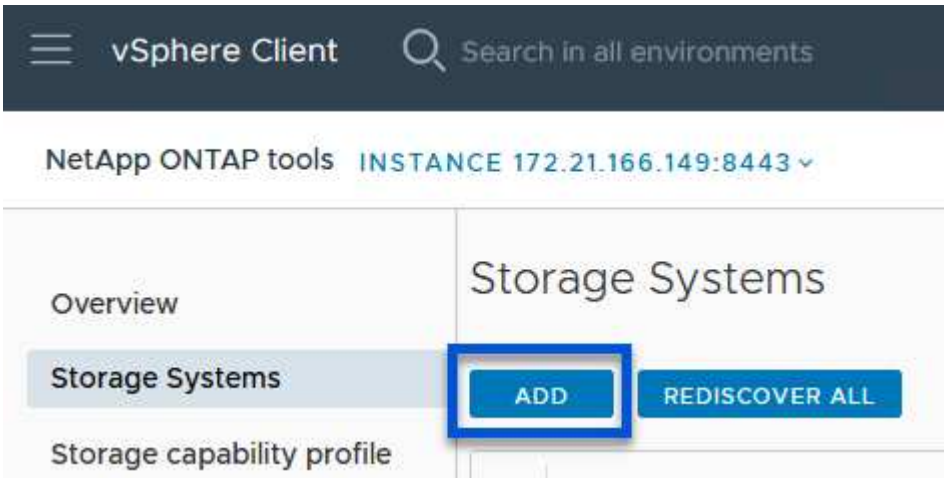
1. Acceda a las herramientas de NetApp ONTAP seleccionándolas en el menú principal en el cliente vSphere.



2. Desde el menú desplegable **INSTANCIA** en la interfaz de ONTAP Tool, seleccione la instancia de ONTAP Tools asociada con el dominio de carga de trabajo que se administrará.

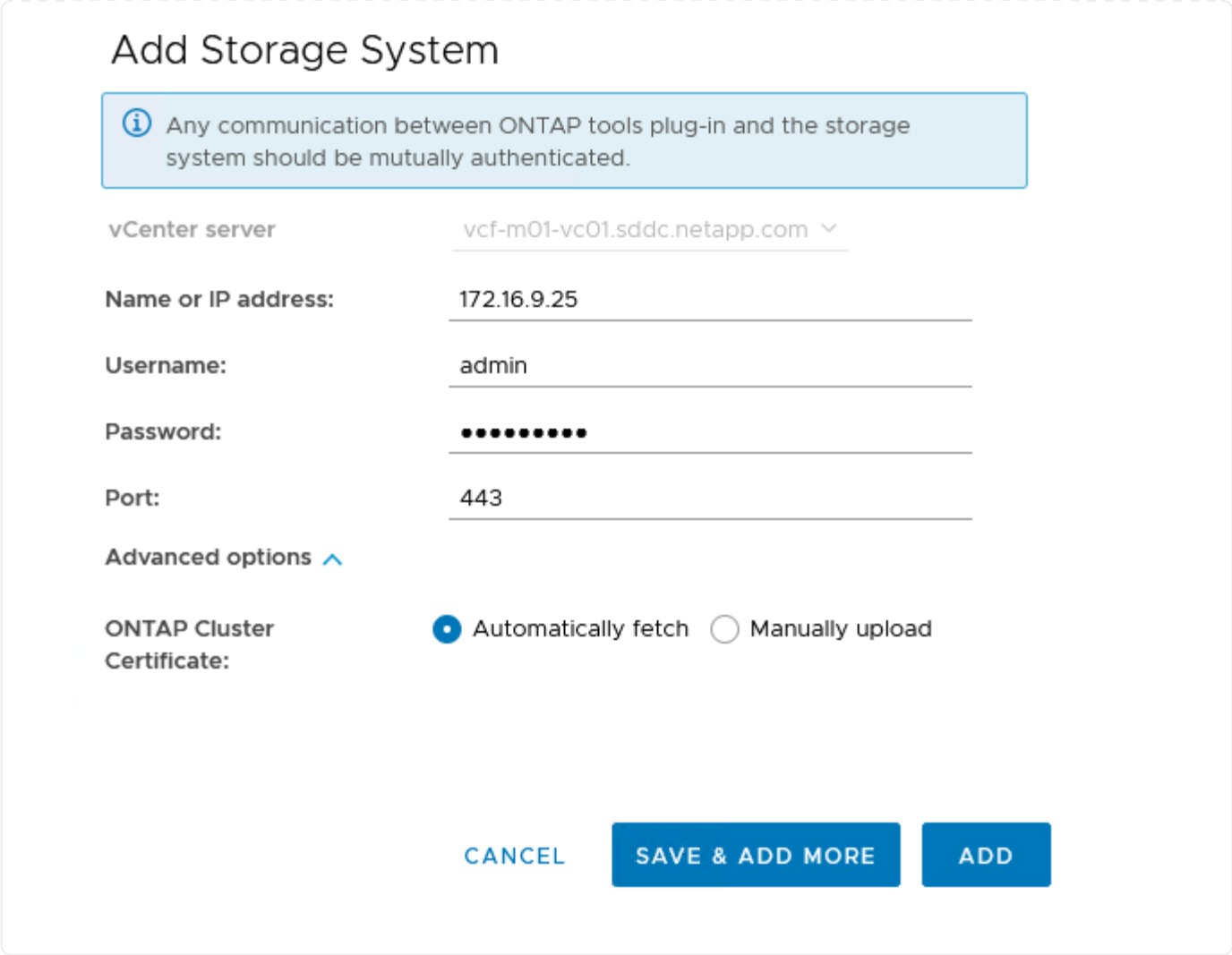


3. En Herramientas de ONTAP , seleccione **Sistemas de almacenamiento** en el menú de la izquierda y luego presione **Agregar**.



4. Complete la dirección IP, las credenciales del sistema de almacenamiento y el número de puerto. Haga clic en **Agregar** para iniciar el proceso de descubrimiento.

> vVol requiere credenciales de clúster ONTAP en lugar de credenciales SVM. Para obtener más información, consulte "Añadir sistemas de almacenamiento" En la documentación de herramientas de ONTAP .

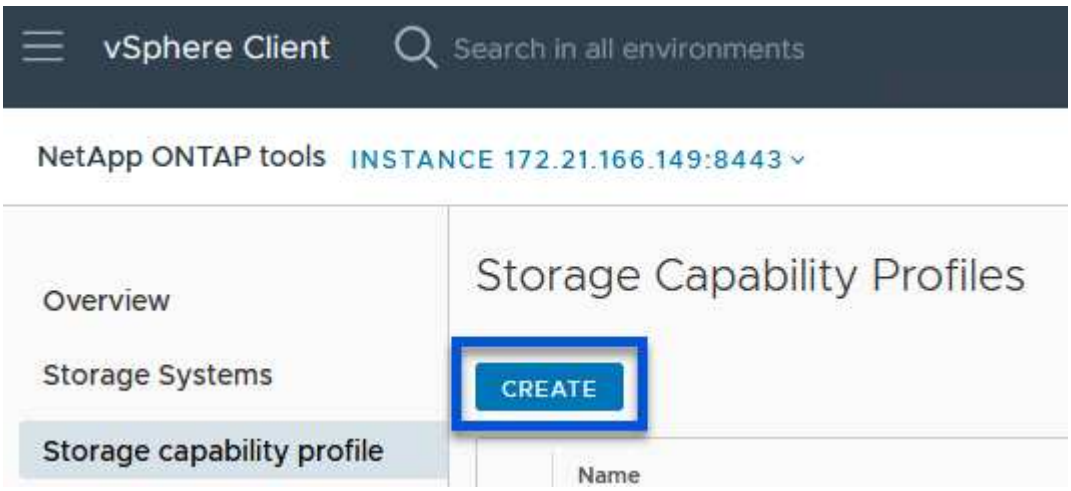

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Crear un perfil de capacidad de almacenamiento en ONTAP Tools

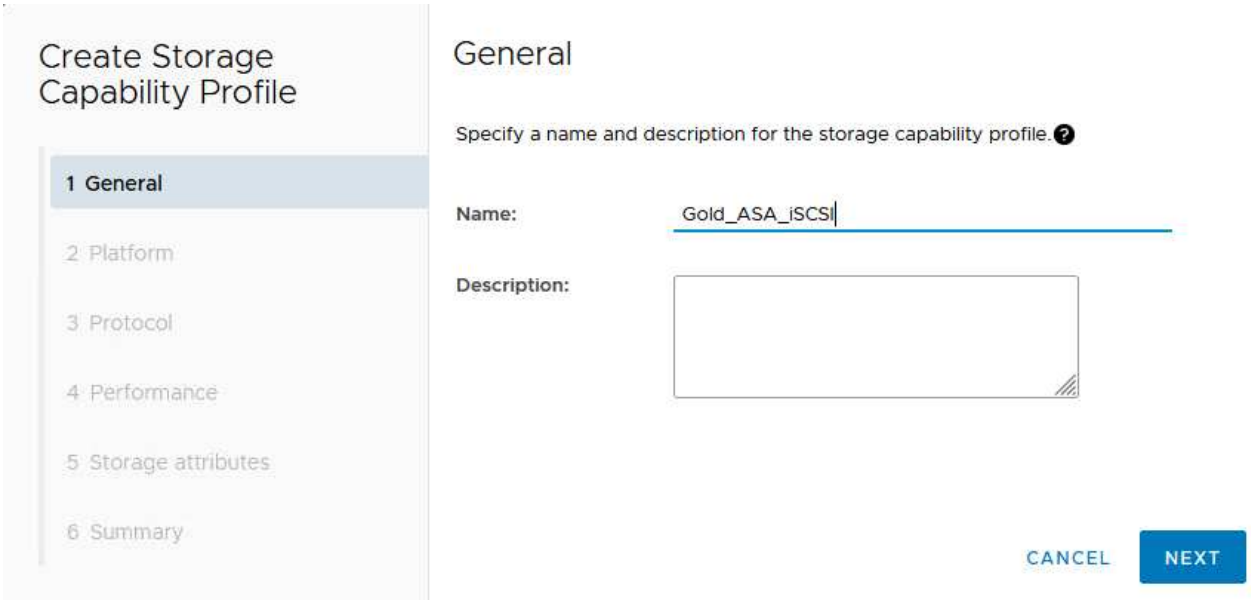
Los perfiles de capacidad de almacenamiento describen las características que ofrece una matriz de almacenamiento o un sistema de almacenamiento. Incluyen definiciones de calidad de servicio y se utilizan para seleccionar sistemas de almacenamiento que cumplen los parámetros definidos en el perfil. Se puede utilizar uno de los perfiles proporcionados o se pueden crear otros nuevos.

Para crear un perfil de capacidad de almacenamiento en ONTAP Tools, complete los siguientes pasos:

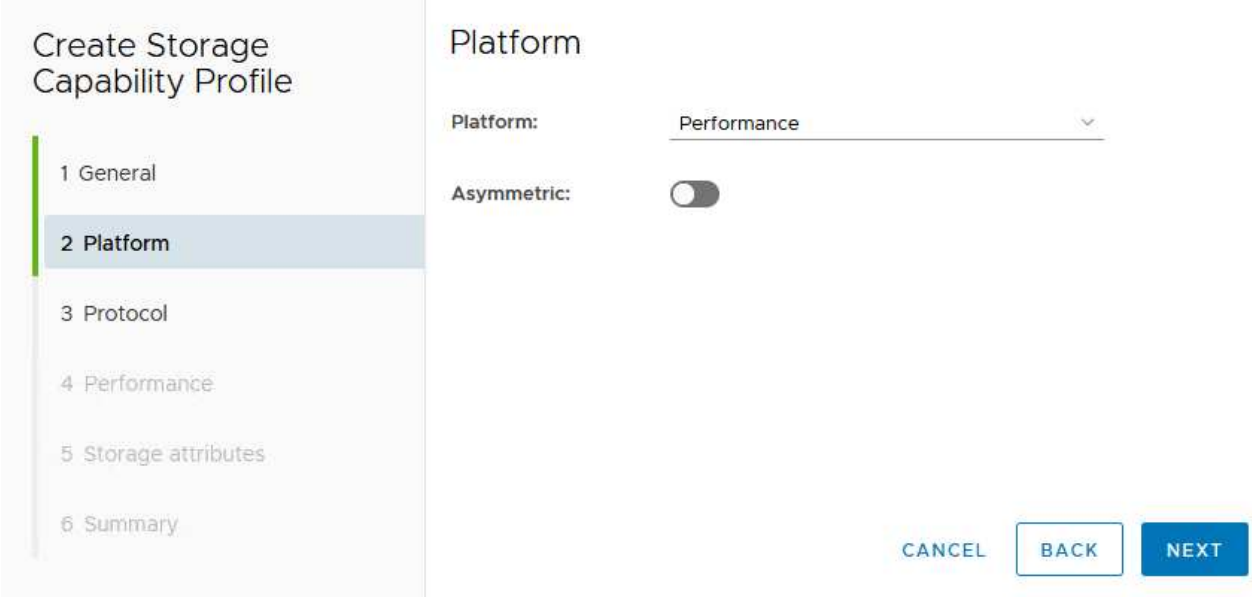
1. En Herramientas de ONTAP , seleccione **Perfil de capacidad de almacenamiento** en el menú de la izquierda y luego presione **Crear**.



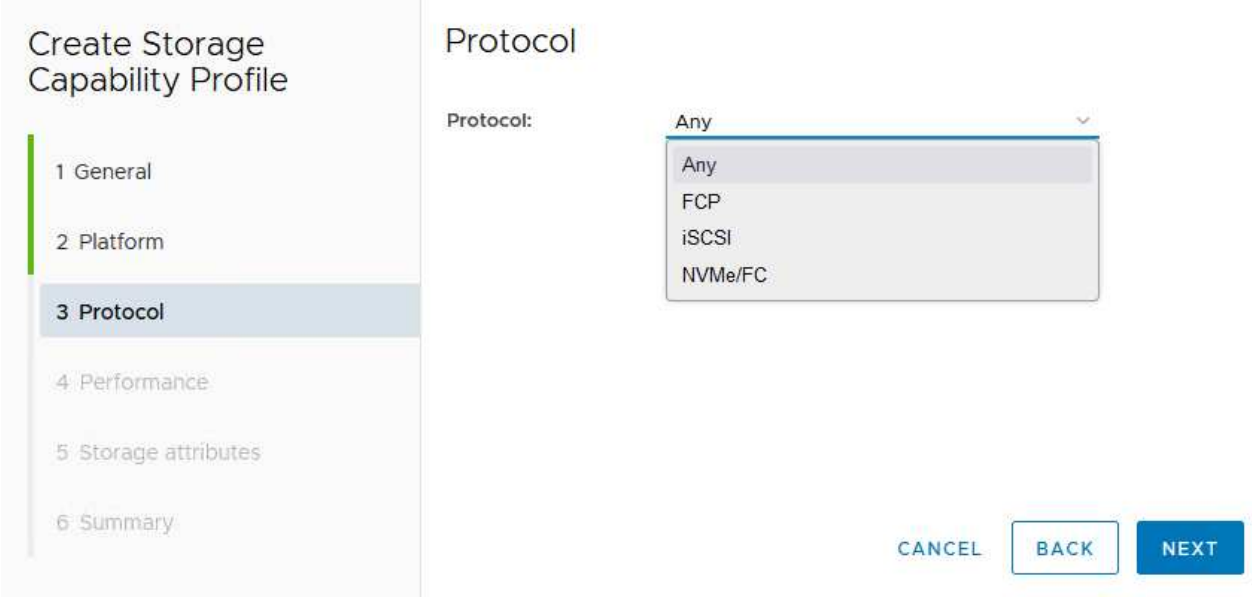
2. En el asistente **Crear perfil de capacidad de almacenamiento** proporcione un nombre y una descripción del perfil y haga clic en **Siguiente**.



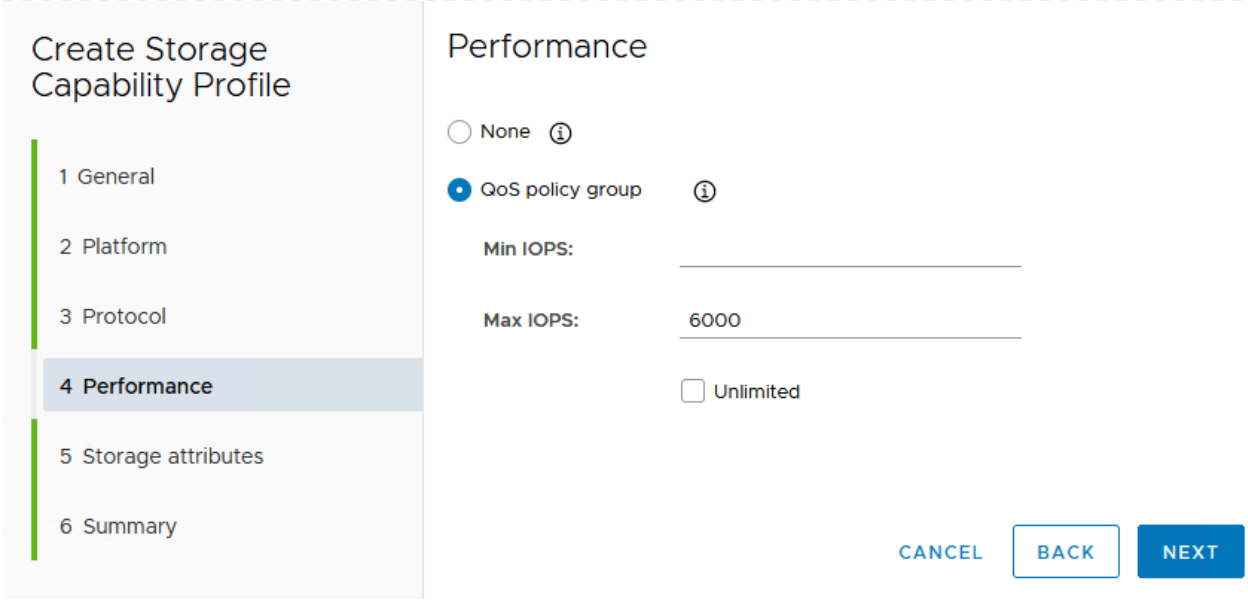
3. Seleccione el tipo de plataforma y especifique que el sistema de almacenamiento será una matriz SAN All-Flash y configure **Asimétrico** como falso.



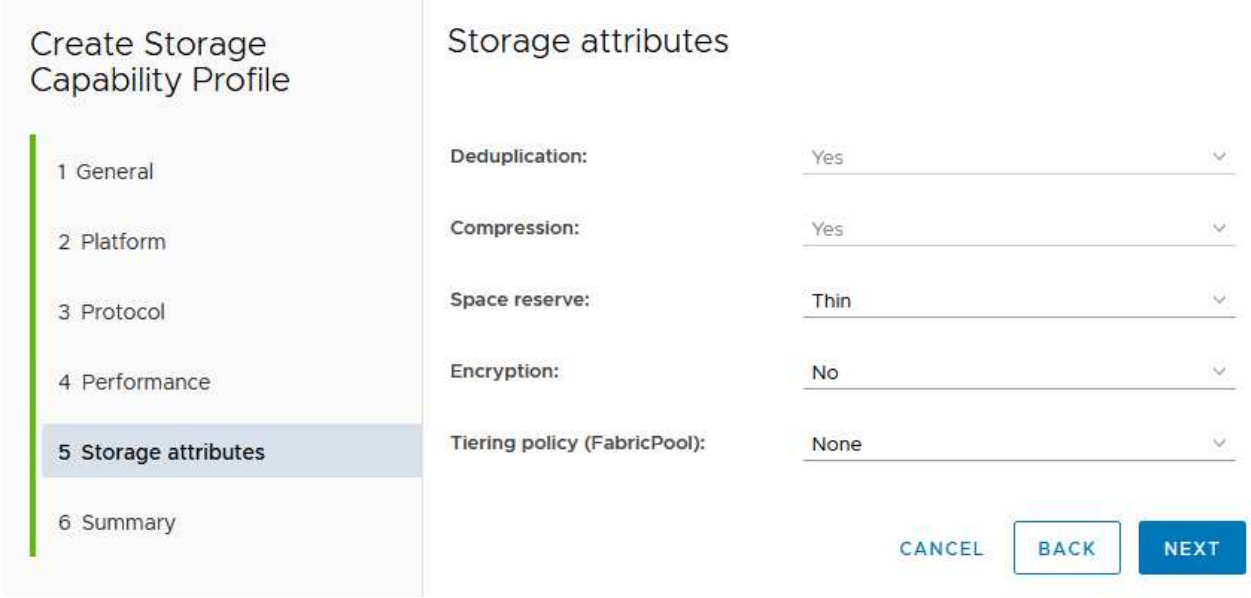
4. A continuación, seleccione la elección del protocolo o **Cualquiera** para permitir todos los protocolos posibles. Haga clic en **Siguiente** para continuar.



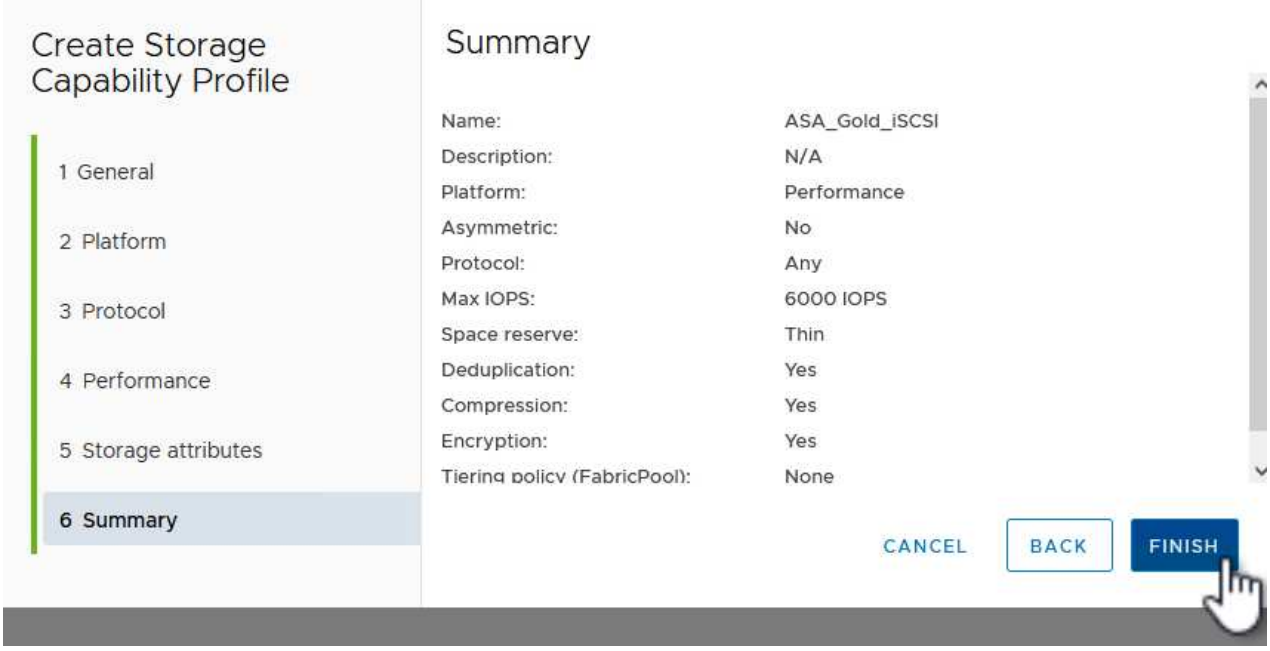
5. La página de **rendimiento** permite configurar la calidad del servicio en forma de IOP mínimas y máximas permitidas.



6. Complete la página de **atributos de almacenamiento** seleccionando la eficiencia del almacenamiento, la reserva de espacio, el cifrado y cualquier política de niveles según sea necesario.



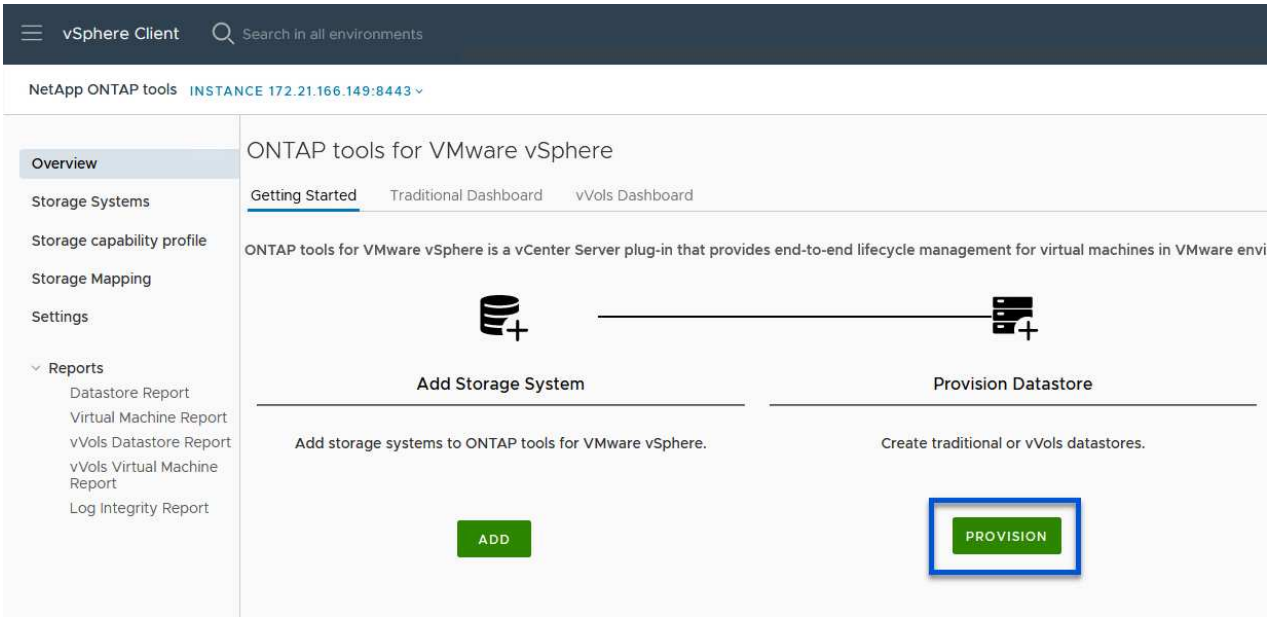
7. Por último, revise el resumen y haga clic en Finalizar para crear el perfil.


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Summary
Name: ASA_Gold_iSCSI
Description: N/A
Platform: Performance
Asymmetric: No
Protocol: Any
Max IOPS: 6000 IOPS
Space reserve: Thin
Deduplication: Yes
Compression: Yes
Encryption: Yes
Tiering policy (FabricPool): None
CANCEL
BACK
FINISH

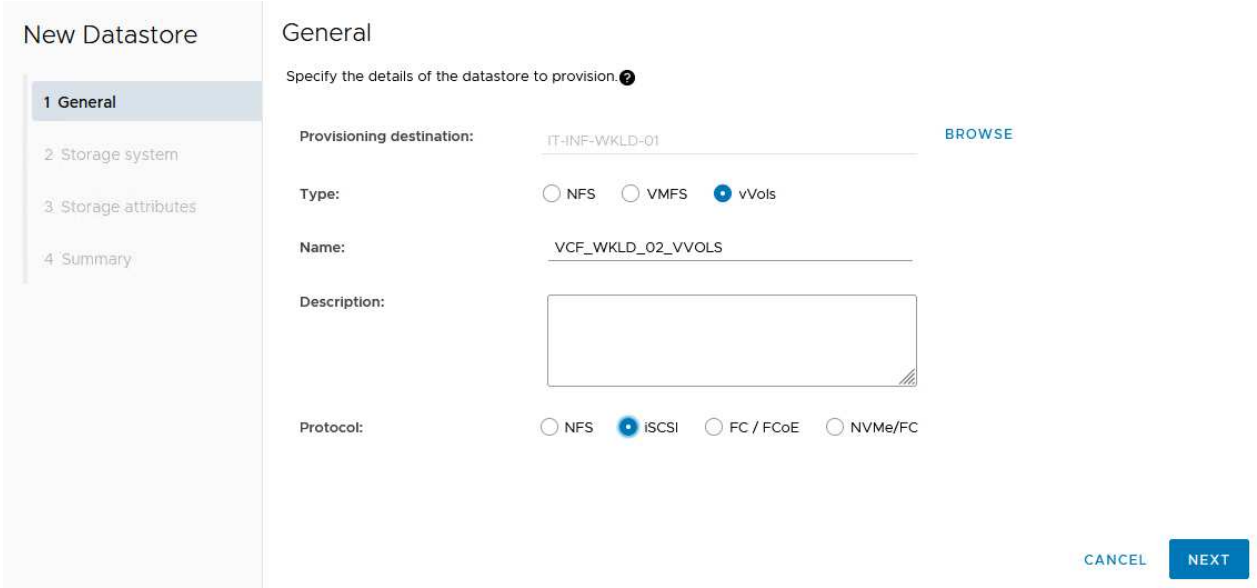
Crear un almacén de datos vVols en ONTAP Tools

Para crear un almacén de datos vVols en ONTAP Tools, complete los siguientes pasos:

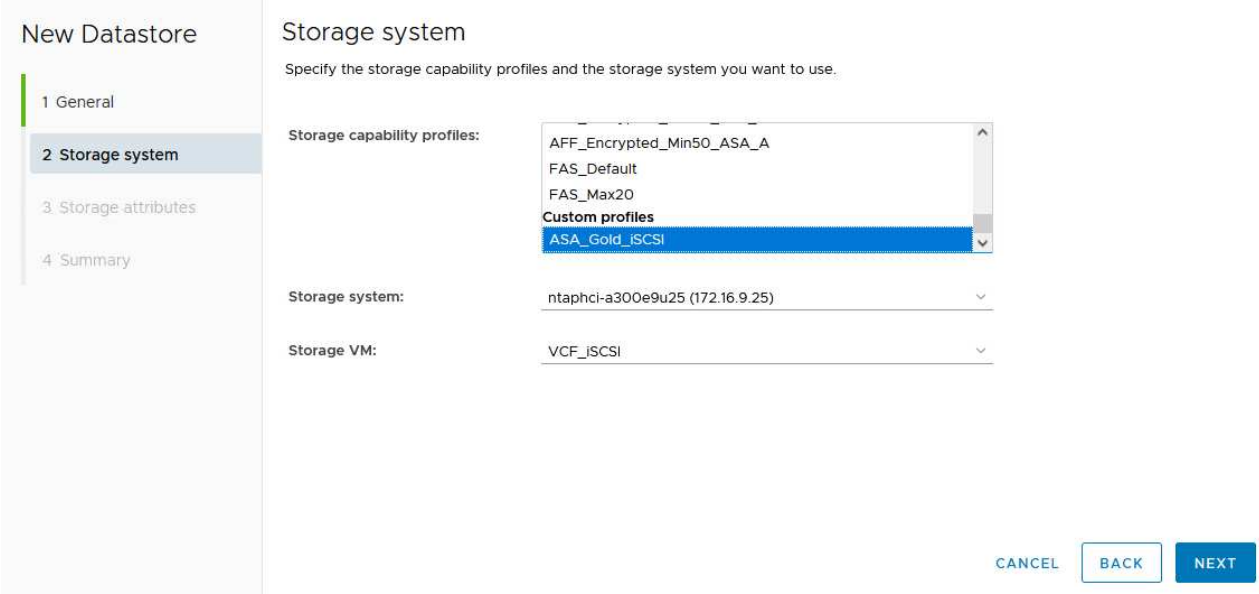
1. En Herramientas de ONTAP , seleccione **Descripción general** y en la pestaña **Introducción** haga clic en **Aprovisionamiento** para iniciar el asistente.



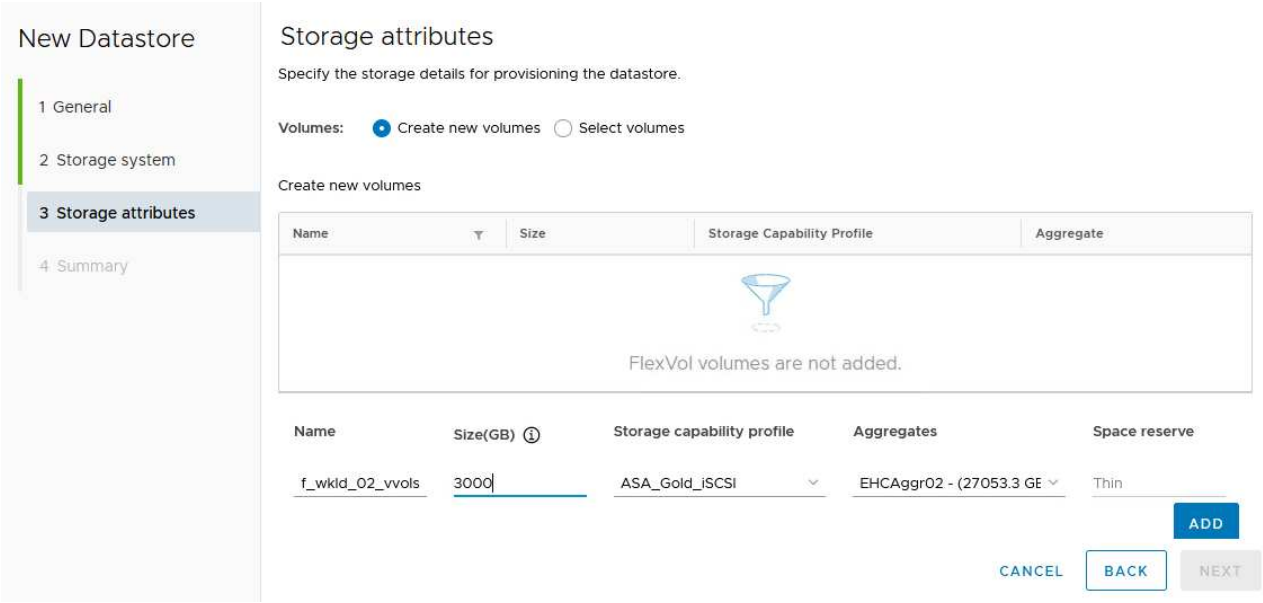
2. En la página **General** del asistente Nuevo almacén de datos, seleccione el centro de datos o el destino del clúster de vSphere. Seleccione * vVols* como el tipo de almacén de datos, complete un nombre para el almacén de datos y seleccione **iSCSI** como protocolo. Haga clic en **Siguiente** para continuar.



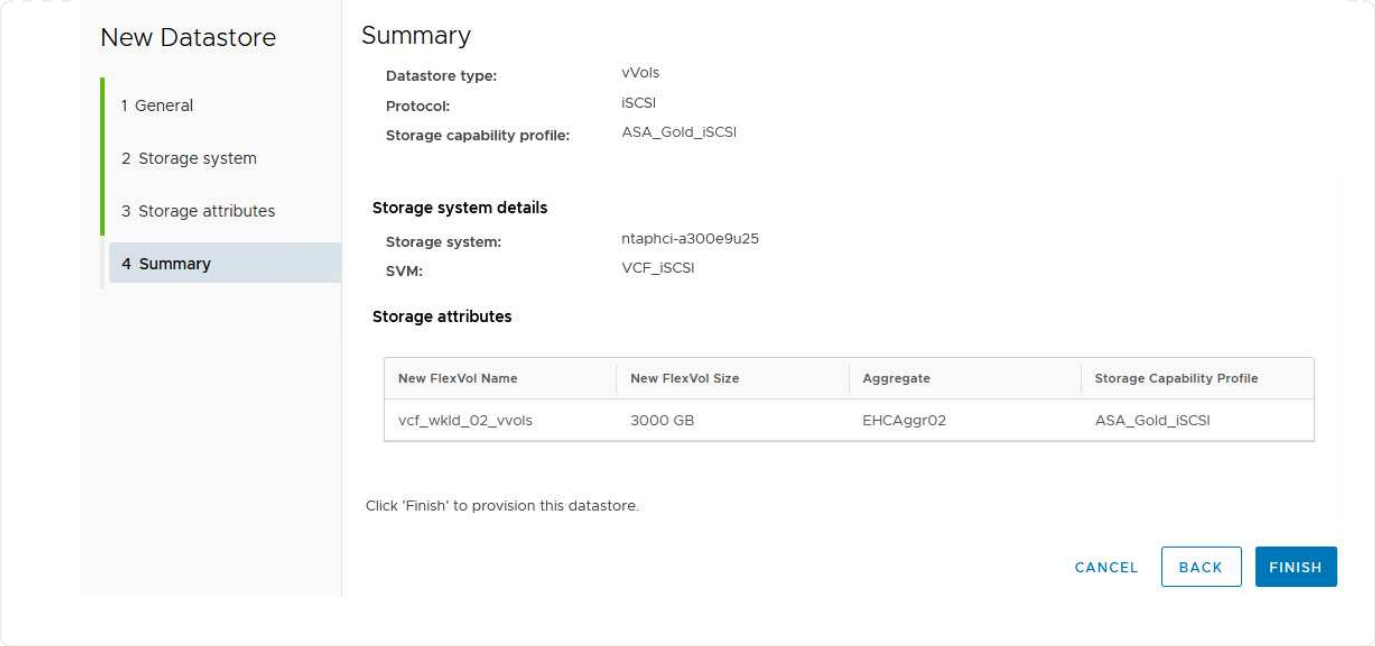
3. En la página **Sistema de almacenamiento**, seleccione un perfil de capacidad de almacenamiento, el sistema de almacenamiento y SVM. Haga clic en **Siguiente** para continuar.



4. En la página **Atributos de almacenamiento**, seleccione crear un nuevo volumen para el almacén de datos y complete los atributos de almacenamiento del volumen que se creará. Haga clic en **Agregar** para crear el volumen y luego en **Siguiente** para continuar.



5. Por último, revise el resumen y haga clic en **Finalizar** para iniciar el proceso de creación del almacén de datos vVol.



Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Agregue NFS y vVols como almacenamiento complementario a los dominios de carga de trabajo VI mediante ONTAP tools for VMware vSphere

En este caso de uso, describimos el procedimiento para utilizar ONTAP Tools for VMware para agregar almacenes de datos NFS y vVols como almacenamiento complementario para un dominio de carga de trabajo de infraestructura virtual (VI) de VMware Cloud Foundation (VCF). Este procedimiento resume la implementación de ONTAP Tools para VMware vSphere, la configuración de una máquina virtual de almacenamiento (SVM) con interfaces lógicas NFS y el aprovisionamiento de almacenes de datos NFS y vVols .

NFS se utiliza como protocolo de almacenamiento para el almacén de datos vVols .

Beneficios de NFS

Simplicidad y facilidad de uso: NFS es fácil de configurar y administrar, lo que lo convierte en una excelente opción para entornos que requieren compartir archivos de manera rápida y sencilla.

Escalabilidad: La arquitectura de ONTAP permite que NFS escale de manera eficiente, soportando las crecientes necesidades de datos sin cambios significativos en la infraestructura.

Flexibilidad: NFS admite una amplia gama de aplicaciones y cargas de trabajo, lo que lo hace versátil para diversos casos de uso, incluidos entornos virtualizados.

Para obtener más información, consulte la "Guía de referencia de NFS v3 para vSphere 8" .

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico NFS.
- Cree un grupo de puertos distribuidos para la red NFS en el dominio de carga de trabajo VI.
- Cree un adaptador vmkernel para NFS en los hosts ESXi para el dominio de carga de trabajo VI.
- Implementar herramientas ONTAP en el dominio de carga de trabajo VI.
- Cree un nuevo almacén de datos NFS en el dominio de carga de trabajo VI.
- Cree un nuevo almacén de datos vVols en el dominio de carga de trabajo VI.

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP AFF o FAS con puertos de datos físicos en conmutadores Ethernet dedicados al tráfico de almacenamiento.
- La implementación del dominio de administración de VCF está completa y el cliente vSphere es accesible.
- Previamente se ha implementado un dominio de carga de trabajo VI.

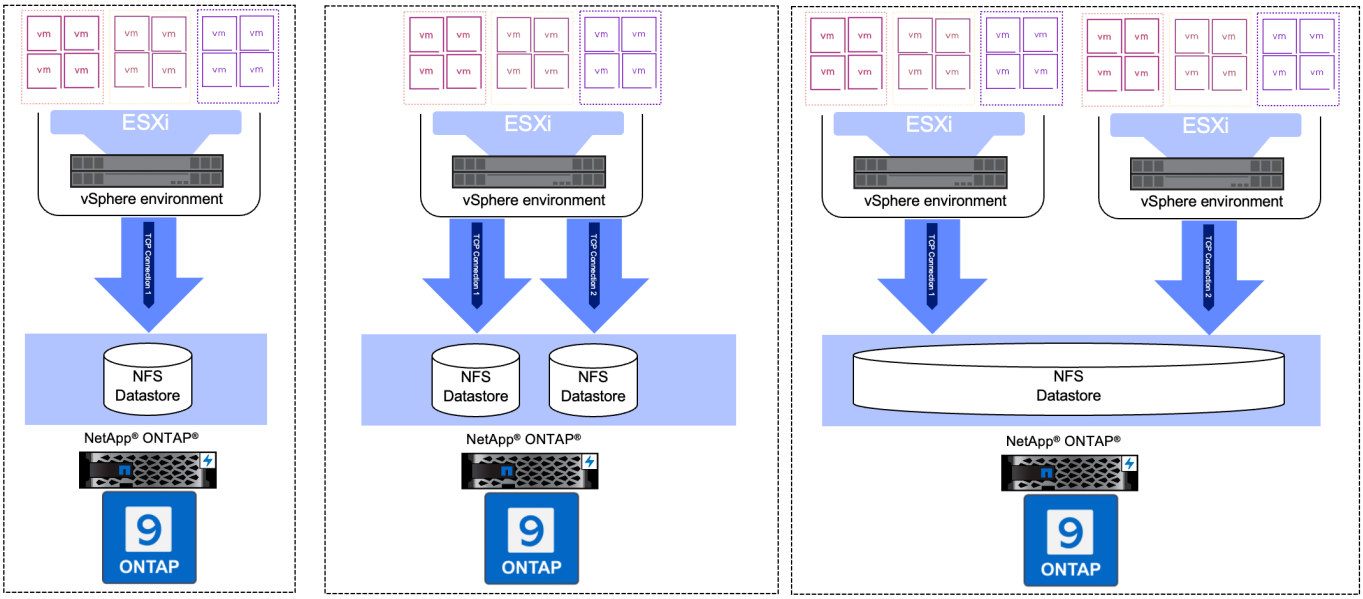
NetApp recomienda diseños de red redundantes para NFS, que brindan tolerancia a fallas para sistemas de almacenamiento, conmutadores, adaptadores de red y sistemas host. Es común implementar NFS con una sola subred o múltiples subredes según los requisitos arquitectónicos.

Referirse a "Mejores prácticas para ejecutar NFS con VMware vSphere" para obtener información detallada específica de VMware vSphere.

Para obtener orientación sobre la red acerca del uso de ONTAP con VMware vSphere, consulte la "Configuración de red - NFS" sección de la documentación de aplicaciones empresariales de NetApp .

Esta documentación demuestra el proceso de creación de una nueva SVM y la especificación de la información de la dirección IP para crear múltiples LIF para el tráfico NFS. Para agregar nuevos LIF a un SVM existente, consulte"Crear una LIF (interfaz de red)" .

Para obtener información completa sobre el uso de NFS con clústeres de vSphere, consulte la"Guía de referencia de NFS v3 para vSphere 8" .



Pasos de implementación

Para implementar ONTAP Tools y usarlo para crear un almacén de datos vVols y NFS en el dominio de administración de VCF, complete los siguientes pasos:

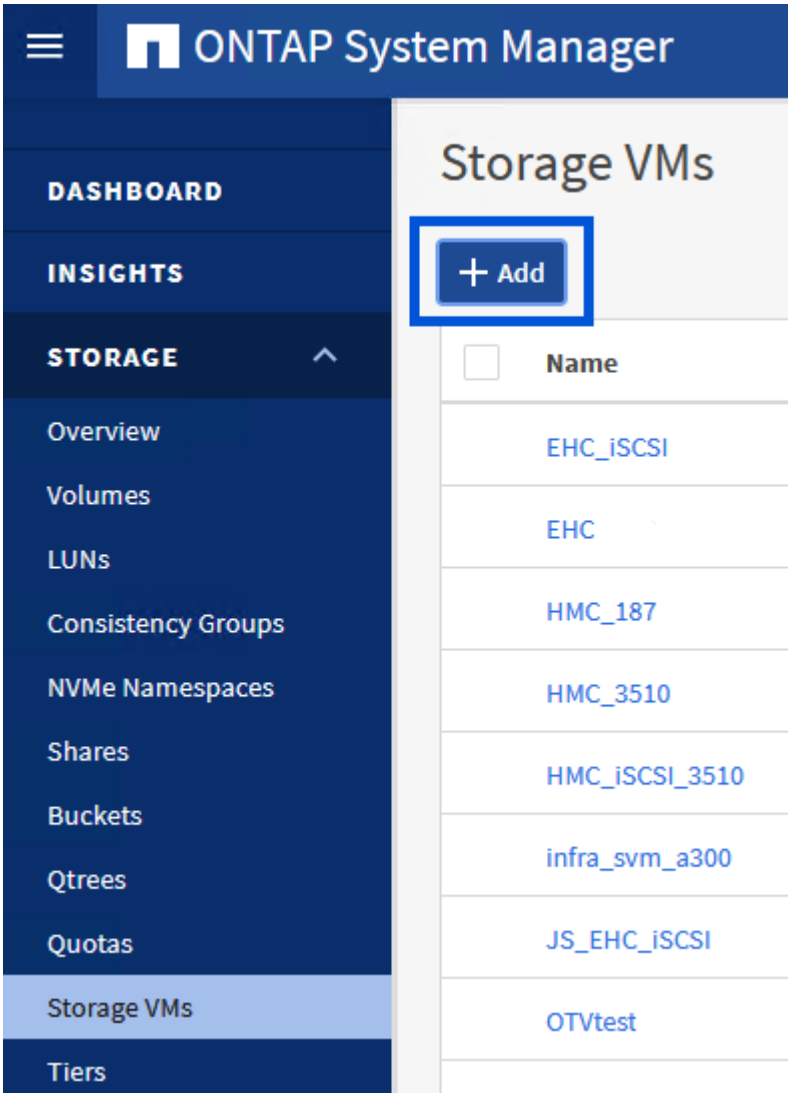
Crear SVM y LIF en el sistema de almacenamiento ONTAP

El siguiente paso se realiza en ONTAP System Manager.

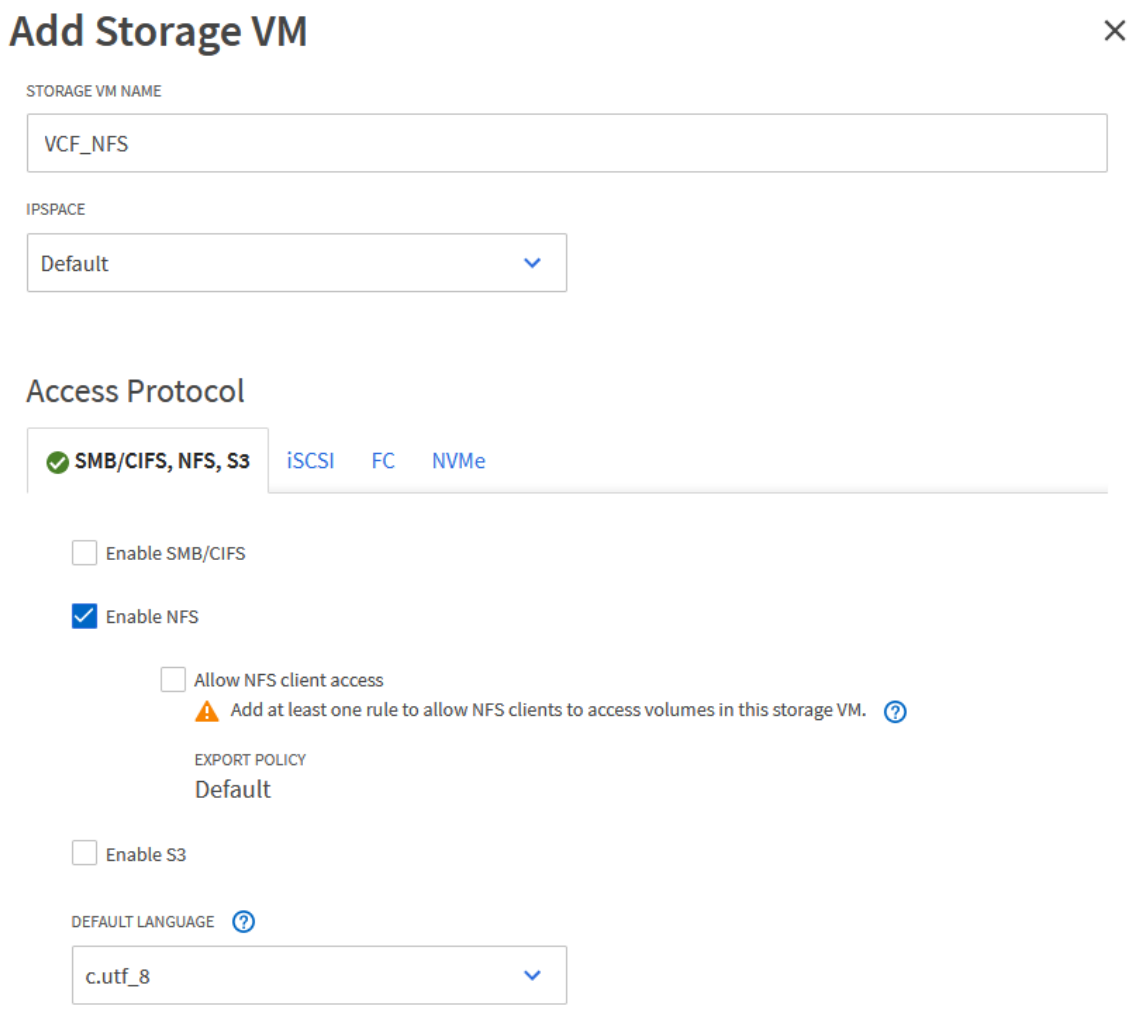
Cree la máquina virtual de almacenamiento y los LIF

Complete los siguientes pasos para crear una SVM junto con múltiples LIF para el tráfico NFS.

1. Desde el Administrador del sistema ONTAP , navegue hasta **Máquinas virtuales de almacenamiento** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.

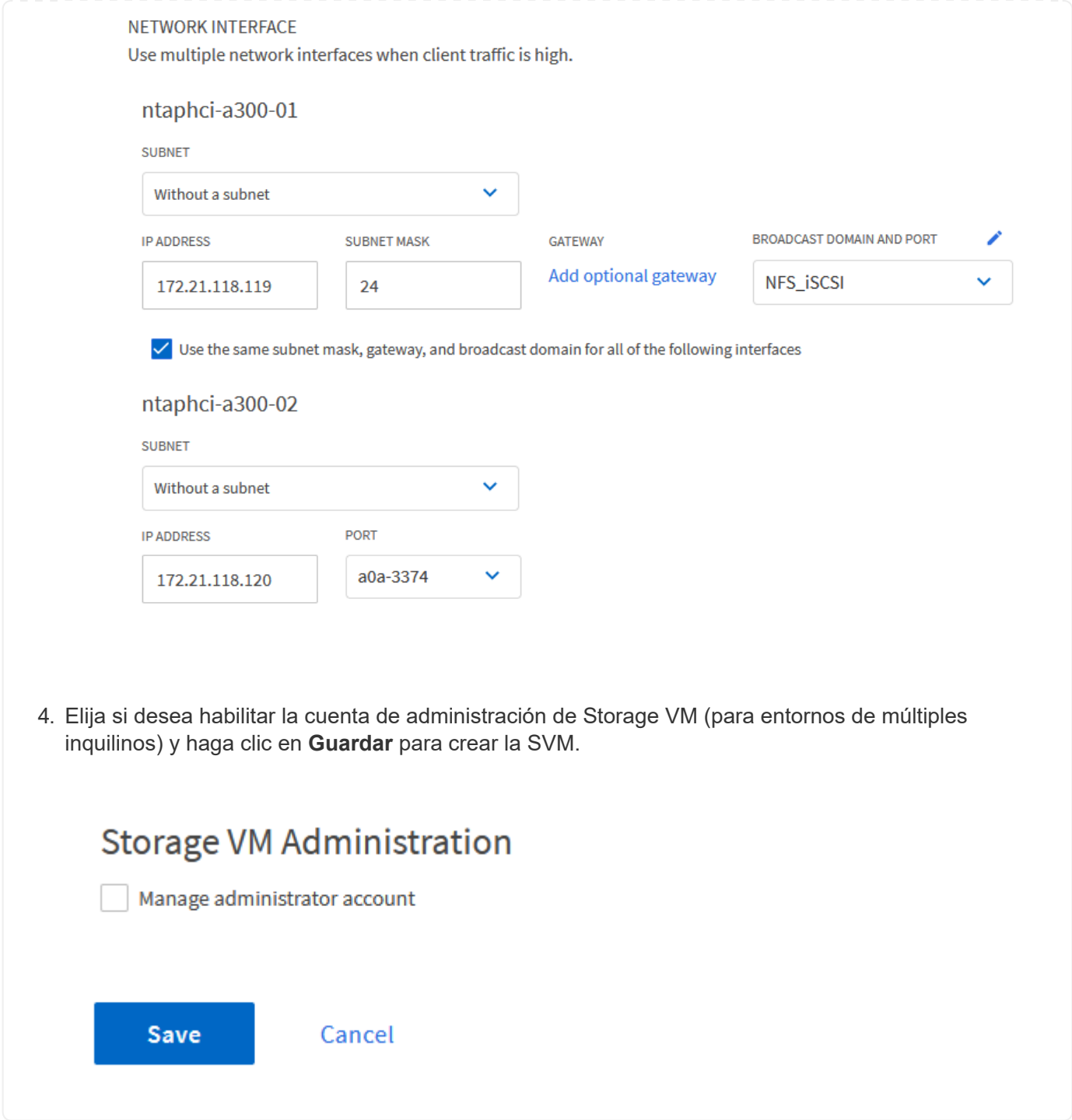


2. En el asistente **Agregar VM de almacenamiento**, proporcione un **Nombre** para la SVM, seleccione el **Espacio IP** y luego, en **Protocolo de acceso**, haga clic en la pestaña **SMB/CIFS, NFS, S3** y marque la casilla para **Habilitar NFS**.



No es necesario marcar el botón **Permitir acceso de cliente NFS** aquí, ya que Ontap Tools para VMware vSphere se utilizará para automatizar el proceso de implementación del almacén de datos. Esto incluye proporcionar acceso de cliente para los hosts ESXi. & # 160;

3. En la sección **Interfaz de red**, complete la **Dirección IP**, la **Máscara de subred** y el **Dominio de transmisión y puerto** para el primer LIF. Para los LIF posteriores, la casilla de verificación se puede habilitar para utilizar configuraciones comunes en todos los LIF restantes o utilizar configuraciones separadas.



4. Elija si desea habilitar la cuenta de administración de Storage VM (para entornos de múltiples inquilinos) y haga clic en **Guardar** para crear la SVM.

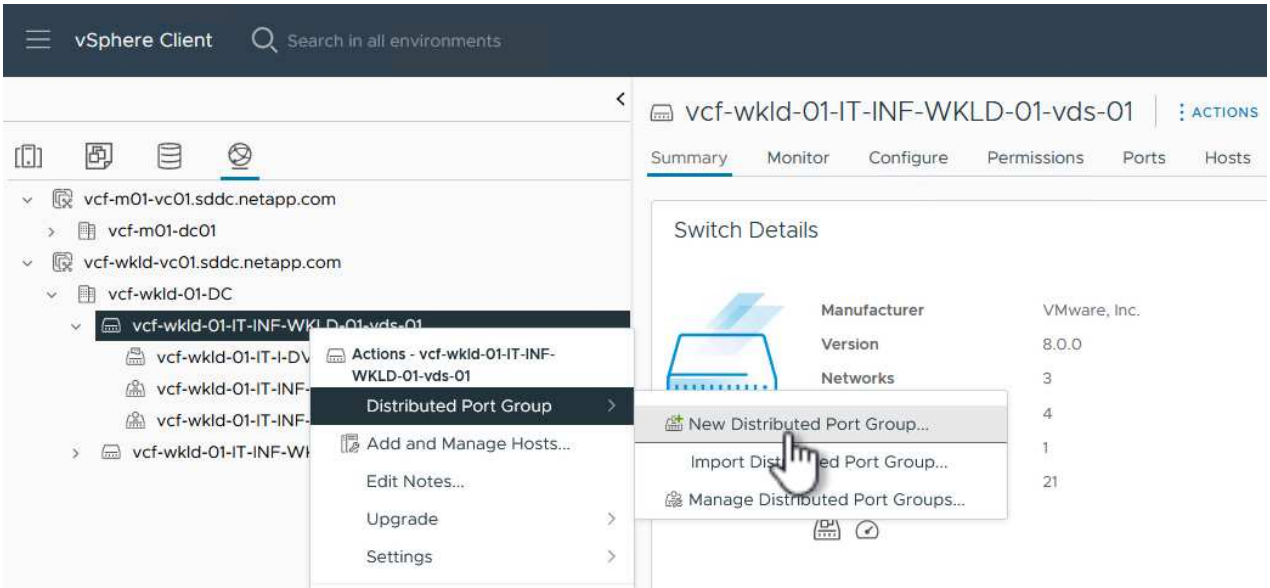
Configurar la red para NFS en hosts ESXi

Los siguientes pasos se realizan en el clúster de dominio de carga de trabajo VI mediante el cliente vSphere. En este caso, se utiliza vCenter Single Sign-On para que el cliente vSphere sea común en los dominios de administración y carga de trabajo.

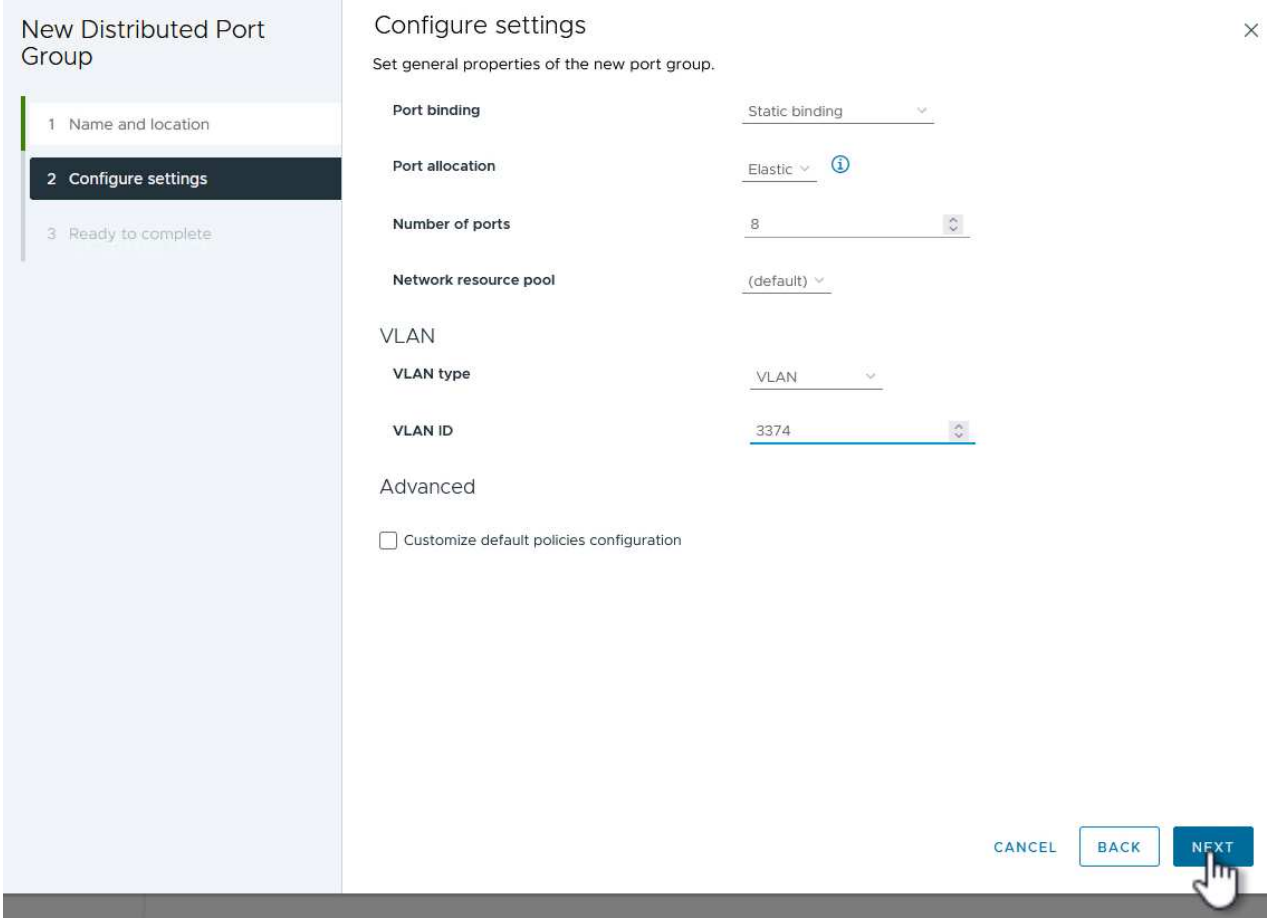
Crear un grupo de puertos distribuidos para el tráfico NFS

Complete lo siguiente para crear un nuevo grupo de puertos distribuidos para que la red transporte tráfico NFS:

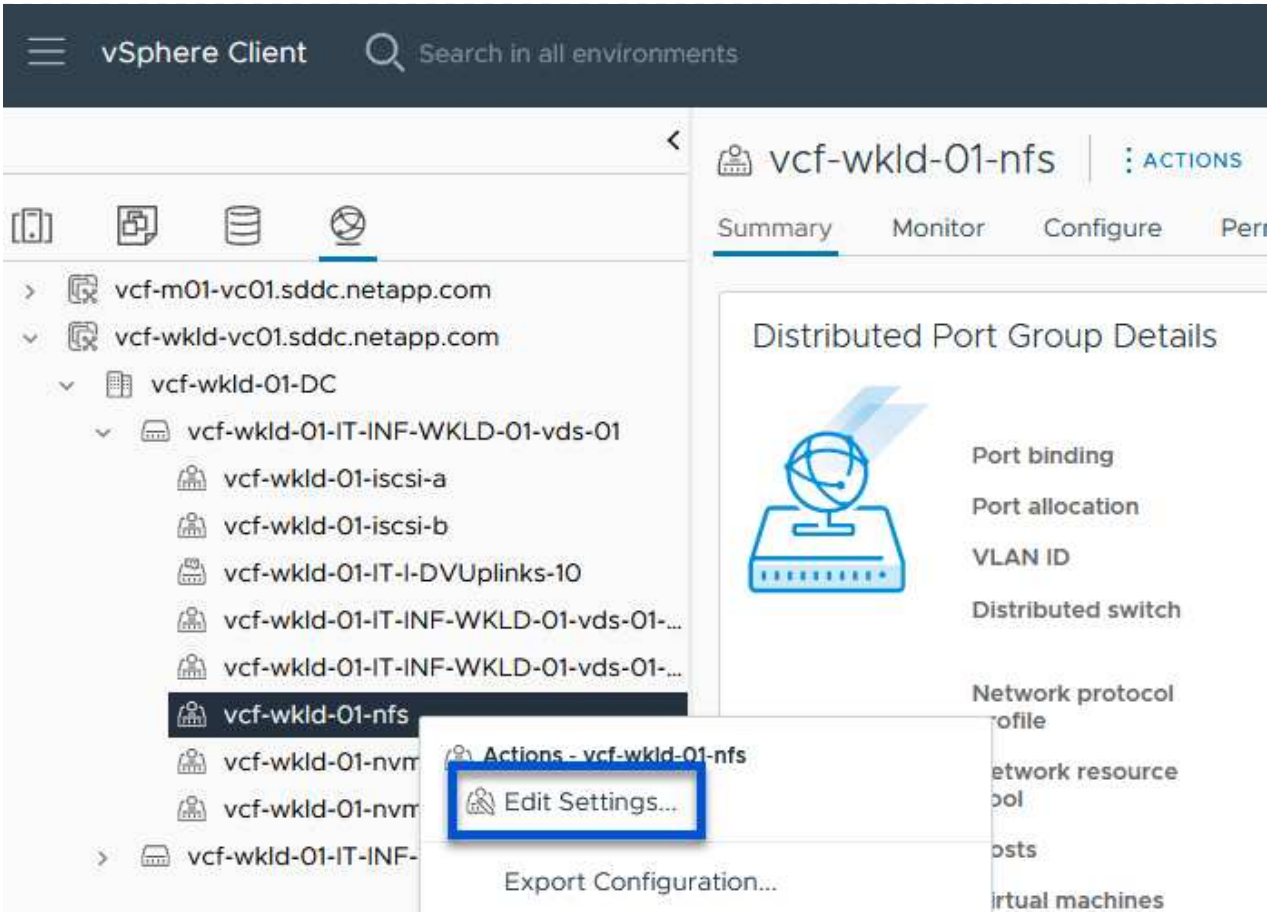
1. Desde el cliente vSphere, navegue a **Inventario > Redes** para el dominio de carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos…**.



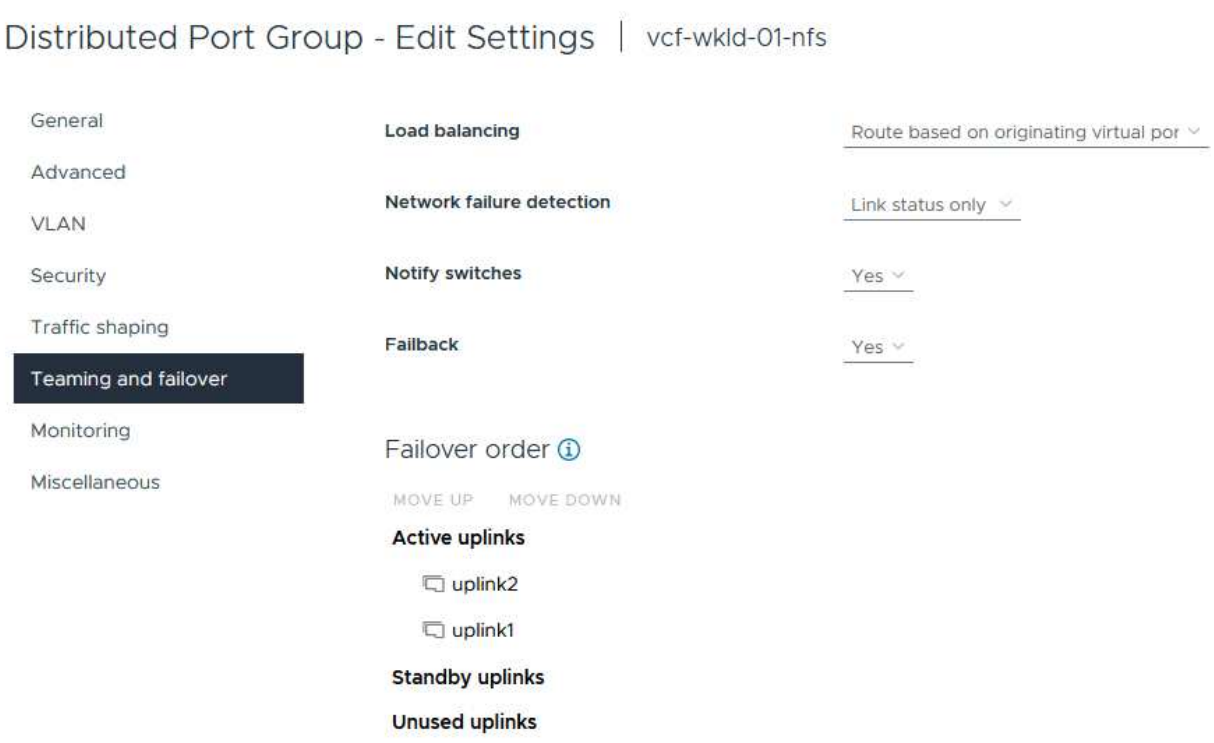
2. En el asistente **Nuevo grupo de puertos distribuidos**, complete un nombre para el nuevo grupo de puertos y haga clic en **Siguiente** para continuar.
3. En la página **Configurar ajustes** complete todas las configuraciones. Si se utilizan VLAN, asegúrese de proporcionar la ID de VLAN correcta. Haga clic en **Siguiente** para continuar.



4. En la página **Listo para completar**, revise los cambios y haga clic en **Finalizar** para crear el nuevo grupo de puertos distribuidos.
5. Una vez creado el grupo de puertos, navegue hasta el grupo de puertos y seleccione la acción **Editar configuración…**.



6. En la página **Grupo de puertos distribuidos - Editar configuración**, navegue hasta **Equipo y conmutación por error** en el menú de la izquierda. Habilite la formación de equipos para los enlaces ascendentes que se utilizarán para el tráfico NFS asegurándose de que estén juntos en el área **Enlaces ascendentes activos**. Mueva los enlaces ascendentes no utilizados a **Enlaces ascendentes no utilizados**.

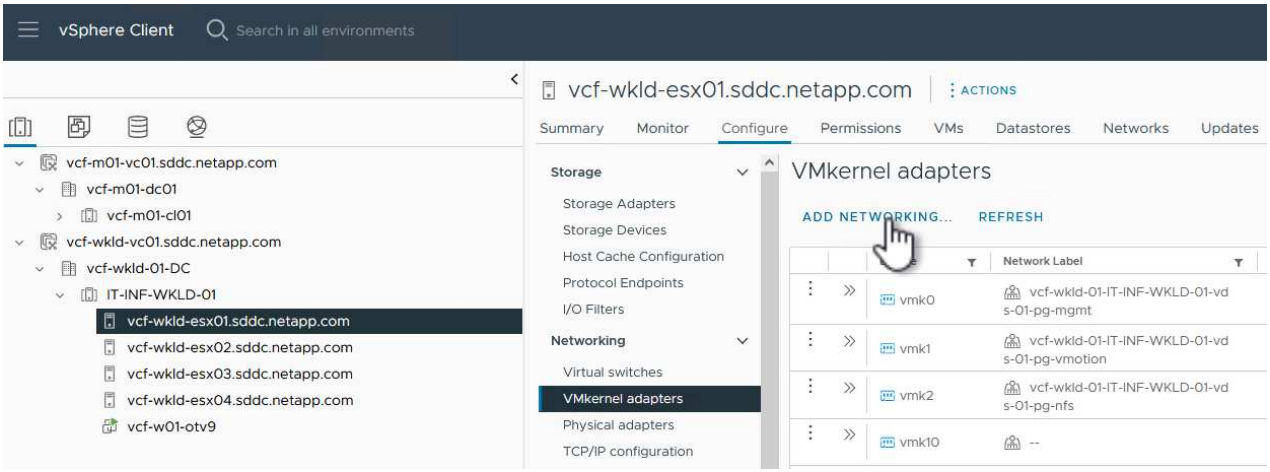


7. Repita este proceso para cada host ESXi del clúster.

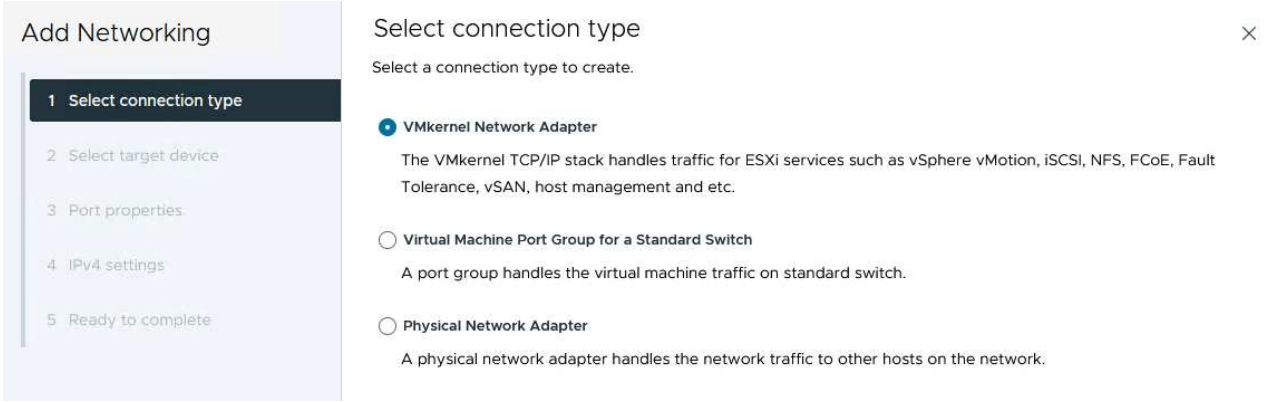
Cree un adaptador VMkernel en cada host ESXi

Repita este proceso en cada host ESXi en el dominio de carga de trabajo.

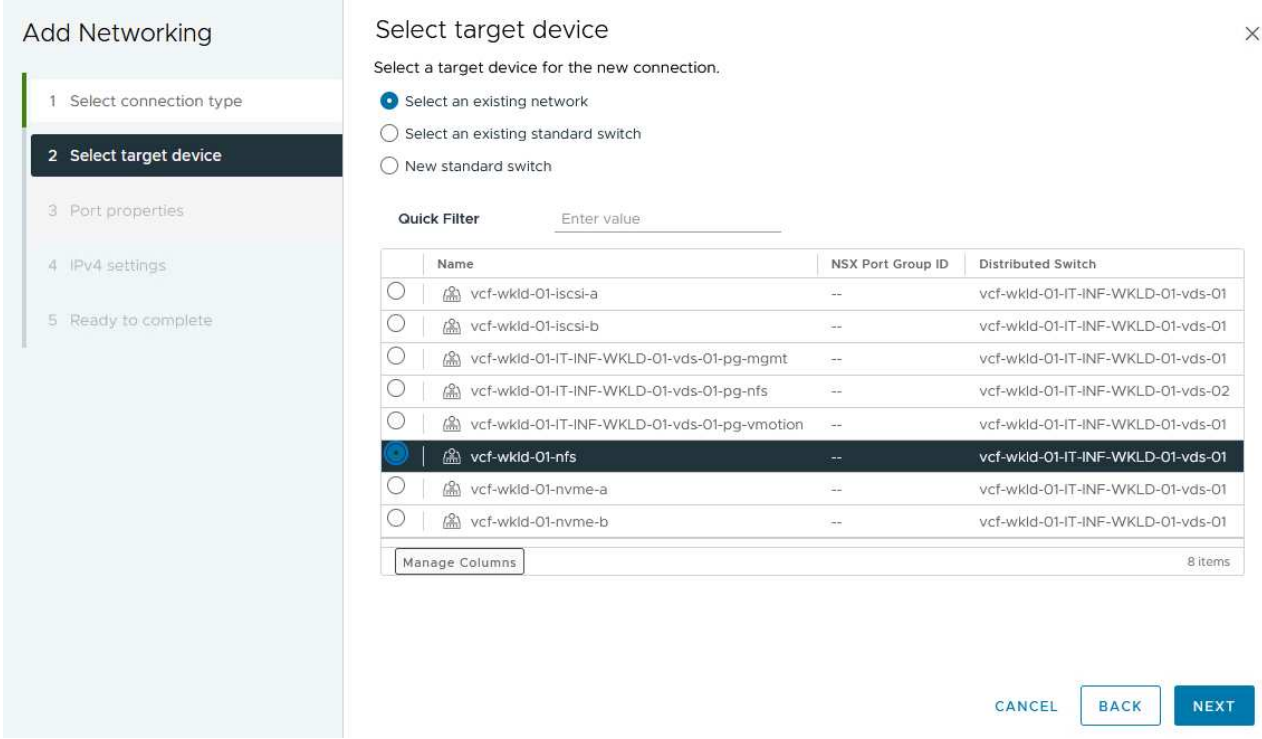
1. Desde el cliente vSphere, navegue a uno de los hosts ESXi en el inventario del dominio de carga de trabajo. Desde la pestaña **Configurar** seleccione **Adaptadores VMkernel** y haga clic en **Agregar red…** para comenzar.



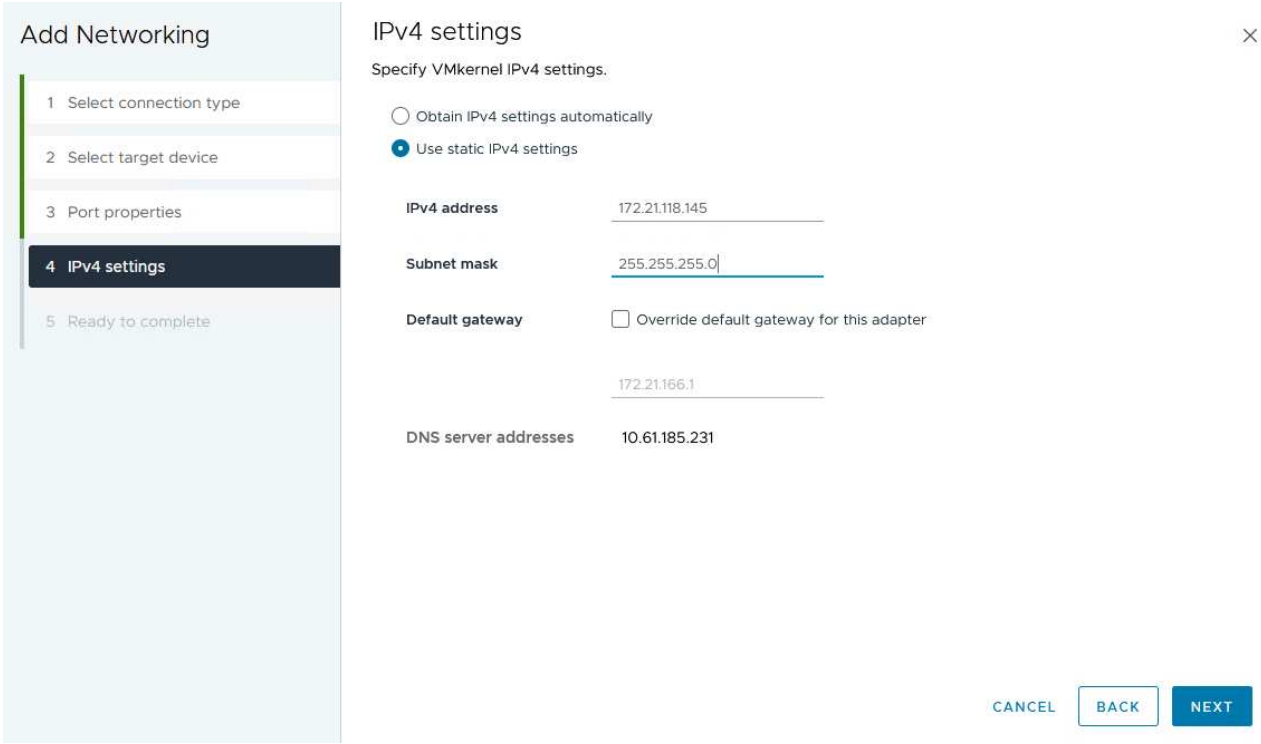
2. En la ventana **Seleccionar tipo de conexión** elija **Adaptador de red VMkernel** y haga clic en **Siguiente** para continuar.



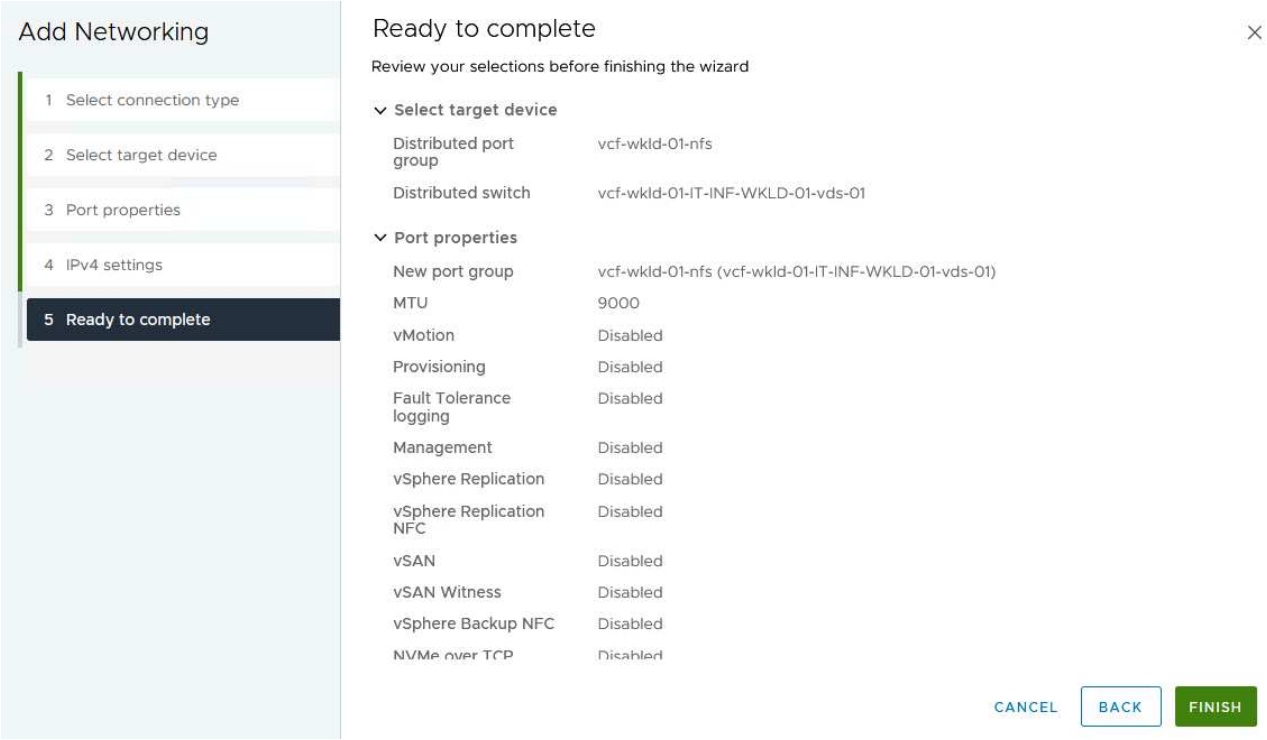
3. En la página **Seleccionar dispositivo de destino**, elija uno de los grupos de puertos distribuidos para NFS que se crearon anteriormente.



4. En la página **Propiedades del puerto** mantenga los valores predeterminados (sin servicios habilitados) y haga clic en **Siguiente** para continuar.
5. En la página de **Configuración de IPv4**, complete la **dirección IP**, la **Máscara de subred** y proporcione una nueva dirección IP de puerta de enlace (solo si es necesario). Haga clic en **Siguiente** para continuar.



6. Revise sus selecciones en la página **Listo para completar** y haga clic en **Finalizar** para crear el adaptador VMkernel.



Implementar y usar herramientas ONTAP para configurar el almacenamiento

Los siguientes pasos se realizan en el clúster de dominio de administración de VCF mediante el cliente vSphere e implican la implementación de OTV, la creación de un almacén de datos NFS vVols y la migración de las máquinas virtuales de administración al nuevo almacén de datos.

Para los dominios de carga de trabajo VI, OTV se instala en el clúster de administración de VCF, pero se registra en el vCenter asociado con el dominio de carga de trabajo VI.

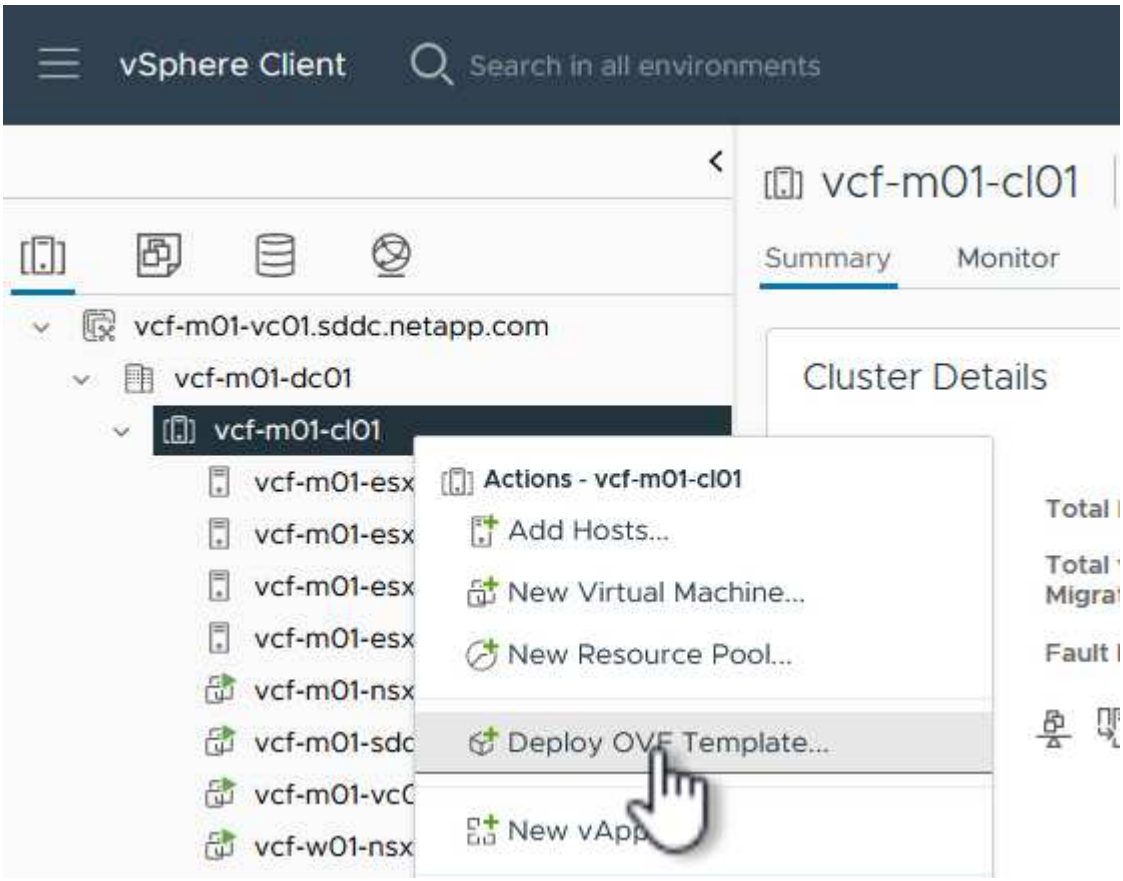
Para obtener información adicional sobre la implementación y el uso de herramientas ONTAP en un entorno de varios vCenter, consulte"Requisitos para registrar herramientas ONTAP en entornos de múltiples servidores vCenter" .

Implementar ONTAP tools for VMware vSphere

Las ONTAP tools for VMware vSphere (OTV) se implementan como un dispositivo de VM y proporcionan una interfaz de usuario vCenter integrada para administrar el almacenamiento de ONTAP .

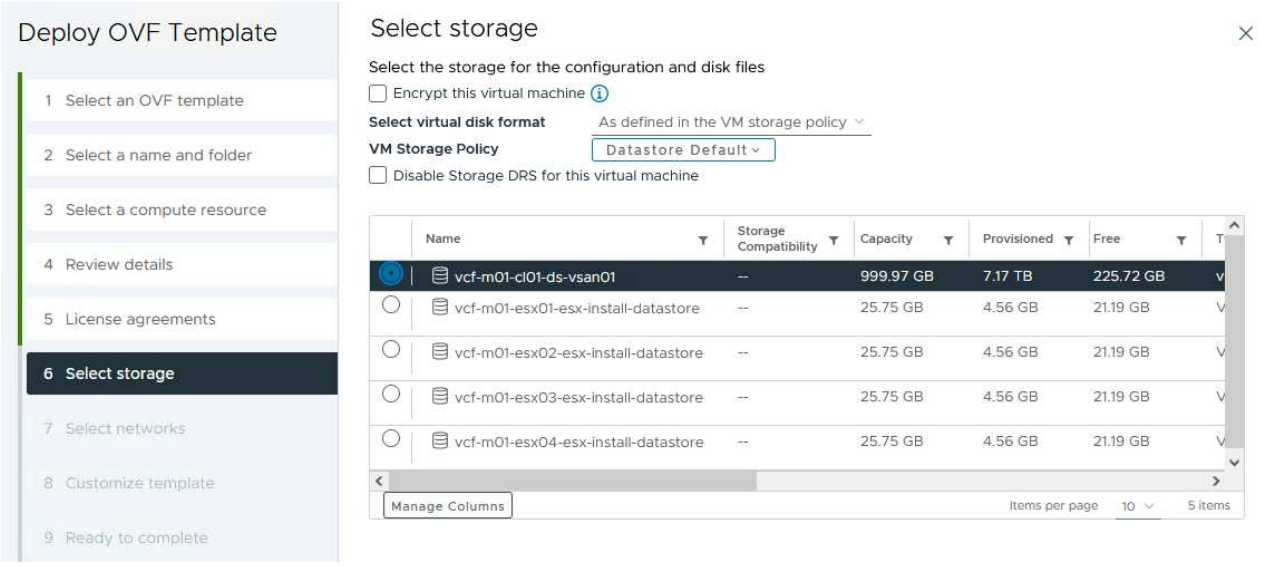
Complete lo siguiente para implementar ONTAP tools for VMware vSphere:

1. Obtenga la imagen OVA de las herramientas ONTAP desde"Sitio de soporte de NetApp" y descargar a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de administración de VCF.
3. Desde la interfaz del dispositivo vCenter, haga clic con el botón derecho en el clúster de administración y seleccione **Implementar plantilla OVF…**

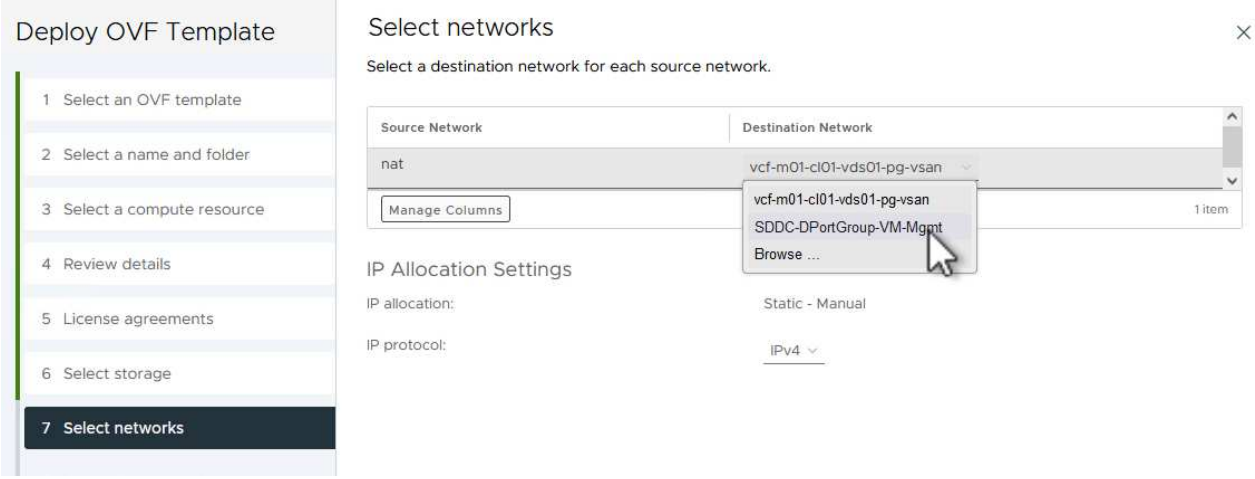


4. En el asistente **Implementar plantilla OVF**, haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de las herramientas ONTAP descargado en el paso anterior.

5. Para los pasos 2 a 5 del asistente, seleccione un nombre y una carpeta para la máquina virtual, seleccione el recurso computacional, revise los detalles y acepte el acuerdo de licencia.
6. Para la ubicación de almacenamiento de los archivos de configuración y de disco, seleccione el almacén de datos vSAN del clúster de dominio de administración de VCF.

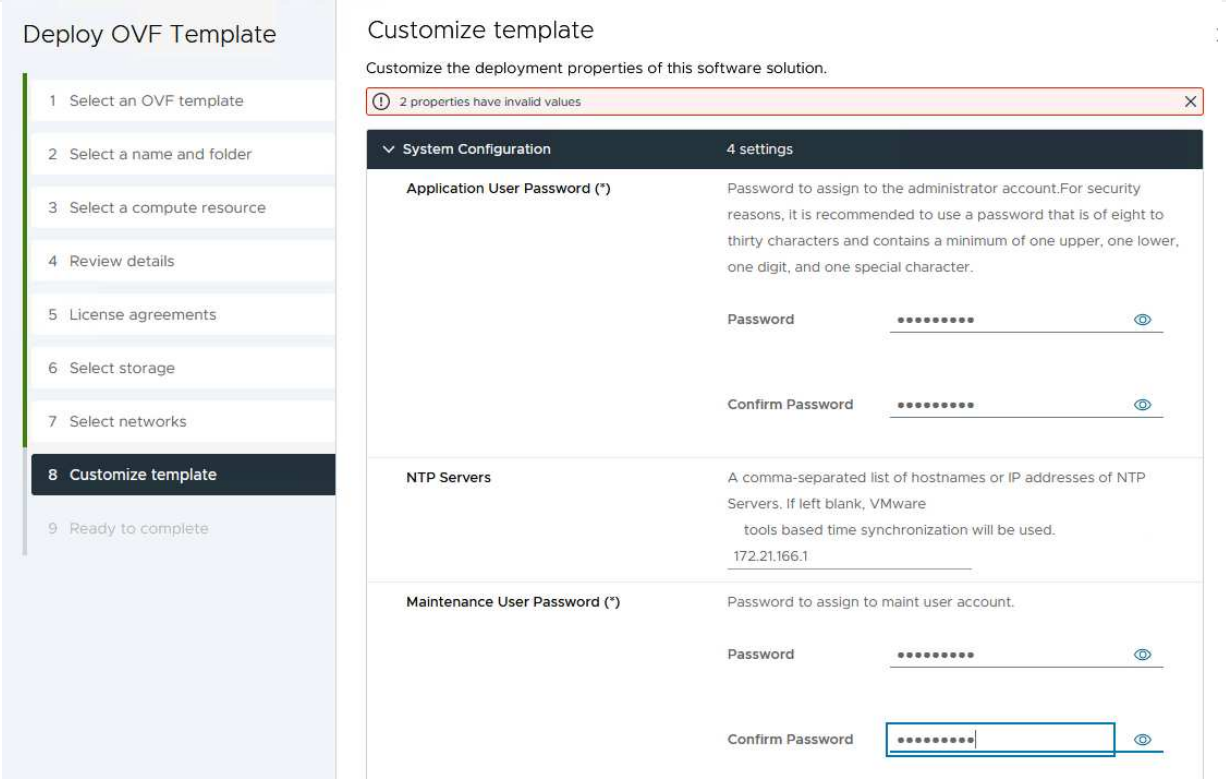


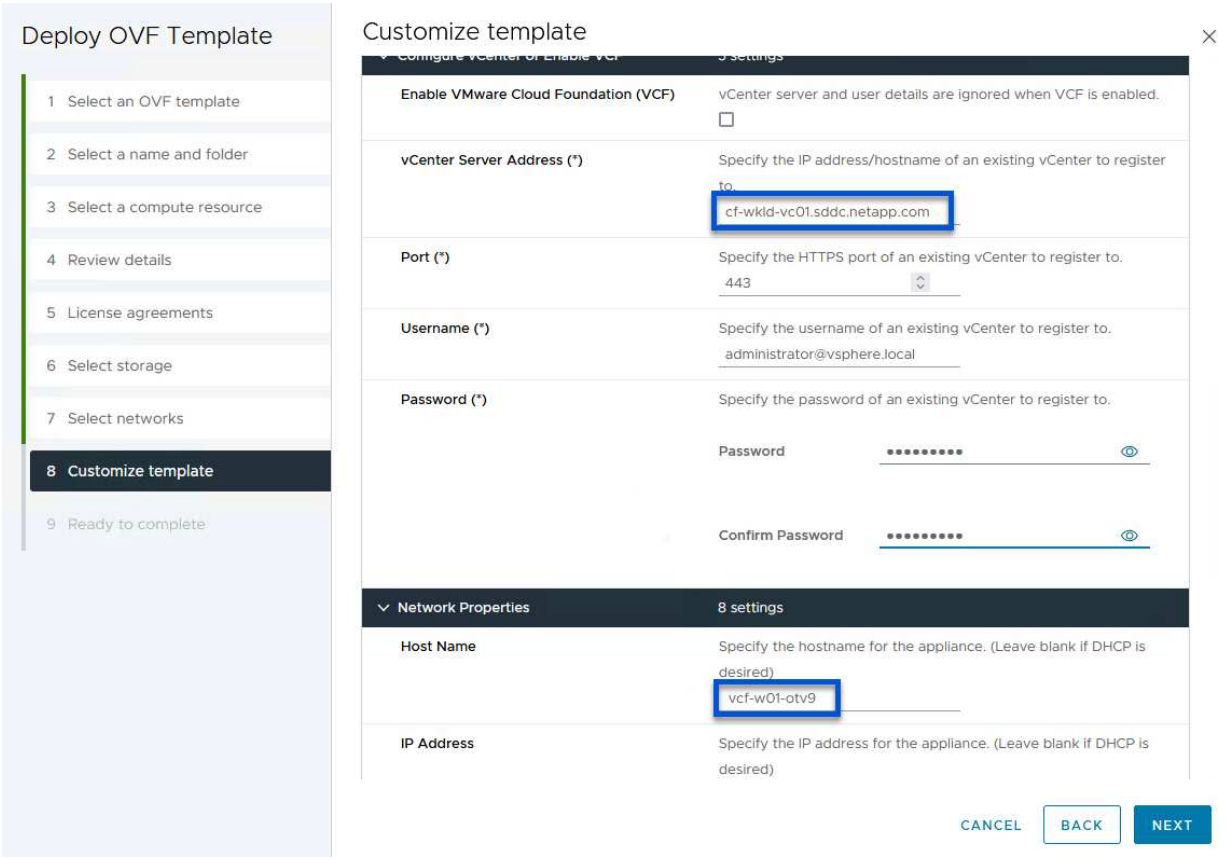
7. En la página Seleccionar red, seleccione la red utilizada para administrar el tráfico.



8. En la página Personalizar plantilla, complete toda la información requerida:
   - Contraseña que se utilizará para el acceso administrativo a OTV.
   - Dirección IP del servidor NTP.
   - Contraseña de la cuenta de mantenimiento de OTV.
   - Contraseña de OTV Derby DB.
   - No marque la casilla para **Habilitar VMware Cloud Foundation (VCF)**. El modo VCF no es necesario para implementar almacenamiento complementario.
   - FQDN o dirección IP del dispositivo vCenter para el **VI Workload Domain**
   - Credenciales para el dispositivo vCenter del **VI Workload Domain**
   - Proporcione los campos de propiedades de red requeridos.

     Haga clic en **Siguiente** para continuar.

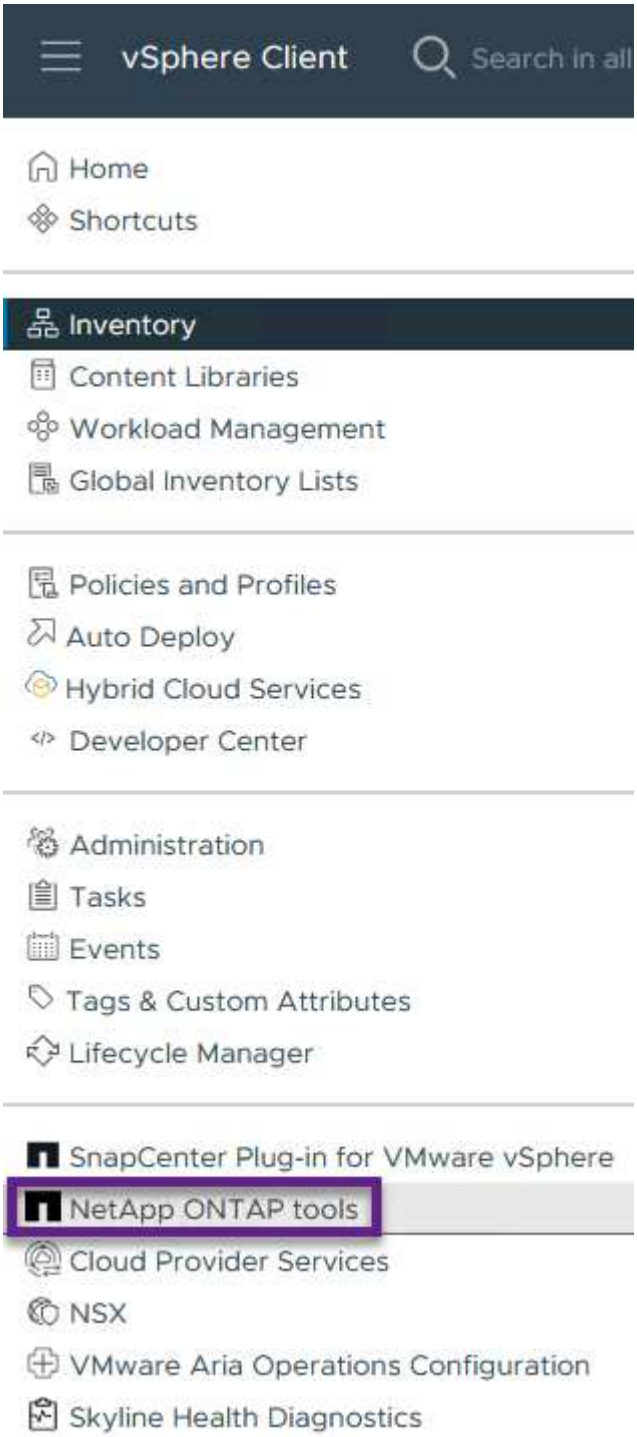




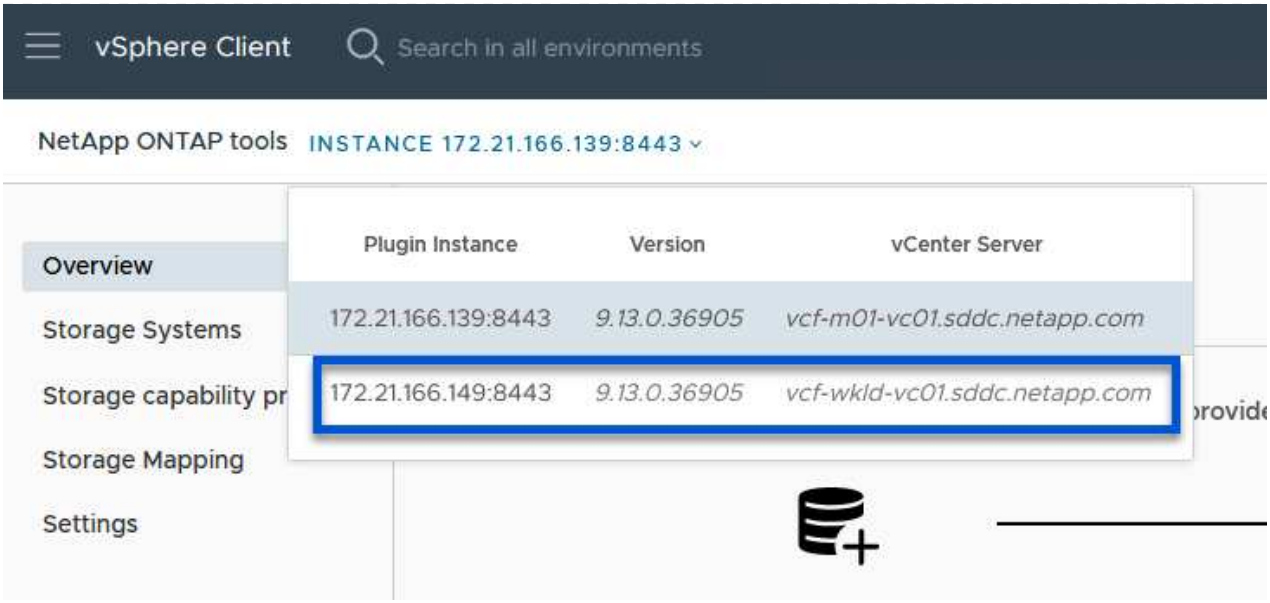
9. Revise toda la información en la página Listo para completar y haga clic en Finalizar para comenzar a implementar el dispositivo OTV.

Agregue un sistema de almacenamiento a ONTAP Tools.

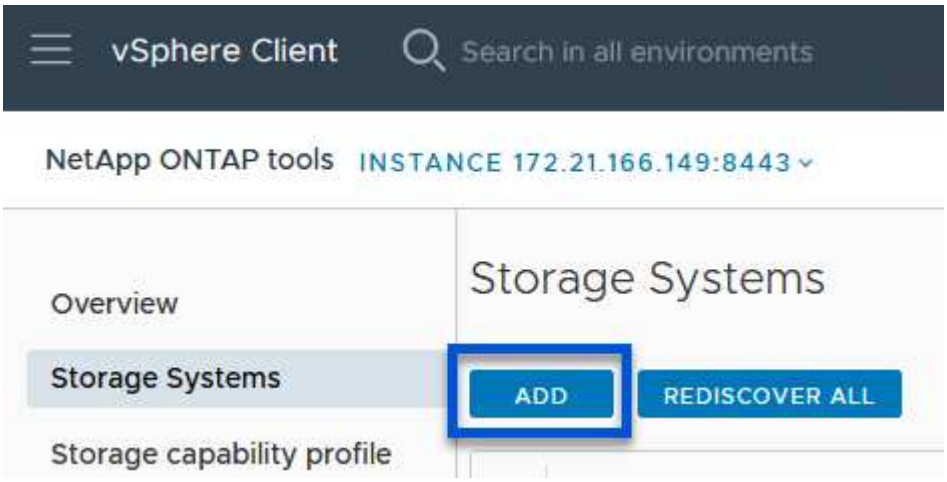
1. Acceda a las herramientas de NetApp ONTAP seleccionándolas en el menú principal en el cliente vSphere.



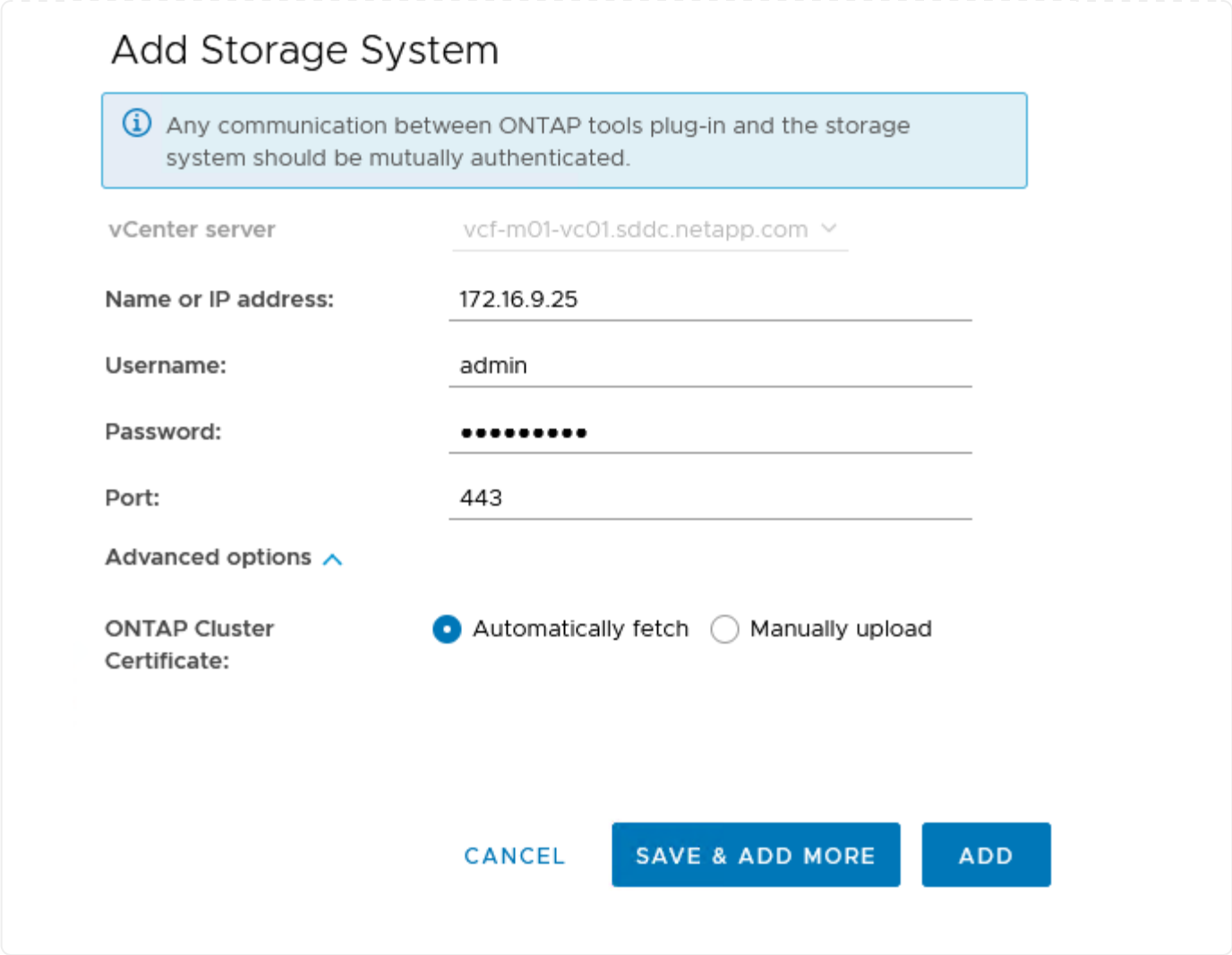
2. Desde el menú desplegable **INSTANCIA** en la interfaz de la herramienta ONTAP , seleccione la instancia de OTV asociada con el dominio de carga de trabajo que se administrará.



3. En Herramientas de ONTAP , seleccione **Sistemas de almacenamiento** en el menú de la izquierda y luego presione **Agregar**.



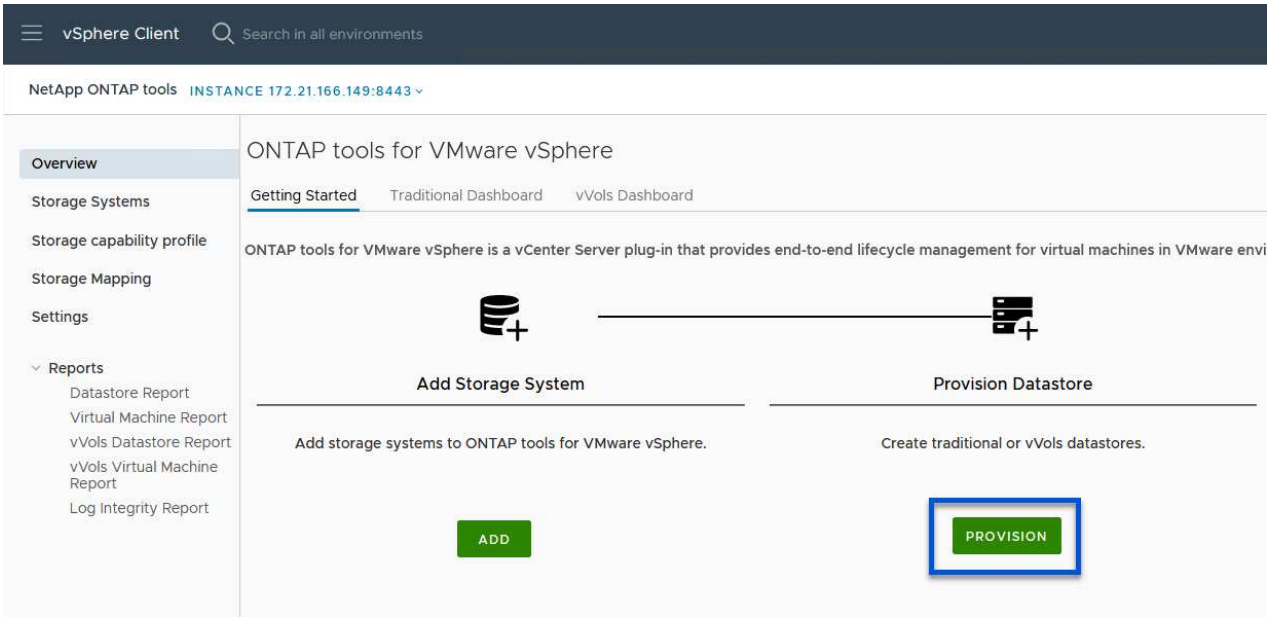
4. Complete la dirección IP, las credenciales del sistema de almacenamiento y el número de puerto. Haga clic en **Agregar** para iniciar el proceso de descubrimiento.


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Crear un almacén de datos NFS en ONTAP Tools

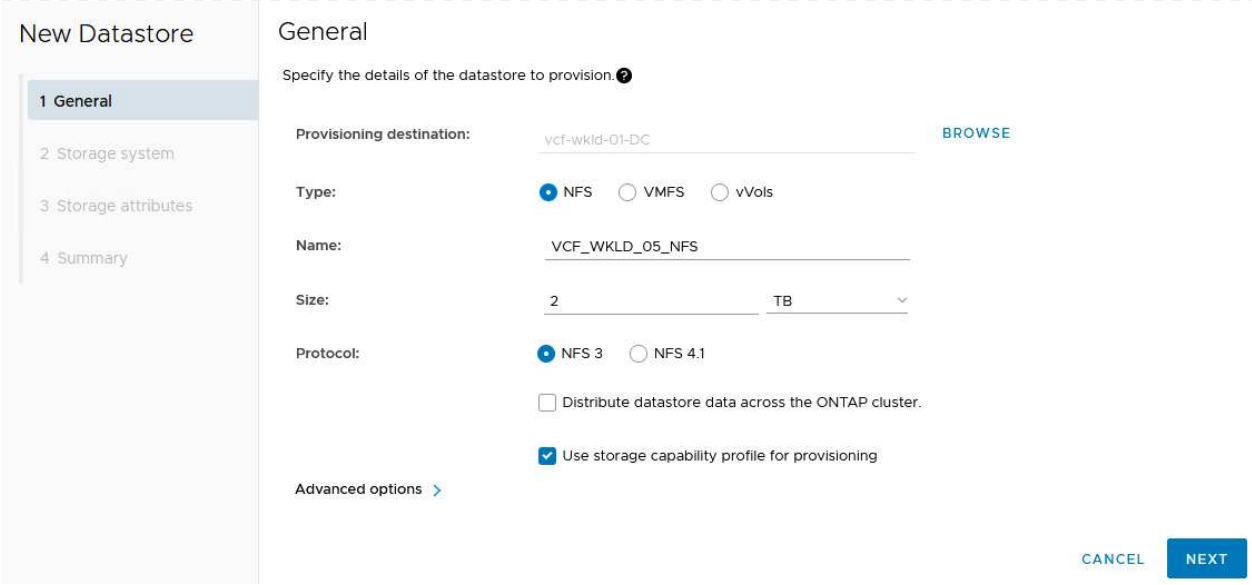
Complete los siguientes pasos para implementar un almacén de datos ONTAP , que se ejecuta en NFS, utilizando las herramientas ONTAP .

1. En Herramientas de ONTAP , seleccione **Descripción general** y en la pestaña **Introducción** haga clic en **Aprovisionamiento** para iniciar el asistente.

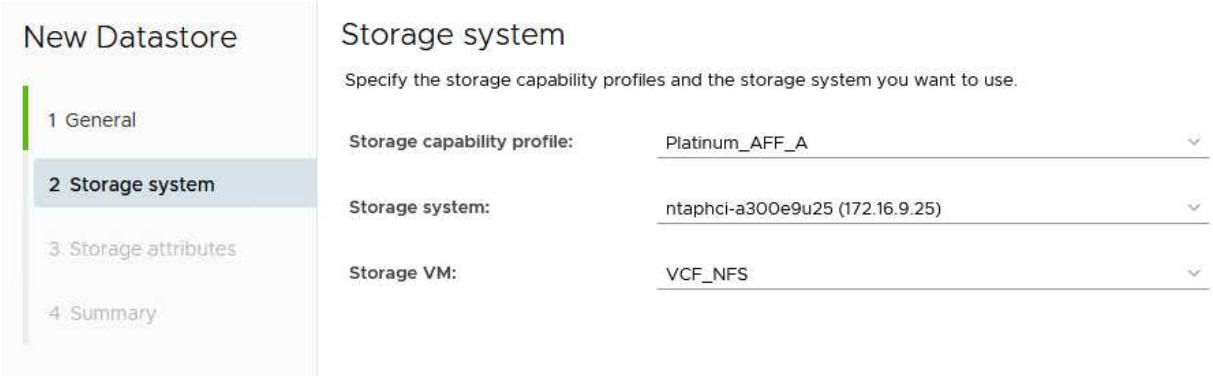


2. En la página **General** del asistente Nuevo almacén de datos, seleccione el centro de datos o el destino del clúster de vSphere. Seleccione **NFS** como tipo de almacén de datos, complete un nombre para el almacén de datos y seleccione el protocolo. Elija si desea utilizar volúmenes FlexGroup y si desea utilizar un archivo de capacidad de almacenamiento para el aprovisionamiento. Haga clic en **Siguiente** para continuar.

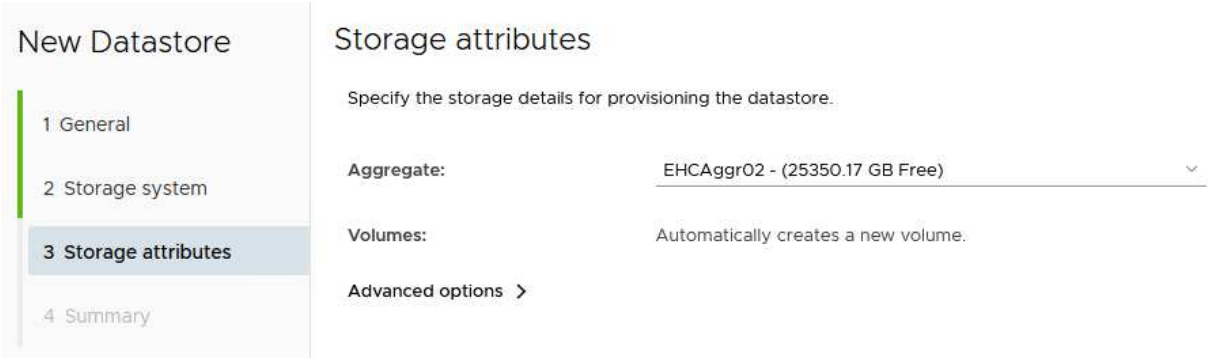
   Nota: Si selecciona **Distribuir los datos del almacén de datos en todo el clúster**, el volumen subyacente se creará como un volumen FlexGroup , lo que impide el uso de perfiles de capacidad de almacenamiento. Referirse a "Configuraciones compatibles y no compatibles con volúmenes FlexGroup" para obtener más información sobre el uso de volúmenes FlexGroup .



3. En la página **Sistema de almacenamiento**, seleccione un perfil de capacidad de almacenamiento, el sistema de almacenamiento y SVM. Haga clic en **Siguiente** para continuar.

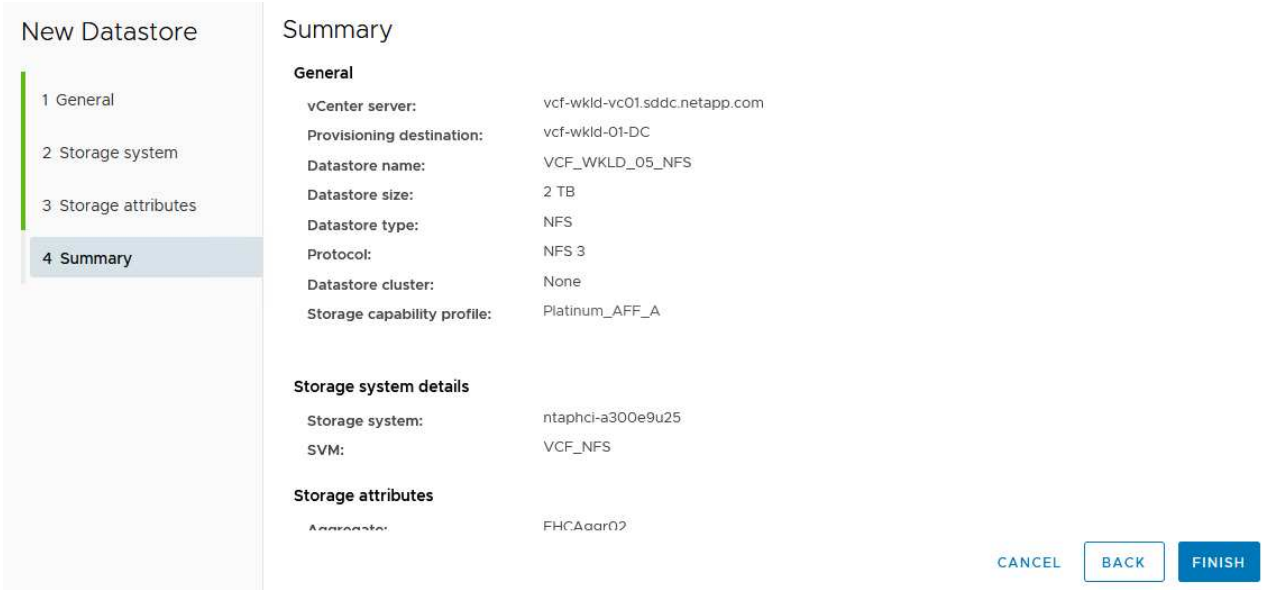


4. En la página **Atributos de almacenamiento** seleccione el agregado a utilizar y luego haga clic en **Siguiente** para continuar.



5. Por último, revise el **Resumen** y haga clic en Finalizar para comenzar a crear el almacén de datos

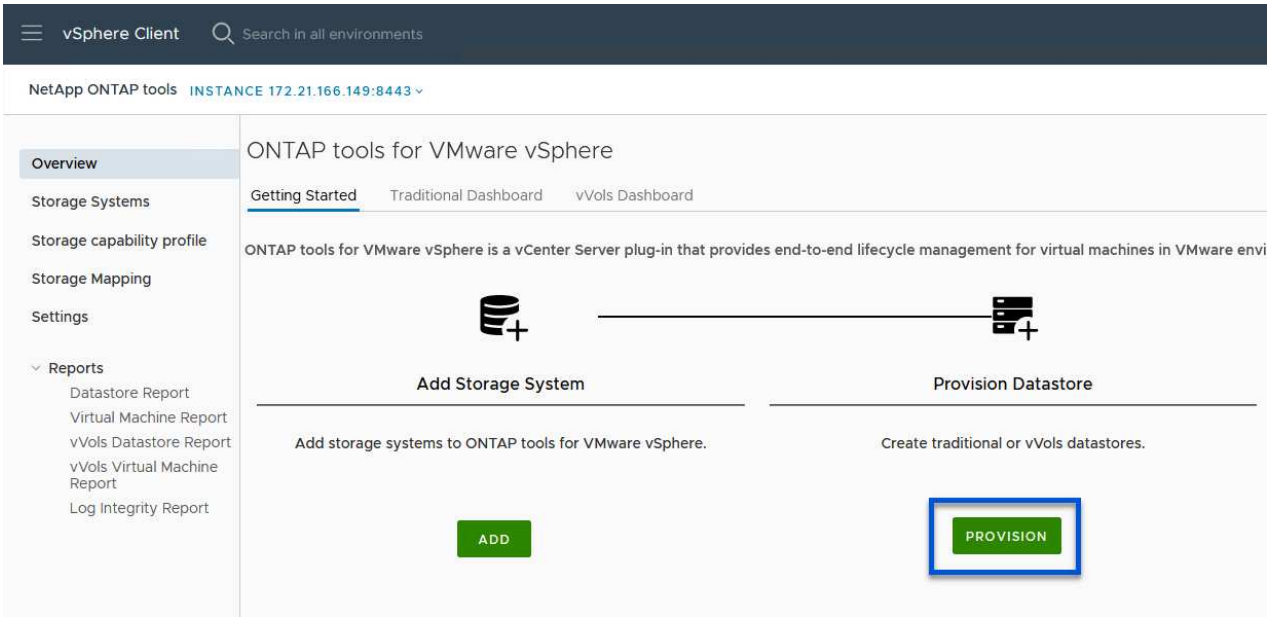
NFS.


New Datastore
1 General
2 Storage system
3 Storage attributes
4 Summary
Summary
General
vCenter server: vcf-wkld-vc01.sddc.netapp.com
Provisioning destination: vcf-wkld-01-DC
Datastore name: VCF_WKLD_05_NFS
Datastore size: 2 TB
Datastore type: NFS
Protocol: NFS 3
Datastore cluster: None
Storage capability profile: Platinum_AFF_A
Storage system details
Storage system: ntaphci-a300e9u25
SVM: VCF_NFS
Storage attributes
CANCEL
BACK
FINISH

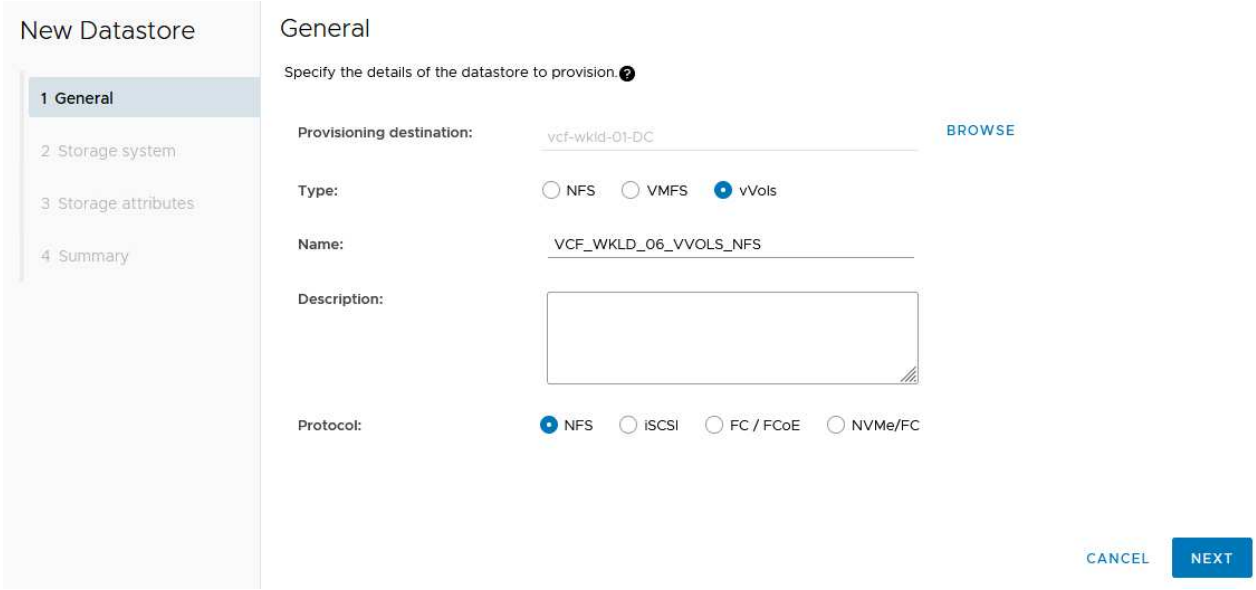
Crear un almacén de datos vVols en ONTAP Tools

Para crear un almacén de datos vVols en ONTAP Tools, complete los siguientes pasos:

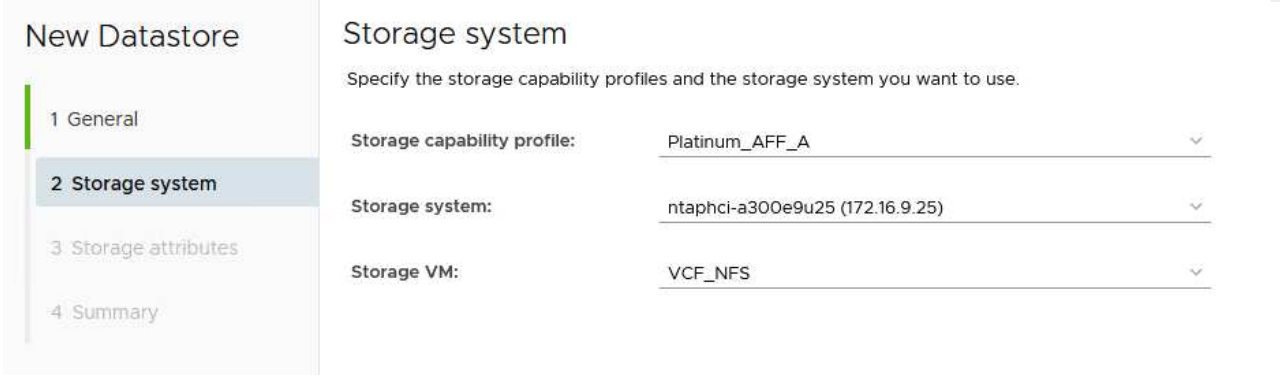
1. En Herramientas de ONTAP , seleccione **Descripción general** y en la pestaña **Introducción** haga clic en **Aprovisionamiento** para iniciar el asistente.



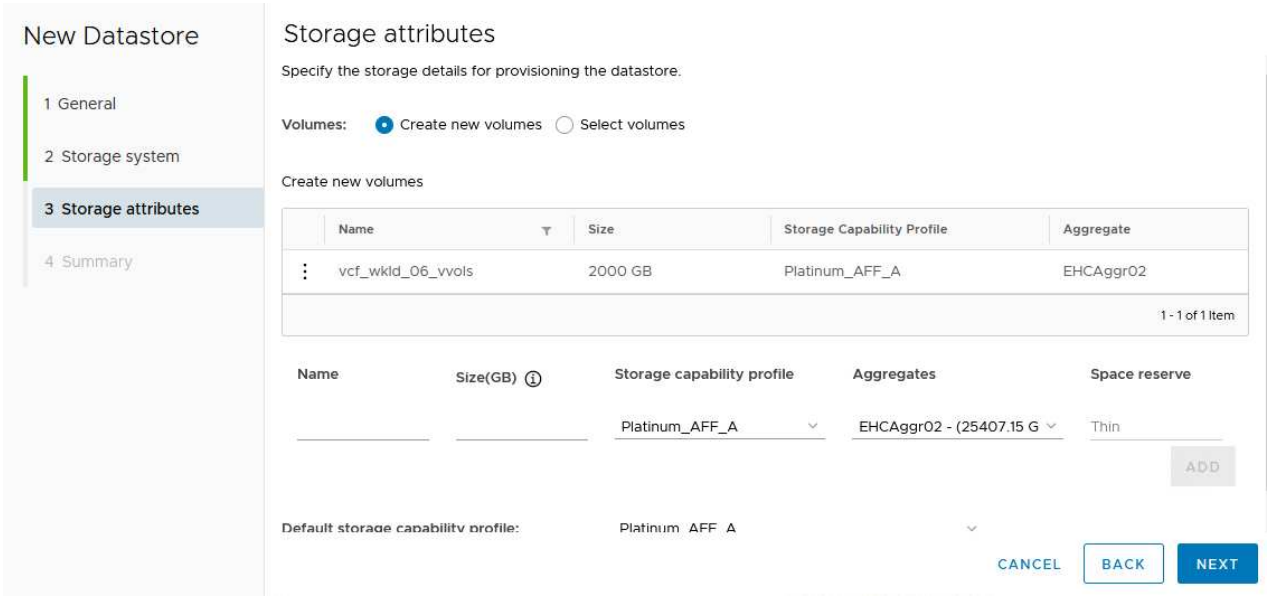
2. En la página **General** del asistente Nuevo almacén de datos, seleccione el centro de datos o el destino del clúster de vSphere. Seleccione * vVols* como el tipo de almacén de datos, complete un nombre para el almacén de datos y seleccione **NFS** como protocolo. Haga clic en **Siguiente** para continuar.



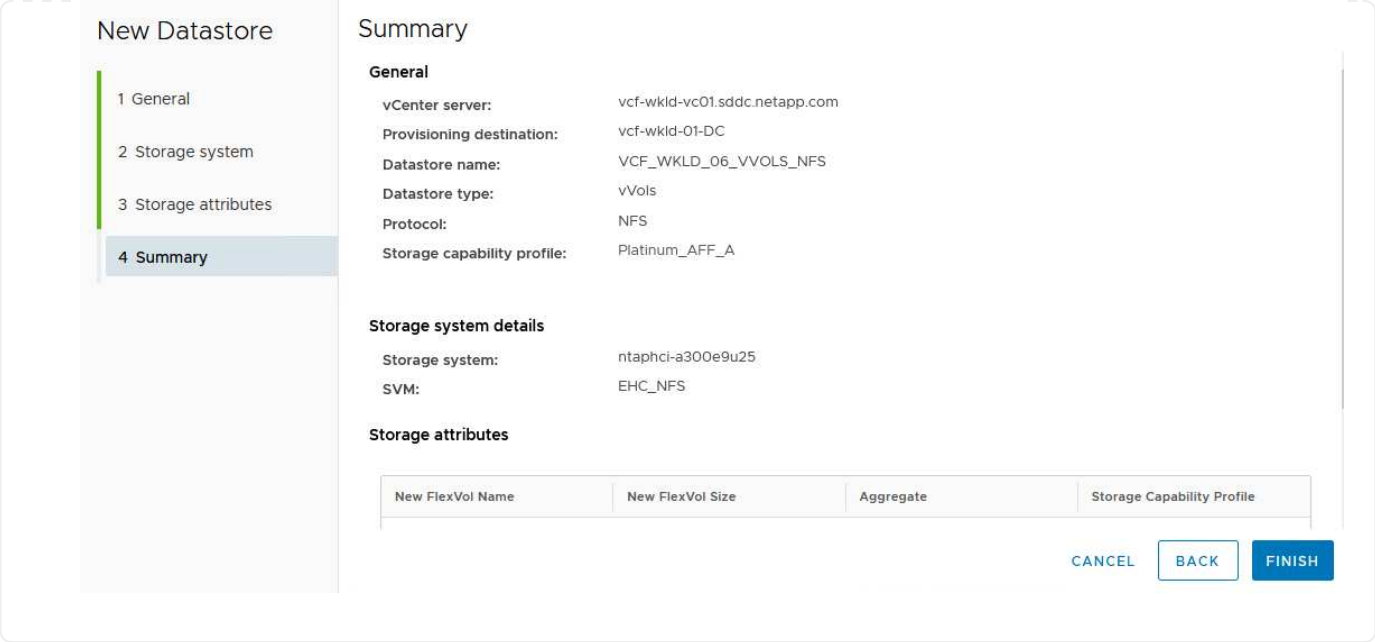
3. En la página **Sistema de almacenamiento**, seleccione un perfil de capacidad de almacenamiento, el sistema de almacenamiento y SVM. Haga clic en **Siguiente** para continuar.



4. En la página **Atributos de almacenamiento**, seleccione crear un nuevo volumen para el almacén de datos y complete los atributos de almacenamiento del volumen que se creará. Haga clic en **Agregar** para crear el volumen y luego en **Siguiente** para continuar.



5. Por último, revise el **Resumen** y haga clic en **Finalizar** para iniciar el proceso de creación del almacén de datos vVol.



Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Agregue NVMe sobre TCP como almacenamiento complementario a los dominios de carga de trabajo de VI

En este caso de uso, describimos el procedimiento para utilizar ONTAP Tools for VMware para configurar NVMe sobre TCP (NVMe/TCP) como almacenamiento complementario para un dominio de carga de trabajo de infraestructura virtual (VI) de VMware Cloud Foundation (VCF). Este procedimiento resume la configuración de una máquina virtual de almacenamiento (SVM) habilitada para NVMe/TCP, la creación de espacios de nombres NVMe, la configuración de la red del host ESXi y la implementación de un almacén de datos VMFS.

Beneficios de NVMe sobre TCP

Alto rendimiento: Ofrece un rendimiento excepcional con baja latencia y altas tasas de transferencia de datos. Esto es crucial para aplicaciones exigentes y operaciones de datos a gran escala.

Escalabilidad: Admite configuraciones escalables, lo que permite a los administradores de TI expandir su infraestructura sin problemas a medida que crecen los requisitos de datos.

Rentable: Se ejecuta a través de conmutadores Ethernet estándar y está encapsulado dentro de datagramas TCP. No se requiere equipo especial para implementarlo.

Para obtener más información sobre los beneficios de NVMe, consulte "¿Qué es NVME?"

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

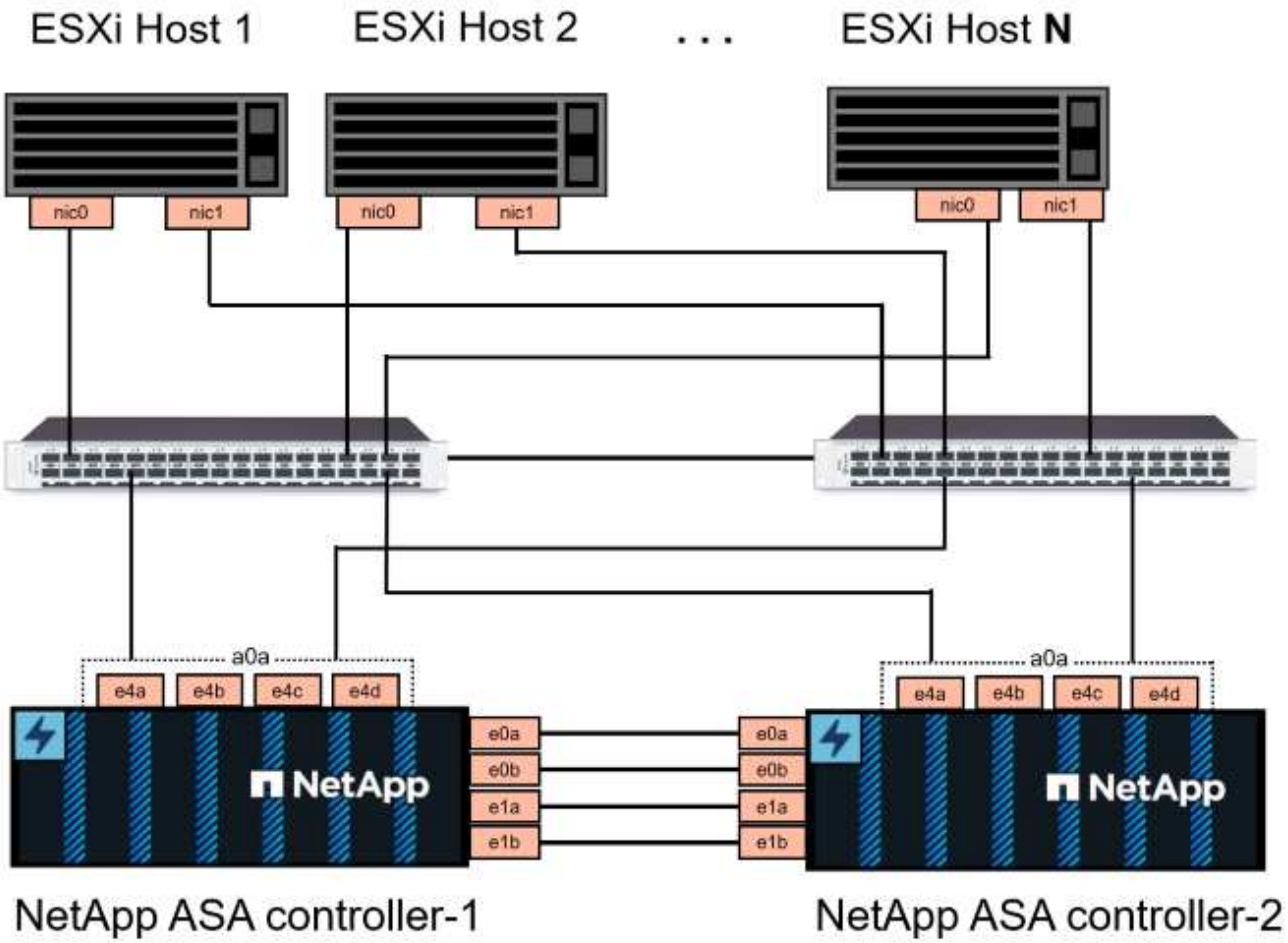
- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico NVMe/TCP.
- Cree grupos de puertos distribuidos para redes iSCSI en el dominio de carga de trabajo VI.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de carga de trabajo VI.
- Agregar adaptadores NVMe/TCP en hosts ESXi.
- Implementar almacén de datos NVMe/TCP.

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP AFF o ASA con puertos de datos físicos en conmutadores Ethernet dedicados al tráfico de almacenamiento.
- La implementación del dominio de administración de VCF está completa y el cliente vSphere es accesible.
- Previamente se ha implementado un dominio de carga de trabajo VI.

NetApp recomienda diseños de red totalmente redundantes para NVMe/TCP. El siguiente diagrama ilustra un ejemplo de una configuración redundante, que proporciona tolerancia a fallas para sistemas de almacenamiento, conmutadores, adaptadores de red y sistemas host. Consulte NetApp"Referencia de configuración de SAN" Para obtener información adicional.



Para rutas múltiples y conmutación por error en múltiples rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet separadas para todas las SVM en configuraciones NVMe/TCP.

Esta documentación demuestra el proceso de creación de una nueva SVM y la especificación de la información de la dirección IP para crear múltiples LIF para el tráfico NVMe/TCP. Para agregar nuevos LIF a un SVM existente, consulte"Crear una LIF (interfaz de red)" .

Para obtener información adicional sobre las consideraciones de diseño de NVMe para los sistemas de almacenamiento ONTAP , consulte"Configuración, soporte y limitaciones de NVMe" .

Pasos de implementación

Para crear un almacén de datos VMFS en un dominio de carga de trabajo VCF mediante NVMe/TCP, complete los siguientes pasos.

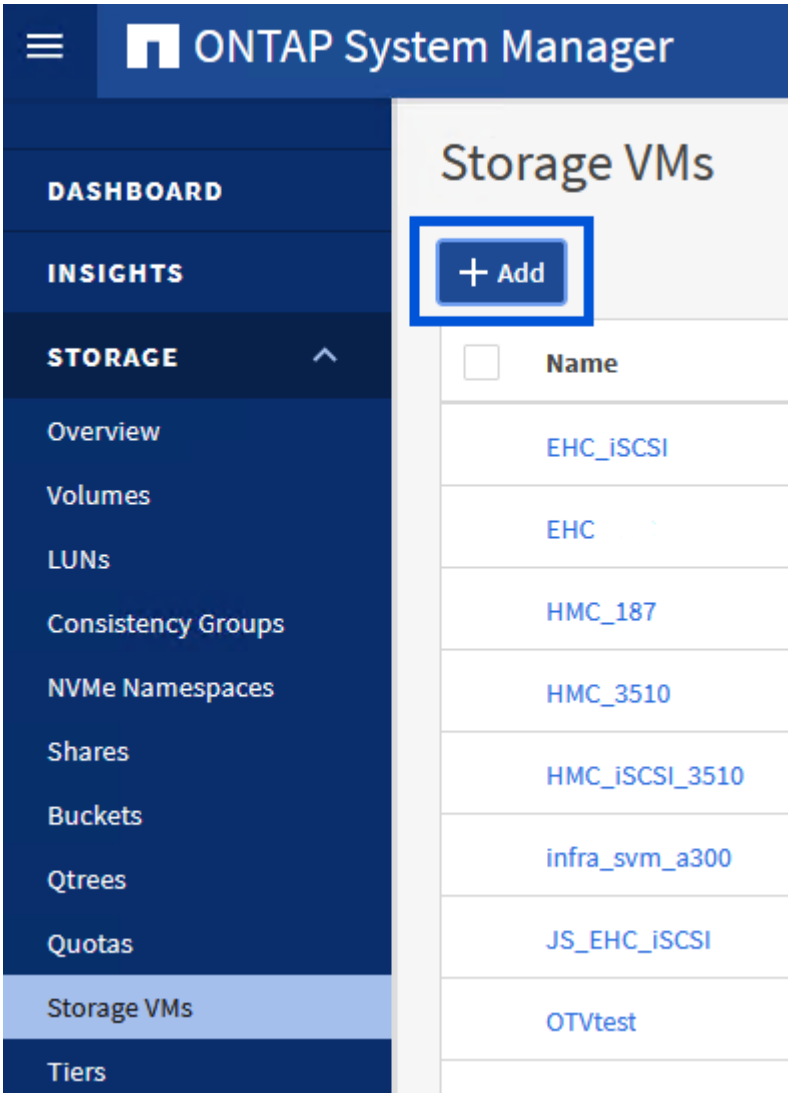
Crear espacios de nombres SVM, LIF y NVMe en el sistema de almacenamiento ONTAP

El siguiente paso se realiza en ONTAP System Manager.

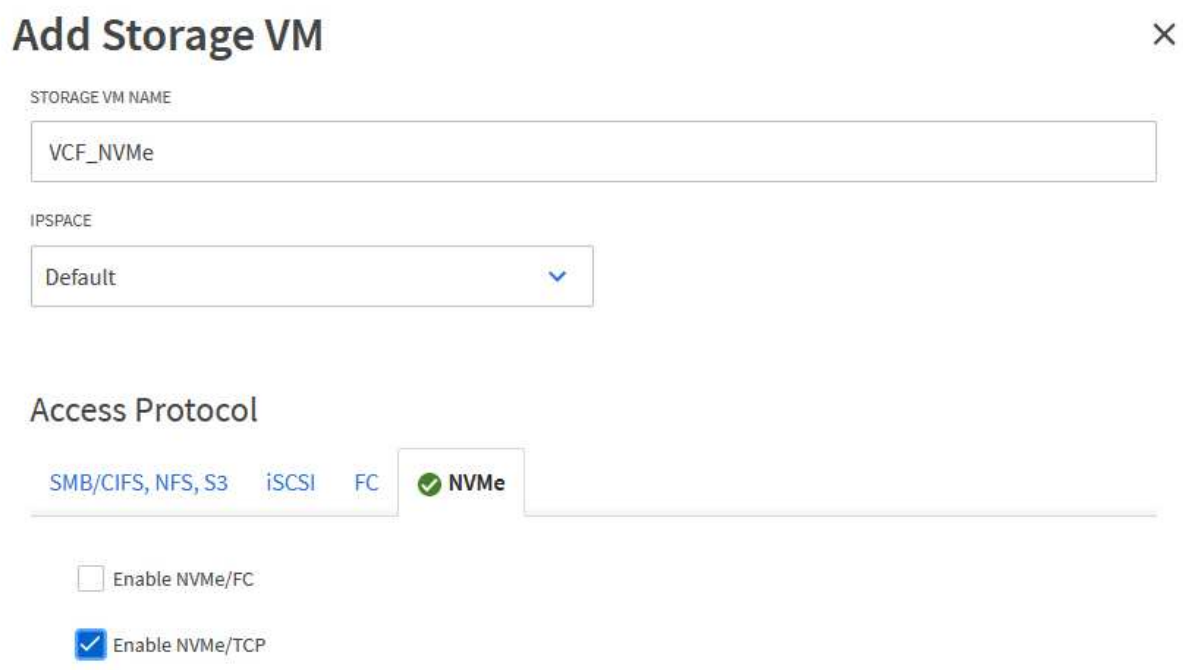
Cree la máquina virtual de almacenamiento y los LIF

Complete los siguientes pasos para crear una SVM junto con múltiples LIF para el tráfico NVMe/TCP.

1. Desde el Administrador del sistema ONTAP , navegue hasta **Máquinas virtuales de almacenamiento** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.

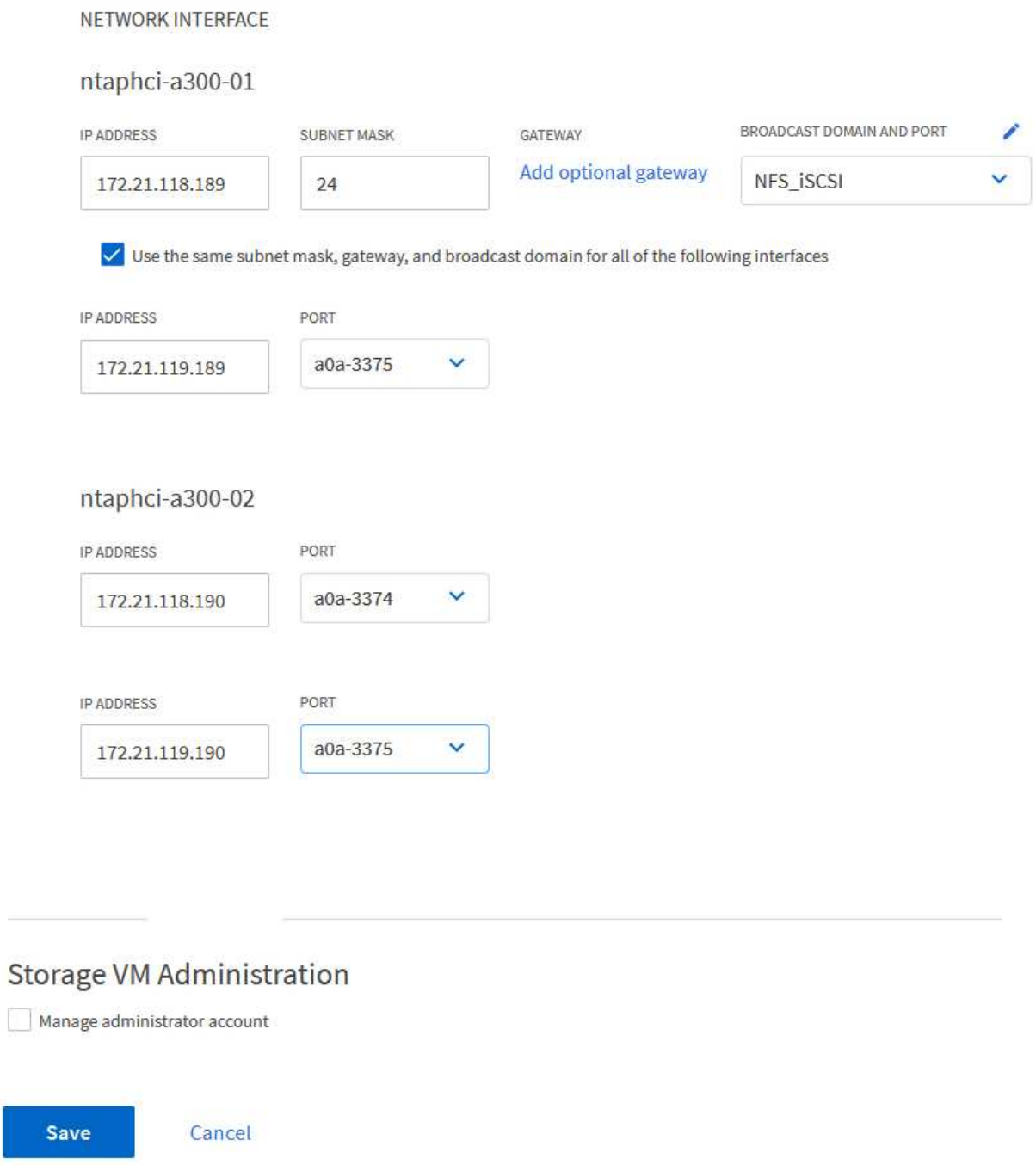


2. En el asistente **Agregar VM de almacenamiento**, proporcione un **Nombre** para la SVM, seleccione el **Espacio de IP** y luego, en **Protocolo de acceso**, haga clic en la pestaña **NVMe** y marque la casilla para **Habilitar NVMe/TCP**.

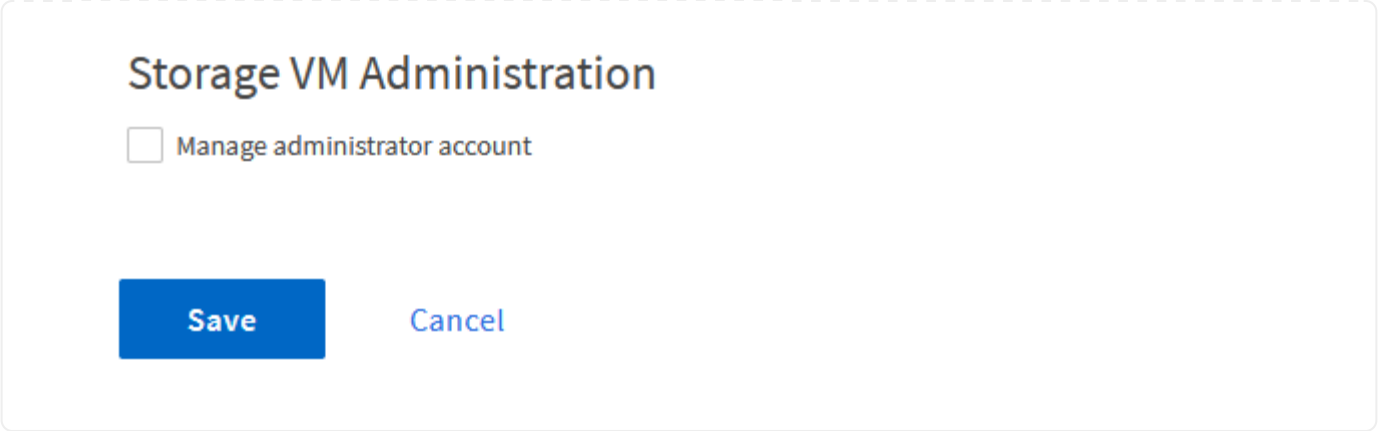


3. En la sección **Interfaz de red**, complete la **Dirección IP**, la **Máscara de subred** y el **Dominio de transmisión y puerto** para el primer LIF. Para los LIF posteriores, la casilla de verificación se puede habilitar para utilizar configuraciones comunes en todos los LIF restantes o utilizar configuraciones separadas.

> Para rutas múltiples y conmutación por error en múltiples rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet separadas para todas las SVM en configuraciones NVMe/TCP.



4. Elija si desea habilitar la cuenta de administración de Storage VM (para entornos de múltiples inquilinos) y haga clic en **Guardar** para crear la SVM.


Storage VM Administration
Manage administrator account
Save
Cancel

Crear el espacio de nombres NVMe

Los espacios de nombres NVMe son análogos a los LUN para iSCSi o FC. Se debe crear el espacio de nombres NVMe antes de poder implementar un almacén de datos VMFS desde vSphere Client. Para crear el espacio de nombres NVMe, primero se debe obtener el nombre calificado NVMe (NQN) de cada host ESXi en el clúster. ONTAP utiliza NQN para proporcionar control de acceso al espacio de nombres.

Complete los siguientes pasos para crear un espacio de nombres NVMe:

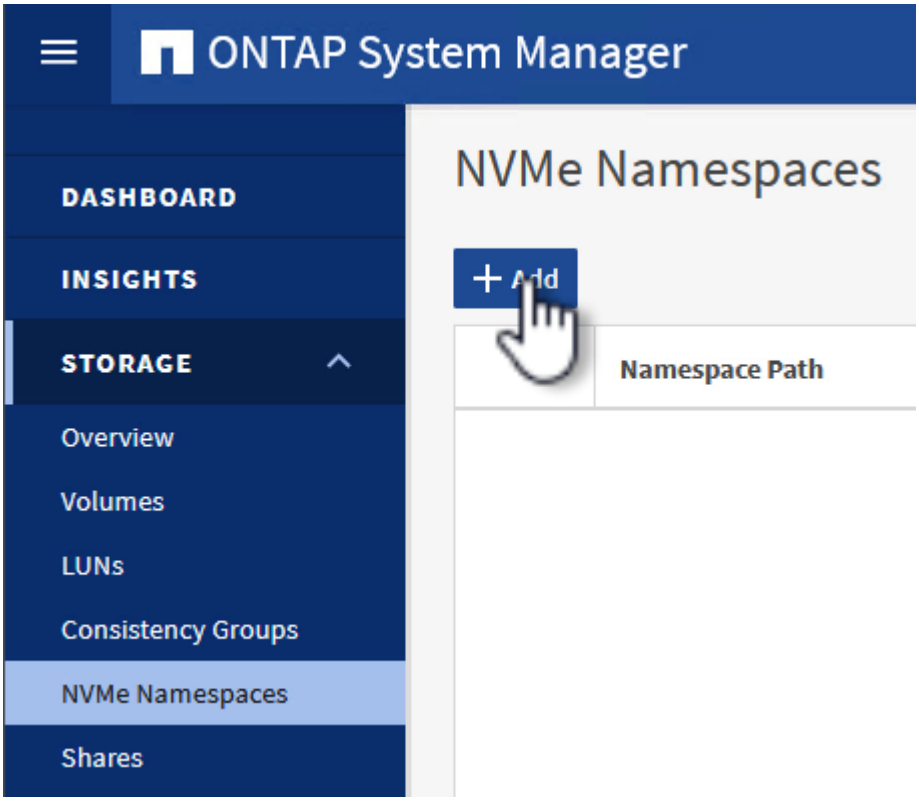
1. Abra una sesión SSH con un host ESXi en el clúster para obtener su NQN. Utilice el siguiente comando desde la CLI:

   ```
   esxcli nvme info get
   ```

   Debería mostrarse una salida similar a la siguiente:

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

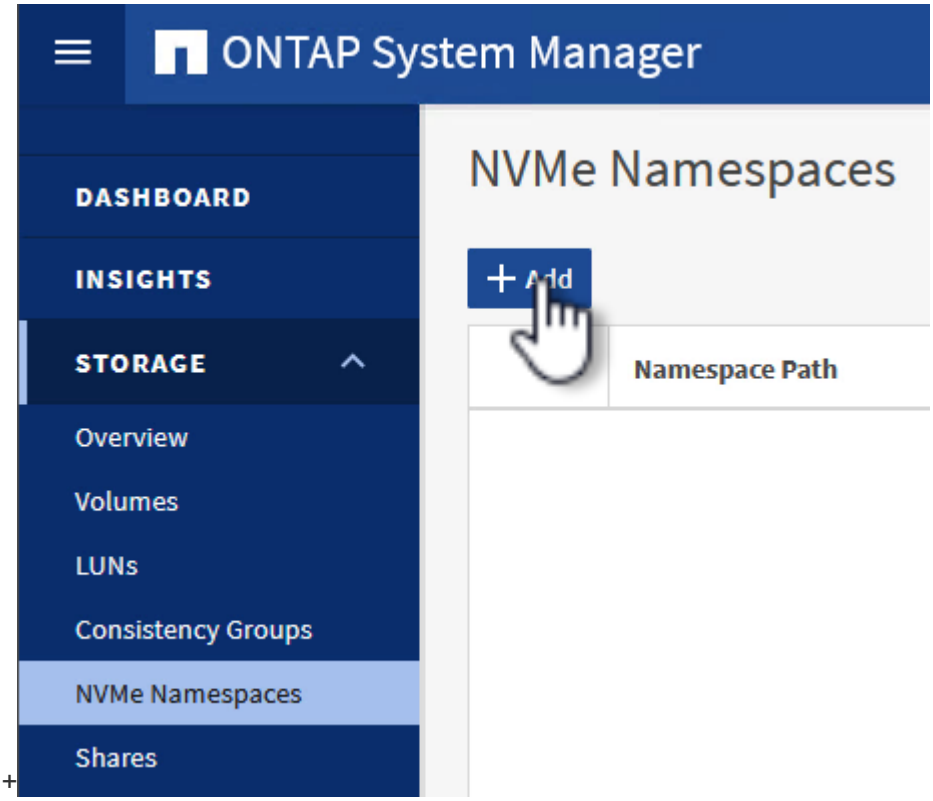
2. Registre el NQN para cada host ESXi en el clúster
3. Desde el Administrador del sistema ONTAP , navegue hasta **Espacios de nombres NVMe** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.



4. En la página **Agregar espacio de nombres NVMe**, complete un prefijo de nombre, la cantidad de espacios de nombres a crear, el tamaño del espacio de nombres y el sistema operativo host que

accederá al espacio de nombres. En la sección **Host NQN**, cree una lista separada por comas de los NQN recopilados previamente de los hosts ESXi que accederán a los espacios de nombres.

Haga clic en **Más opciones** para configurar elementos adicionales como la política de protección de instantáneas. Por último, haga clic en **Guardar** para crear el espacio de nombres NVMe.



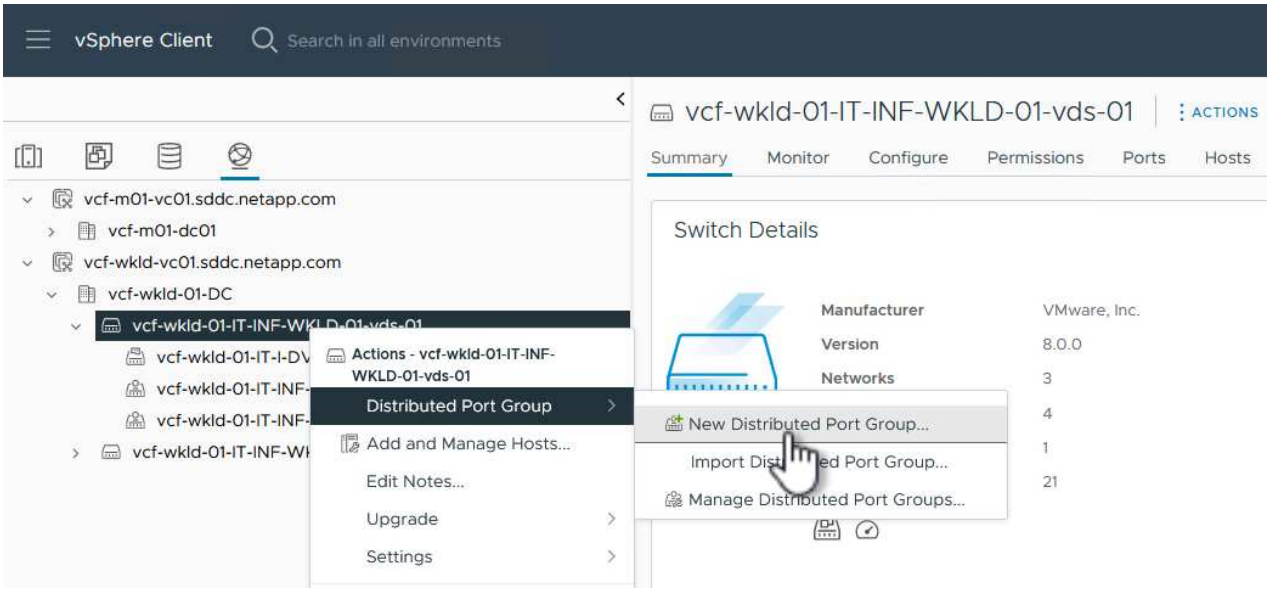
Configurar adaptadores de software NVMe y de red en hosts ESXi

Los siguientes pasos se realizan en el clúster de dominio de carga de trabajo VI mediante el cliente vSphere. En este caso, se utiliza vCenter Single Sign-On para que el cliente vSphere sea común a los dominios de administración y de carga de trabajo.

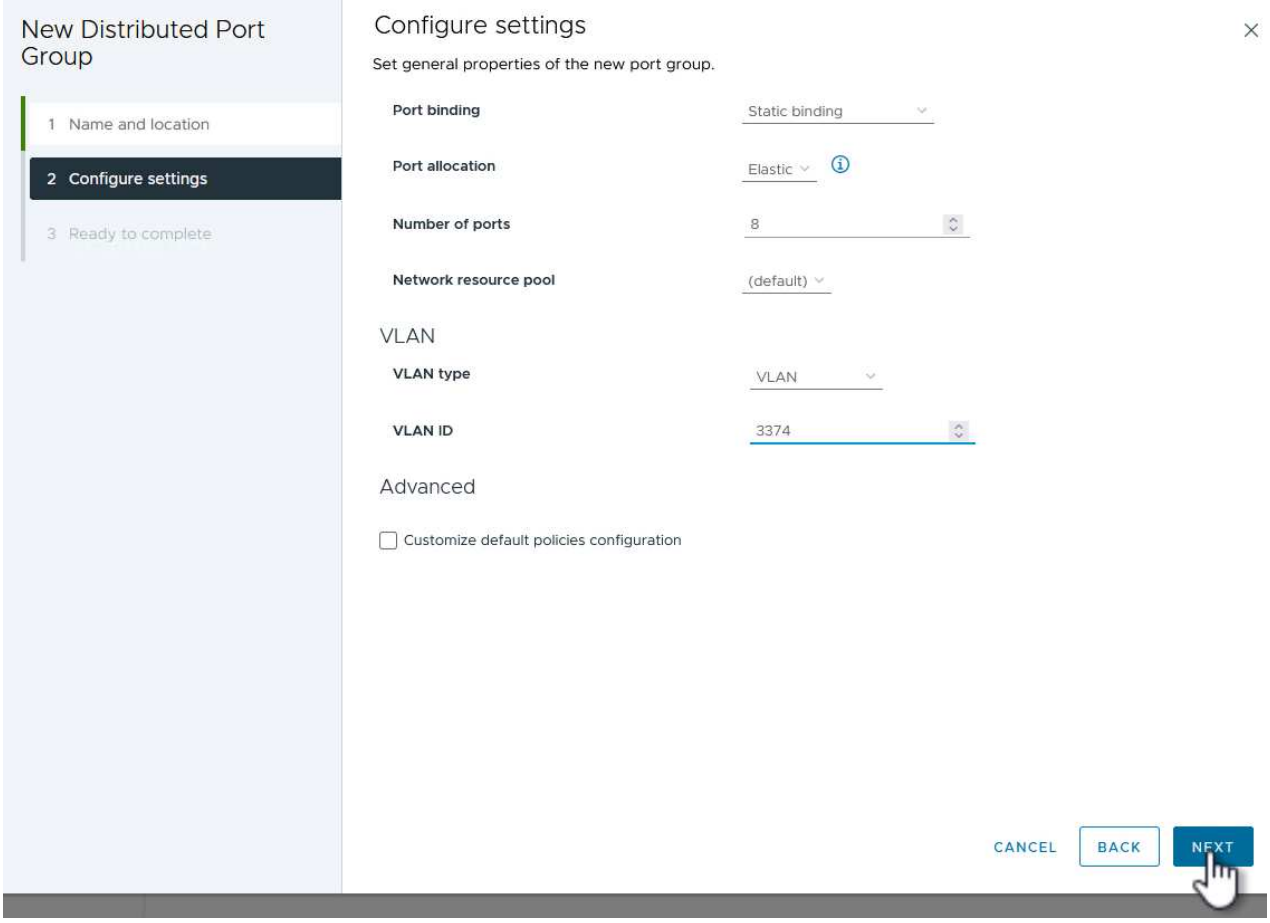
Crear grupos de puertos distribuidos para el tráfico NVME/TCP

Complete lo siguiente para crear un nuevo grupo de puertos distribuidos para cada red NVMe/TCP:

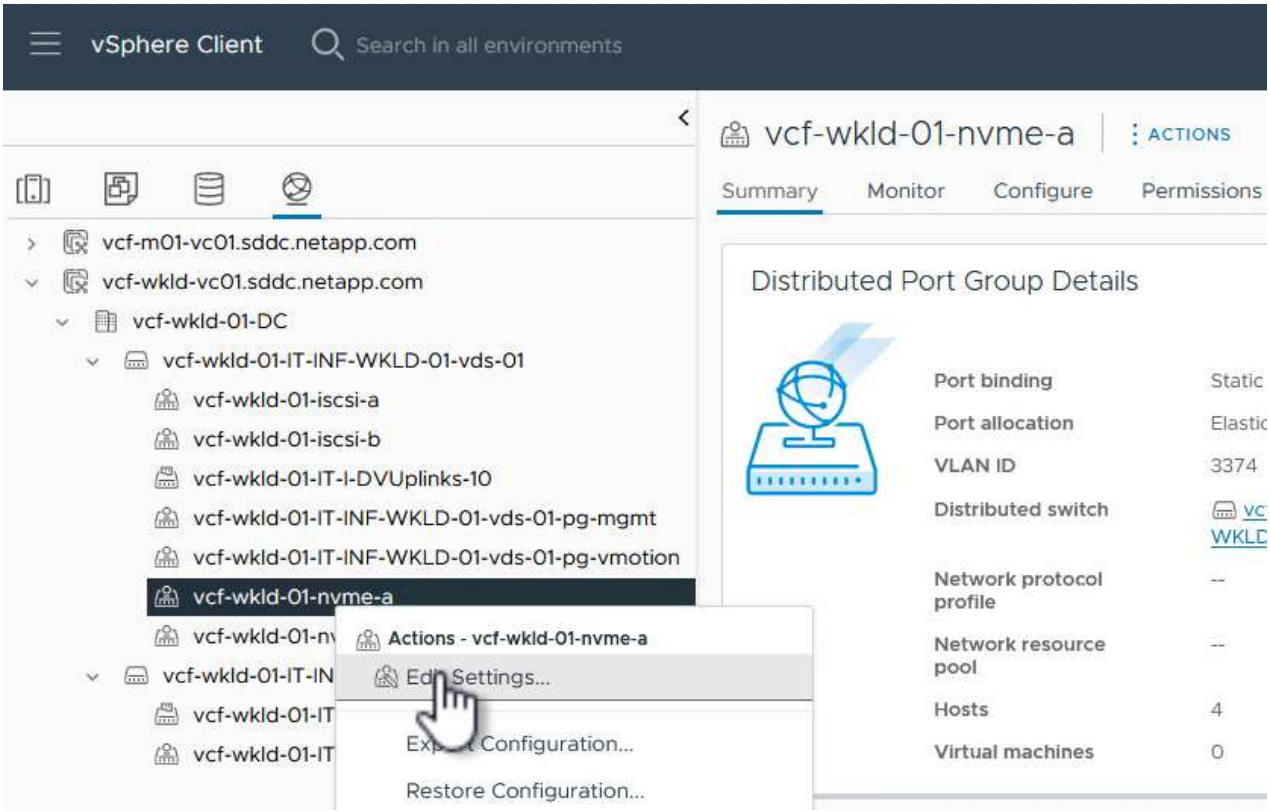
1. Desde el cliente vSphere, navegue a **Inventario > Redes** para el dominio de carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos…**.



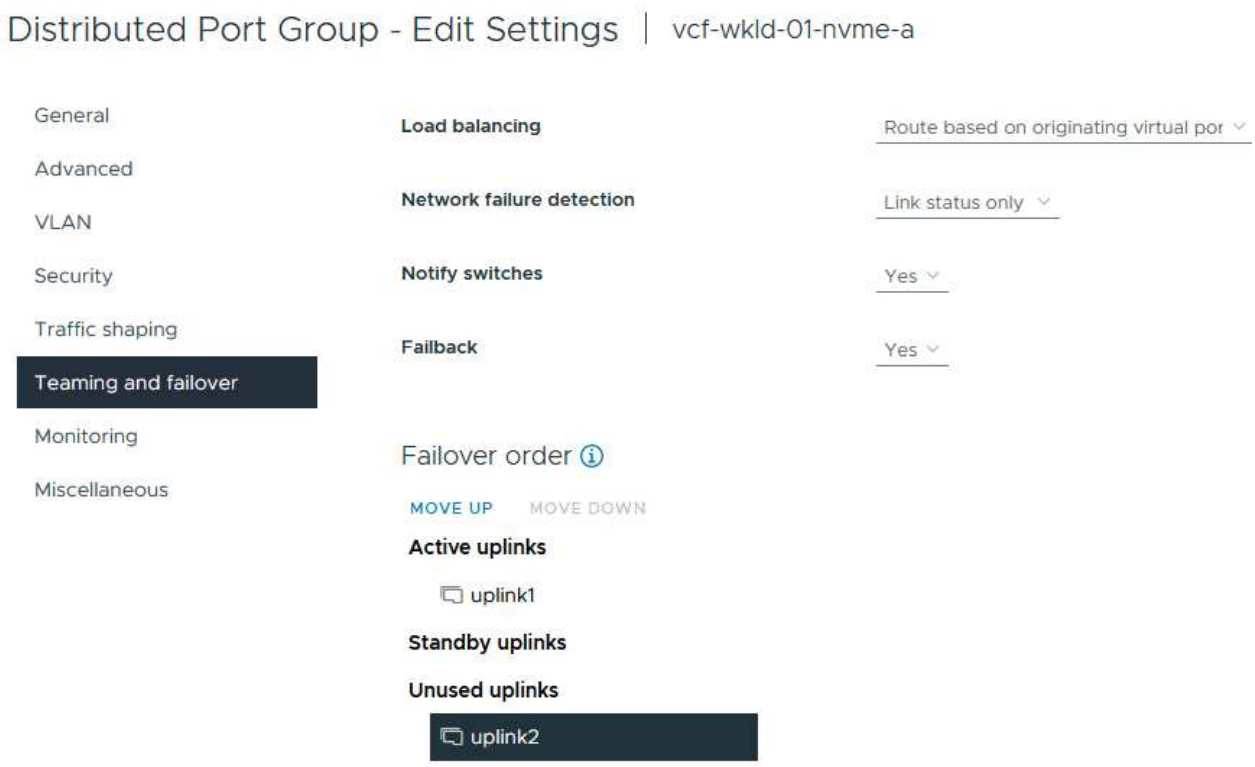
2. En el asistente **Nuevo grupo de puertos distribuidos**, complete un nombre para el nuevo grupo de puertos y haga clic en **Siguiente** para continuar.
3. En la página **Configurar ajustes** complete todas las configuraciones. Si se utilizan VLAN, asegúrese de proporcionar la ID de VLAN correcta. Haga clic en **Siguiente** para continuar.



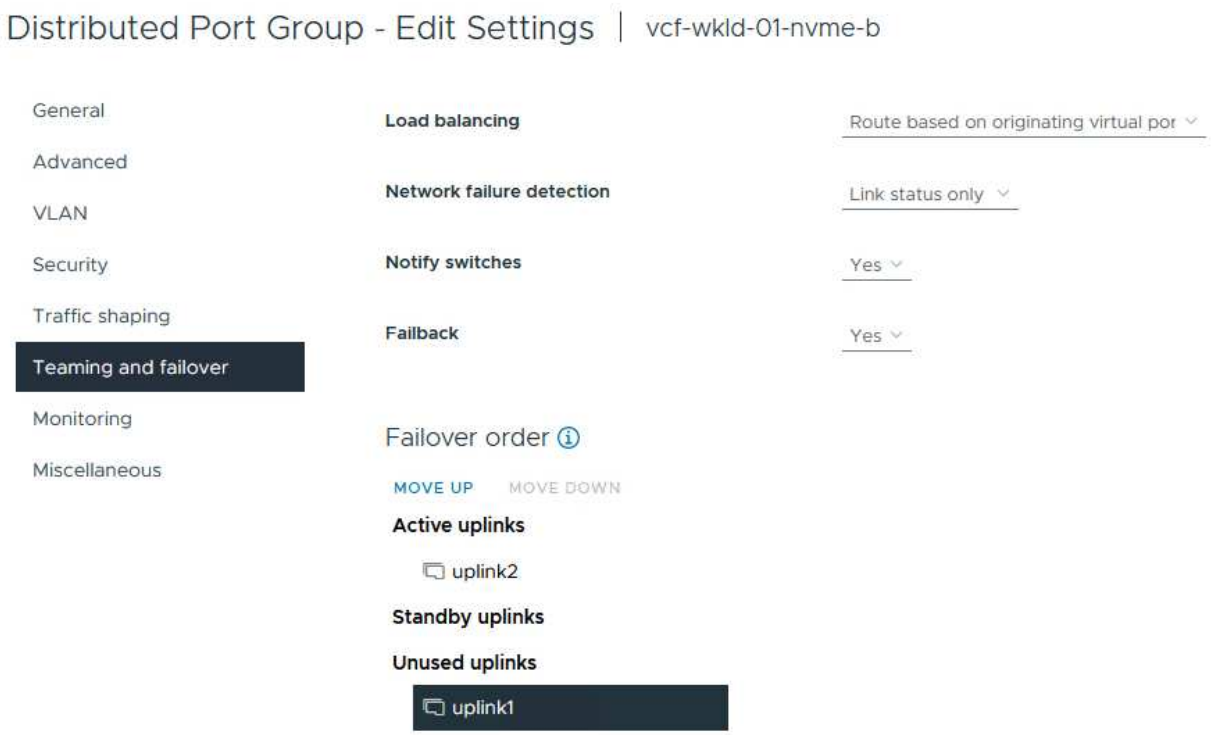
4. En la página **Listo para completar**, revise los cambios y haga clic en **Finalizar** para crear el nuevo grupo de puertos distribuidos.
5. Repita este proceso para crear un grupo de puertos distribuidos para la segunda red NVMe/TCP que se esté utilizando y asegúrese de haber ingresado el **VLAN ID** correcto.
6. Una vez que se hayan creado ambos grupos de puertos, navegue hasta el primer grupo de puertos y seleccione la acción **Editar configuración…**.



7. En la página **Grupo de puertos distribuidos - Editar configuración**, navegue a **Equipo y conmutación por error** en el menú de la izquierda y haga clic en **uplink2** para moverlo hacia abajo a **Enlaces ascendentes no utilizados**.



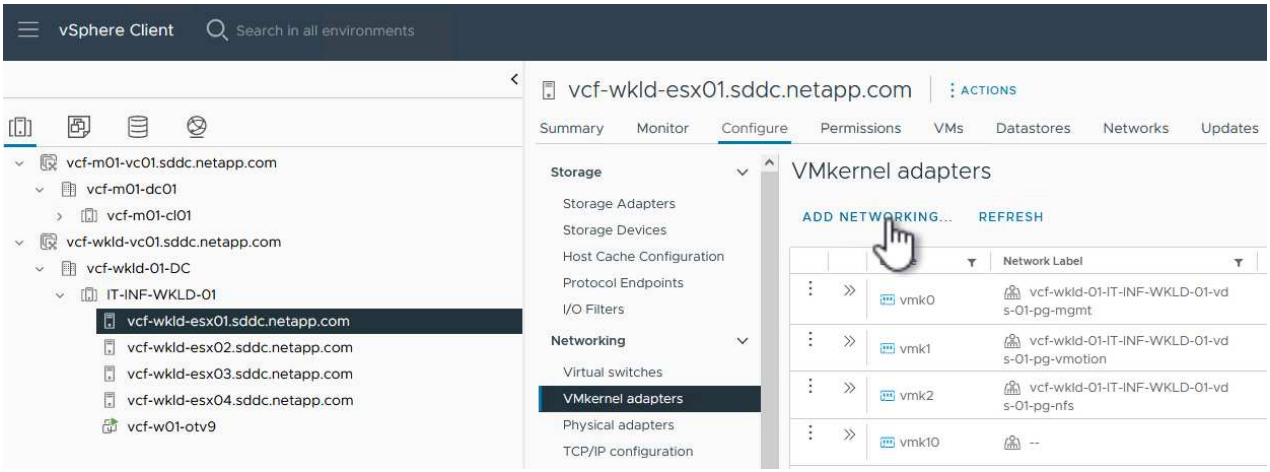
8. Repita este paso para el segundo grupo de puertos NVMe/TCP. Sin embargo, esta vez mueva **uplink1** a **Unused uplinks**.



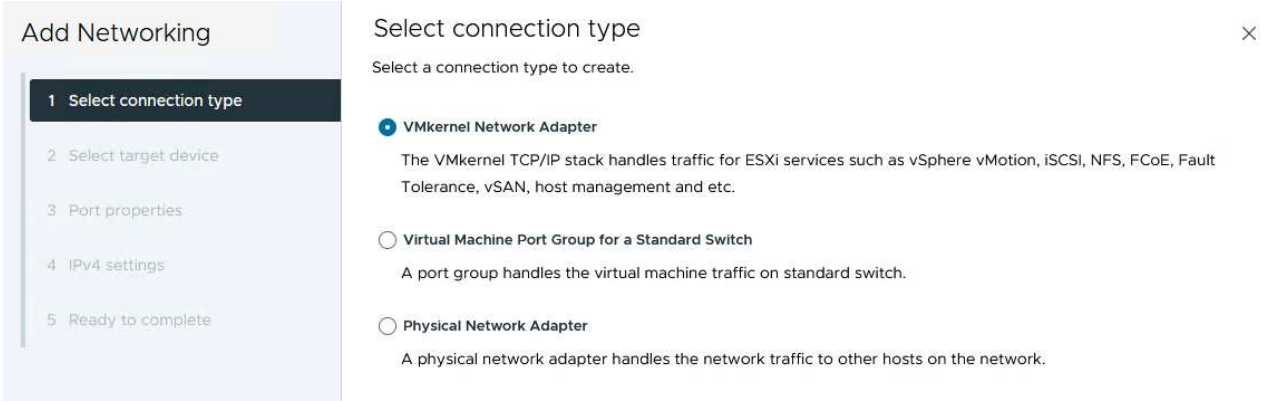
Cree adaptadores VMkernel en cada host ESXi

Repita este proceso en cada host ESXi en el dominio de carga de trabajo.

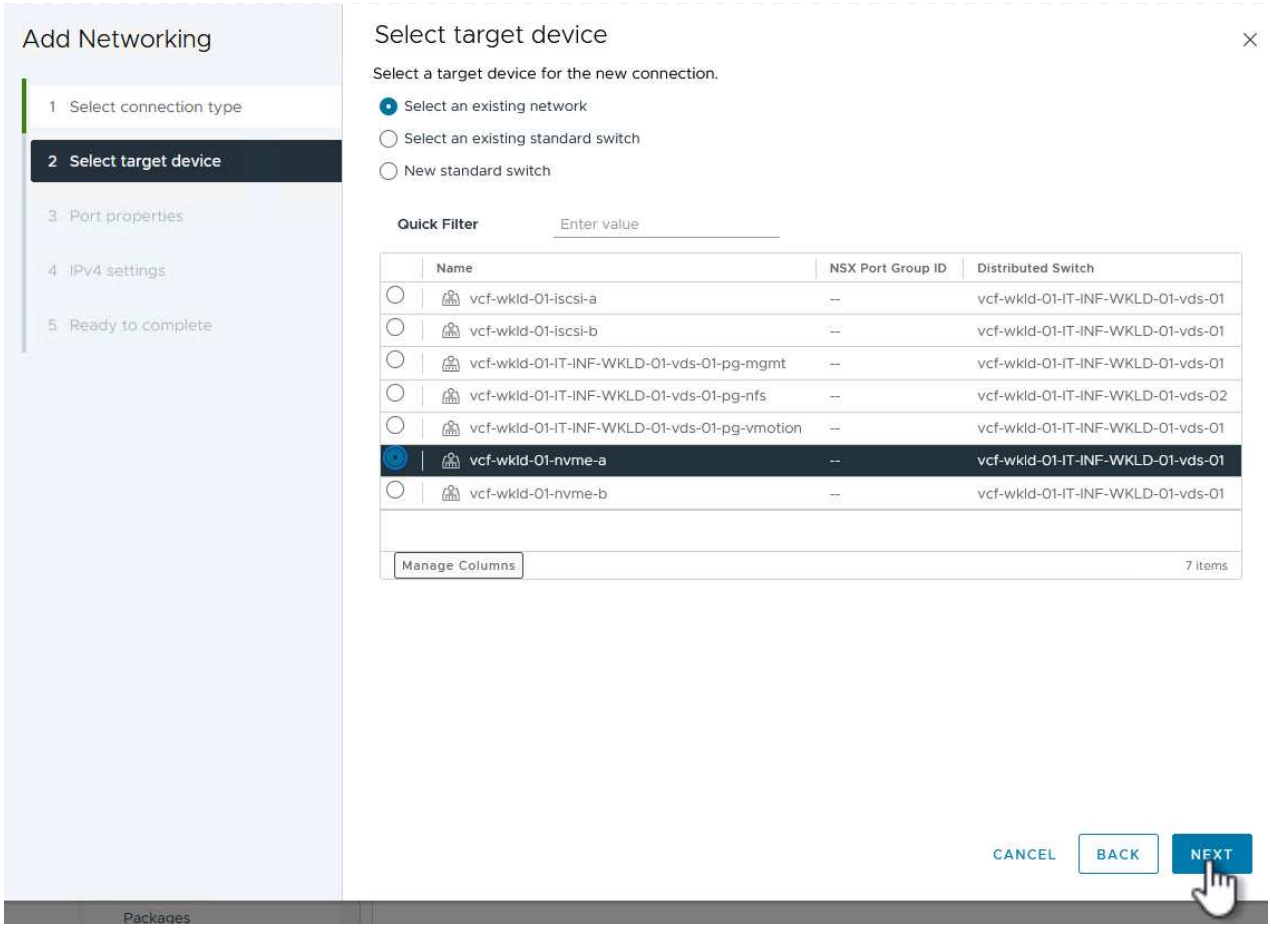
1. Desde el cliente vSphere, navegue a uno de los hosts ESXi en el inventario del dominio de carga de trabajo. Desde la pestaña **Configurar** seleccione **Adaptadores VMkernel** y haga clic en **Agregar red…** para comenzar.



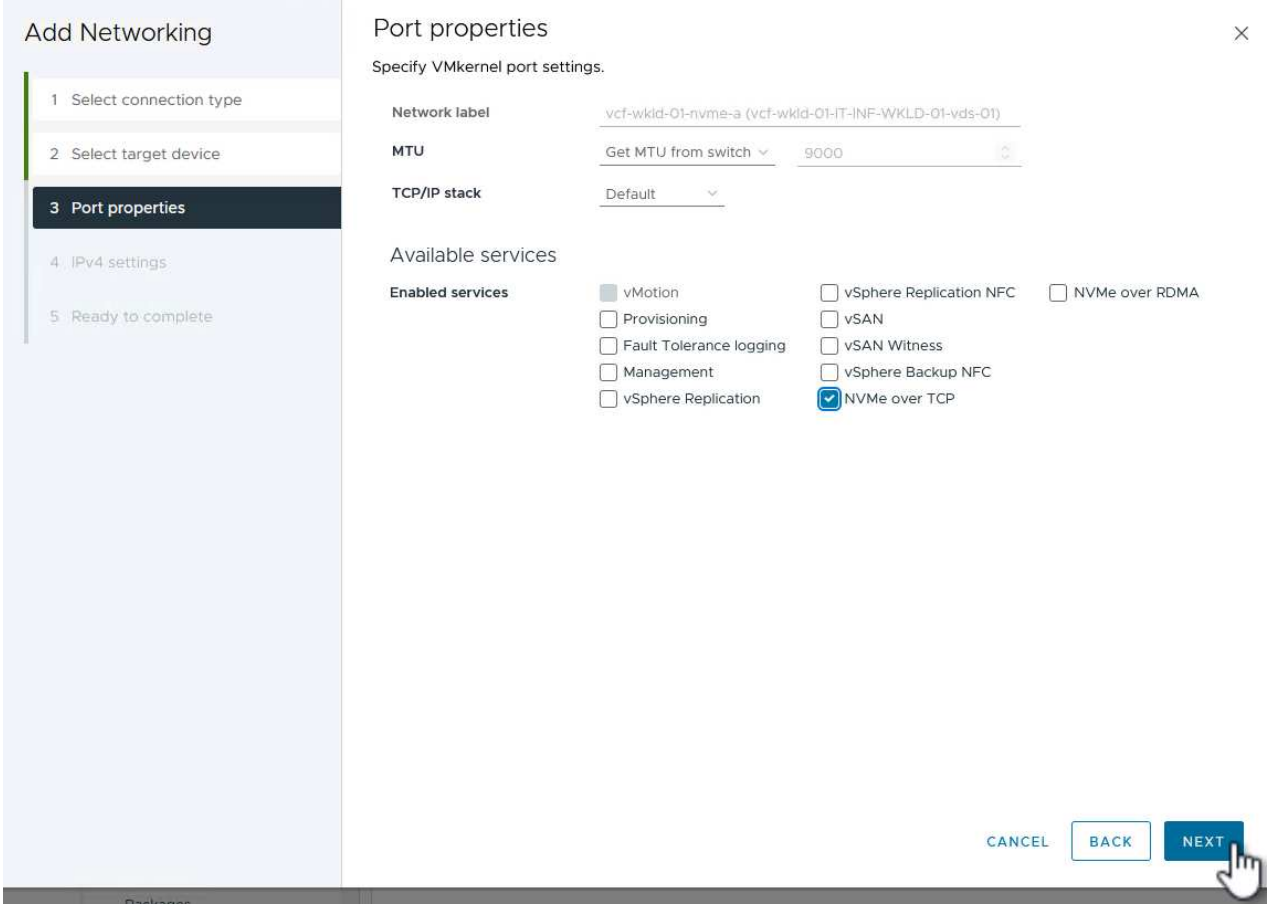
2. En la ventana **Seleccionar tipo de conexión** elija **Adaptador de red VMkernel** y haga clic en **Siguiente** para continuar.



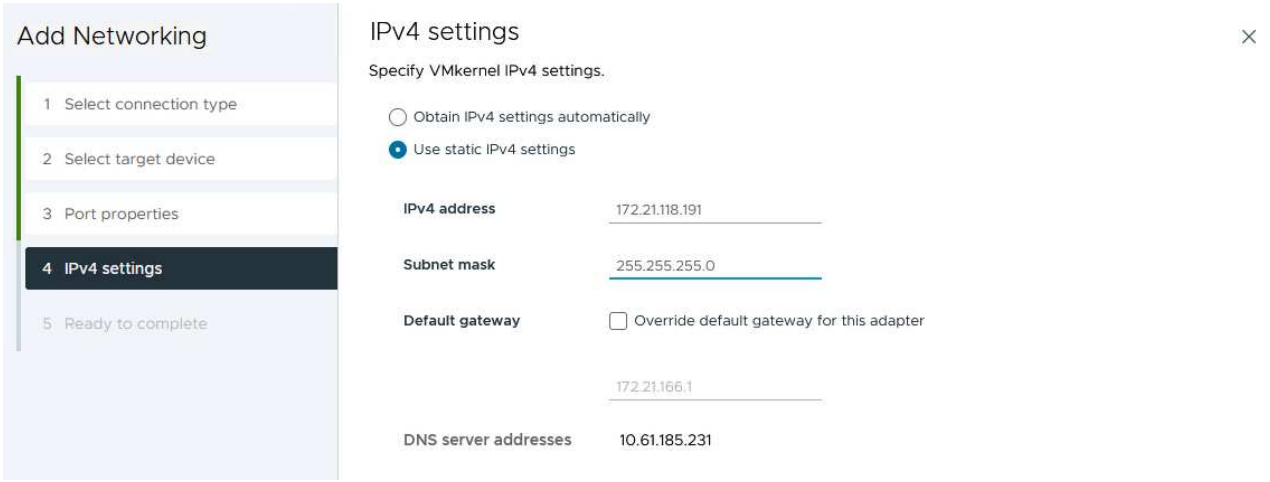
3. En la página **Seleccionar dispositivo de destino**, elija uno de los grupos de puertos distribuidos para iSCSI que se crearon anteriormente.



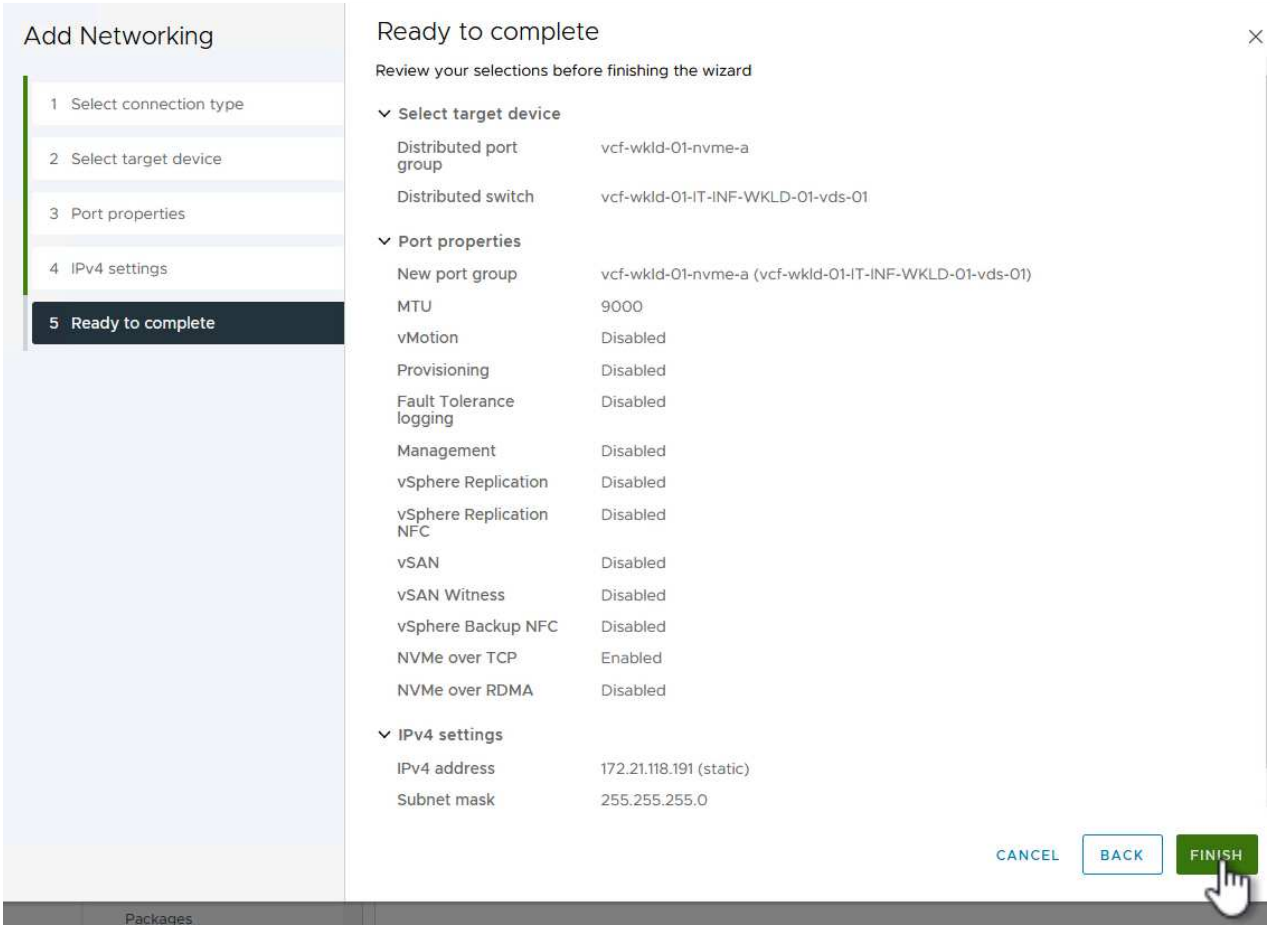
4. En la página **Propiedades del puerto**, haga clic en el cuadro **NVMe sobre TCP** y haga clic en **Siguiente** para continuar.



5. En la página de **Configuración de IPv4**, complete la **dirección IP**, la **Máscara de subred** y proporcione una nueva dirección IP de puerta de enlace (solo si es necesario). Haga clic en **Siguiente** para continuar.



6. Revise sus selecciones en la página **Listo para completar** y haga clic en **Finalizar** para crear el adaptador VMkernel.



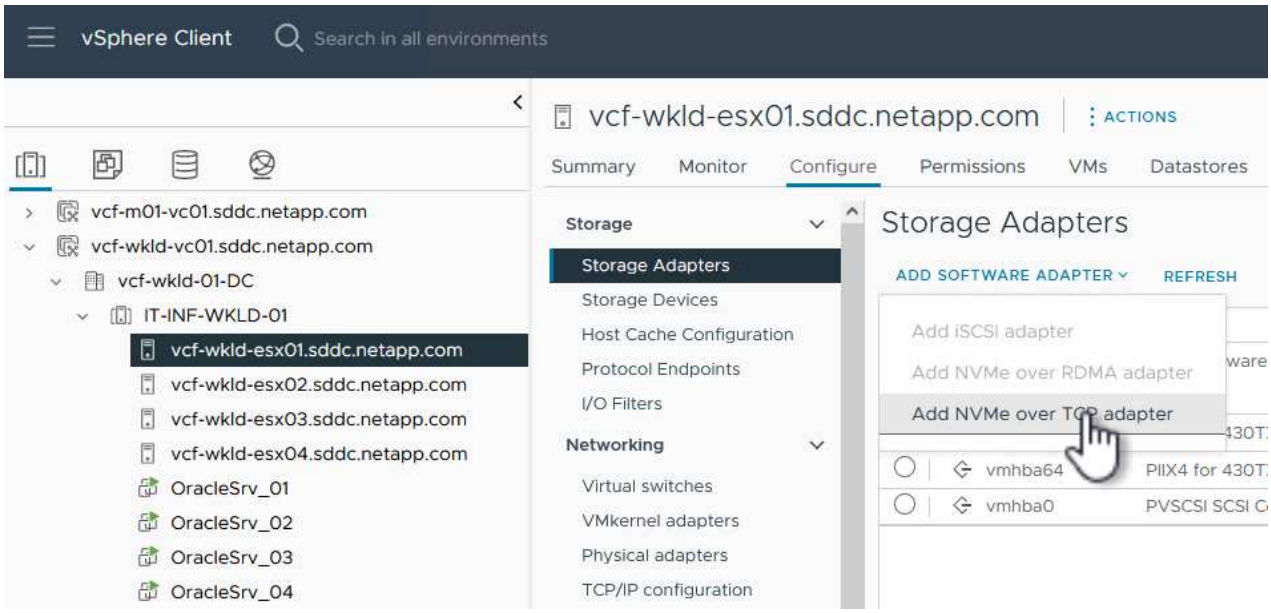
7. Repita este proceso para crear un adaptador VMkernel para la segunda red iSCSI.

Agregar adaptador NVMe sobre TCP

Cada host ESXi en el clúster de dominio de carga de trabajo debe tener un adaptador de software NVMe sobre TCP instalado para cada red NVMe/TCP establecida dedicada al tráfico de almacenamiento.

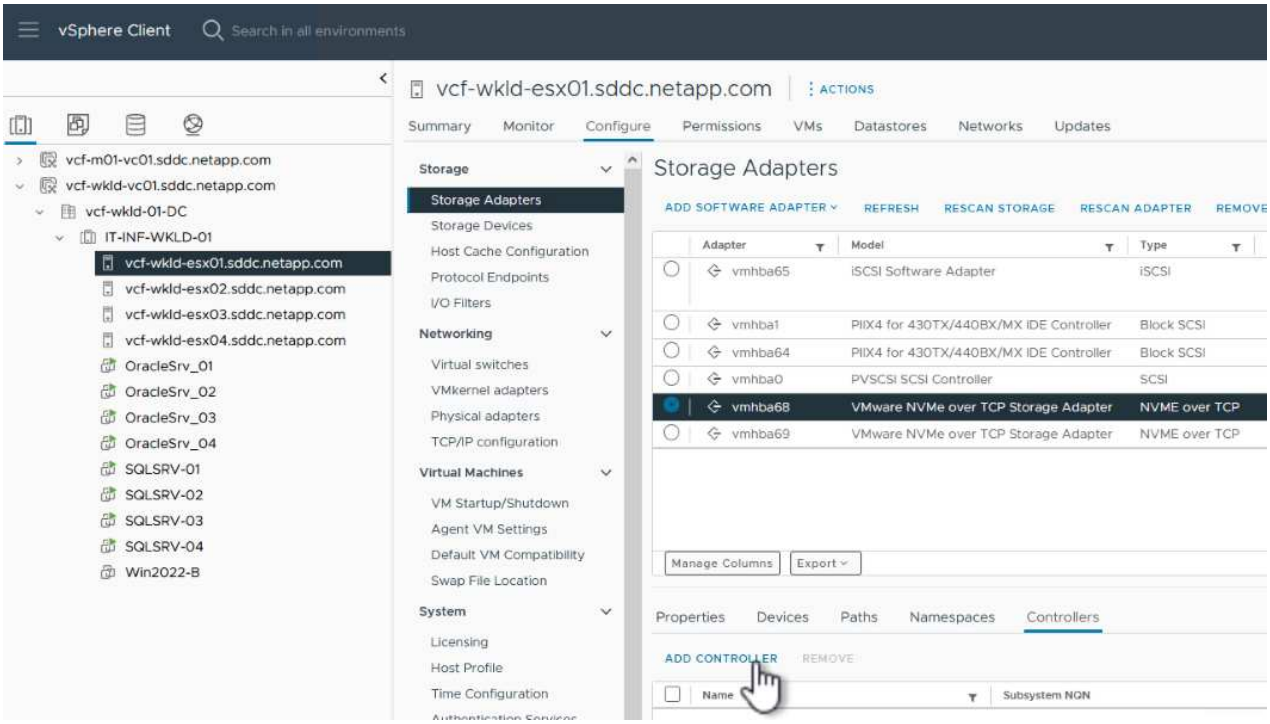
Para instalar adaptadores NVMe sobre TCP y descubrir los controladores NVMe, complete los siguientes pasos:

1. En el cliente vSphere, navegue a uno de los hosts ESXi en el clúster del dominio de carga de trabajo. Desde la pestaña **Configurar**, haga clic en **Adaptadores de almacenamiento** en el menú y luego, en el menú desplegable **Agregar adaptador de software**, seleccione **Agregar adaptador NVMe sobre TCP**.

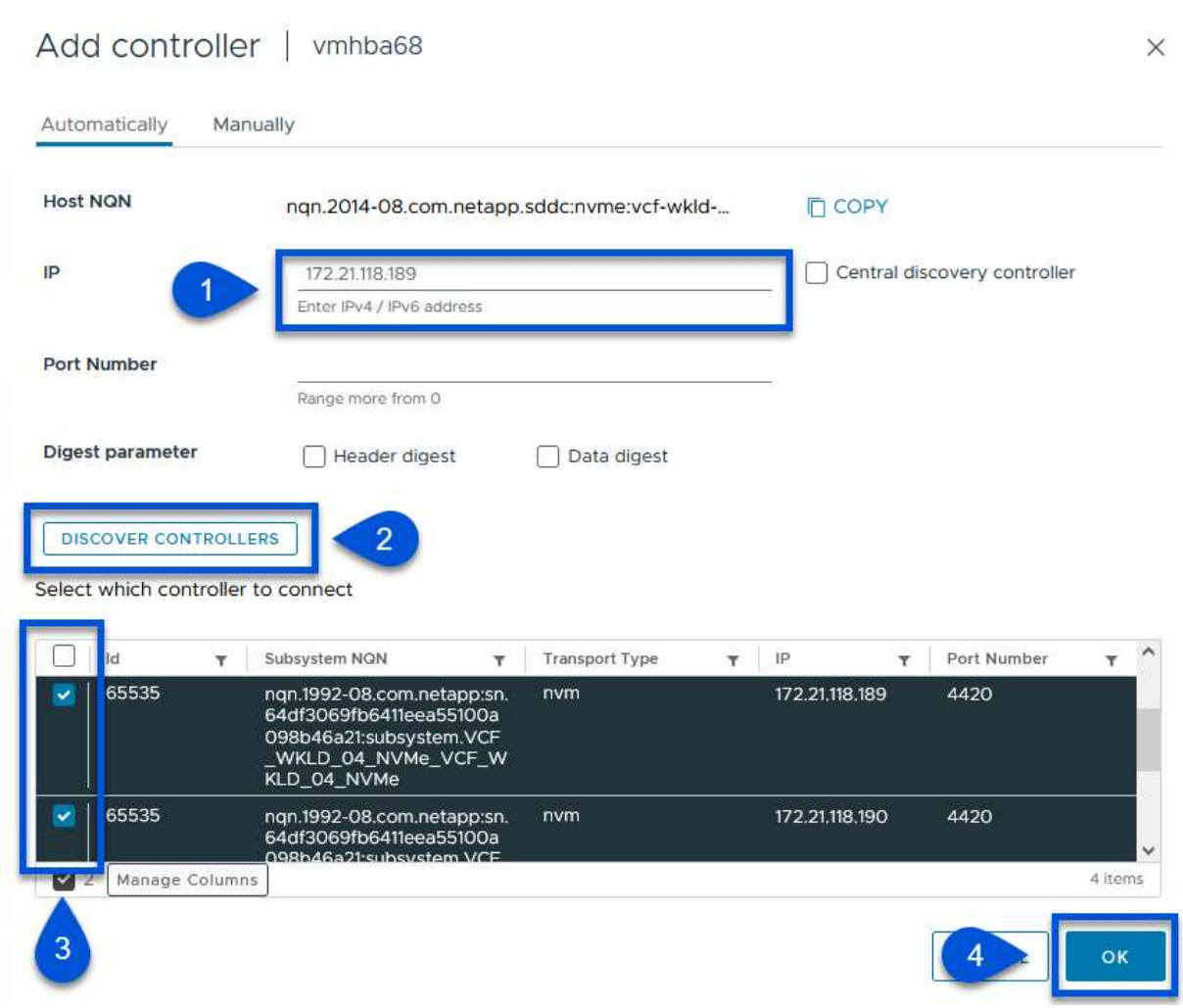


2. En la ventana **Agregar software adaptador NVMe sobre TCP**, acceda al menú desplegable **Adaptador de red física** y seleccione el adaptador de red física correcto en el cual desea habilitar el adaptador NVMe.

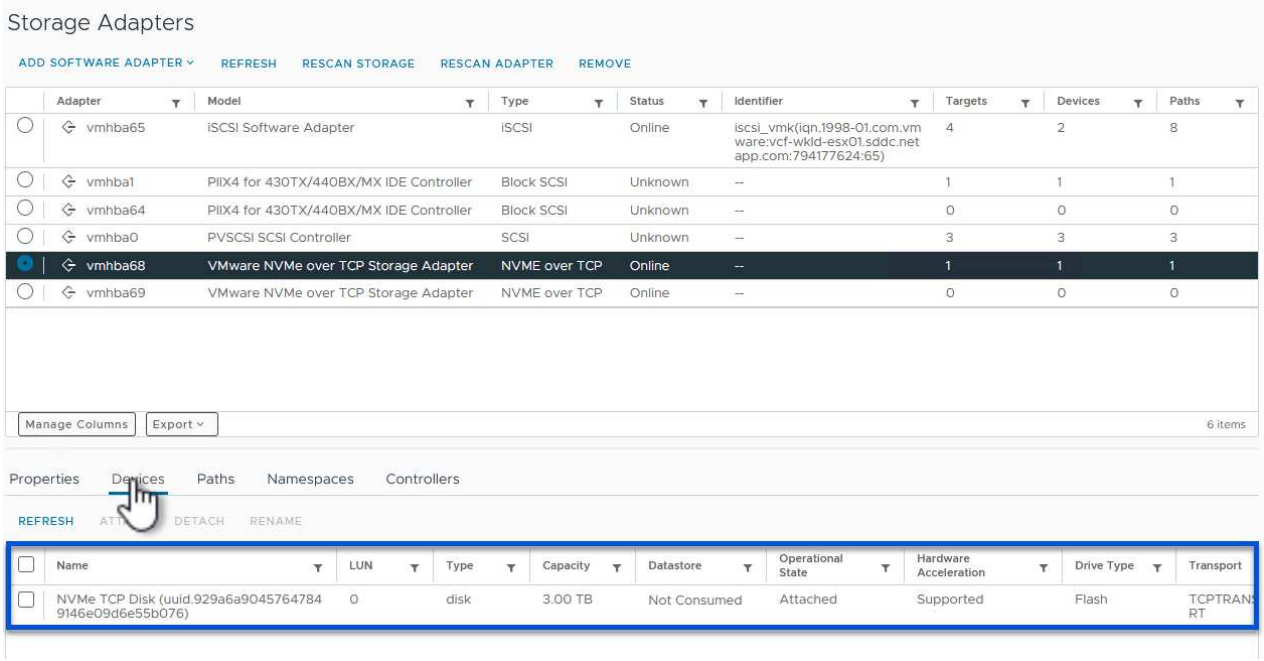
3. Repita este proceso para la segunda red asignada al tráfico NVMe sobre TCP, asignando el adaptador físico correcto.
4. Seleccione uno de los adaptadores NVMe sobre TCP recién instalados y, en la pestaña **Controladores**, seleccione **Agregar controlador**.



5. En la ventana **Agregar controlador**, seleccione la pestaña **Automáticamente** y complete los siguientes pasos.
    - Complete una dirección IP para una de las interfaces lógicas SVM en la misma red que el adaptador físico asignado a este adaptador NVMe sobre TCP.
    - Haga clic en el botón **Descubrir controladores**.
    - En la lista de controladores descubiertos, haga clic en la casilla de verificación de los dos controladores con direcciones de red alineadas con este adaptador NVMe sobre TCP.
    - Haga clic en el botón **Aceptar** para agregar los controladores seleccionados.



6. Después de unos segundos deberías ver el espacio de nombres NVMe aparecer en la pestaña Dispositivos.

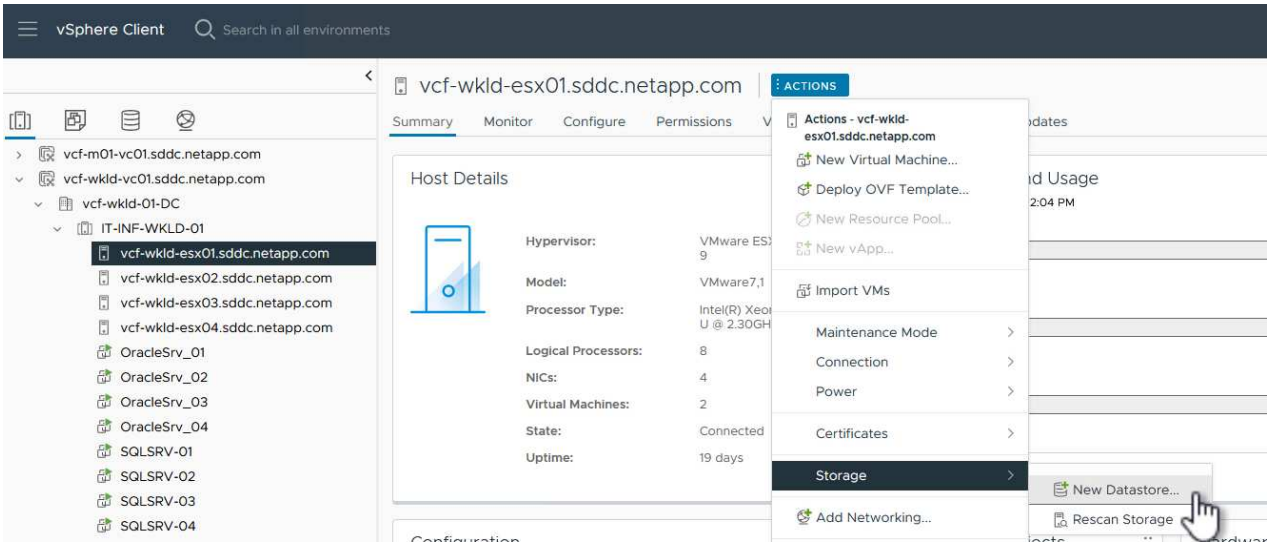


7. Repita este procedimiento para crear un adaptador NVMe sobre TCP para la segunda red establecida para el tráfico NVMe/TCP.

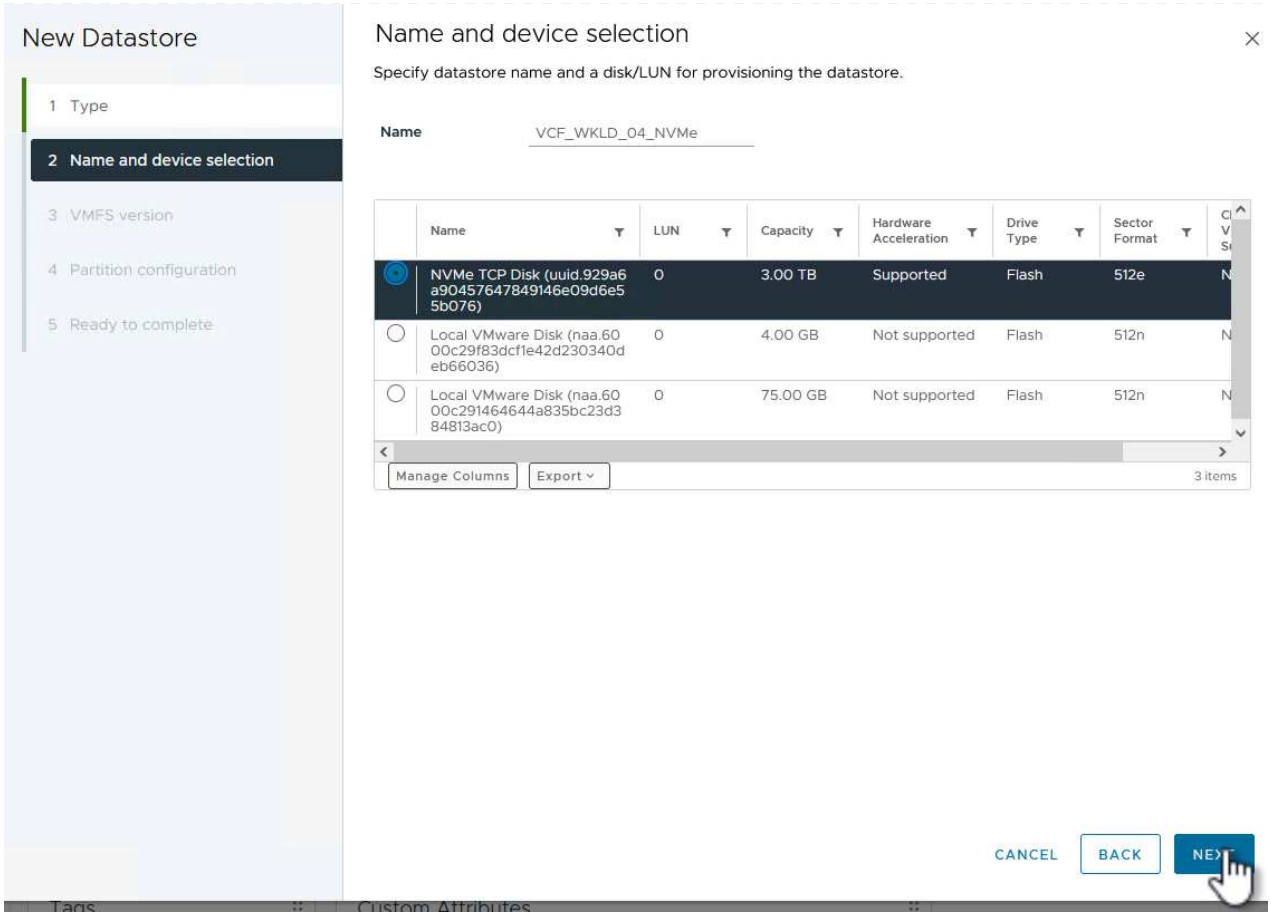
Implementar un almacén de datos NVMe sobre TCP

Para crear un almacén de datos VMFS en el espacio de nombres NVMe, complete los siguientes pasos:

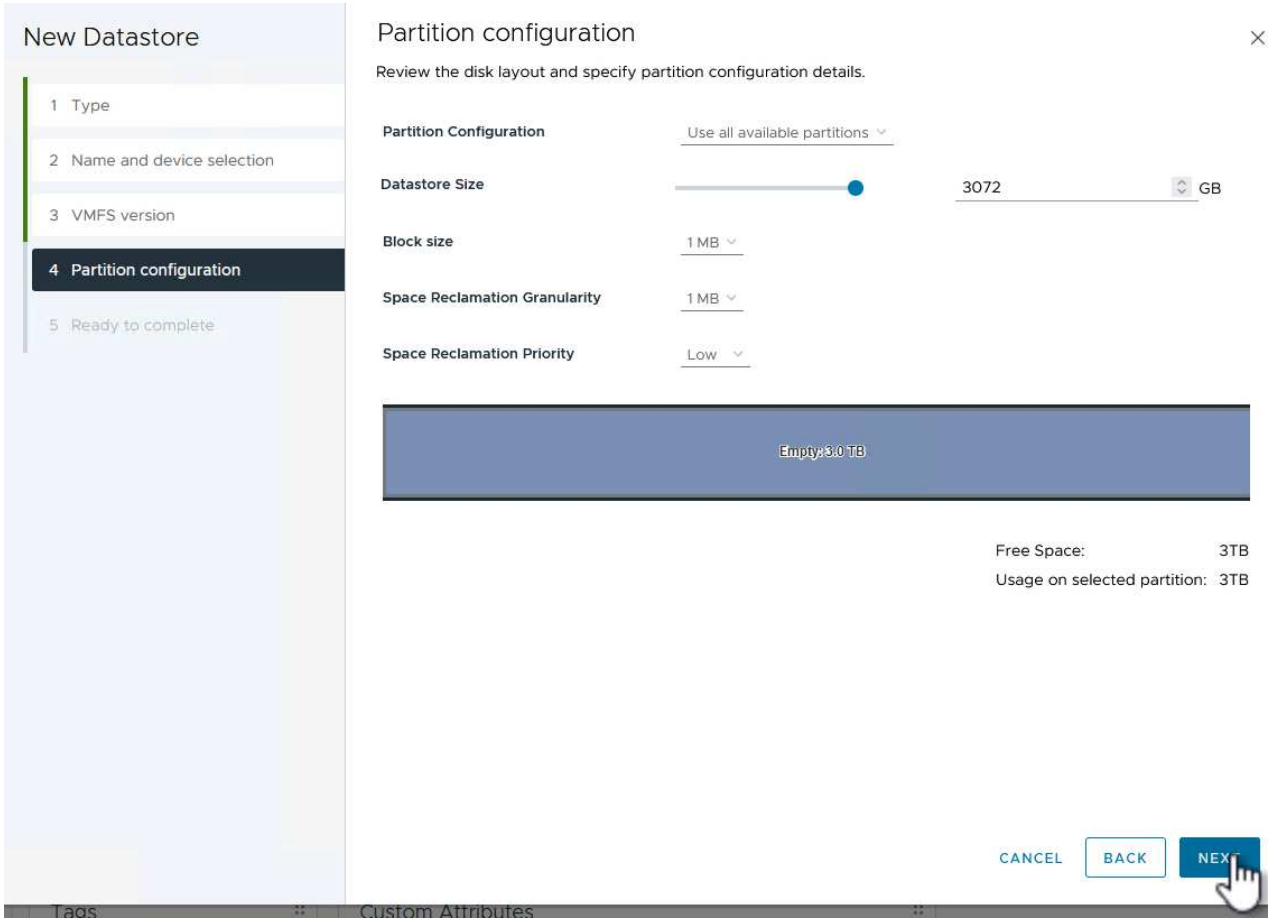
1. En el cliente vSphere, navegue a uno de los hosts ESXi en el clúster del dominio de carga de trabajo. Desde el menú **Acciones**, seleccione **Almacenamiento > Nuevo almacén de datos…**.



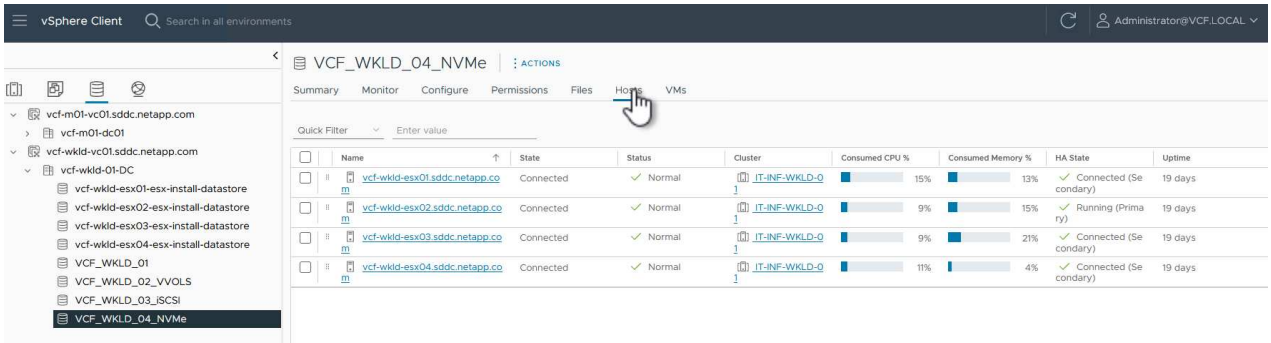
2. En el asistente **Nuevo almacén de datos**, seleccione **VMFS** como tipo. Haga clic en **Siguiente** para continuar.
3. En la página **Selección de nombre y dispositivo**, proporcione un nombre para el almacén de datos y seleccione el espacio de nombres NVMe de la lista de dispositivos disponibles.



4. En la página **Versión VMFS**, seleccione la versión de VMFS para el almacén de datos.
5. En la página **Configuración de partición**, realice los cambios que desee en el esquema de partición predeterminado. Haga clic en **Siguiente** para continuar.



6. En la página **Listo para completar**, revise el resumen y haga clic en **Finalizar** para crear el almacén de datos.
7. Navegue hasta el nuevo almacén de datos en el inventario y haga clic en la pestaña **Hosts**. Si se configura correctamente, todos los hosts ESXi del clúster deberían aparecer en la lista y tener acceso al nuevo almacén de datos.



Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Agregue un almacén de datos VMFS basado en FC como almacenamiento complementario a los dominios de carga de trabajo de VI

En este caso de uso, describimos el procedimiento para configurar un almacén de datos VMFS utilizando Fibre Channel (FC) como almacenamiento complementario para un dominio de carga de trabajo de infraestructura virtual (VI) de VMware Cloud Foundation (VCF). Este procedimiento resume la implementación de ONTAP Tools para VMware vSphere, el registro del servidor vCenter de carga de trabajo VI, la definición del backend de almacenamiento y el aprovisionamiento del almacén de datos FC.

Beneficios del canal de fibra

Alto rendimiento: FC proporciona velocidades de transferencia de datos de alta velocidad, lo que lo hace ideal para aplicaciones que requieren acceso rápido y confiable a grandes cantidades de datos.

Baja latencia: Latencia muy baja, lo cual es crucial para aplicaciones sensibles al rendimiento, como bases de datos y entornos virtualizados.

Confiabilidad: Las redes FC son conocidas por su robustez y confiabilidad, con características como redundancia incorporada y corrección de errores.

Ancho de banda dedicado: FC proporciona ancho de banda dedicado para el tráfico de almacenamiento, lo que reduce el riesgo de congestión de la red.

Para obtener más información sobre el uso de Fibre Channel con sistemas de almacenamiento NetApp , consulte "Aprovisionamiento de SAN con FC" .

Descripción general del escenario

El almacén de datos complementario VCF se aprovisiona como parte de las operaciones del día 2 mediante vCenter. Este escenario cubre los siguientes pasos de alto nivel:

- Implementación de herramientas ONTAP en el dominio de gestión
- Registrar servidores vCenter de carga de trabajo VI en las herramientas ONTAP
- Definir el backend de almacenamiento en el complemento de herramientas ONTAP para VMware vSphere
- Aprovisionar VMFS en el transporte FC

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP AFF o ASA con puertos FC conectados a conmutadores FC.
- SVM creado con FC lifs.
- vSphere con HBA FC conectados a conmutadores FC.
- La zonificación de iniciador-destino único está configurada en los conmutadores FC.

> Utilice la interfaz lógica SVM FC en la configuración de zona en lugar de puertos FC físicos en los sistemas ONTAP .

NetApp recomienda múltiples rutas para LUN FC.

Para obtener información completa sobre la configuración del canal de fibra en los sistemas de almacenamiento ONTAP , consulte "Gestión de almacenamiento SAN" en la documentación de ONTAP 9.

Para obtener más información sobre el uso de VMFS con sistemas de almacenamiento ONTAP , consulte la"Guía de implementación para VMFS" .

Pasos de implementación para el dominio de carga de trabajo VI

Para implementar ONTAP Tools y usarlo para crear un almacén de datos VMFS en el dominio de carga de trabajo VCF VI, complete los siguientes pasos:

- "Registrar la carga de trabajo VI vCenter para habilitar el complemento vCenter"
- "Definir el backend de almacenamiento mediante la interfaz del cliente vSphere"
- "Aprovisionar VMFS en FC"

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Demostración en vídeo de esta solución

Almacén de datos VMFS(FC) como almacenamiento complementario para el dominio de administración de VCF

Proteger VCF con SnapCenter

Obtenga información sobre cómo proteger los dominios de carga de trabajo VCF con el complemento SnapCenter para VMware vSphere

Obtenga información sobre las soluciones de NetApp que puede utilizar para proteger las cargas de trabajo de VMware Cloud Foundation (VCF) con el SnapCenter Plug-in for VMware vSphere. Este complemento simplifica la copia de seguridad y la recuperación, garantizando copias de seguridad consistentes con las aplicaciones y optimizando el almacenamiento con las tecnologías de eficiencia de NetApp.

Admite flujos de trabajo automatizados y operaciones escalables al tiempo que proporciona una integración perfecta con el cliente vSphere. Con la replicación de SnapMirror , que proporciona copias de seguridad secundarias en las instalaciones o en la nube, se ofrece protección de datos sólida y eficiencia operativa en entornos virtualizados.

Consulte las siguientes soluciones para obtener más detalles.

- "Proteger el dominio de carga de trabajo VCF"
- "Proteger múltiples dominios de carga de trabajo de VCF"
- "Proteger el dominio de carga de trabajo VCF con NVMe"
- "Protección de datos 3-2-1 para VMware con complemento SnapCenter y BlueXP backup and recovery para máquinas virtuales"

Proteja un dominio de carga de trabajo VCF con el complemento SnapCenter para VMware vSphere

En este caso de uso, describimos el procedimiento para utilizar el complemento SnapCenter para VMware vSphere para realizar copias de seguridad y restaurar máquinas virtuales y almacenes de datos en un dominio de carga de trabajo de VMware Cloud Foundation (VCF). Este procedimiento resume la implementación del complemento SnapCenter para VMware vSphere, la adición de sistemas de almacenamiento, la creación de políticas de respaldo y la realización de restauraciones de máquinas virtuales y archivos.

iSCSI se utiliza como protocolo de almacenamiento para el almacén de datos VMFS en esta solución.

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Implemente el SnapCenter Plug-in for VMware vSphere (SCV) en el dominio de carga de trabajo VI.
- Añadir sistemas de almacenamiento a SCV.
- Crear políticas de respaldo en SCV.
- Crear grupos de recursos en SCV.
- Utilice SCV para realizar copias de seguridad de almacenes de datos o máquinas virtuales específicas.
- Utilice SCV para restaurar las máquinas virtuales a una ubicación alternativa en el clúster.
- Utilice SCV para restaurar archivos a un sistema de archivos de Windows.

Prerrequisitos

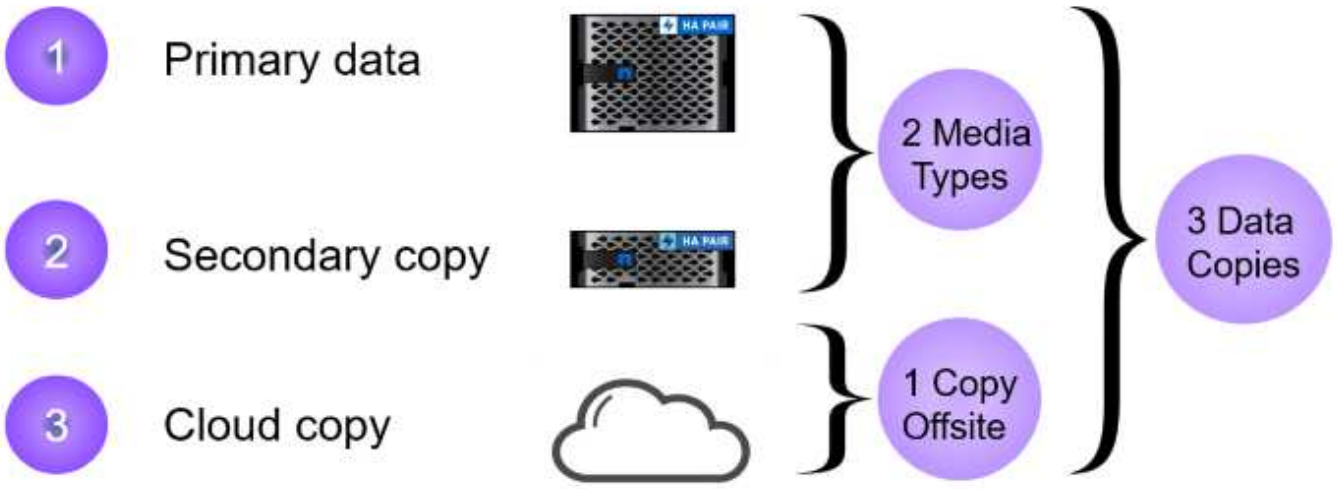
Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento ONTAP ASA con almacenes de datos VMFS iSCSI asignados al clúster de dominio de carga de trabajo.
- Un sistema de almacenamiento ONTAP secundario configurado para recibir copias de seguridad secundarias mediante SnapMirror.
- La implementación del dominio de administración de VCF está completa y el cliente vSphere es accesible.
- Previamente se ha implementado un dominio de carga de trabajo VI.
- Hay máquinas virtuales presentes en el clúster que SCV está diseñado para proteger.

Para obtener información sobre cómo configurar almacenes de datos VMFS iSCSI como almacenamiento complementario, consulte**"iSCSI como almacenamiento complementario para dominios de administración que utilizan herramientas ONTAP para VMware"** en esta documentación. El proceso para usar OTV para implementar almacenes de datos es idéntico para los dominios de administración y carga de

trabajo.

> Además de replicar copias de seguridad realizadas con SCV en un almacenamiento secundario, se pueden realizar copias de seguridad externas de datos en un almacenamiento de objetos en uno de los tres (3) proveedores de nube líderes que utilizan la BlueXP backup and recovery NetApp BlueXP para máquinas virtuales. Para obtener más información consulte la solución."Protección de datos 3-2-1 para VMware con complemento SnapCenter y BlueXP backup and recovery para máquinas virtuales" .



Pasos de implementación

Para implementar el complemento SnapCenter y usarlo para crear copias de seguridad y restaurar máquinas virtuales y almacenes de datos, complete los siguientes pasos:

Implementar y usar SCV para proteger datos en un dominio de carga de trabajo VI

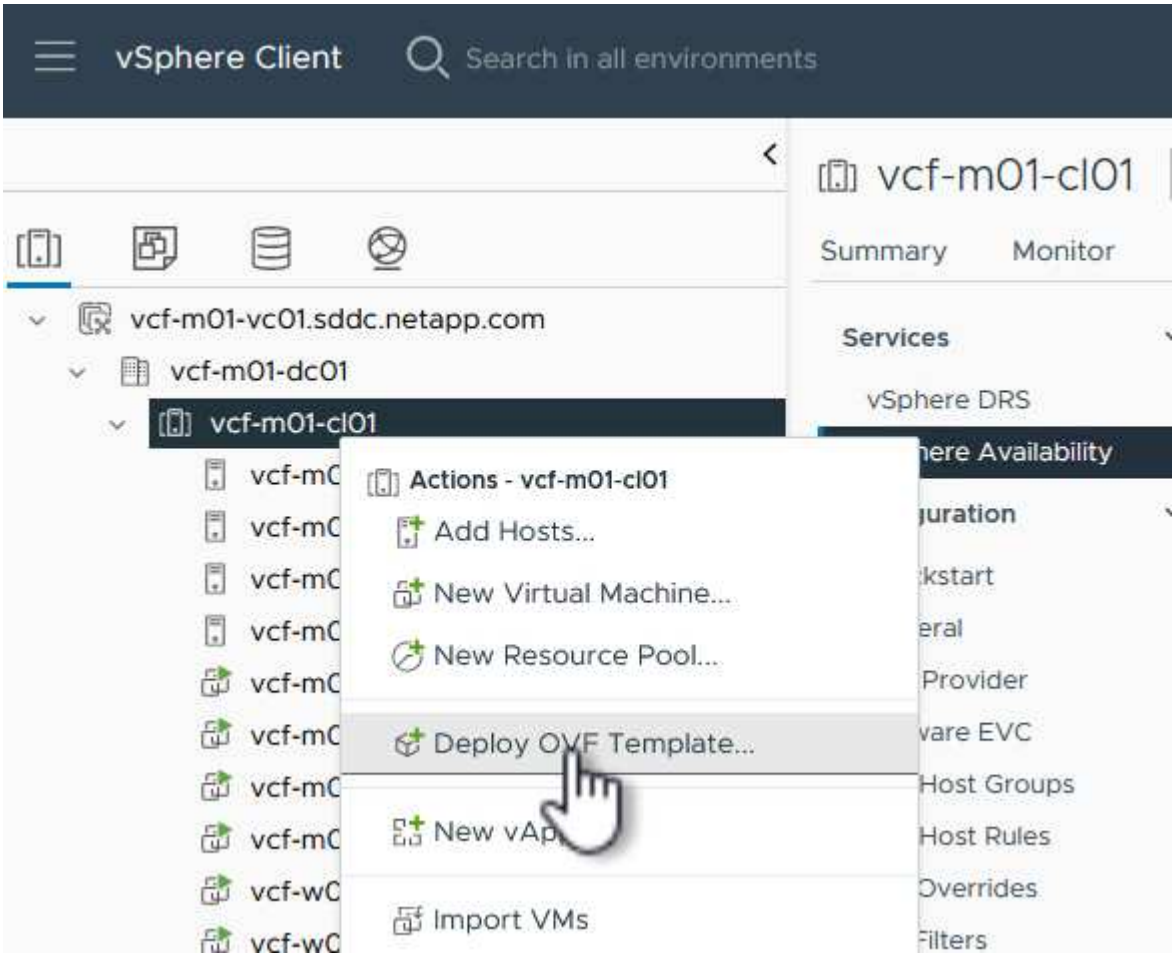
Complete los siguientes pasos para implementar, configurar y usar SCV para proteger datos en un dominio de carga de trabajo VI:

Implementar el SnapCenter Plug-in for VMware vSphere

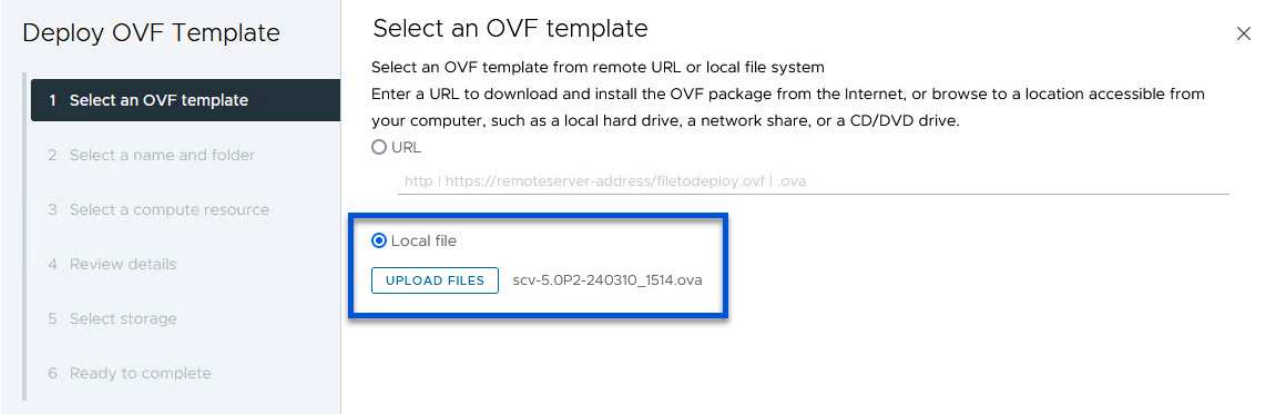
El complemento SnapCenter está alojado en el dominio de administración de VCF, pero registrado en vCenter para el dominio de carga de trabajo de VI. Se requiere una instancia de SCV para cada instancia de vCenter y tenga en cuenta que un dominio de carga de trabajo puede incluir varios clústeres administrados por una sola instancia de vCenter.

Complete los siguientes pasos desde el cliente vCenter para implementar SCV en el dominio de carga de trabajo de VI:

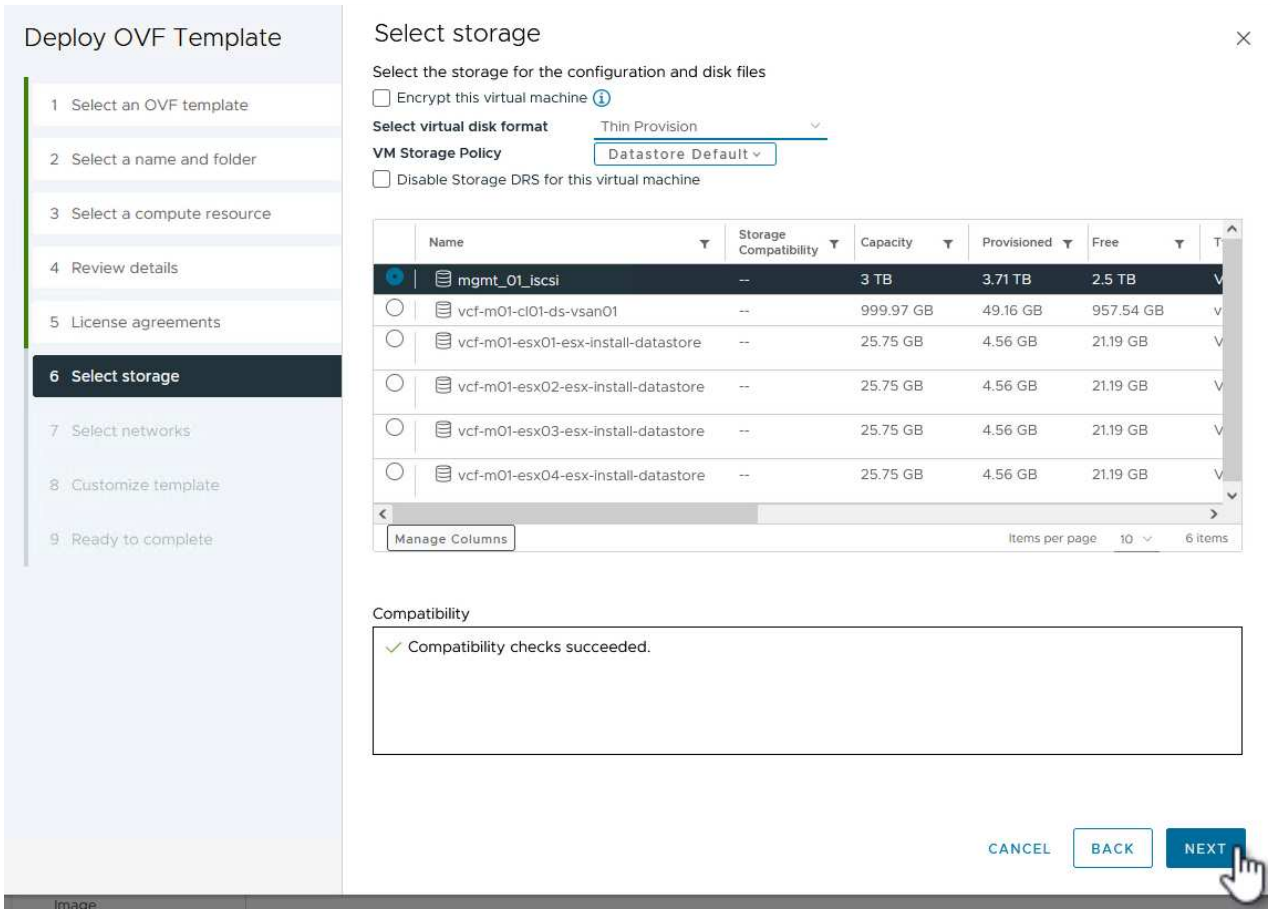
1. Descargue el archivo OVA para la implementación de SCV desde el área de descargas del sitio de soporte de NetApp"**AQUÍ**" .
2. Desde el dominio de administración vCenter Client, seleccione **Implementar plantilla OVF…**.



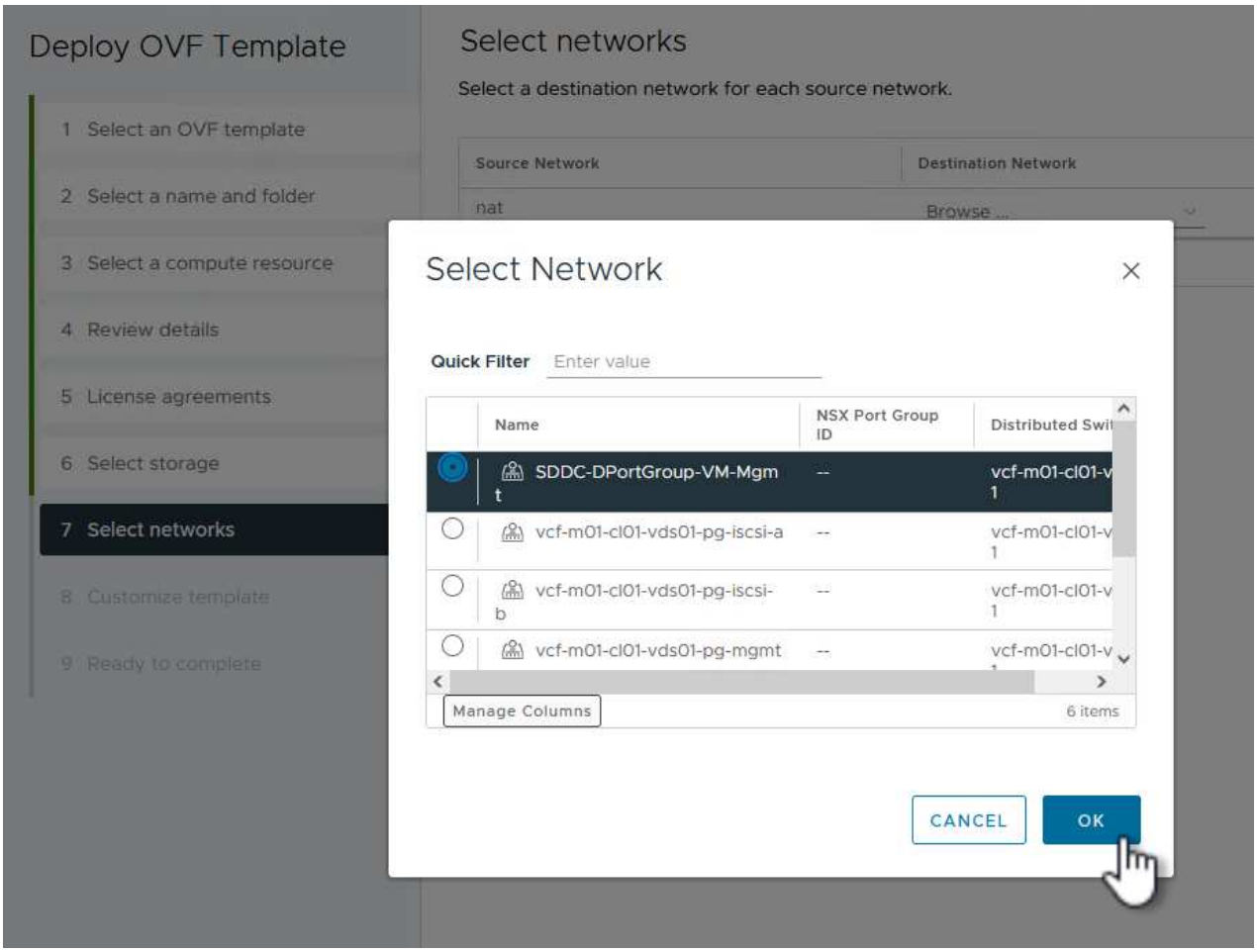
3. En el asistente **Implementar plantilla OVF**, haga clic en el botón de opción **Archivo local** y luego seleccione cargar la plantilla OVF descargada previamente. Haga clic en **Siguiente** para continuar.



4. En la página **Seleccionar nombre y carpeta**, proporcione un nombre para la máquina virtual del agente de datos SCV y una carpeta en el dominio de administración. Haga clic en **Siguiente** para continuar.
5. En la página **Seleccionar un recurso computacional**, seleccione el clúster de dominio de administración o el host ESXi específico dentro del clúster donde instalar la máquina virtual.
6. Revise la información correspondiente a la plantilla OVF en la página **Revisar detalles** y acepte los términos de licencia en la página **Acuerdos de licencia**.
7. En la página **Seleccionar almacenamiento**, elija el almacén de datos en el que se instalará la máquina virtual y seleccione el **formato de disco virtual** y la **Política de almacenamiento de la máquina virtual**. En esta solución, la VM se instalará en un almacén de datos VMFS iSCSI ubicado en un sistema de almacenamiento ONTAP , como se implementó anteriormente en una sección separada de esta documentación. Haga clic en **Siguiente** para continuar.



8. En la página **Seleccionar red**, seleccione la red de administración que puede comunicarse con el dispositivo vCenter del dominio de carga de trabajo y con los sistemas de almacenamiento ONTAP primario y secundario.



9. En la página **Personalizar plantilla** complete toda la información requerida para la implementación:
   - FQDN o IP y credenciales para el dispositivo vCenter del dominio de carga de trabajo.
   - Credenciales para la cuenta administrativa de SCV.
   - Credenciales para la cuenta de mantenimiento de SCV.
   - Detalles de propiedades de red IPv4 (también se puede utilizar IPv6).
   - Configuración de fecha y hora.

     Haga clic en **Siguiente** para continuar.

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

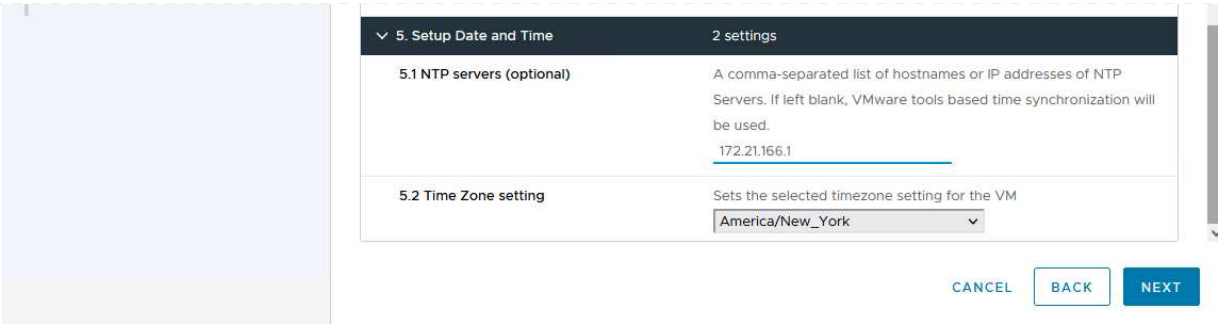
1. Register to existing vCenter	4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com
1.2 vCenter username	administrator@vcf.local
1.3 vCenter password	Password ••••••••• Confirm Password •••••••••
1.4 vCenter port	443
2. Create SCV Credentials	**2 settings**
2.1 Username	admin
2.2 Password	Password ••••••••• Confirm Password •••••••••
3. System Configuration	**1 settings**

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

4.2 Setup IPv4 Network Properties	6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) 172.21.166.148
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) 255.255.255.0
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) 172.21.166.1
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) 10.61.185.231
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) 10.61.186.231
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) netapp.com,sddc.netapp.com
3.3 Setup IPv6 Network Properties	**6 settings**
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired)
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired)

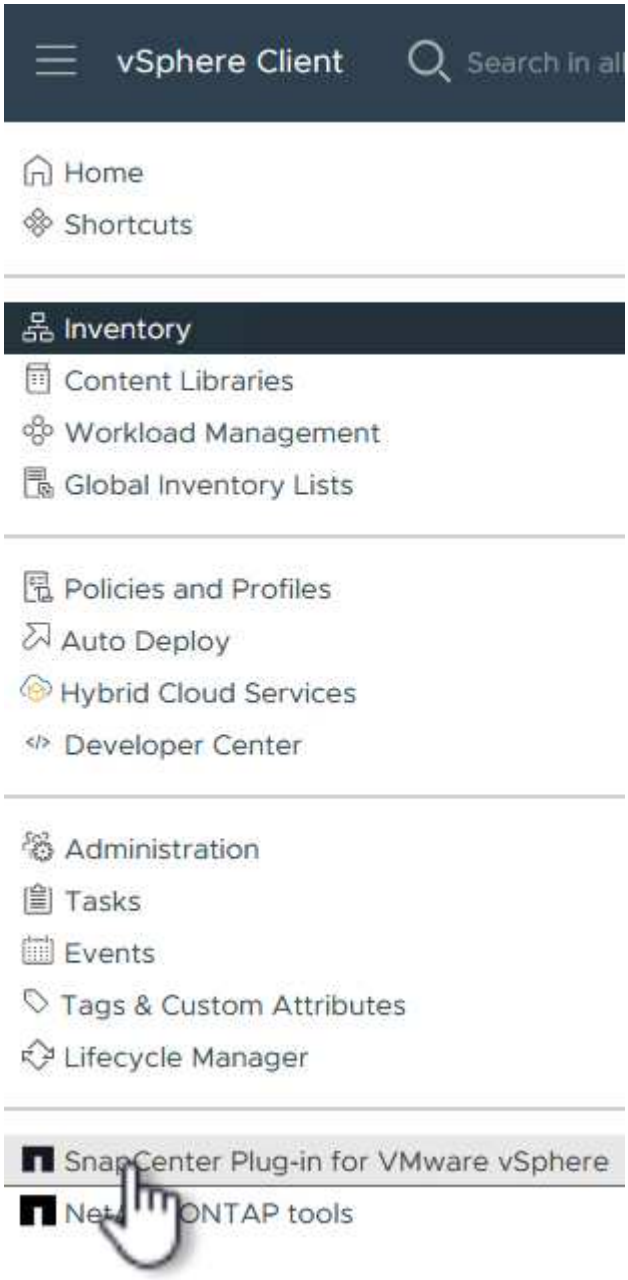


10. Finalmente, en la página **Listo para completar**, revise todas las configuraciones y haga clic en Finalizar para iniciar la implementación.

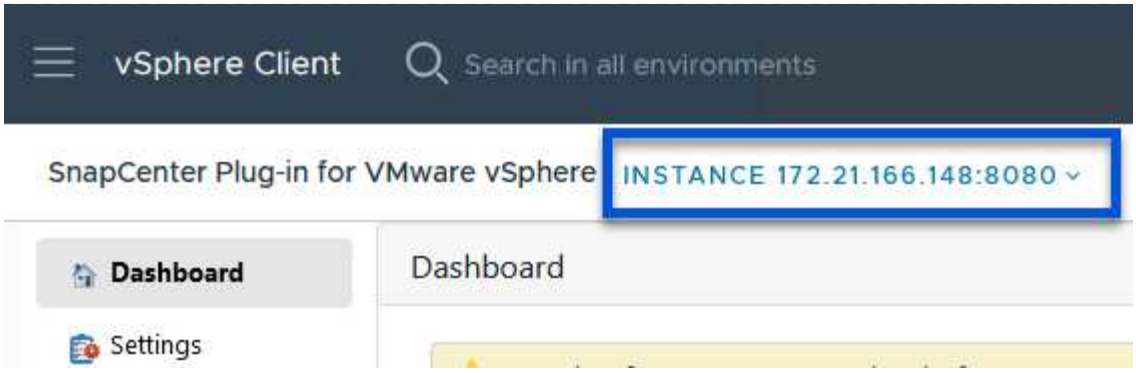
Añadir sistemas de almacenamiento a SCV

Una vez instalado el complemento SnapCenter , complete los siguientes pasos para agregar sistemas de almacenamiento a SCV:

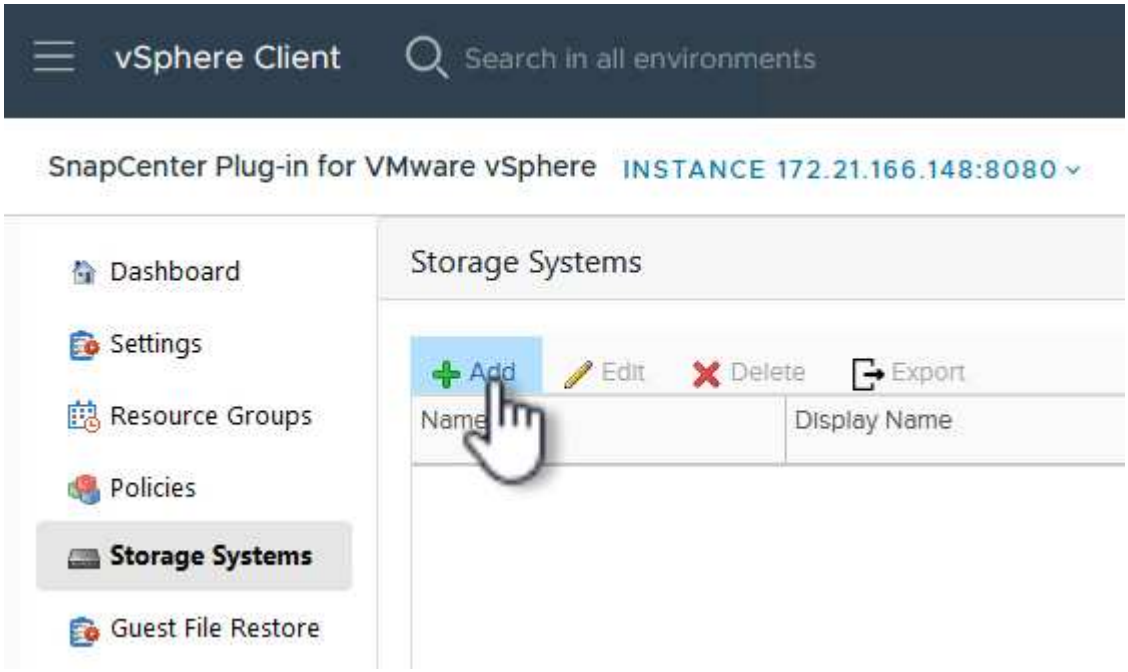
1. Se puede acceder a SCV desde el menú principal del cliente vSphere.



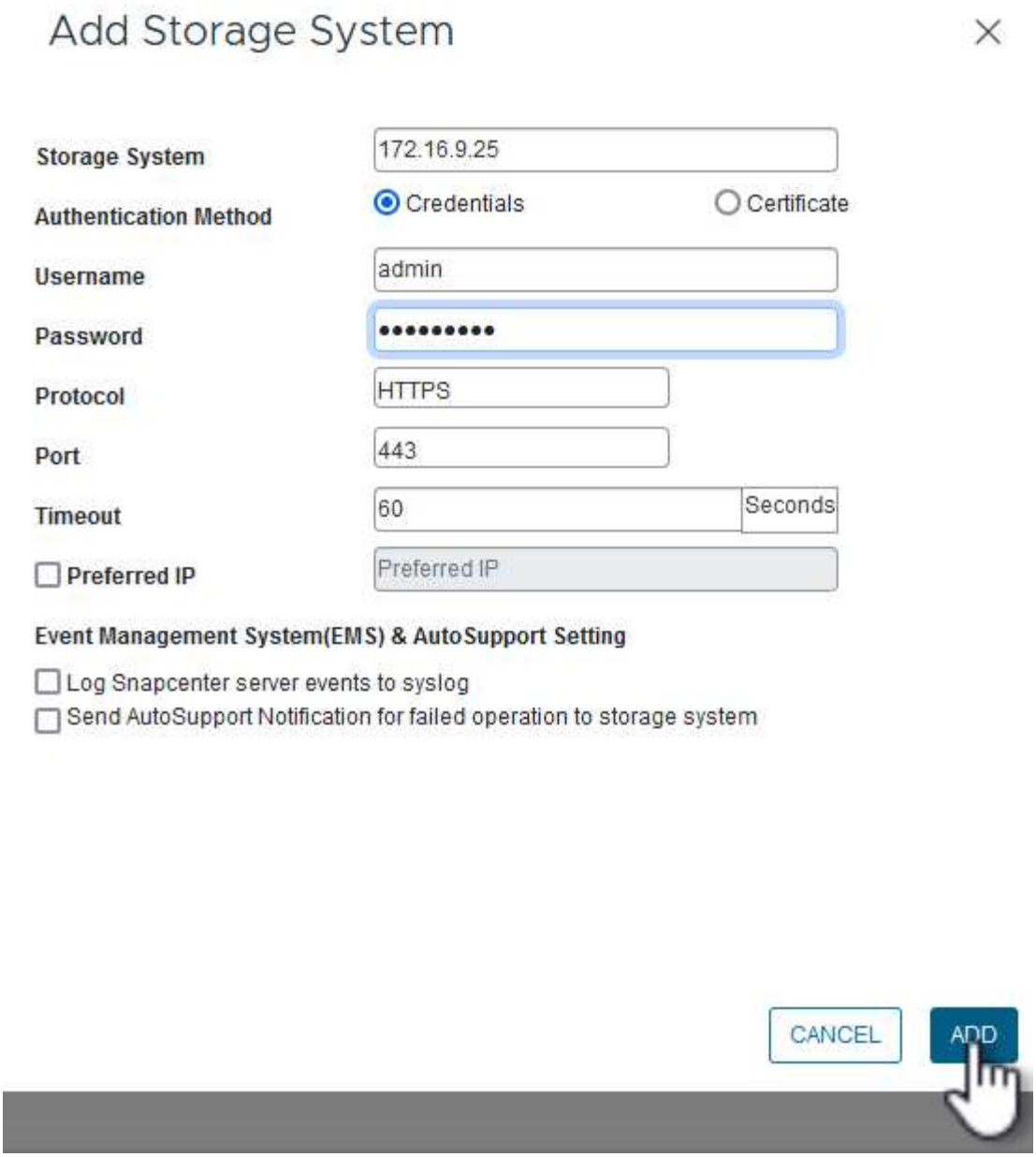
2. En la parte superior de la interfaz de usuario de SCV, seleccione la instancia de SCV correcta que coincida con el clúster de vSphere que se protegerá.



3. Vaya a **Sistemas de almacenamiento** en el menú de la izquierda y haga clic en **Agregar** para comenzar.



4. En el formulario **Agregar sistema de almacenamiento**, complete la dirección IP y las credenciales del sistema de almacenamiento ONTAP que se agregará y haga clic en **Agregar** para completar la acción.



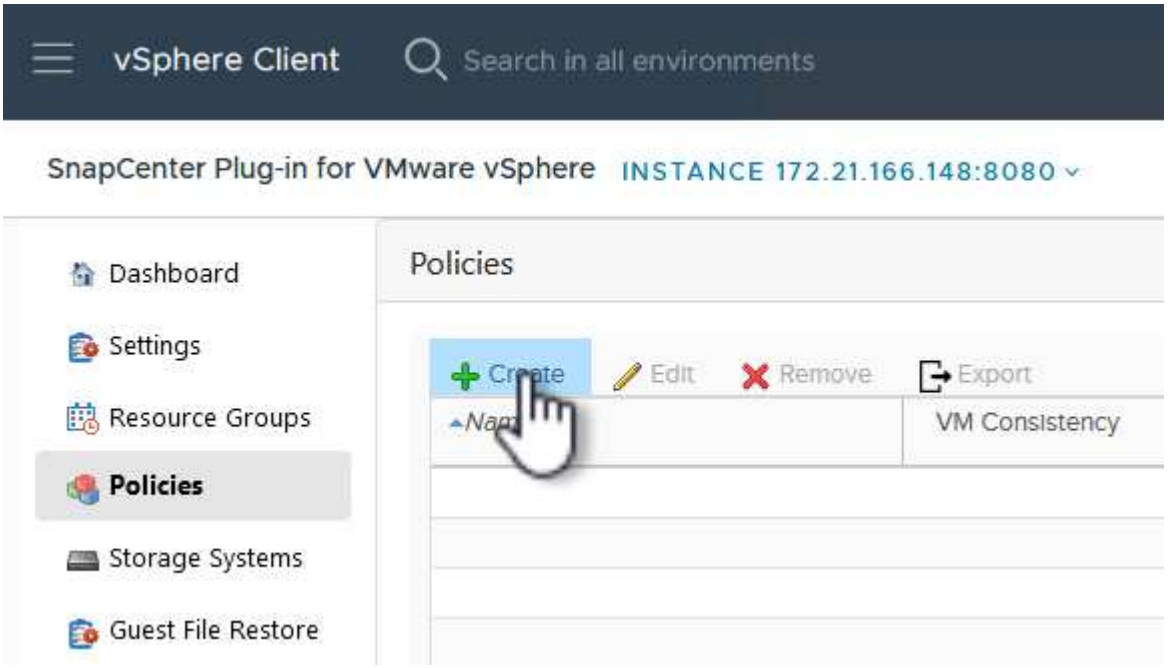
5. Repita este procedimiento para cualquier sistema de almacenamiento adicional que se vaya a administrar, incluido cualquier sistema que se vaya a utilizar como destino de respaldo secundario.

Configurar políticas de respaldo en SCV

Para obtener más información sobre la creación de políticas de respaldo de SCV, consulte"Crear políticas de respaldo para máquinas virtuales y almacenes de datos" .

Complete los siguientes pasos para crear una nueva política de respaldo:

1. En el menú de la izquierda, seleccione **Políticas** y haga clic en **Crear** para comenzar.



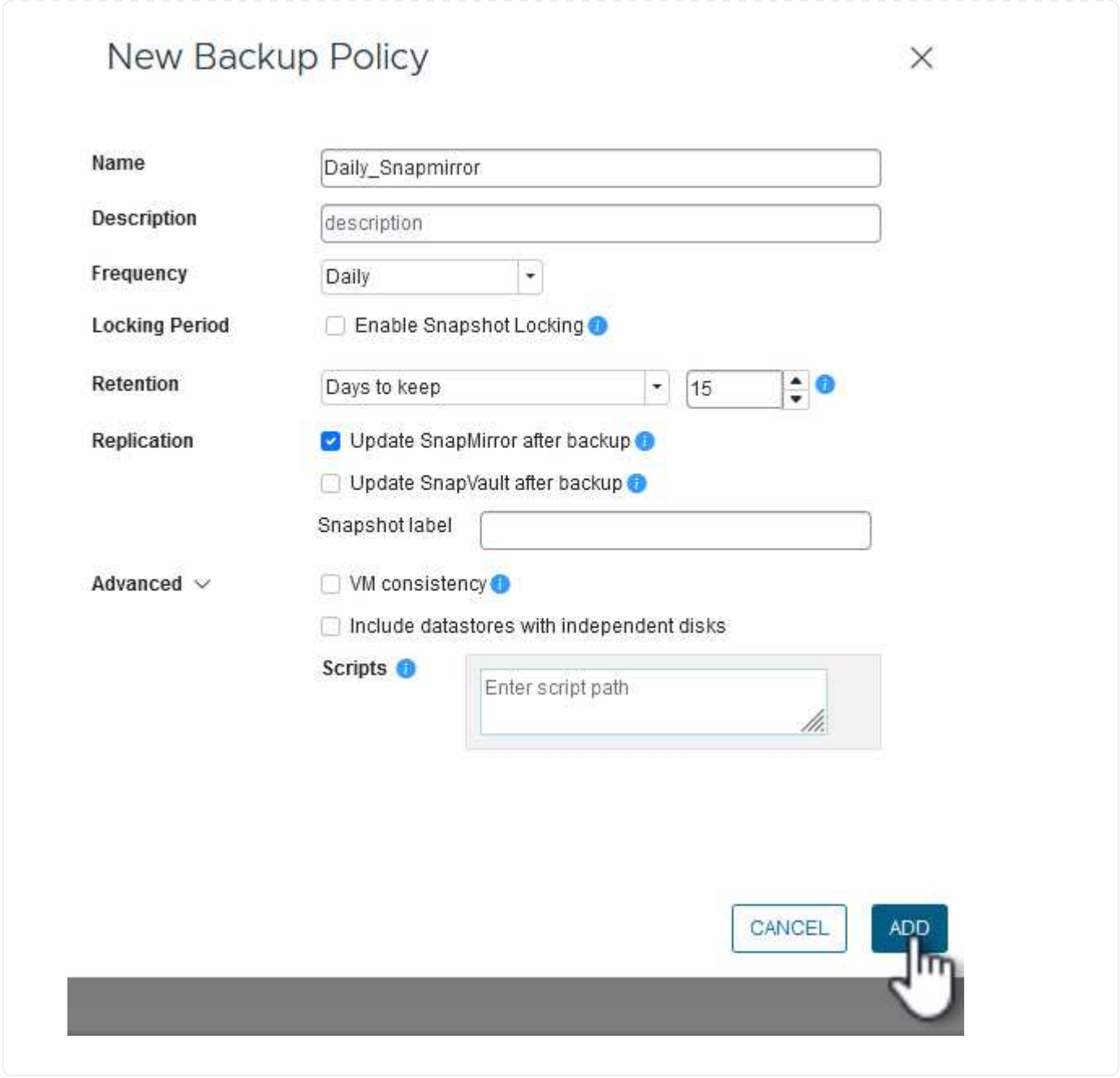
2. En el formulario **Nueva política de copias de seguridad**, proporcione un **Nombre** y una **Descripción** para la política, la **Frecuencia** con la que se realizarán las copias de seguridad y el **Período de retención** que especifica durante cuánto tiempo se conserva la copia de seguridad.

   Período de bloqueo habilita la función ONTAP SnapLock para crear instantáneas a prueba de manipulaciones y permite configurar el período de bloqueo.

   Para **Replicación**, seleccione para actualizar las relaciones subyacentes de SnapMirror o SnapVault para el volumen de almacenamiento de ONTAP .

   > La replicación de SnapMirror y SnapVault son similares en que ambas utilizan la tecnología ONTAP SnapMirror para replicar de forma asincrónica volúmenes de almacenamiento a un sistema de almacenamiento secundario para mayor protección y seguridad. Para las relaciones de SnapMirror , el programa de retención especificado en la política de respaldo de SCV regirá la retención tanto del volumen principal como del secundario. Con las relaciones de SnapVault , se puede establecer un programa de retención independiente en el sistema de almacenamiento secundario para programas de retención diferentes o de mayor duración. En este caso, la etiqueta de la instantánea se especifica en la política de respaldo de SCV y en la política asociada con el volumen secundario, para identificar a qué volúmenes aplicar el programa de retención independiente.

   Elija cualquier opción avanzada adicional y haga clic en **Agregar** para crear la política.

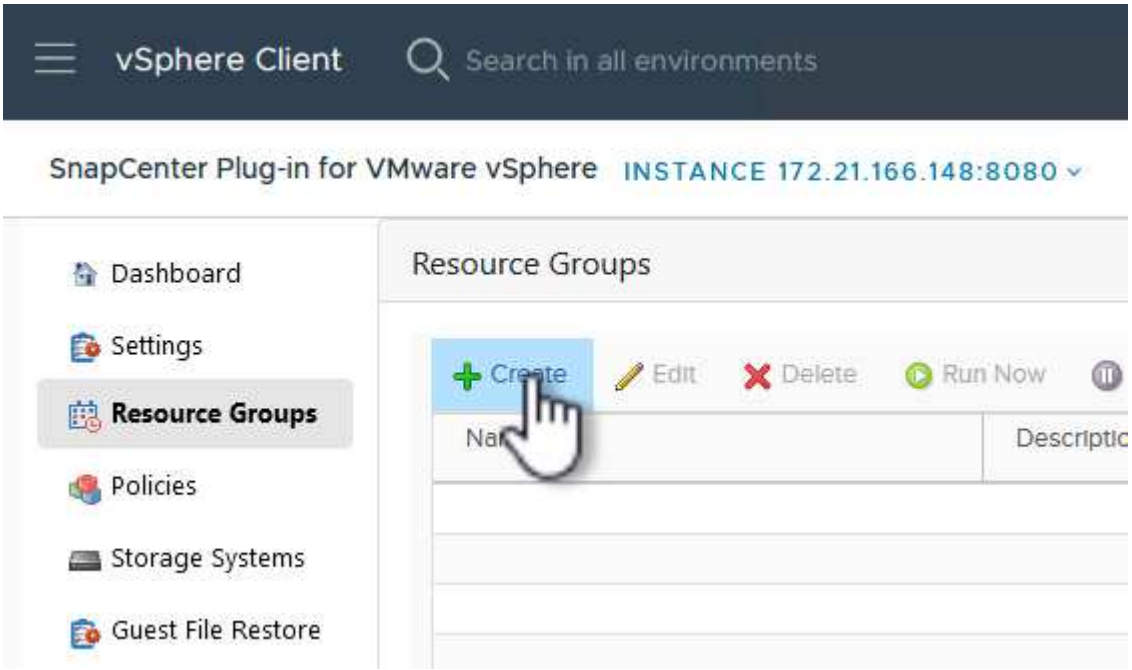

New Backup Policy
Name
Daily_Snapmirror
Description
description
Frequency
Daily
Locking Period
Enable Snapshot Locking
Retention
Days to keep
15
Replication
Update SnapMirror after backup
Update SnapVault after backup
Snapshot label
Advanced
VM consistency
Include datastores with independent disks
Scripts
Enter script path
CANCEL
ADD

Crear grupos de recursos en SCV

Para obtener más información sobre la creación de grupos de recursos de SCV, consulte"Crear grupos de recursos" .

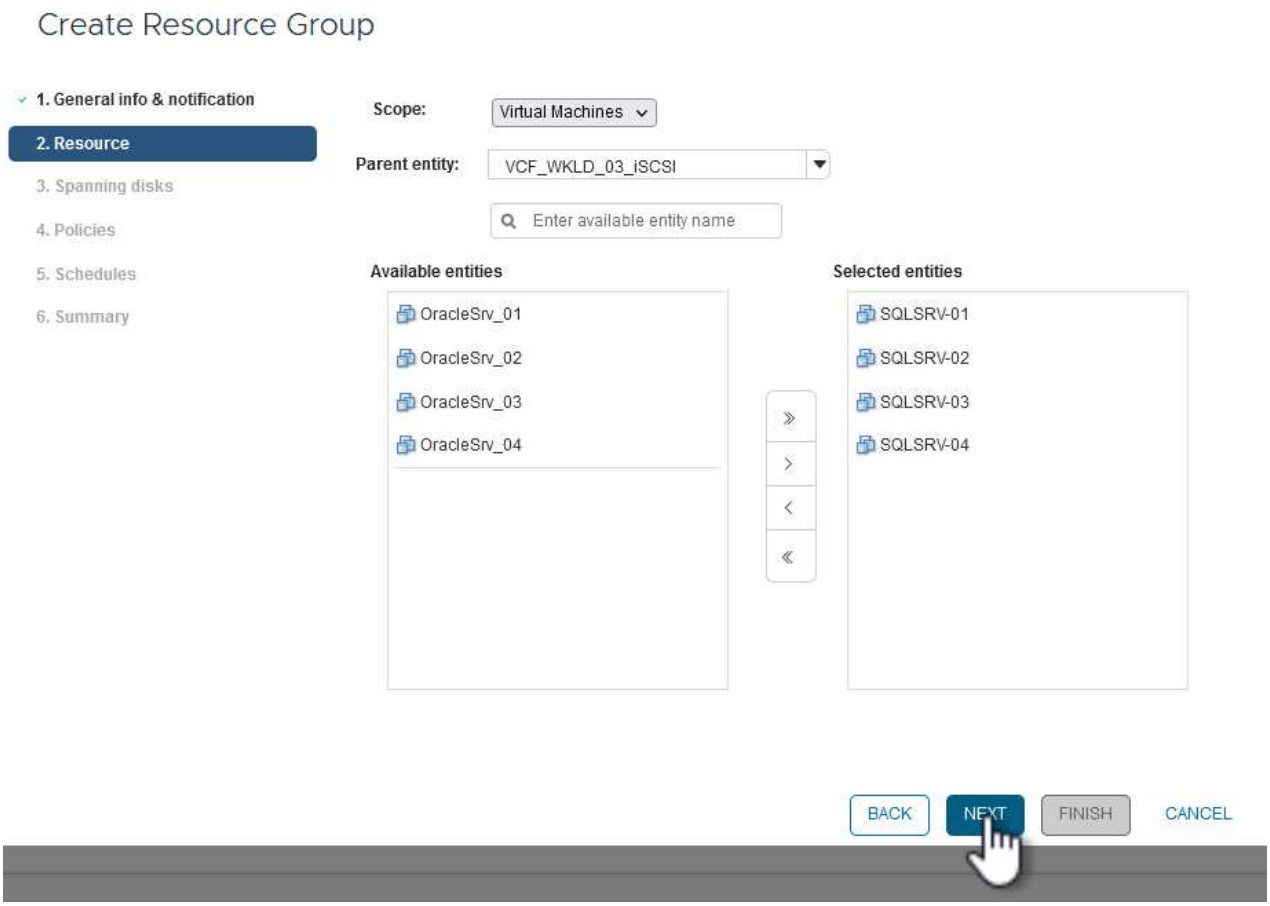
Complete los siguientes pasos para crear un nuevo grupo de recursos:

1. En el menú de la izquierda, seleccione **Grupos de recursos** y haga clic en **Crear** para comenzar.

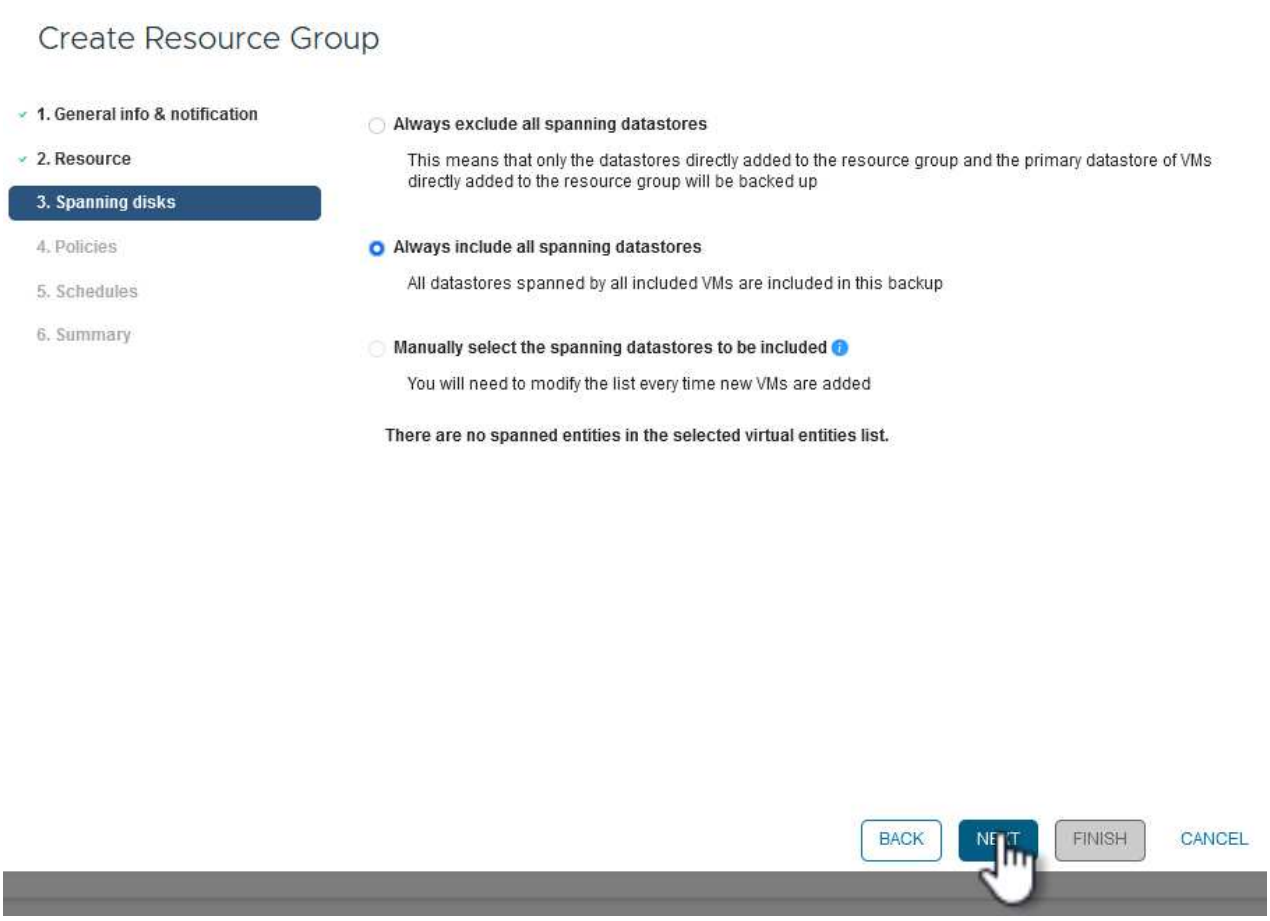


2. En la página **Información general y notificaciones**, proporcione un nombre para el grupo de recursos, configuraciones de notificación y cualquier opción adicional para nombrar las instantáneas.
3. En la página **Recursos**, seleccione los almacenes de datos y las máquinas virtuales que se protegerán en el grupo de recursos. Haga clic en **Siguiente** para continuar.

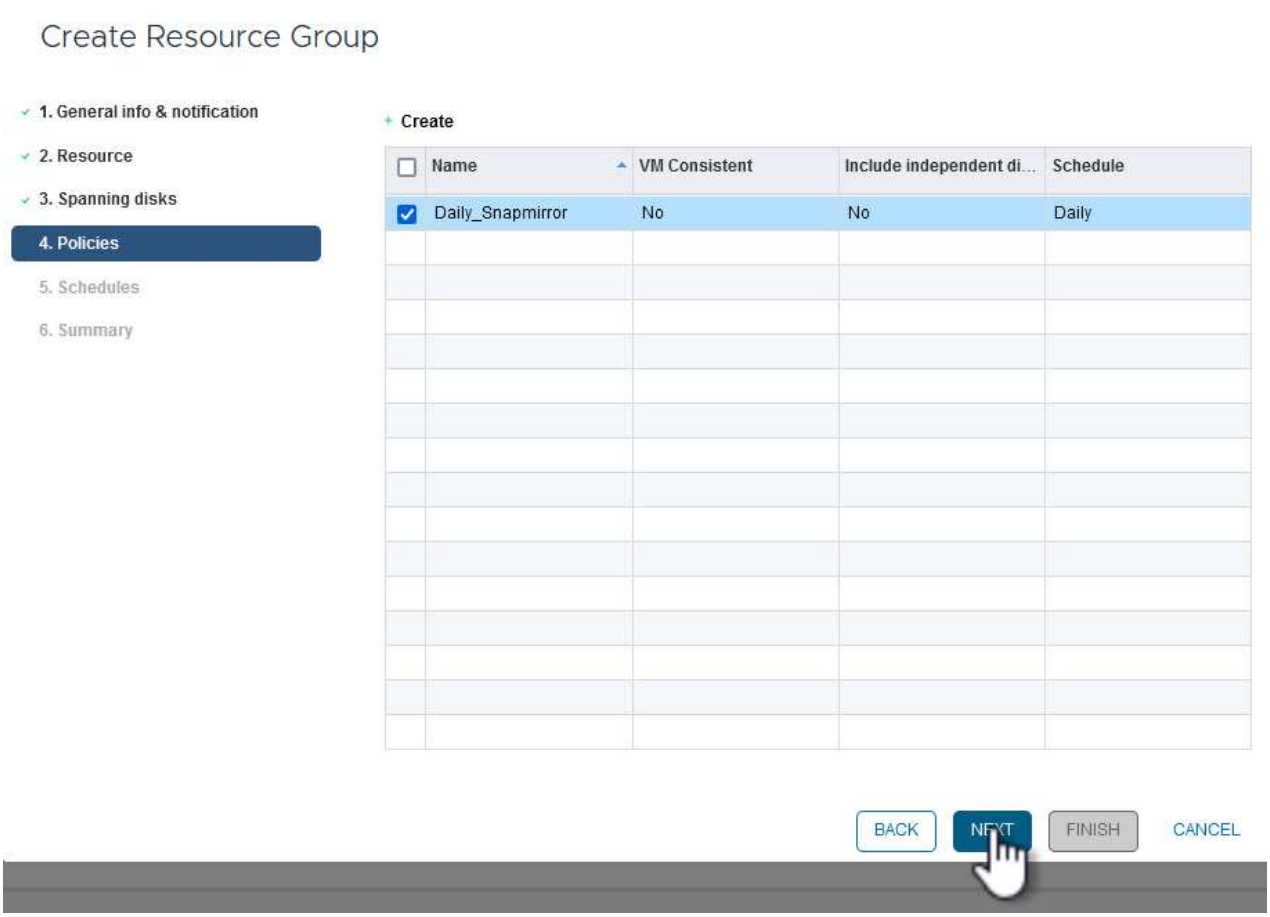
> Incluso cuando solo se seleccionan máquinas virtuales específicas, siempre se realiza un respaldo de todo el almacén de datos. Esto se debe a que ONTAP toma instantáneas del volumen que aloja el almacén de datos. Sin embargo, tenga en cuenta que seleccionar solo máquinas virtuales específicas para realizar la copia de seguridad limita la capacidad de restaurar solo a esas máquinas virtuales.



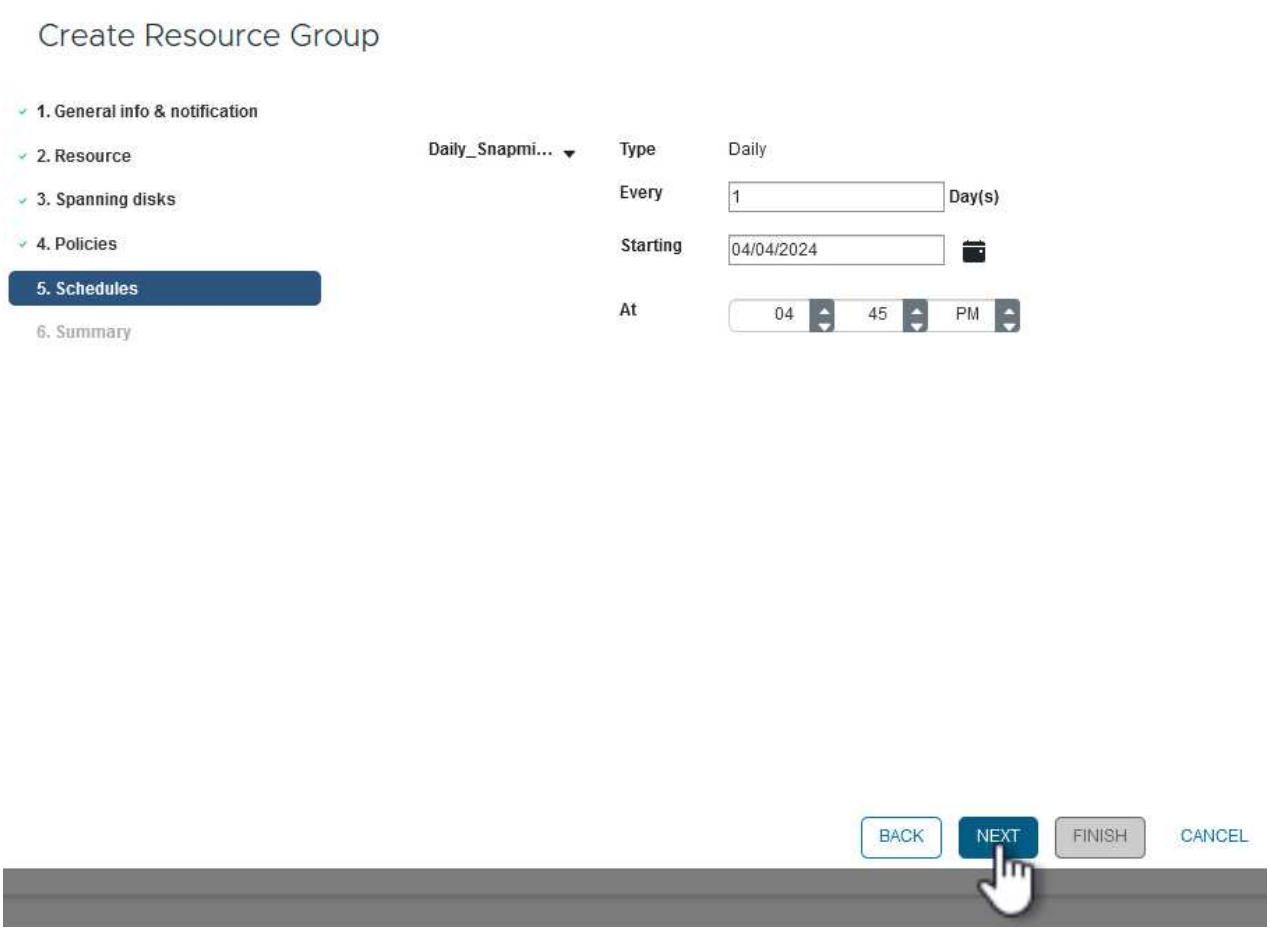
4. En la página **Discos de expansión**, seleccione la opción para manejar las máquinas virtuales con VMDK que abarcan varios almacenes de datos. Haga clic en **Siguiente** para continuar.



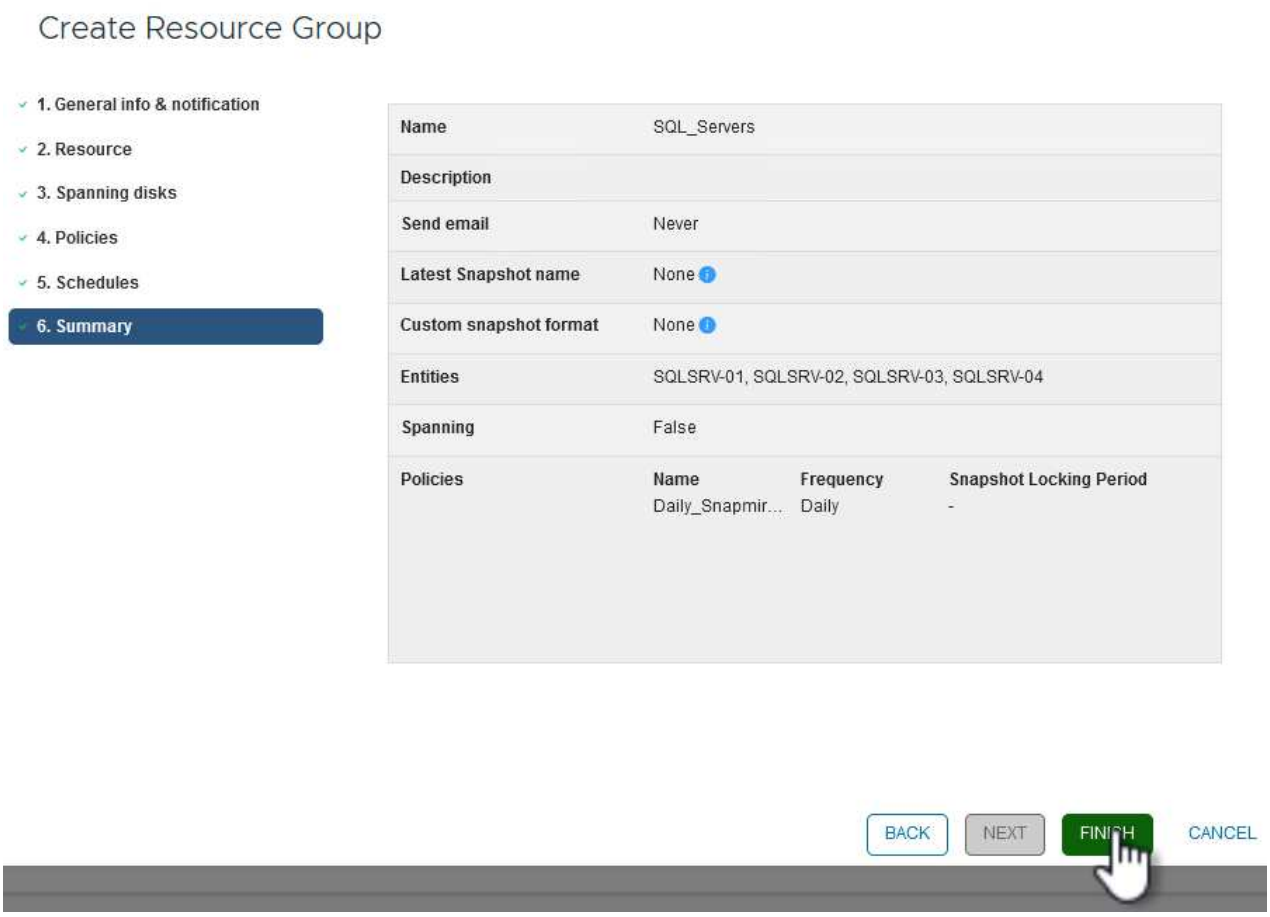
5. En la página **Políticas**, seleccione una política creada previamente o varias políticas que se utilizarán con este grupo de recursos. Haga clic en **Siguiente** para continuar.



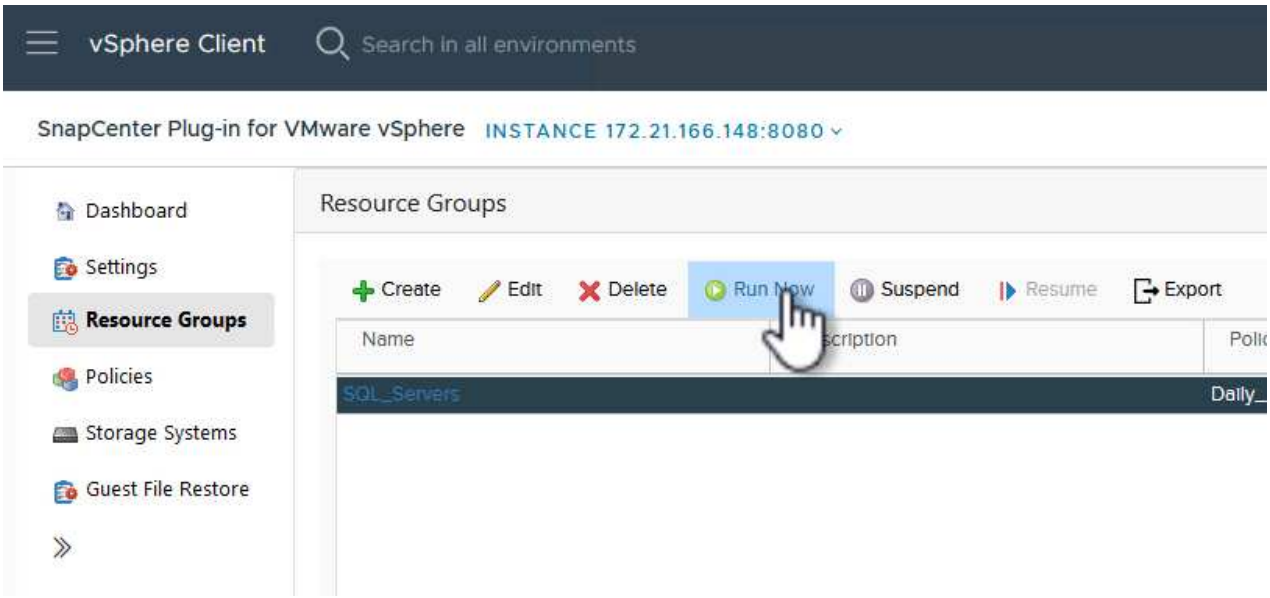
6. En la página **Horarios**, establezca cuándo se ejecutará la copia de seguridad configurando la recurrencia y la hora del día. Haga clic en **Siguiente** para continuar.



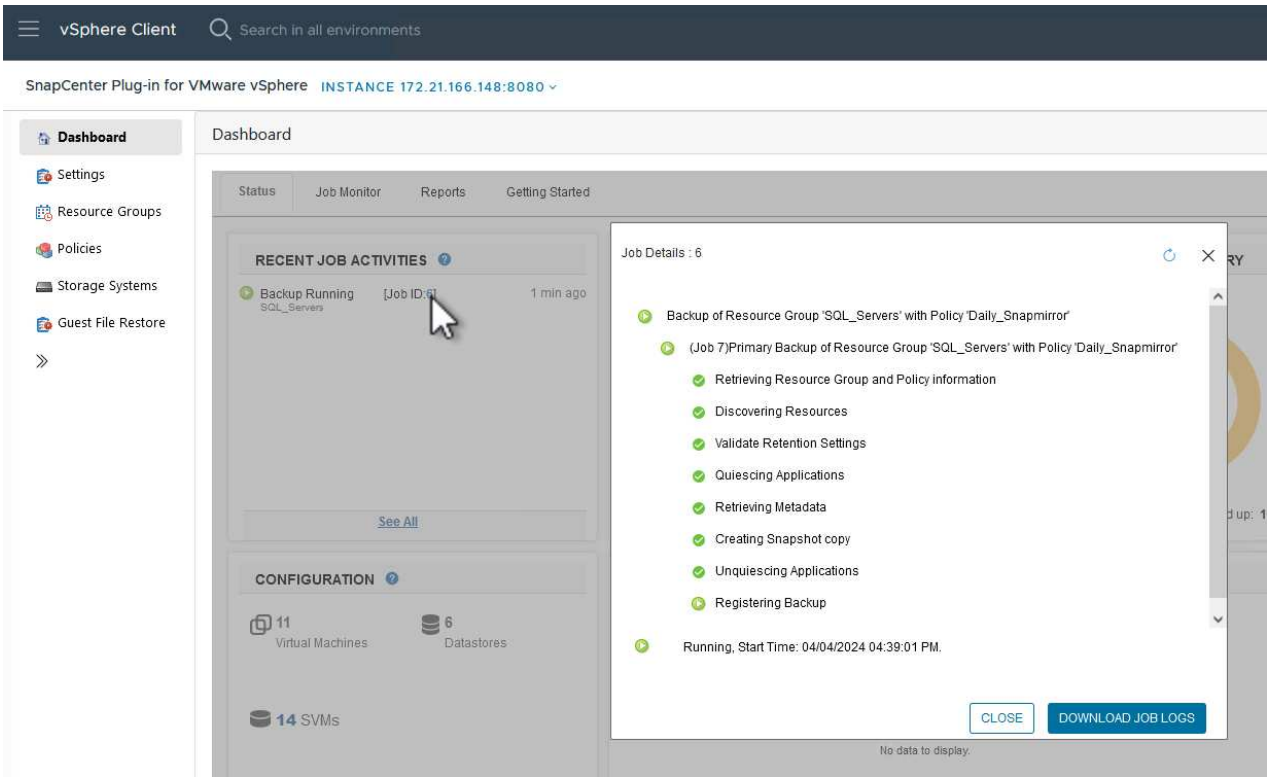
7. Finalmente revise el **Resumen** y haga clic en **Finalizar** para crear el grupo de recursos.



8. Con el grupo de recursos creado, haga clic en el botón **Ejecutar ahora** para ejecutar la primera copia de seguridad.



9. Vaya al **Panel de control** y, en **Actividades laborales recientes**, haga clic en el número junto a **ID de trabajo** para abrir el monitor de trabajo y ver el progreso del trabajo en ejecución.



Utilice SCV para restaurar máquinas virtuales, VMDK y archivos

El complemento SnapCenter permite restaurar máquinas virtuales, VMDK, archivos y carpetas desde copias de seguridad primarias o secundarias.

Las máquinas virtuales se pueden restaurar en el host original, en un host alternativo en el mismo vCenter Server o en un host ESXi alternativo administrado por el mismo vCenter o cualquier vCenter en modo vinculado.

Las máquinas virtuales vVol se pueden restaurar al host original.

Los VMDK en máquinas virtuales tradicionales se pueden restaurar en el almacén de datos original o en uno alternativo.

Los VMDK en las máquinas virtuales vVol se pueden restaurar al almacén de datos original.

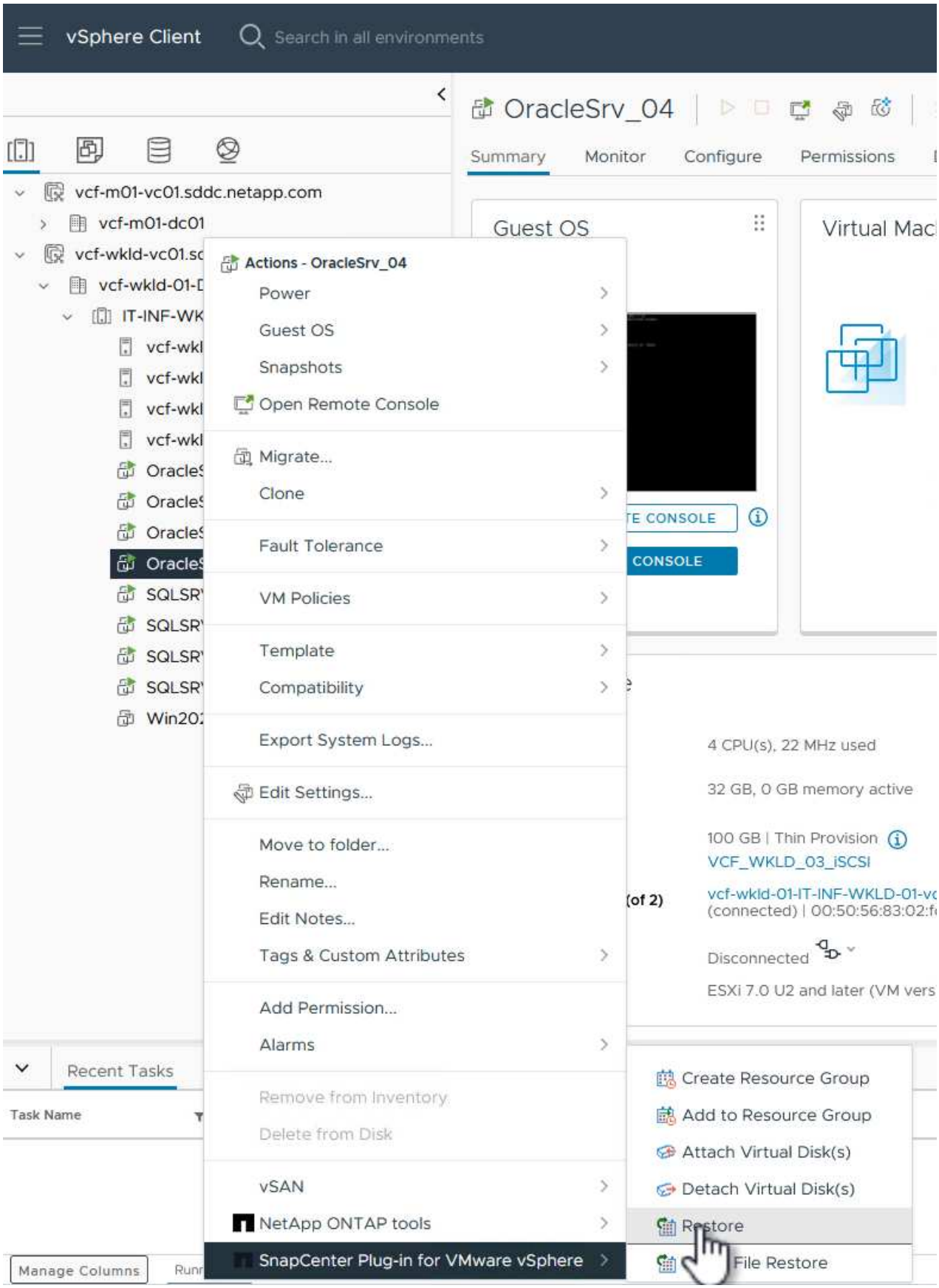
Se pueden restaurar archivos y carpetas individuales en una sesión de restauración de archivos invitados, lo que adjunta una copia de respaldo de un disco virtual y luego restaura los archivos o carpetas seleccionados.

Complete los siguientes pasos para restaurar máquinas virtuales, VMDK o carpetas individuales.

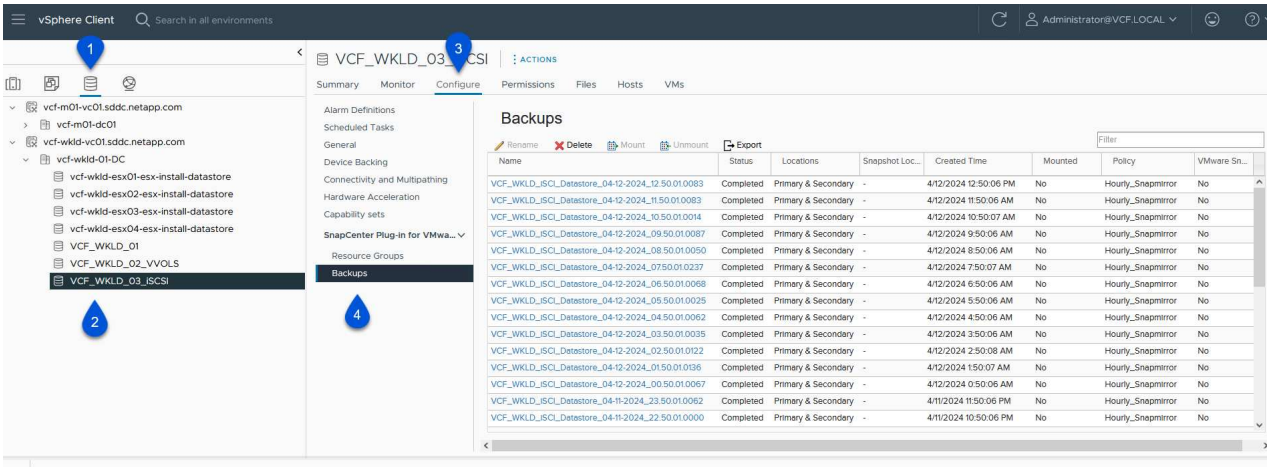
Restaurar máquinas virtuales mediante el complemento SnapCenter

Complete los siguientes pasos para restaurar una máquina virtual con SCV:

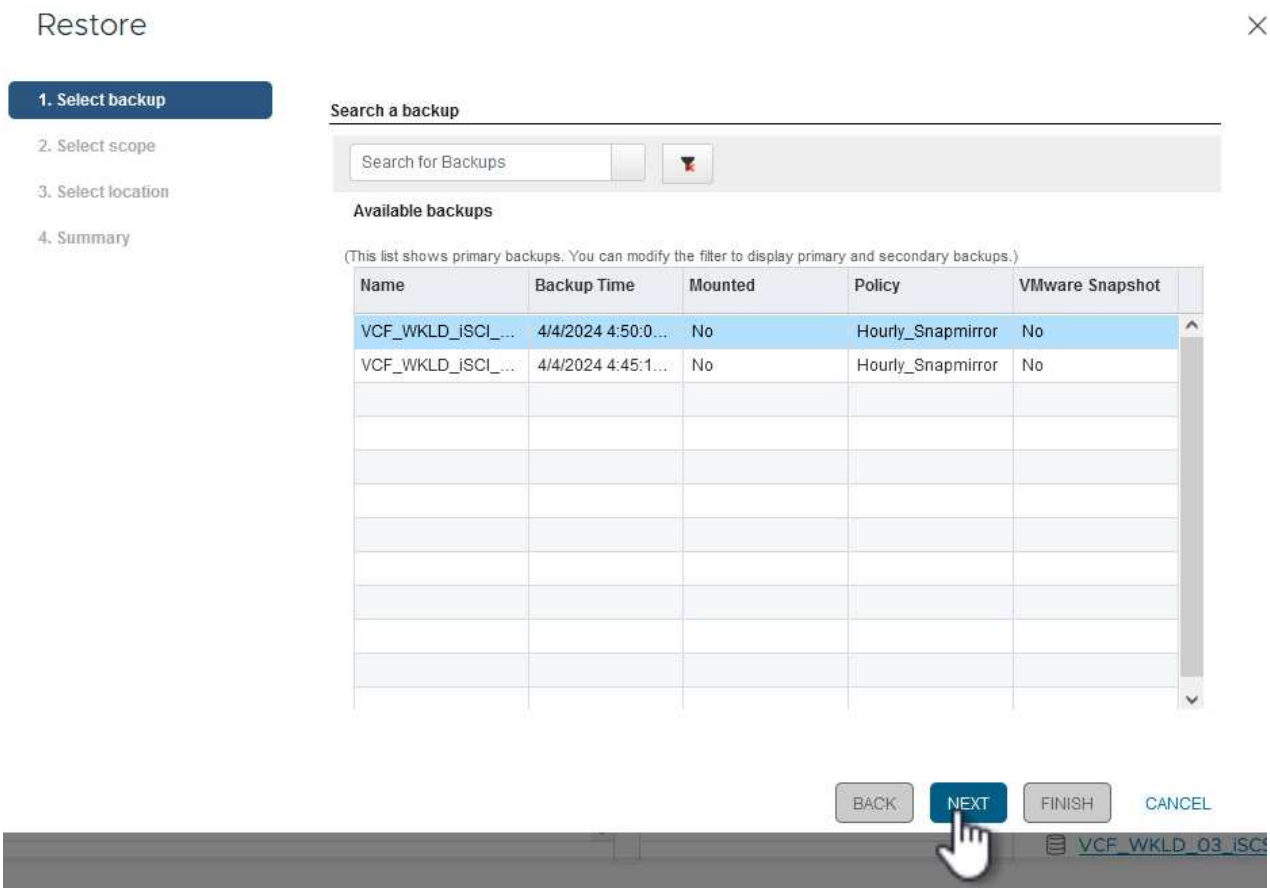
1. Navegue hasta la máquina virtual que se restaurará en el cliente vSphere, haga clic con el botón derecho y navegue hasta * SnapCenter Plug-in for VMware vSphere*. Seleccione **Restaurar** en el submenú.


vSphere Client
Search in all environments
OracleSrv_04
Summary
Monitor
Configure
Permissions
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
vcf-wkl
vcf-wkl
vcf-wkl
vcf-wkl
Oracle
Oracle
Oracle
Oracle
SQLSR
SQLSR
SQLSR
SQLSR
Win20
Guest OS
Virtual Mac
TE CONSOLE
CONSOLE
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
(of 2)
vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore

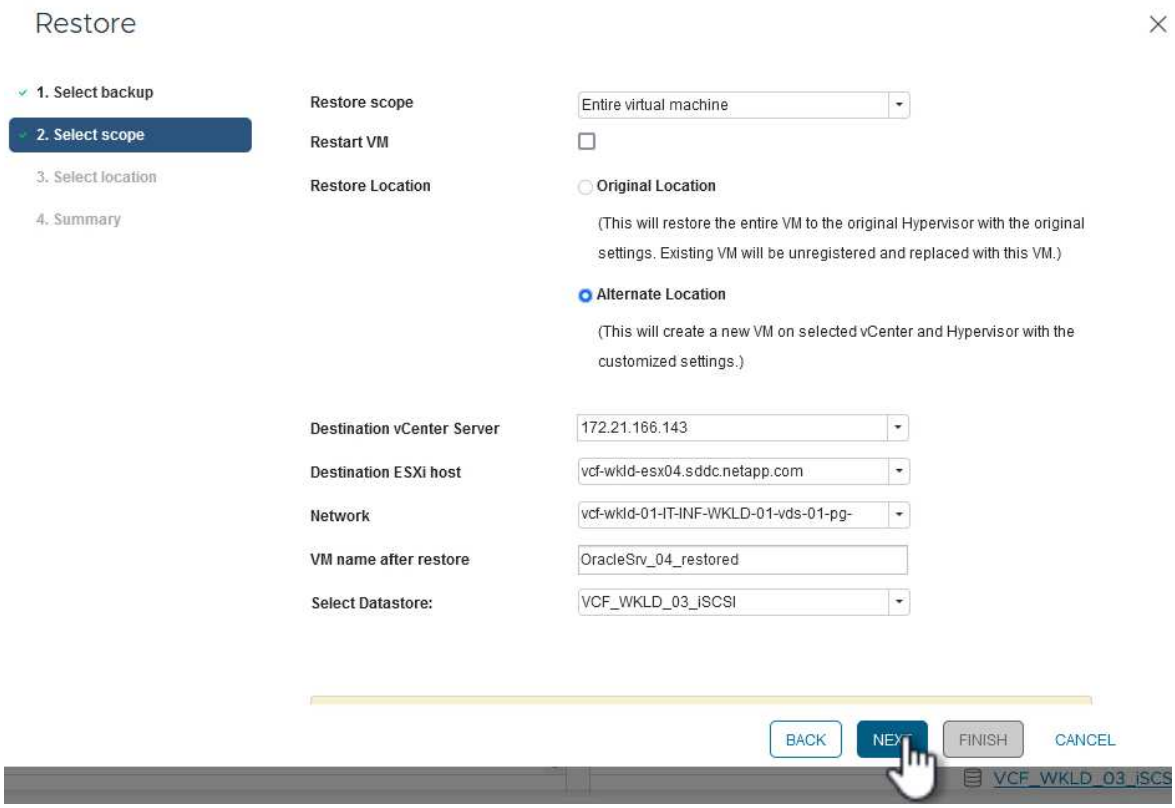
Una alternativa es navegar hasta el almacén de datos en el inventario y luego, en la pestaña **Configurar**, ir a * SnapCenter Plug-in for VMware vSphere > Copias de seguridad*. Desde la copia de seguridad elegida, seleccione las máquinas virtuales que se restaurarán.



2. En el asistente **Restaurar** seleccione la copia de seguridad que se utilizará. Haga clic en **Siguiente** para continuar.

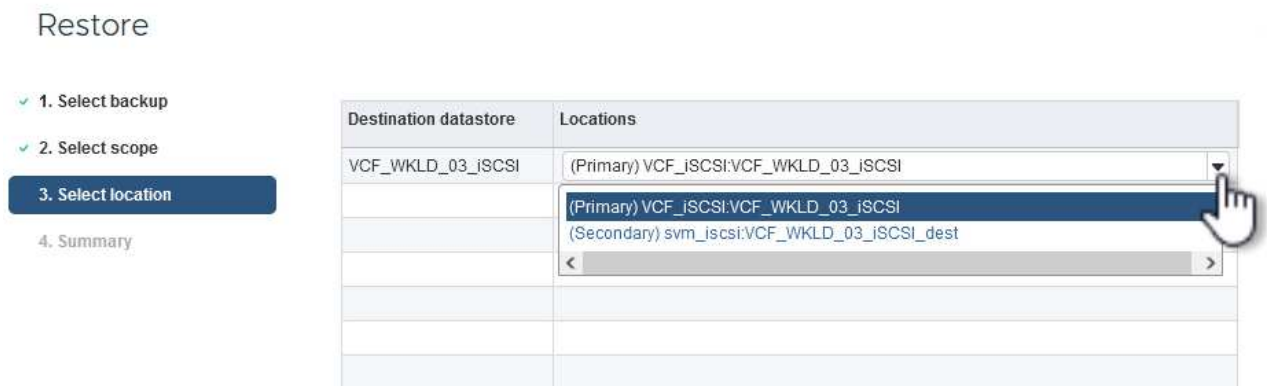


3. En la página **Seleccionar alcance** complete todos los campos obligatorios:
    - **Restaurar alcance**: seleccione esta opción para restaurar toda la máquina virtual.
    - **Reiniciar VM**: elige si deseas iniciar la VM después de la restauración.
    - **Restaurar ubicación**: elige restaurar a la ubicación original o a una ubicación alternativa. Al elegir ubicación alternativa seleccione las opciones de cada uno de los campos:
        - **Servidor vCenter de destino**: vCenter local o vCenter alternativo en modo vinculado
        - **Host ESXi de destino**
        - **Red**
        - **Nombre de la máquina virtual después de la restauración**
        - **Seleccionar almacén de datos:**

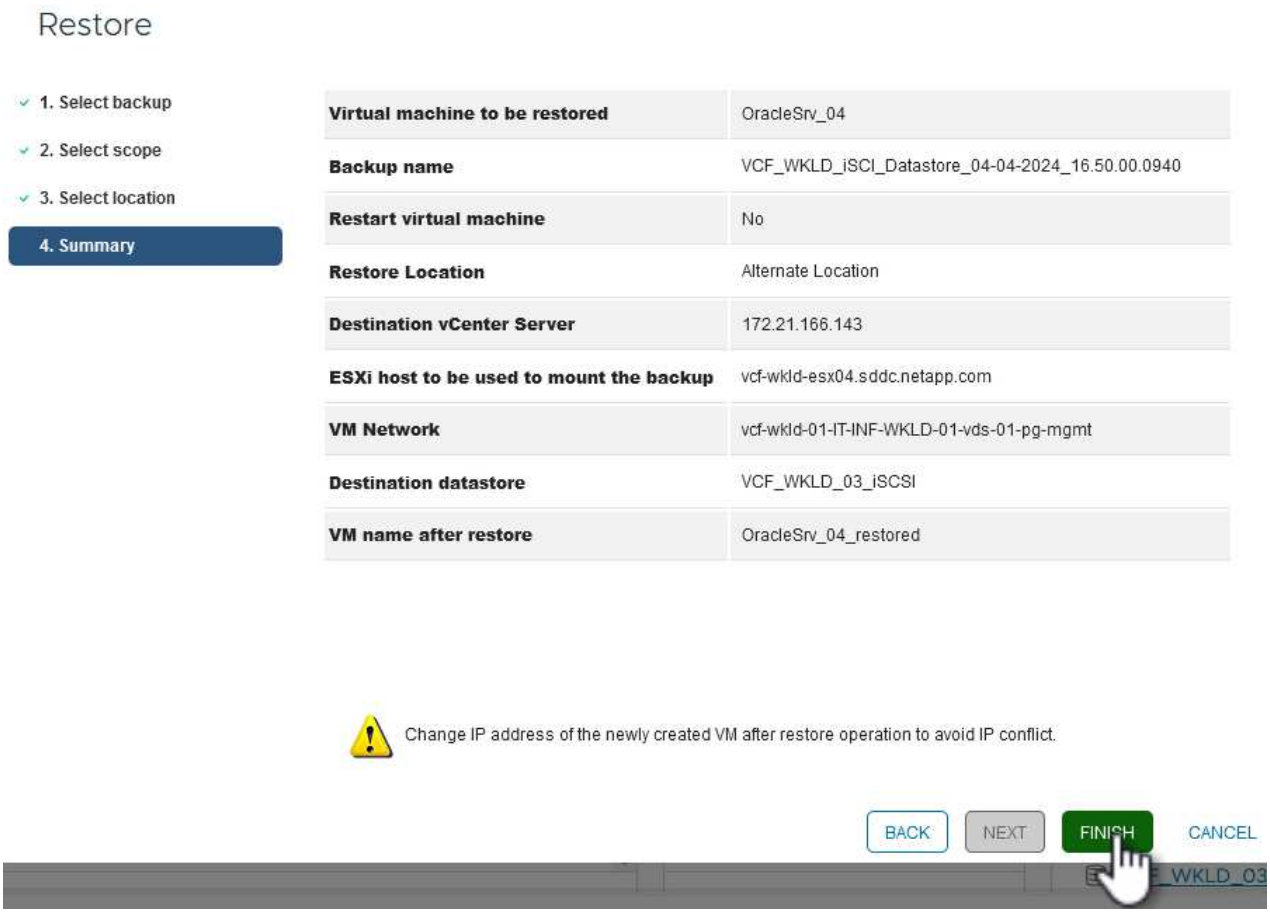


Haga clic en **Siguiente** para continuar.

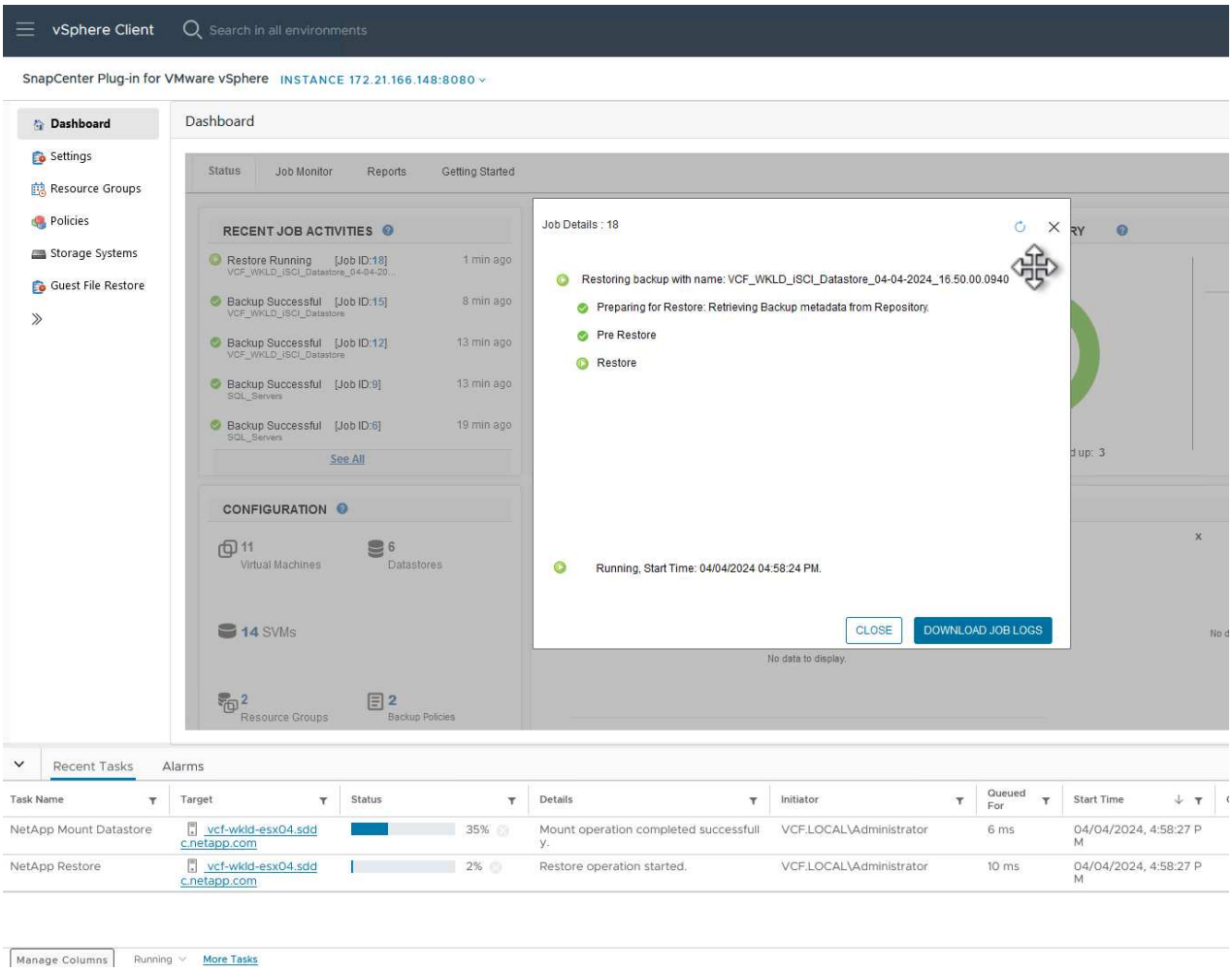
4. En la página **Seleccionar ubicación**, elija restaurar la VM desde el sistema de almacenamiento ONTAP primario o secundario. Haga clic en **Siguiente** para continuar.



5. Por último, revise el **Resumen** y haga clic en **Finalizar** para iniciar el trabajo de restauración.



6. El progreso del trabajo de restauración se puede monitorear desde el panel **Tareas recientes** en vSphere Client y desde el monitor de trabajos en SCV.

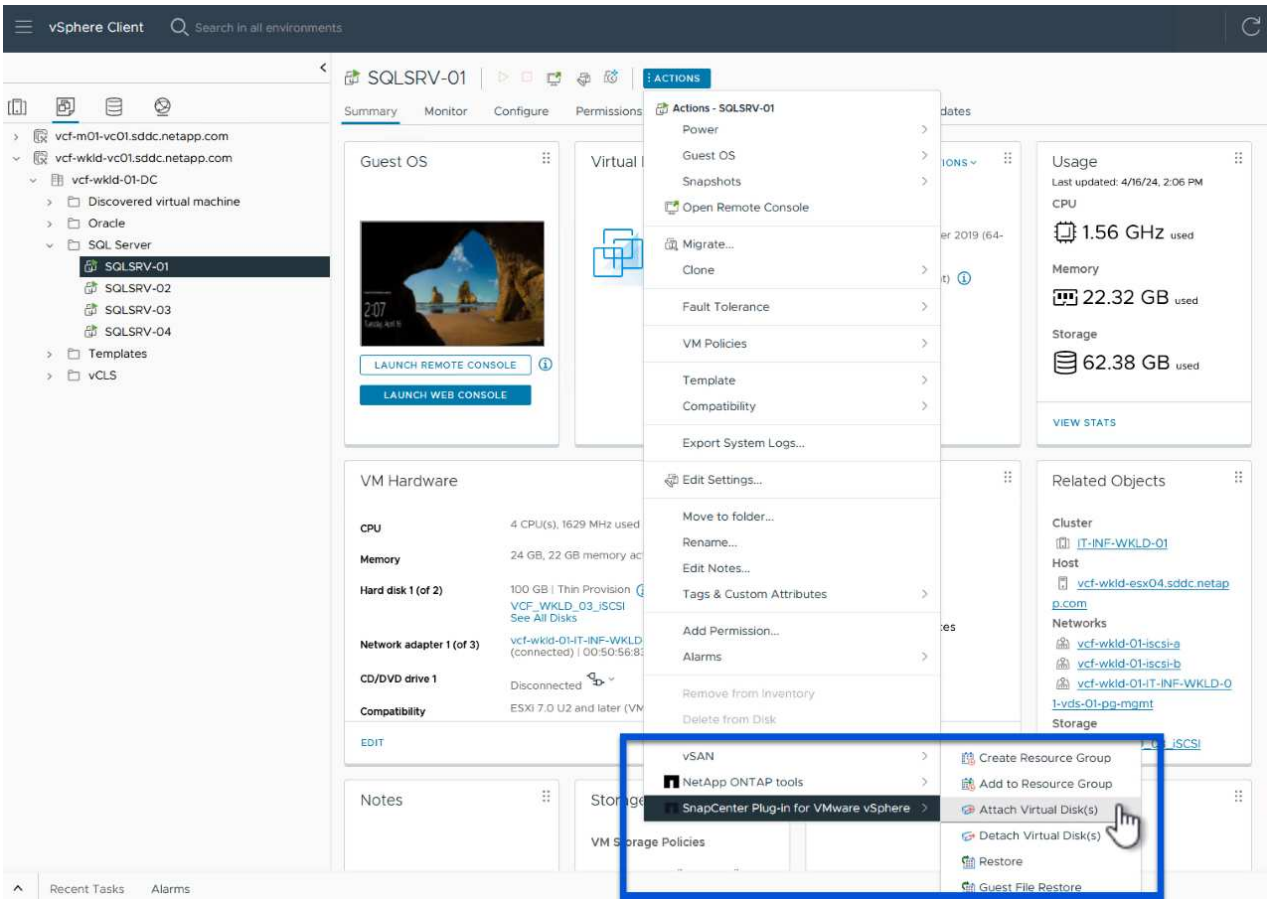

vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Dashboard
Status
Job Monitor
Reports
Getting Started
RECENT JOB ACTIVITIES
Restore Running [Job ID:18] 1 min ago
Backup Successful [Job ID:15] 8 min ago
Backup Successful [Job ID:12] 13 min ago
Backup Successful [Job ID:9] 13 min ago
Backup Successful [Job ID:6] 19 min ago
See All
CONFIGURATION
11 Virtual Machines
6 Datastores
14 SVMs
2 Resource Groups
2 Backup Policies
Job Details : 18
Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Preparing for Restore: Retrieving Backup metadata from Repository.
Pre Restore
Restore
Running, Start Time: 04/04/2024 04:58:24 PM.
CLOSE
DOWNLOAD JOB LOGS
No data to display.
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
NetApp Mount Datastore
vcf-wkld-esx04.sddc.netapp.com
35%
Mount operation completed successfully.
VCF.LOCAL\Administrator
6 ms
04/04/2024, 4:58:27 PM
NetApp Restore
vcf-wkld-esx04.sddc.netapp.com
2%
Restore operation started.
VCF.LOCAL\Administrator
10 ms
04/04/2024, 4:58:27 PM
Manage Columns
Running
More Tasks

Restaurar VMDK mediante el complemento SnapCenter

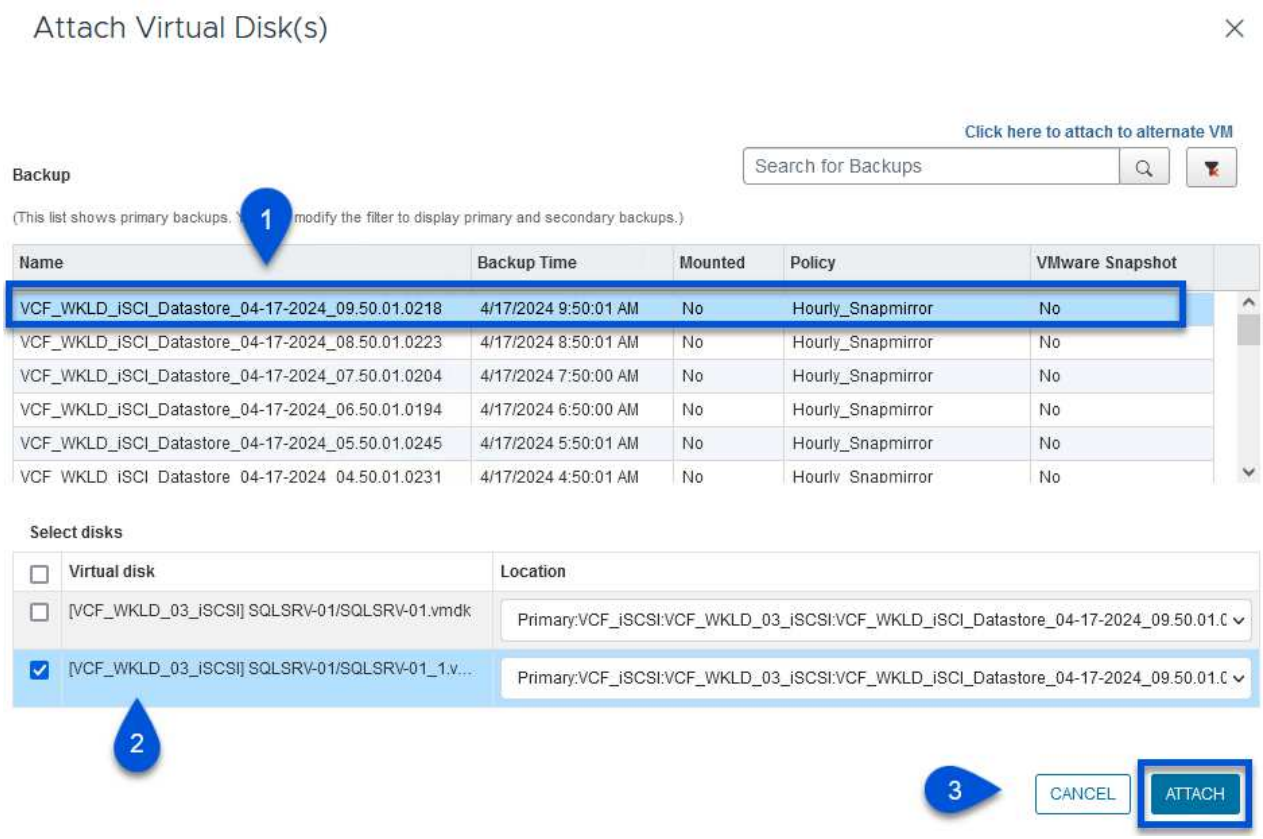
ONTAP Tools permite la restauración completa de VMDK a su ubicación original o la capacidad de adjuntar un VMDK como un nuevo disco a un sistema host. En este escenario, se conectará un VMDK a un host de Windows para acceder al sistema de archivos.

Para adjuntar un VMDK desde una copia de seguridad, complete los siguientes pasos:

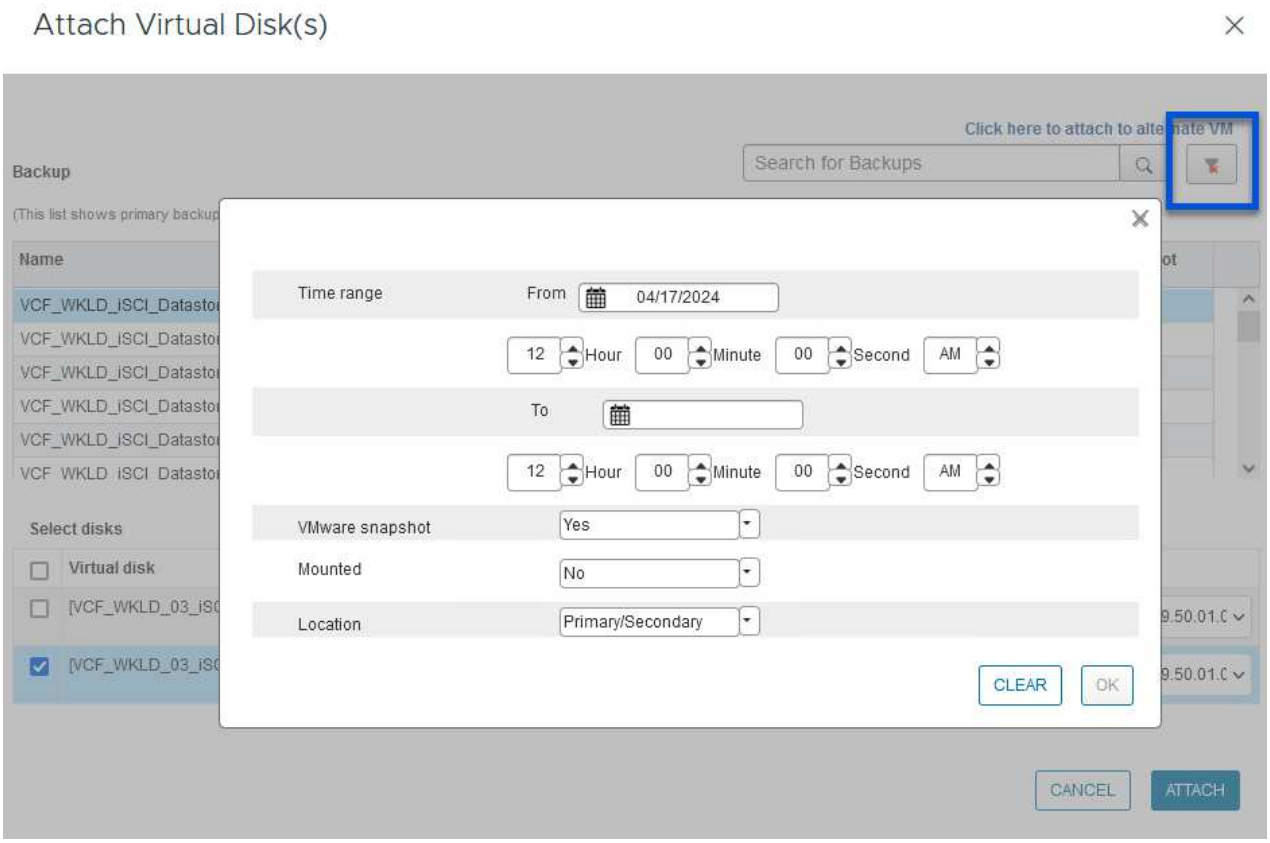
1. En vSphere Client, navegue hasta una máquina virtual y, desde el menú **Acciones**, seleccione * SnapCenter Plug-in for VMware vSphere > Conectar discos virtuales*.



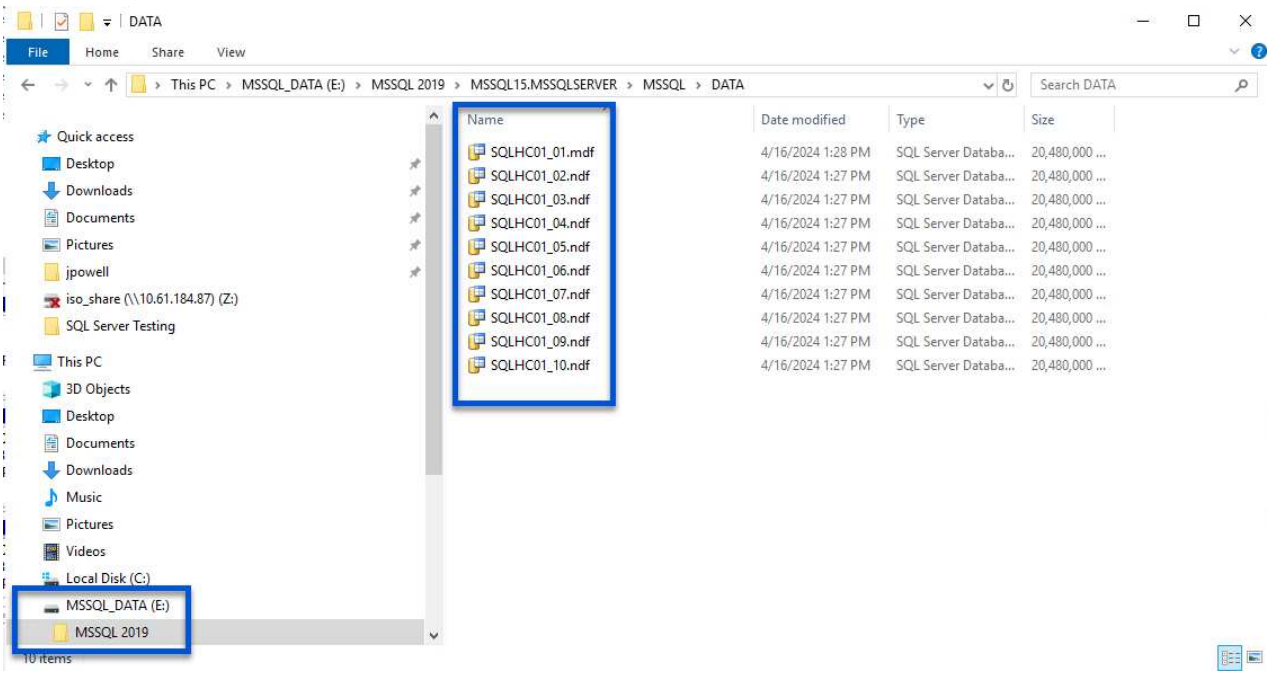
2. En el asistente **Adjuntar discos virtuales**, seleccione la instancia de respaldo que se utilizará y el VMDK particular que se adjuntará.



Las opciones de filtro se pueden utilizar para localizar copias de seguridad y mostrar copias de seguridad de sistemas de almacenamiento primarios y secundarios.



3. Después de seleccionar todas las opciones, haga clic en el botón **Adjuntar** para comenzar el proceso de restauración y adjuntar el VMDK al host.
4. Una vez completado el procedimiento de conexión, se puede acceder al disco desde el sistema operativo del sistema host. En este caso, SCV adjuntó el disco con su sistema de archivos NTFS a la unidad E: de nuestro servidor SQL de Windows y los archivos de base de datos SQL en el sistema de archivos son accesibles a través del Explorador de archivos.



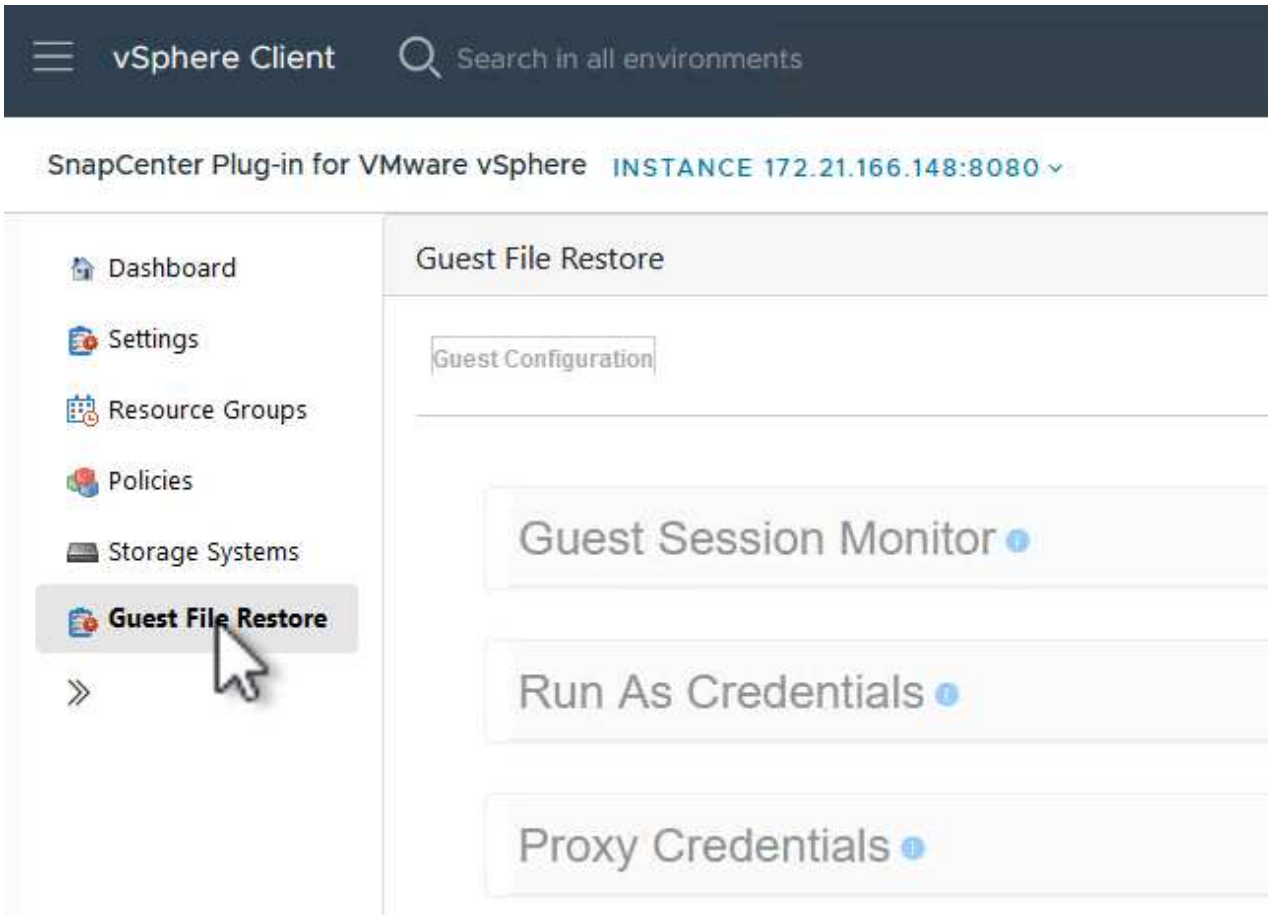
Restauración del sistema de archivos invitado mediante el complemento SnapCenter

Las herramientas de ONTAP permiten restaurar sistemas de archivos invitados desde un VMDK en sistemas operativos Windows Server. Esto se realiza de forma centralizada desde la interfaz del complemento SnapCenter .

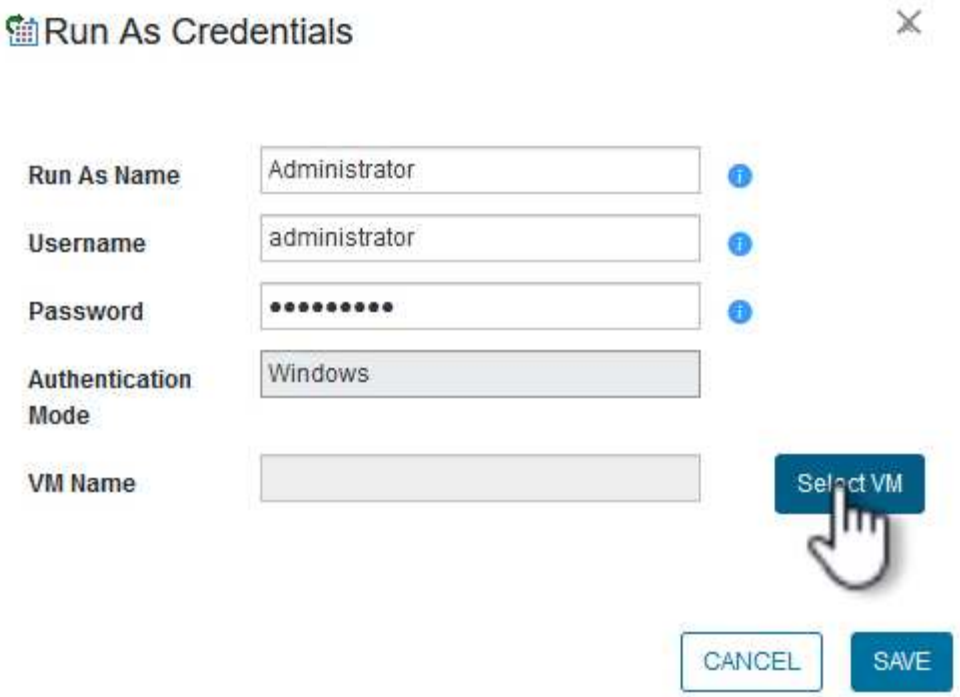
Para obtener información detallada, consulte"Restaurar archivos y carpetas de invitados" en el sitio de documentación de SCV.

Para realizar una restauración del sistema de archivos invitado para un sistema Windows, complete los siguientes pasos:

1. El primer paso es crear credenciales Ejecutar como para proporcionar acceso al sistema host de Windows. En vSphere Client, navegue hasta la interfaz del complemento CSV y haga clic en **Restaurar archivo invitado** en el menú principal.

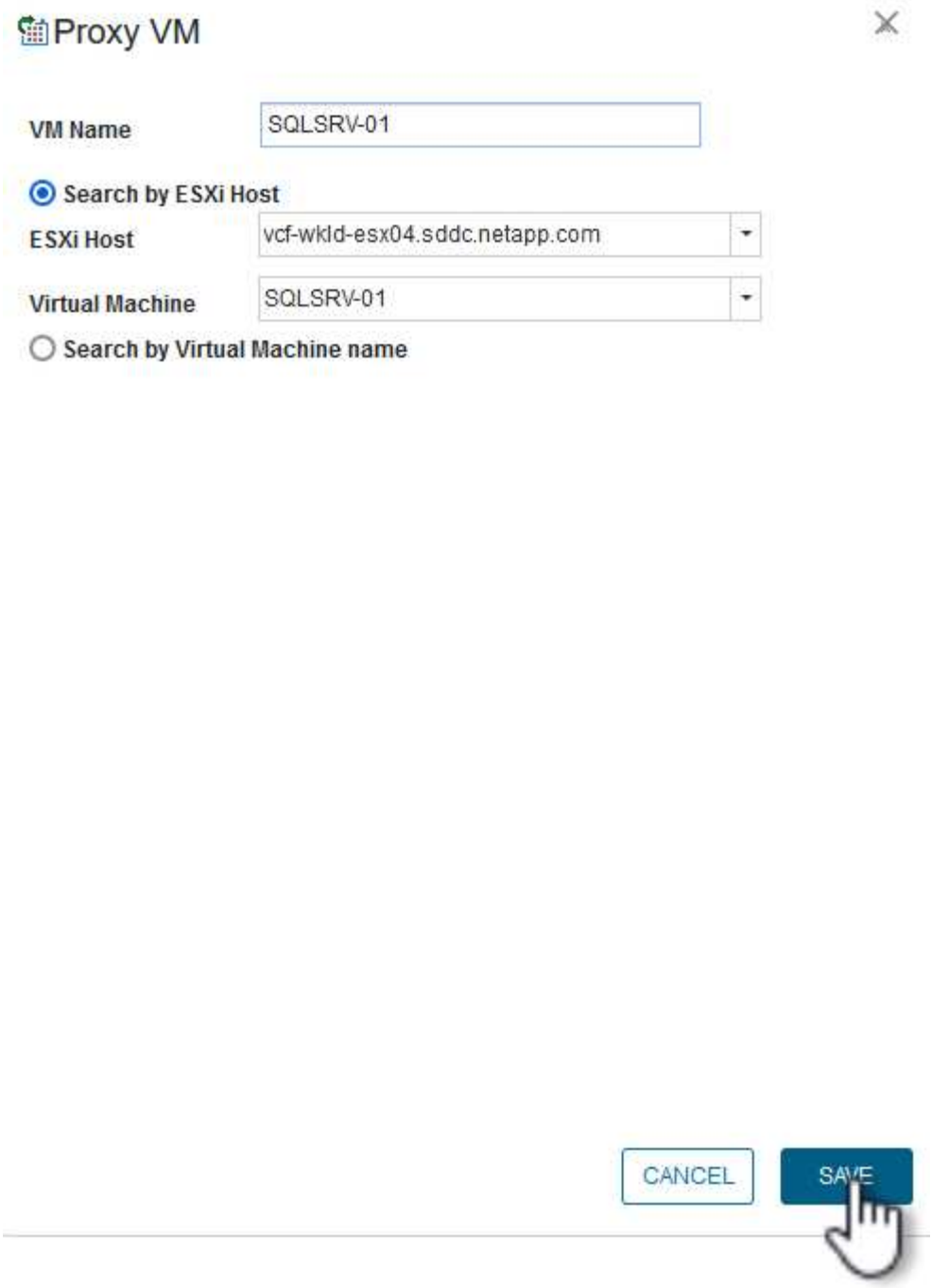


2. En **Ejecutar como credenciales**, haga clic en el ícono **+** para abrir la ventana **Ejecutar como credenciales**.
3. Complete un nombre para el registro de credenciales, un nombre de usuario de administrador y una contraseña para el sistema Windows y luego haga clic en el botón **Seleccionar VM** para seleccionar una VM Proxy opcional que se utilizará para la

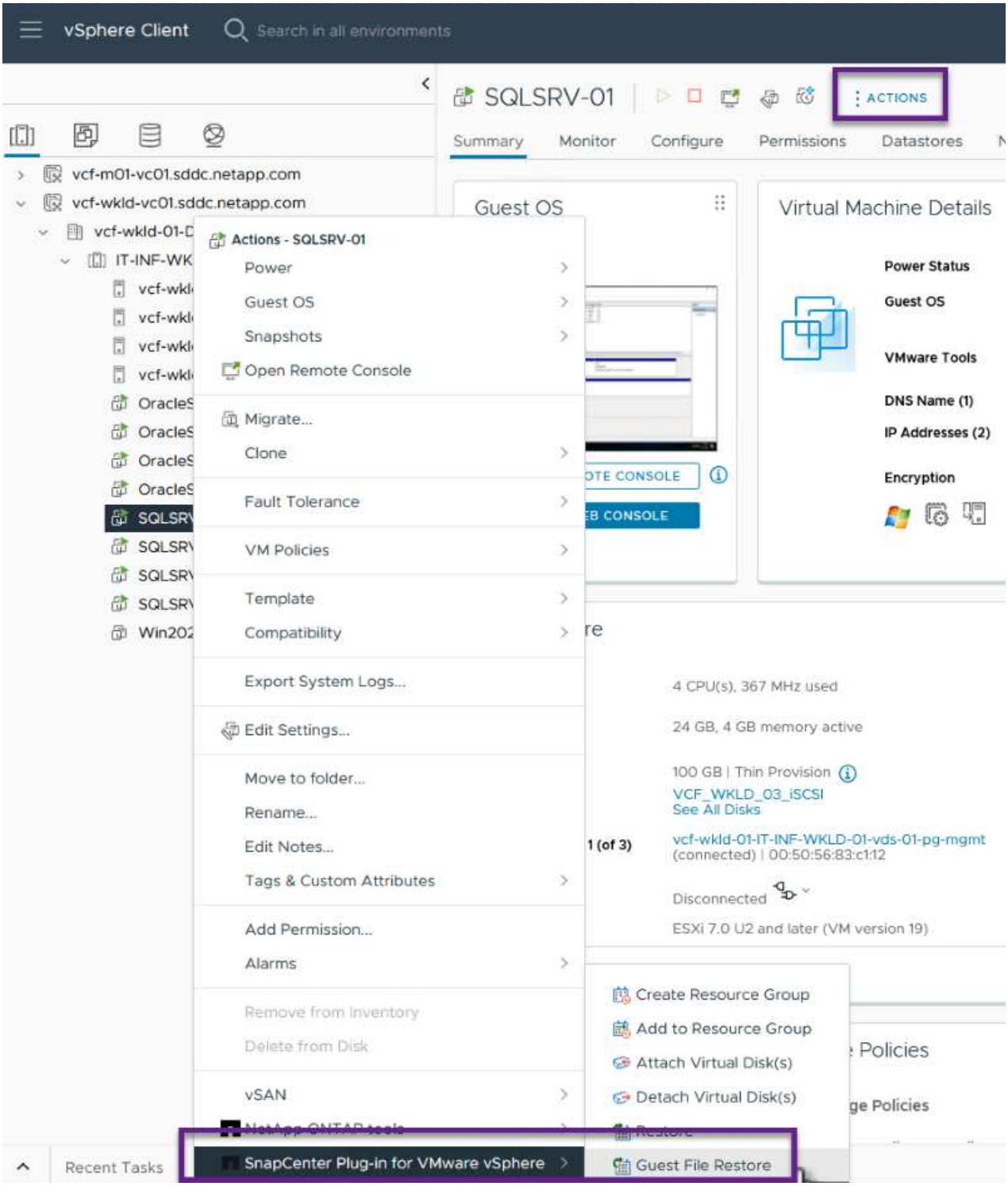


restauración.

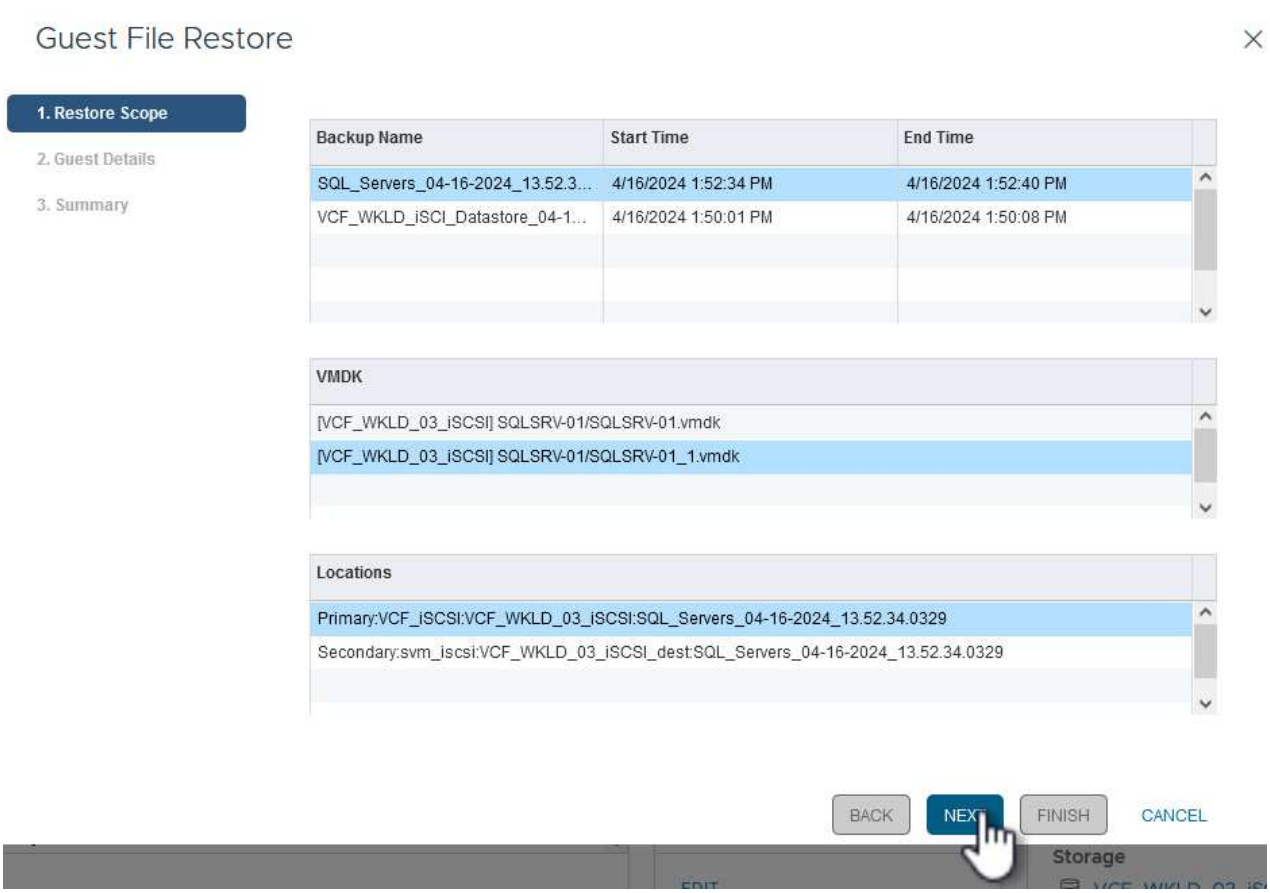
4. En la página Proxy VM, proporcione un nombre para la VM y ubiquela buscándola por host ESXi o por nombre. Una vez seleccionado, haga clic en **Guardar**.



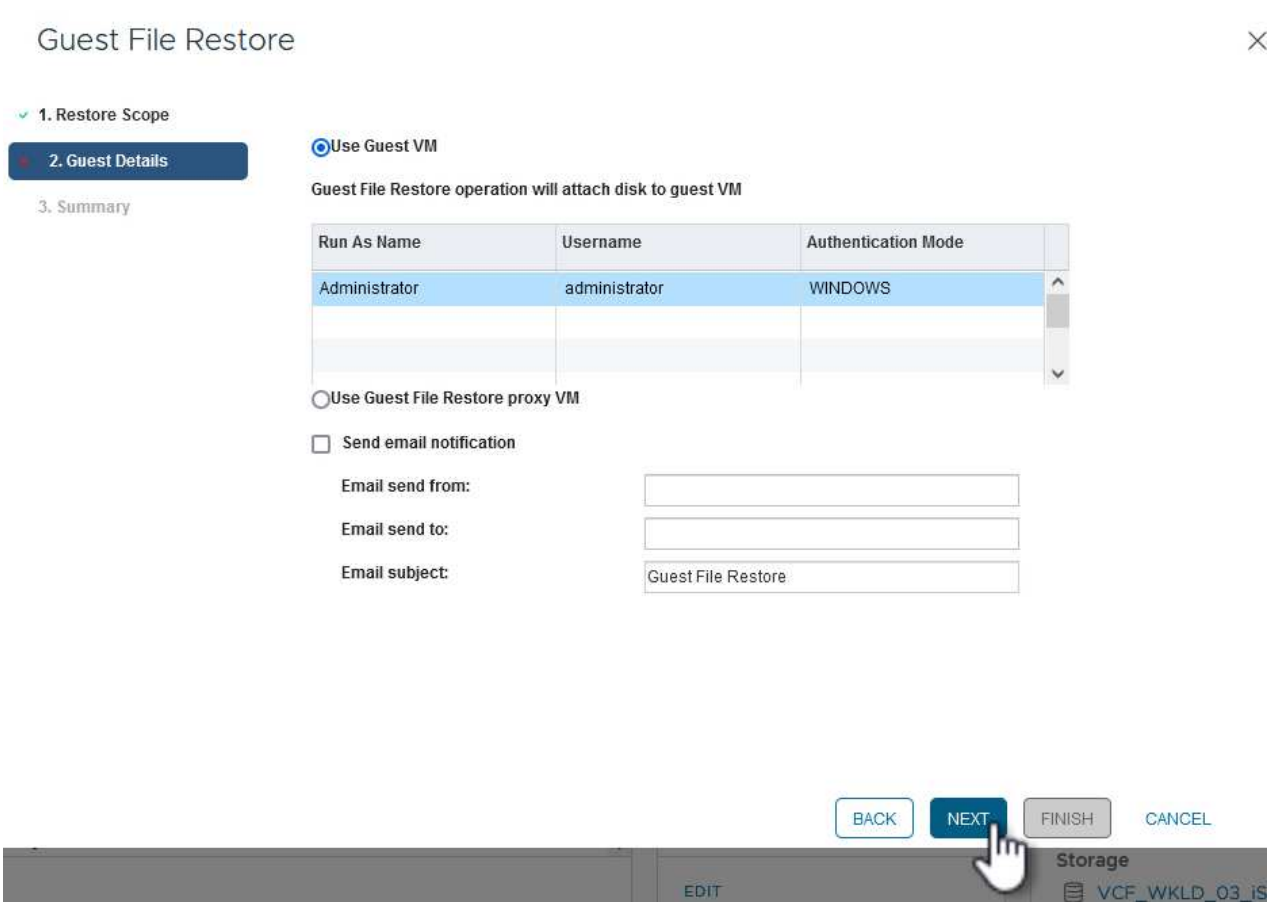
5. Haga clic en **Guardar** nuevamente en la ventana **Ejecutar como credenciales** para completar el guardado del registro.
6. A continuación, navegue hasta una VM en el inventario. Desde el menú **Acciones** o haciendo clic derecho en la máquina virtual, seleccione * SnapCenter Plug-in for VMware vSphere > Restaurar archivos invitados*.



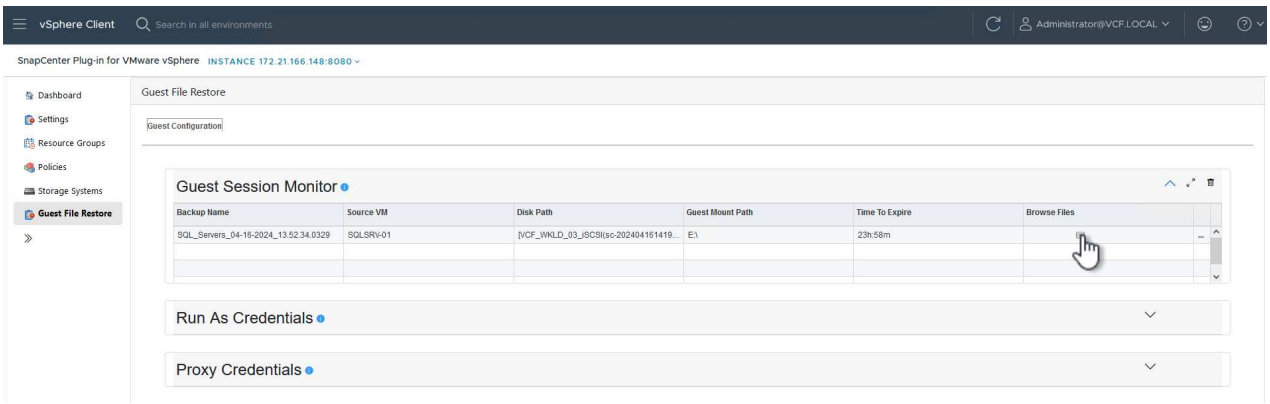
7. En la página **Restaurar alcance** del asistente **Restaurar archivo invitado**, seleccione la copia de seguridad desde la cual restaurar, el VMDK en particular y la ubicación (principal o secundaria) desde la cual restaurar el VMDK. Haga clic en **Siguiente** para continuar.



8. En la página **Detalles del invitado**, seleccione utilizar **VM invitada** o **Usar VM proxy de restauración de archivos invitado** para la restauración. Además, complete la configuración de notificaciones por correo electrónico aquí si lo desea. Haga clic en **Siguiente** para continuar.



9. Por último, revise la página **Resumen** y haga clic en **Finalizar** para comenzar la sesión de restauración del sistema de archivos invitado.
10. De regreso a la interfaz del complemento SnapCenter , navegue a **Restaurar archivo invitado** nuevamente y vea la sesión en ejecución en **Monitor de sesión invitado**. Haga clic en el icono debajo de **Explorar archivos** para continuar.



11. En el asistente **Exploración de archivos invitados**, seleccione la carpeta o los archivos que desea restaurar y la ubicación del sistema de archivos donde restaurarlos. Por último, haga clic en **Restaurar** para iniciar el proceso de **Restaurar**.

Guest File Browse

Select File(s)/Folder(s) to Restore

E:\MSSQL 2019

Enter Pattern

	Name	Size
☐	MSSQL15.MSSQLSERVER	

Selected 0 Files / 1 Directory

Name	Path	Size	Delete
MSSQL 2019	E:\MSSQL 2019		

Select Restore Location

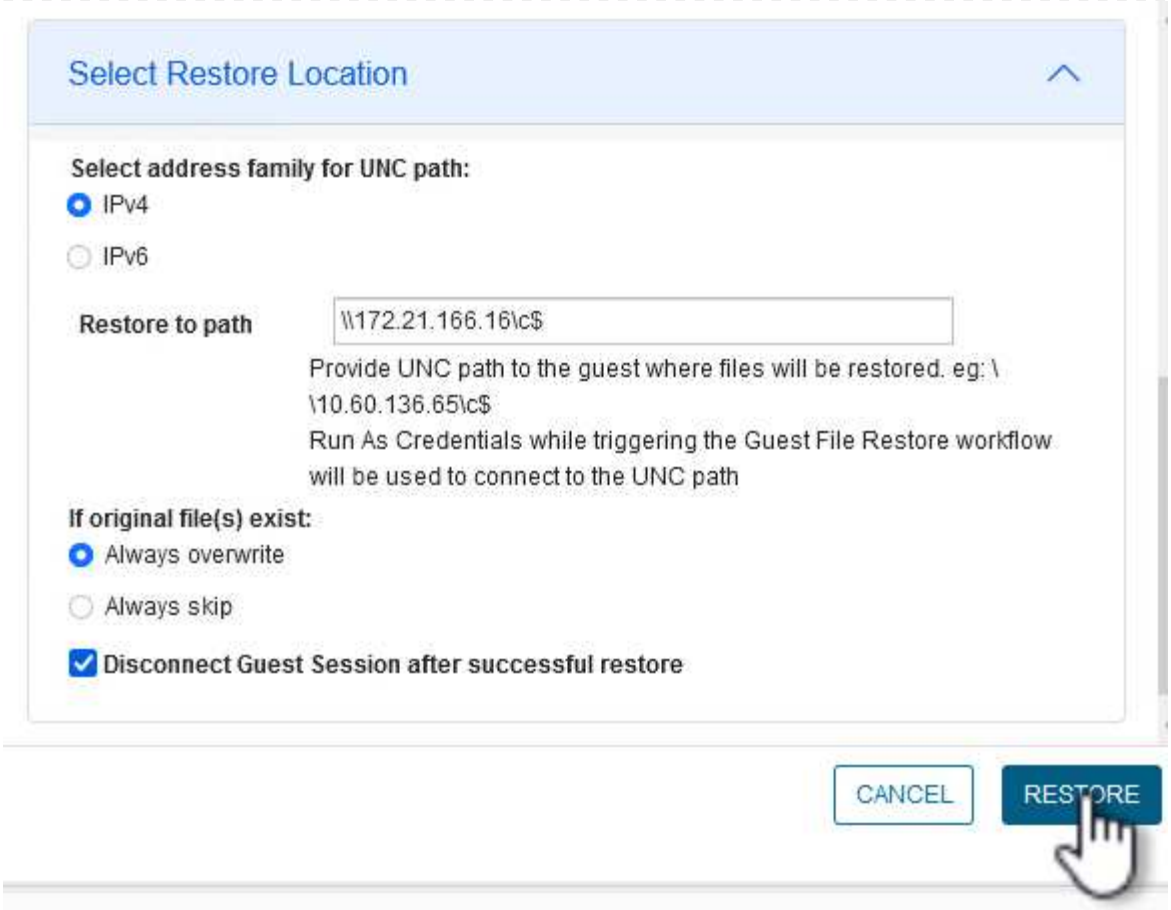
Select address family for UNC path:

IPv4

Either Files to Restore or Restore Location is not selected!

CANCEL

RESTORE



12. El trabajo de restauración se puede supervisar desde el panel de tareas de vSphere Client.

Información adicional

Para obtener información sobre la configuración de VCF, consulte "Documentación de VMware Cloud Foundation" .

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte "Documentación de ONTAP 9" centro.

Para obtener información sobre el uso del SnapCenter Plug-in for VMware vSphere, consulte la "Documentación del SnapCenter Plug-in for VMware vSphere" .

Proteja los dominios de administración y carga de trabajo de VCF mediante el complemento SnapCenter para VMware vSphere

Utilice el SnapCenter Plug-in for VMware vSphere para proteger varios dominios VCF. Este procedimiento incluye la configuración del complemento para cada dominio, la configuración de políticas de respaldo y la realización de operaciones de restauración.

Los dominios de carga de trabajo de VMware Cloud Foundation (VCF) permiten a las organizaciones separar lógicamente los recursos en diferentes dominios para agrupar diferentes cargas de trabajo, mejorar la seguridad y la tolerancia a fallas.

Introducción

Los dominios pueden escalar de forma independiente, cumplir con normativas específicas y proporcionar multitenencia. La protección de datos para VMware Cloud Foundation (VCF) es un aspecto fundamental para garantizar la disponibilidad, integridad y capacidad de recuperación de los datos en todo el dominio de administración y los dominios de carga de trabajo. El SnapCenter Plug-in for VMware vSphere NetApp SnapCenter para VMware vSphere (SCV) es una potente herramienta que integra las capacidades de protección de datos de NetApp en los entornos VMware. Simplifica la copia de seguridad, la restauración y la clonación de máquinas virtuales (VM) VMware vSphere alojadas en el almacenamiento de NetApp .

Este documento proporciona pasos de implementación sobre cómo proteger múltiples dominios VCF con SCV.

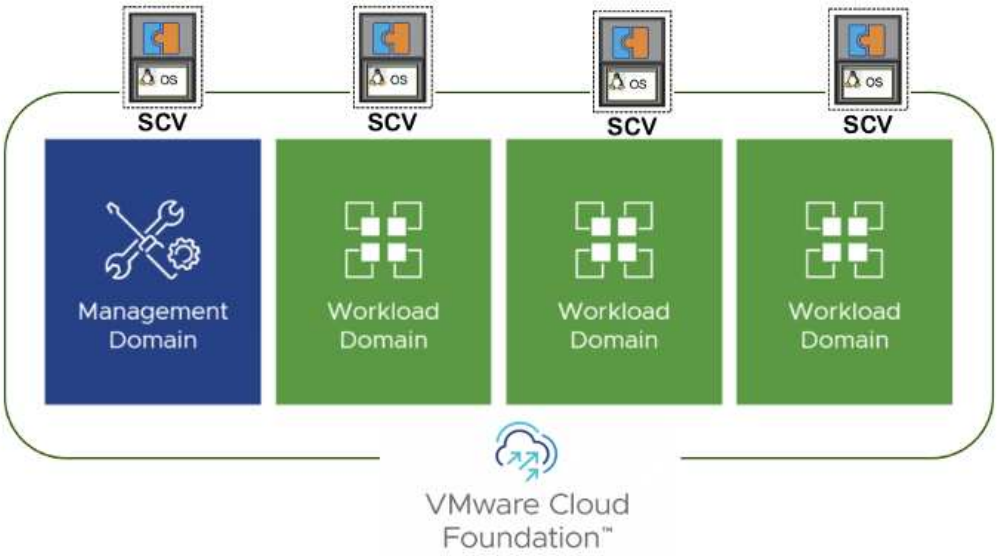
Audiencia

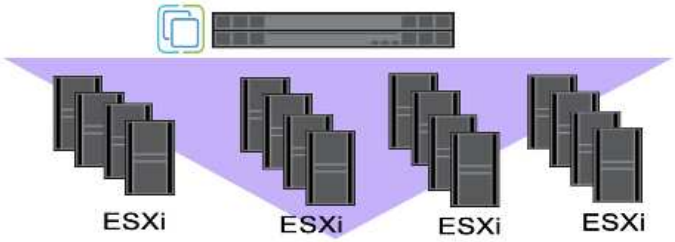
Arquitectos de soluciones o administradores de almacenamiento que garantizan la protección de datos y la recuperación ante desastres para dominios de carga de trabajo de VMware VCF.

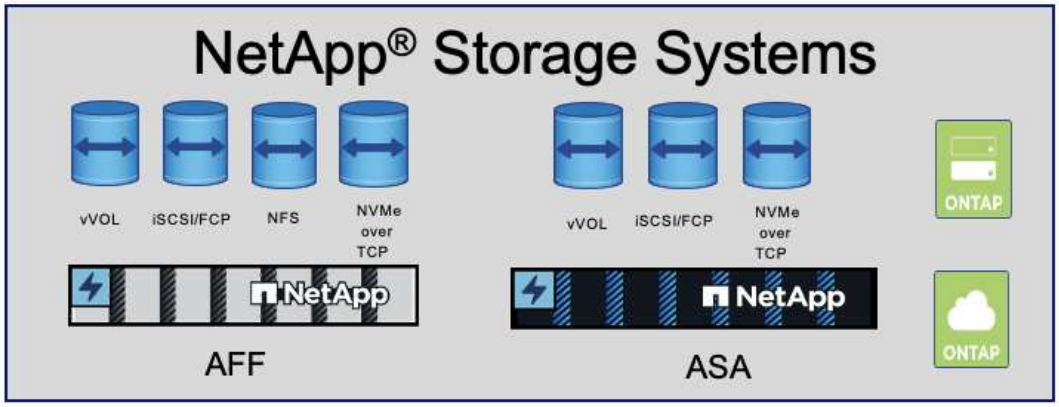
Descripción general de la arquitectura

SCV se implementa como un dispositivo virtual Linux que utiliza un archivo OVA para brindar operaciones de respaldo y restauración rápidas, eficientes en términos de espacio, consistentes ante fallos y consistentes con las máquinas virtuales para máquinas virtuales, almacenes de datos, archivos y carpetas. SCV utiliza una arquitectura de complemento remoto. Se implementaron y alojaron varios SCV en el dominio de administración VCF vCenter. El dominio SCV y VCF tienen una relación de uno a uno, por lo tanto, el dominio de administración de VCF y cada dominio de carga de trabajo requieren un SCV.

Datos que se encuentran en los sistemas primarios ONTAP FAS, AFF o All SAN Array (ASA) y se replican en los sistemas secundarios ONTAP FAS, AFF o ASA . SCV también funciona con SnapCenter Server para soportar operaciones de respaldo y restauración basadas en aplicaciones en entornos VMware para complementos específicos de la aplicación SnapCenter . Para más información consultar,"Documentación del SnapCenter Plug-in for VMware vSphere ."



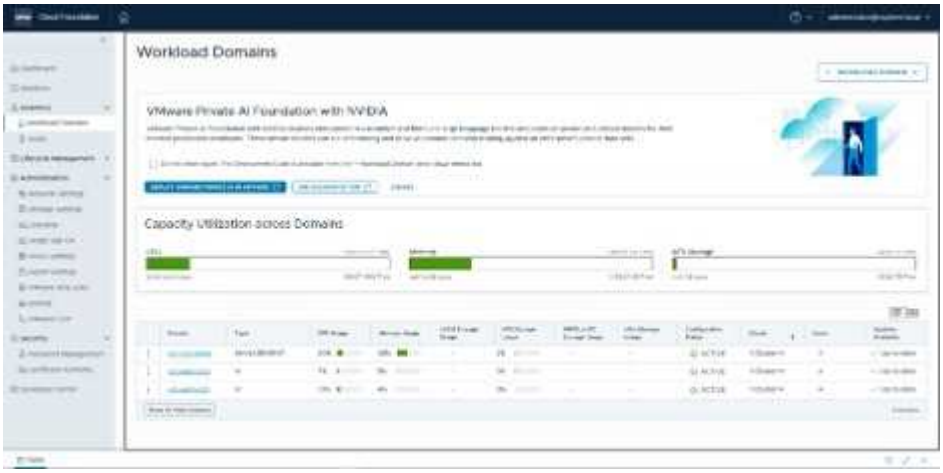




La regla de copia de seguridad 3-2-1 es una estrategia de protección de datos que implica hacer tres copias de los datos, almacenarlas en dos tipos de medios diferentes y mantener una copia fuera del sitio. BlueXP backup and recovery es una herramienta basada en la nube para la gestión de datos que proporciona un único plano de control para una amplia gama de operaciones de respaldo y recuperación en entornos locales y en la nube. Parte de la suite de BlueXP backup and recovery NetApp BlueXP es una función que se integra con SCV (en las instalaciones) para extender una copia de los datos al almacenamiento de objetos en la nube. Esto establece una tercera copia de los datos fuera del sitio que proviene de las copias de seguridad del almacenamiento primario o secundario. La BlueXP backup and recovery facilita la configuración de políticas de almacenamiento que transfieren copias de sus datos desde cualquiera de estas dos ubicaciones locales. Para más detalles, consulte"Protección de datos 3-2-1 para VMware con complemento SnapCenter y BlueXP backup and recovery para máquinas virtuales" .

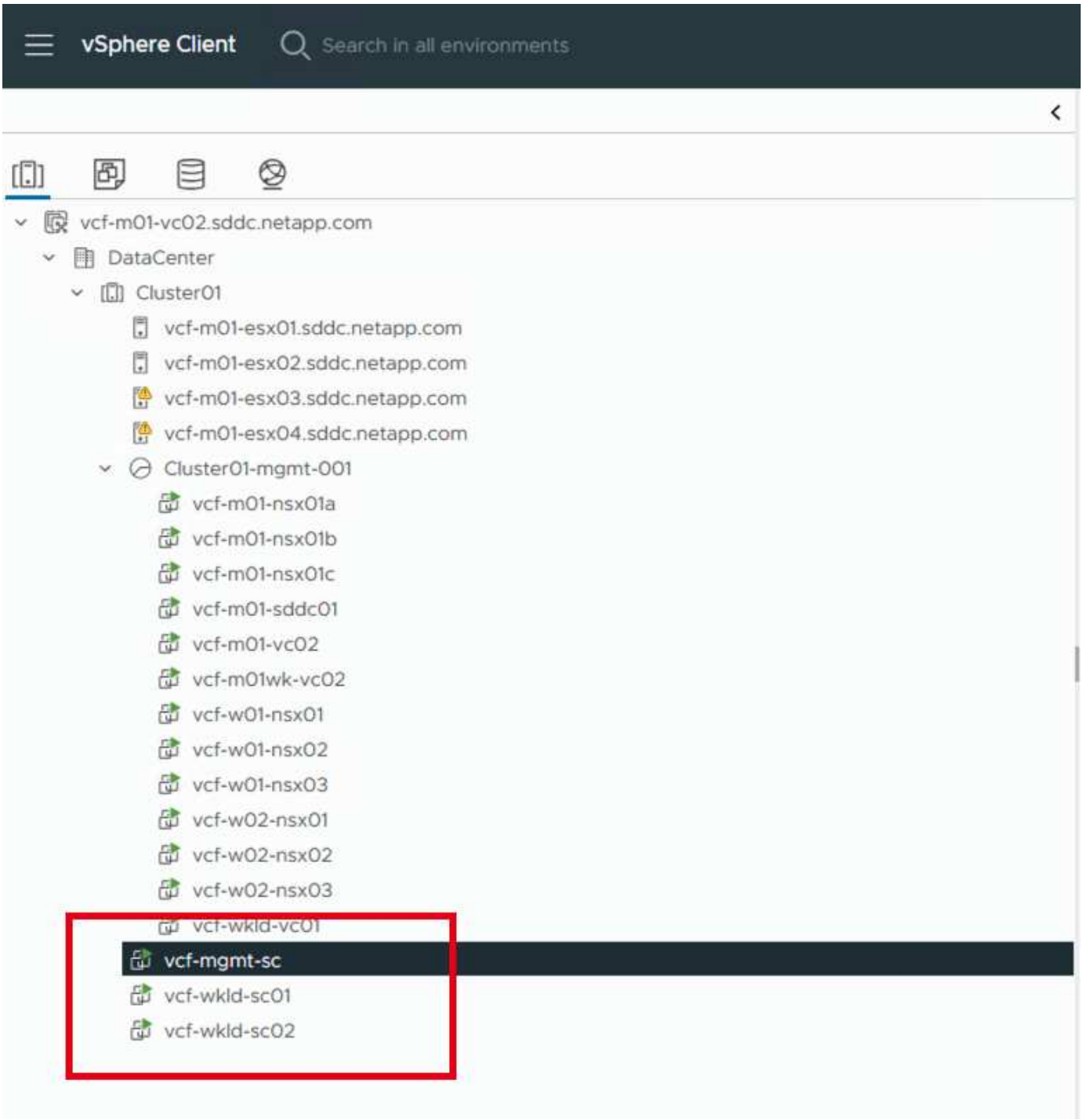
Implementar un VCF con dominio de administración y múltiples dominios de carga de trabajo

Un dominio de carga de trabajo VCF es un grupo de hosts ESXi con uno o más clústeres vSphere, aprovisionados por SDDC Manager y listos para aplicaciones. En el siguiente ejemplo de VCF, se implementaron un dominio de administración y dos dominios de carga de trabajo. Para obtener más detalles sobre cómo implementar VCF con almacenamiento NetApp , consulte"Documentación de implementación de NetApp VCF."



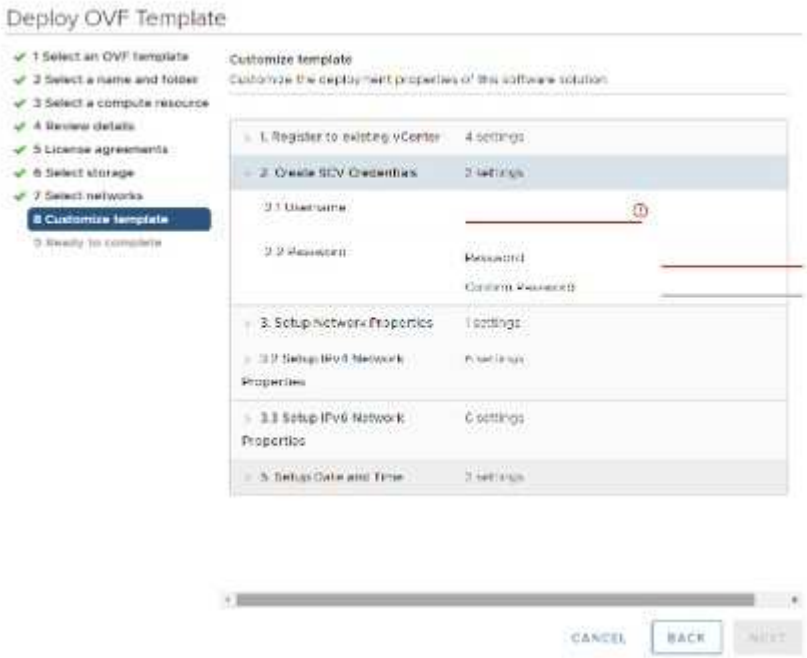
Pasos de implementación, configuración y restauración de SCV

En función de la cantidad de dominios de carga de trabajo y del dominio de administración, es necesario implementar varios SCV. Con dos dominios de carga de trabajo y un dominio de administración, el siguiente ejemplo muestra que se implementan tres SCV en el dominio de administración de VCF vCenter.


vSphere Client
Search in all environments
vcf-m01-vc02.sddc.netapp.com
DataCenter
Cluster01
vcf-m01-esx01.sddc.netapp.com
vcf-m01-esx02.sddc.netapp.com
vcf-m01-esx03.sddc.netapp.com
vcf-m01-esx04.sddc.netapp.com
Cluster01-mgmt-001
vcf-m01-nsx01a
vcf-m01-nsx01b
vcf-m01-nsx01c
vcf-m01-sddc01
vcf-m01-vc02
vcf-m01wk-vc02
vcf-w01-nsx01
vcf-w01-nsx02
vcf-w01-nsx03
vcf-w02-nsx01
vcf-w02-nsx02
vcf-w02-nsx03
vcf-wkld-vc01
vcf-mgmt-sc
vcf-wkld-sc01
vcf-wkld-sc02

Implementar SCV para el dominio de administración y cada dominio de carga de trabajo

1. "Descargue el dispositivo virtual abierto (OVA)."
2. Inicie sesión con vSphere Client en vCenter Server. Vaya a Administración > Certificados > Administración de certificados. Agregue certificados raíz de confianza e instale cada certificado en la carpeta certs. Una vez instalados los certificados, se puede verificar e implementar OVA.
3. Inicie sesión en el dominio de carga de trabajo VCF vCenter e implemente la plantilla OVF para iniciar el asistente de implementación de



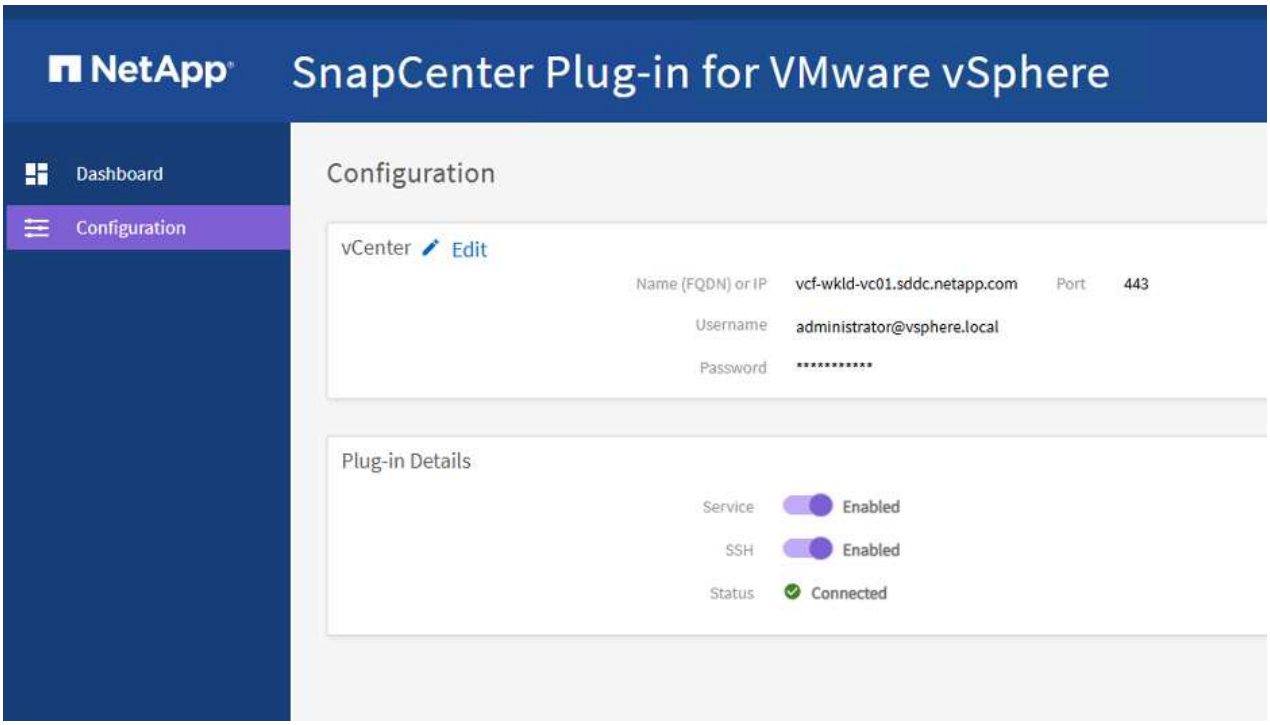
VMware.

4. Encienda OVA para iniciar SCV y luego haga clic en Instalar herramientas de VMware.
5. Genere el token MFA desde la consola OVA, menú de configuración del

sistema.

```
System Configuration Menu:
--------------------------
   1 ) Reboot virtual machine
   2 ) Shut down virtual machine
   3 ) Change 'maint' user password
   4 ) Change time zone
   5 ) Change NTP server
   6 ) Enable SSH access
   7 ) Increase jail disk size (/jail)
   8 ) Upgrade
   9 ) Install VMware Tools
  10 ) Generate MFA Token

   b ) Back
   x ) Exit

 Enter your choice: 10


Generating MFA Token... Your MFA Token is : 435164

 Press ENTER to continue._
```

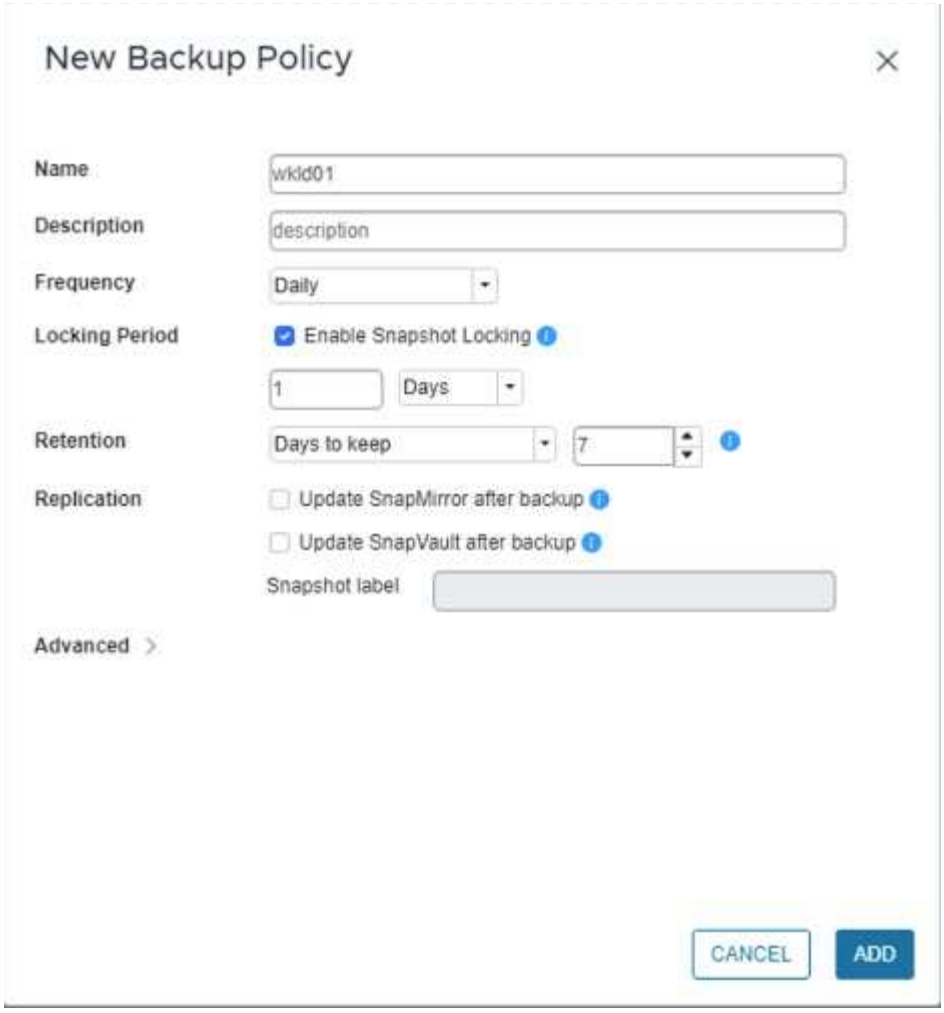
6. Inicie sesión en la GUI de administración de SCV con el nombre de usuario y la contraseña de administrador configurados en el momento de la implementación y el token MFA generado mediante la consola de mantenimiento.
   `https://<appliance-IP-address>:8080` para acceder a la GUI de administración.



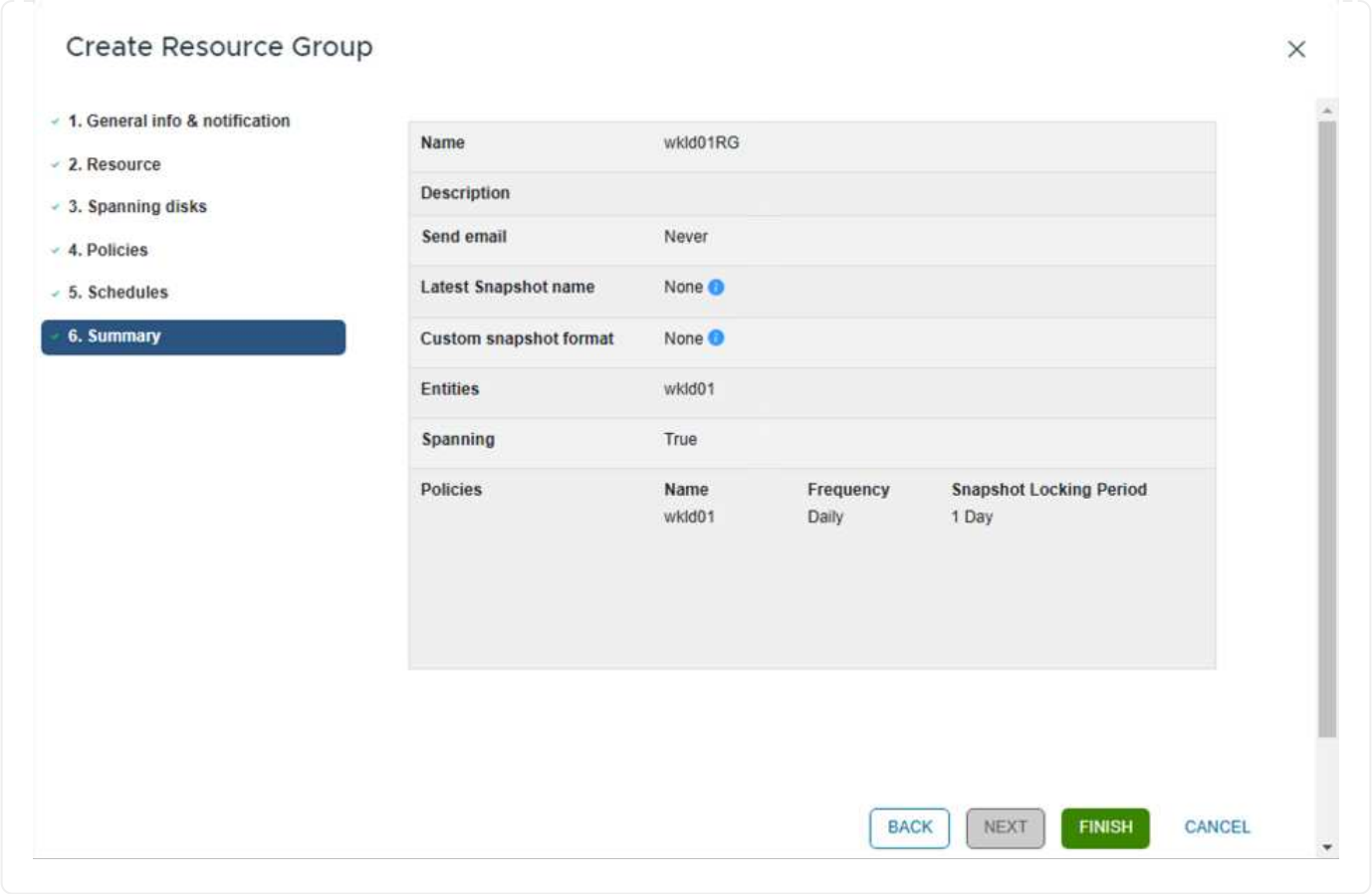
Configurar SCV

Para realizar una copia de seguridad o restaurar máquinas virtuales, primero agregue los clústeres de almacenamiento o las máquinas virtuales que alojan los almacenes de datos, luego cree políticas de copia de seguridad para la retención y la frecuencia, y configure un grupo de recursos para proteger los recursos.

1. Inicie sesión en el cliente web de vCenter y haga clic en Menú en la barra de herramientas y seleccione SnapCenter Plug-in for VMware vSphere y Agregar un almacenamiento. En el panel de navegación izquierdo del complemento SCV, haga clic en Sistemas de almacenamiento y luego seleccione Agregar opción. En el cuadro de diálogo Agregar sistema de almacenamiento, ingrese la información básica del SVM o clúster y seleccione Agregar. Ingrese la dirección IP de almacenamiento de NetApp e inicie sesión.
2. Para crear una nueva política de respaldo, en el panel de navegación izquierdo del complemento SCV, haga clic en Políticas y seleccione Nueva política. En la página Nueva política de respaldo, ingrese la información de configuración de la política y haga clic en Agregar.



3. En el panel de navegación izquierdo del complemento SCV, haga clic en Grupos de recursos y luego seleccione Crear. Ingrese la información requerida en cada página del asistente Crear grupo de recursos, seleccione las máquinas virtuales y los almacenes de datos que se incluirán en el grupo de recursos y, a continuación, seleccione las políticas de respaldo que se aplicarán al grupo de recursos y especifique la programación de respaldo.

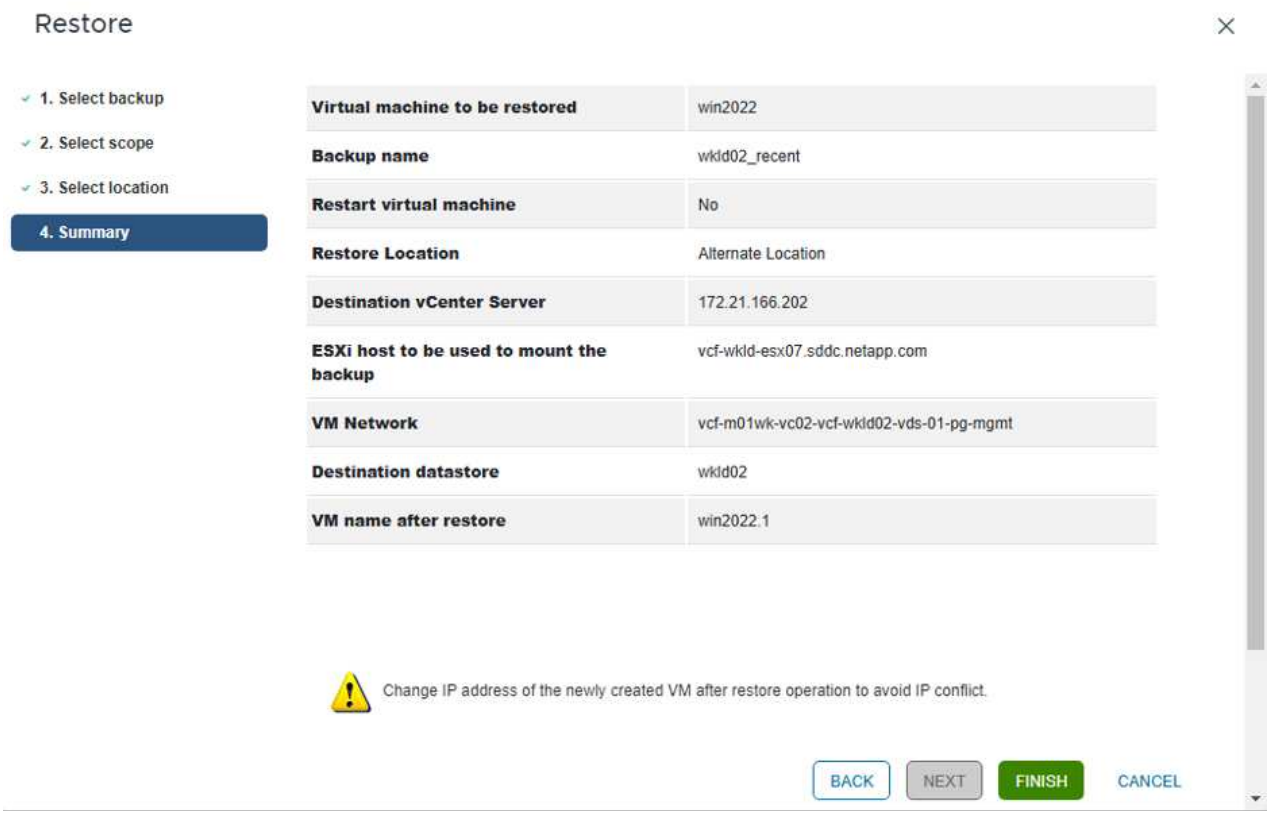

Create Resource Group
1. General info & notification
2. Resource
3. Spanning disks
4. Policies
5. Schedules
6. Summary
Name
wkld01RG
Description
Send email
Never
Latest Snapshot name
None
Custom snapshot format
None
Entities
wkld01
Spanning
True
Policies
Name
wkld01
Frequency
Daily
Snapshot Locking Period
1 Day
BACK
NEXT
FINISH
CANCEL

Restaurar copia de seguridad de máquinas virtuales y archivos o carpetas

Se pueden restaurar máquinas virtuales, VMDK, archivos y carpetas de las copias de seguridad. La máquina virtual se puede restaurar en el host original o en un host alternativo en el mismo vCenter Server, o en un host ESXi alternativo administrado por el mismo vCenter. Puede montar un almacén de datos tradicional desde una copia de seguridad si desea acceder a los archivos de la copia de seguridad. Puede montar la copia de seguridad en el mismo host ESXi donde se creó la copia de seguridad o en un host ESXi alternativo que tenga el mismo tipo de VM y configuraciones de host. Un almacén de datos puede montarse varias veces en un host. También se pueden restaurar archivos y carpetas individuales en una sesión de restauración de archivos de invitado, que adjunta una copia de respaldo de un disco virtual y luego restaura los archivos o carpetas seleccionados. También se pueden restaurar archivos y carpetas.

Pasos para restaurar la máquina virtual

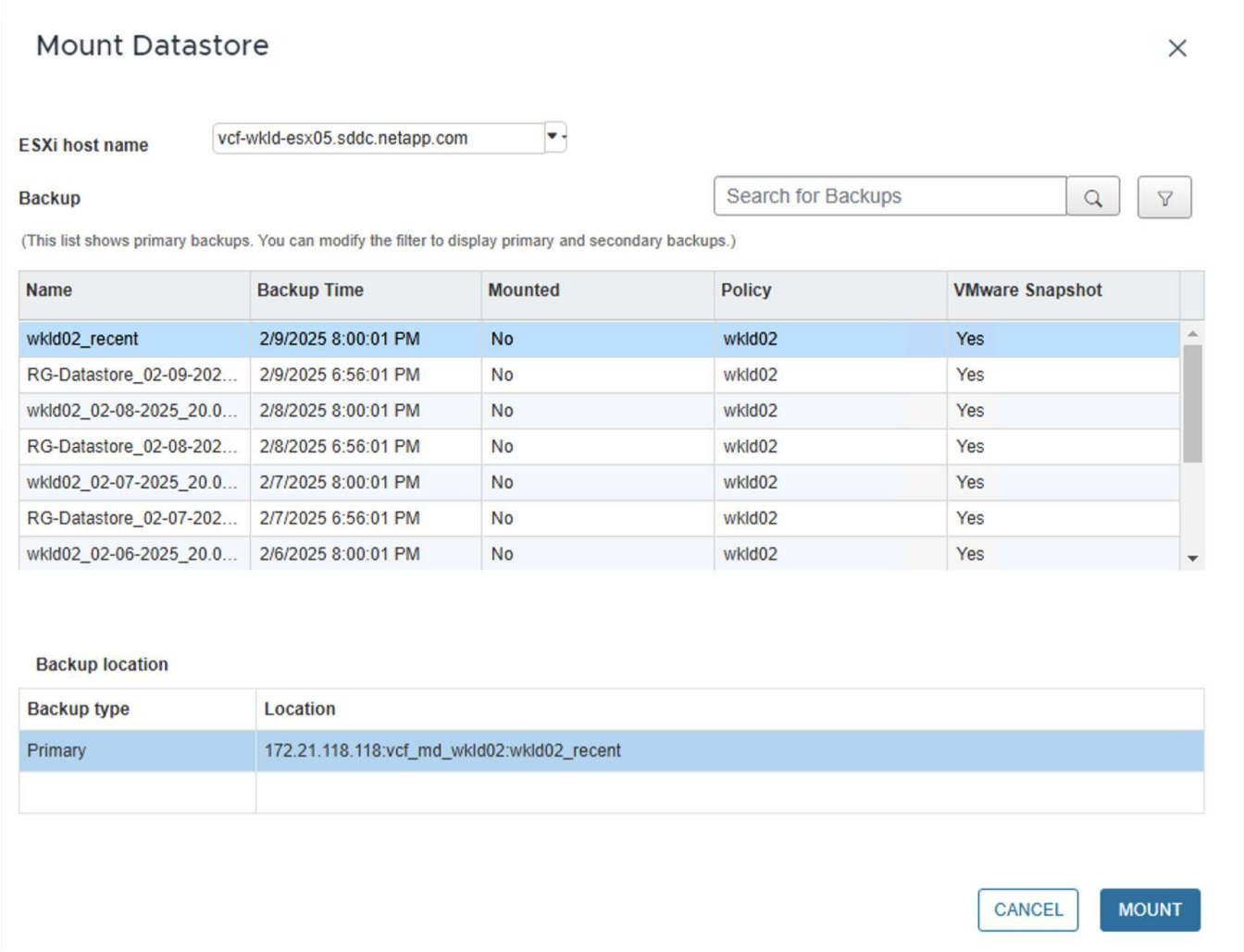
1. En la GUI del cliente VMware vSphere, haga clic en Menú en la barra de herramientas y seleccione Máquinas virtuales y plantillas en la lista desplegable, haga clic con el botón derecho en una máquina virtual y seleccione SnapCenter Plug-in for VMware vSphere en la lista desplegable y, luego, seleccione Restaurar en la lista desplegable secundaria para iniciar el asistente.
2. En el Asistente de restauración, seleccione la instantánea de copia de seguridad que desea restaurar y seleccione Toda la máquina virtual en el campo Alcance de la restauración, seleccione la ubicación de restauración y luego ingrese la información de destino donde se debe montar la copia de seguridad. En la página Seleccionar ubicación, seleccione la ubicación para el almacén de datos restaurado. Revise la página Resumen y haga clic en Finalizar.



3. Supervise el progreso de la operación haciendo clic en Tareas recientes en la parte inferior de la pantalla.

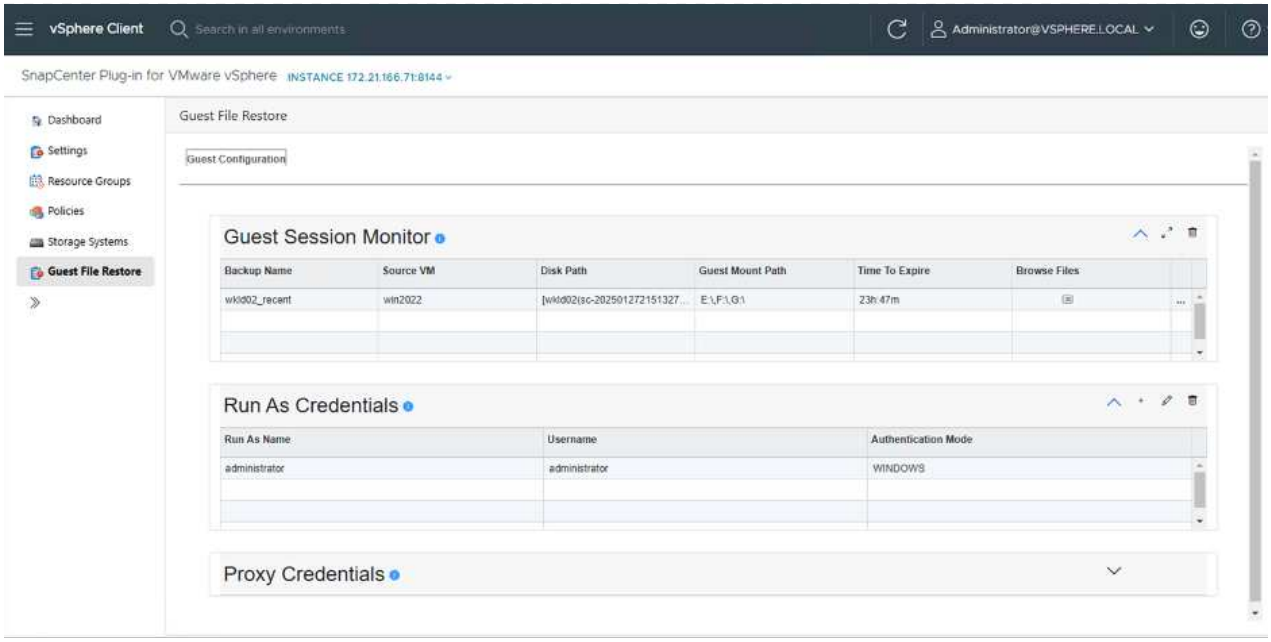
Pasos para restaurar el almacén de datos

1. Haga clic con el botón derecho en un almacén de datos y seleccione SnapCenter Plug-in for VMware vSphere > Montar copia de seguridad.
2. En la página Montar almacén de datos, seleccione una copia de seguridad y una ubicación de copia de seguridad (principal o secundaria) y, luego, haga clic en Montar.

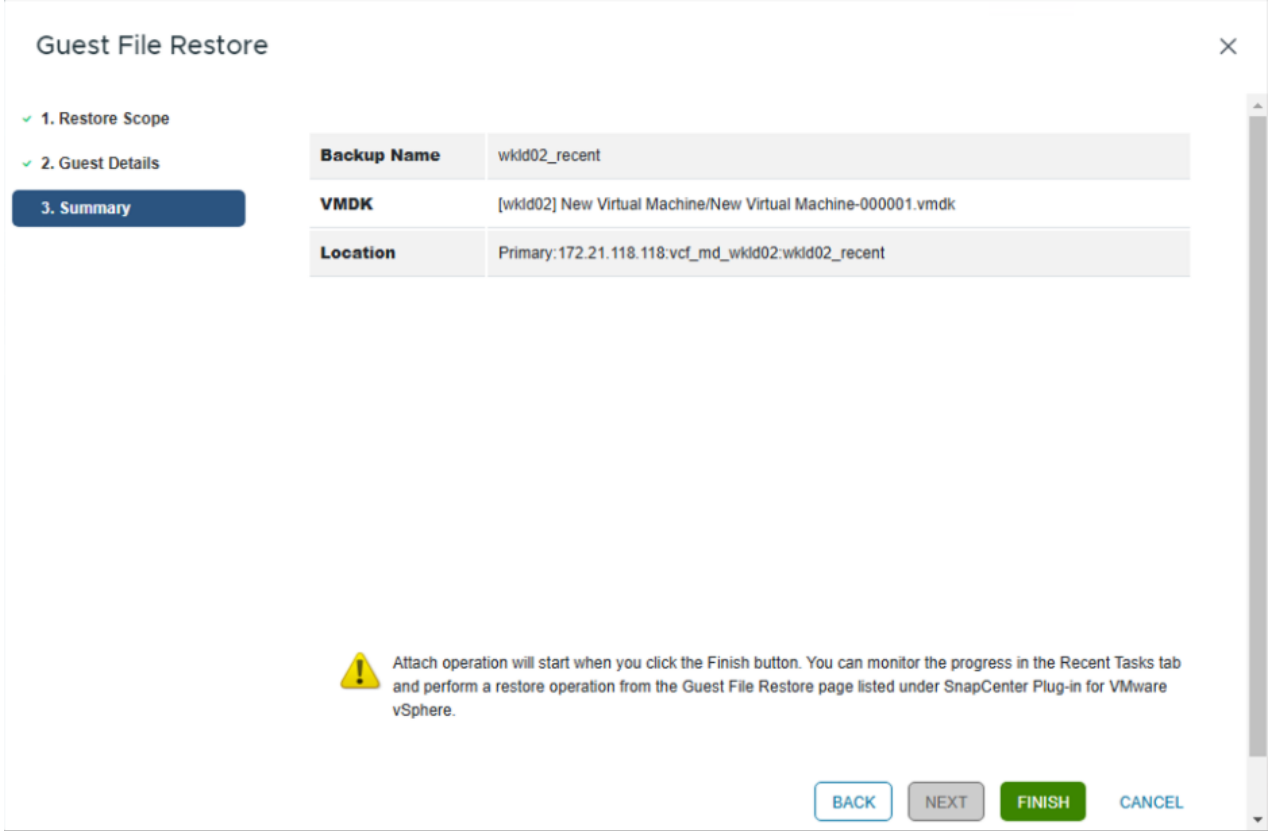


Pasos para restaurar archivos y carpetas

1. Cuando adjunta un disco virtual para operaciones de restauración de archivos o carpetas invitados, la máquina virtual de destino para la adjuntación debe tener credenciales configuradas antes de realizar la restauración. Desde el SnapCenter Plug-in for VMware vSphere , en complementos, seleccione la sección Restaurar archivos de invitado y ejecutar como credenciales e ingrese las credenciales de usuario. Para el nombre de usuario, debe ingresar “Administrador”.



2. Haga clic con el botón derecho en la máquina virtual desde el cliente vSphere y seleccione SnapCenter Plug-in for VMware vSphere > Restaurar archivos invitados. En la página Ámbito de restauración, especifique el nombre de la copia de seguridad, el disco virtual VMDK y la ubicación: principal o secundaria. Haga clic en Resumen para confirmar.



NetApp SnapCenter para múltiples dominios VCP centraliza la protección de datos, reduce de manera eficiente el tiempo y el espacio de almacenamiento necesarios para las copias de seguridad mediante instantáneas de NetApp , admite entornos VMware a gran escala con funciones robustas de copia de

seguridad y replicación, y permite la recuperación granular de máquinas virtuales completas, VMDK específicos o archivos individuales.

Demostración en video para proteger múltiples dominios VCF con SCV

Proteja varios dominios de VMware VCF con NetApp SCV

Proteja los dominios de carga de trabajo VCF con almacenamiento NVMe sobre TCP y el complemento SnapCenter para VMware vSphere

Utilice el SnapCenter Plug-in for VMware vSphere para proteger los dominios de carga de trabajo VCF con NVMe. Este procedimiento incluye configurar el complemento, configurar NVMe sobre TCP para un rendimiento óptimo y realizar operaciones de respaldo, restauración o clonación.

NVMe (Non-Volatile Memory Express) sobre TCP es un protocolo de red de vanguardia que facilita la transferencia de datos de alta velocidad entre los servidores VMware Cloud Foundation ESXi y el almacenamiento de NetApp , incluidos All Flash FAS (AFF) y All SAN Array (ASA).

Introducción

El aprovechamiento de NVMe sobre TCP proporciona baja latencia y alto rendimiento para cargas de trabajo exigentes. La integración de NVMe sobre TCP con el SnapCenter Plug-in for VMware vSphere NetApp SnapCenter para VMware vSphere (SCV) ofrece una poderosa combinación para una gestión de datos eficiente, mejorando las operaciones de respaldo, restauración y clonación dentro de entornos VMware.

Beneficios de NVMe sobre TCP

- Alto rendimiento: ofrece un rendimiento excepcional con baja latencia y altas tasas de transferencia de datos. Esto es crucial para aplicaciones exigentes y operaciones de datos a gran escala.
- Escalabilidad: admite configuraciones escalables, lo que permite a los administradores de TI expandir su infraestructura sin problemas a medida que crecen los requisitos de datos.
- Eficiencia: permite operaciones de respaldo y restauración más rápidas, lo que reduce el tiempo de inactividad y mejora la disponibilidad general del sistema.

Este documento proporciona pasos para implementar y administrar SCV en entornos de VMware Cloud Foundation (VCF), con un enfoque en aprovechar NVMe sobre TCP para lograr un rendimiento óptimo.

Audiencia

Arquitectos de soluciones o administradores de almacenamiento que garantizan la protección de datos y la recuperación ante desastres para dominios de carga de trabajo de VMware VCF.

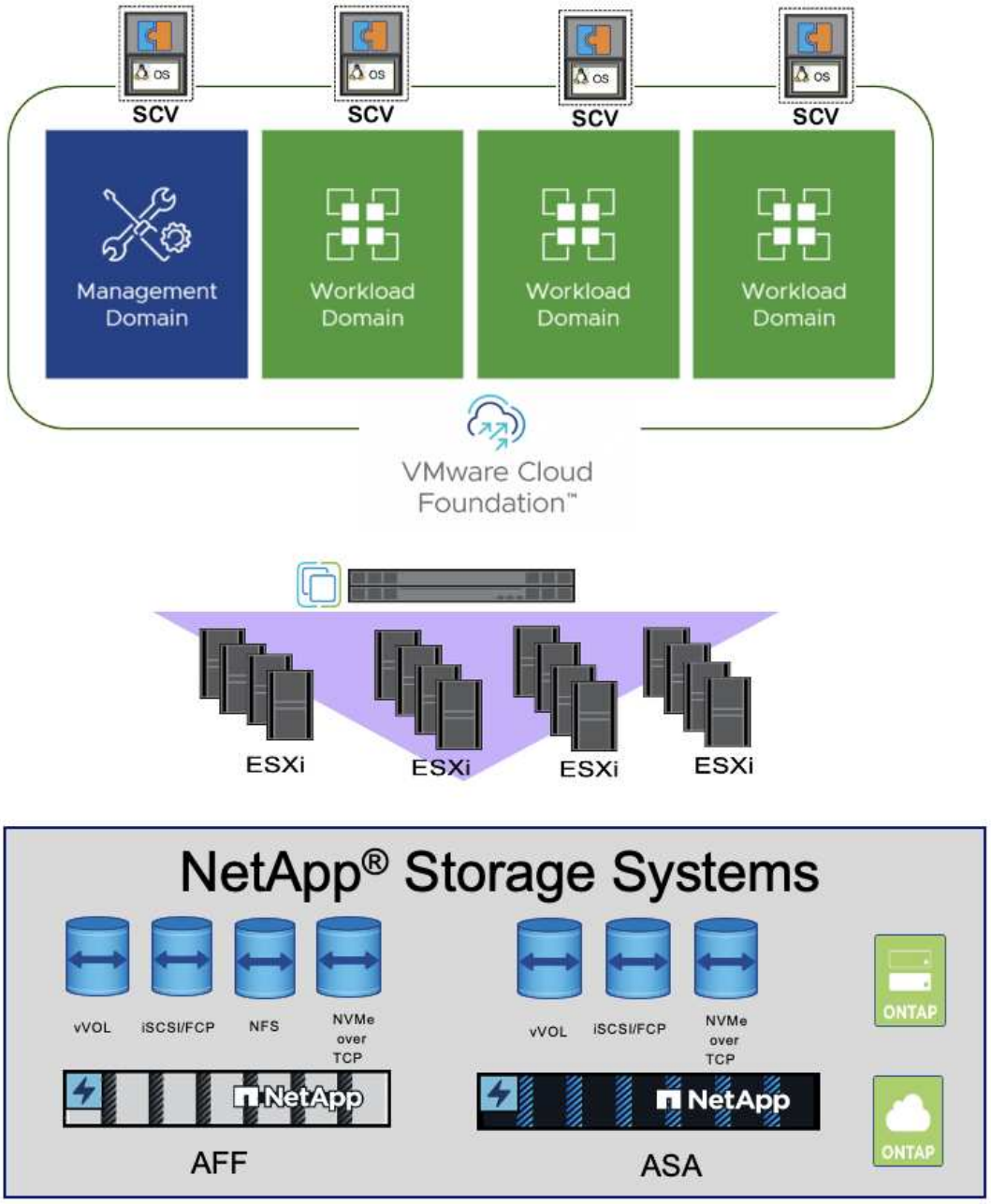
Descripción general de la arquitectura

SCV es una herramienta poderosa diseñada para facilitar operaciones de respaldo y restauración rápidas, eficientes en términos de espacio, consistentes ante fallos y consistentes con las máquinas virtuales para máquinas virtuales, almacenes de datos y archivos y carpetas en entornos VMware. SCV se implementa como un dispositivo virtual Linux que utiliza un archivo OVA y aprovecha una arquitectura de complemento remoto.

Arquitectura de implementación de SCV

- Implementación de dispositivo virtual: SCV se implementa como un dispositivo virtual Linux mediante un archivo OVA. Este método de implementación garantiza un proceso de configuración optimizado y eficiente.
- Arquitectura de complemento remoto: SCV utiliza una arquitectura de complemento remoto, lo que permite escalabilidad y flexibilidad en la gestión de múltiples instancias.
- Relación uno a uno: cada dominio VCF requiere una instancia SCV dedicada, lo que garantiza operaciones de respaldo y restauración aisladas y eficientes.

Con ONTAP 9.10.1 y versiones posteriores, NetApp AFF y ASA admiten NVMe sobre TCP. Datos que se encuentran en sistemas primarios AFF o ASA y se pueden replicar en sistemas secundarios ONTAP AFF o ASA . SCV también funciona con SnapCenter Server para soportar operaciones de respaldo y restauración basadas en aplicaciones en entornos VMware para complementos específicos de la aplicación SnapCenter . Para más información consultar,"Documentación del SnapCenter Plug-in for VMware vSphere" y"Proteja las cargas de trabajo con SnapCenter"



La regla de copia de seguridad 3-2-1 es una estrategia de protección de datos que implica hacer tres copias de los datos, almacenarlas en dos tipos de medios diferentes y mantener una copia fuera del sitio. BlueXP backup and recovery 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 respaldo y recuperación en entornos locales y en la nube. Parte de la suite de BlueXP backup and recovery NetApp BlueXP es una función que se integra con SCV (en las instalaciones) para extender una copia de los datos al almacenamiento de objetos en la nube. Esto establece una tercera copia de los datos fuera del sitio que proviene de las copias de seguridad del almacenamiento primario o secundario. La BlueXP backup and recovery facilita la configuración de políticas de almacenamiento que transfieren copias de sus datos desde cualquiera de estas dos ubicaciones locales. Para más detalles, consulte"Protección de datos 3-2-1 para VMware con complemento SnapCenter y BlueXP backup and recovery para máquinas virtuales" .

Pasos de implementación de SCV para VCF en NVMe

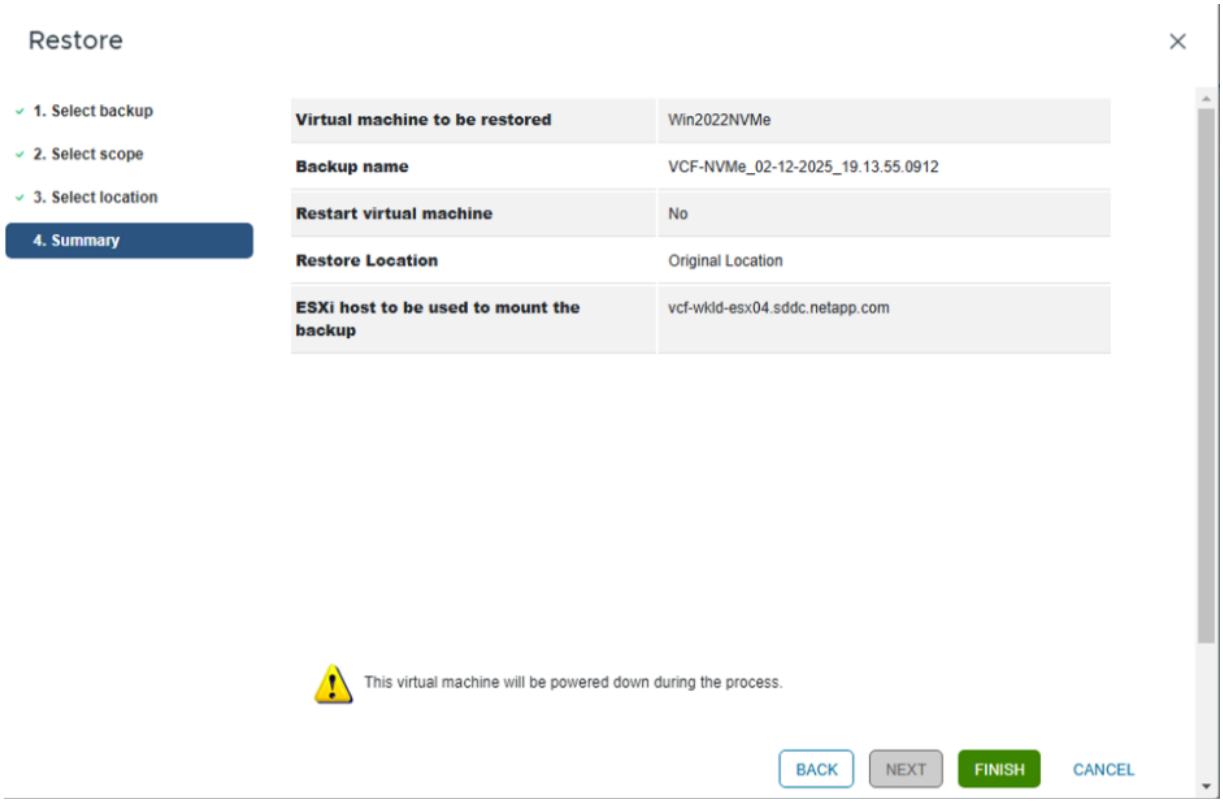
El"ONTAP tools for VMware vSphere" (OTV) proporciona una solución potente y eficiente para administrar el almacenamiento de NetApp en entornos VMware. Al integrarse directamente con vCenter Server, OTV simplifica la gestión del almacenamiento, mejora la protección de datos y optimiza el rendimiento. Si bien es opcional, la implementación de OTV puede mejorar significativamente las capacidades de administración y la eficiencia general de los entornos VMware.

- "Cree un almacenamiento NVMe/TCP para dominios de carga de trabajo VCF"
- "Configurar NetApp SnapCenter para VMware vSphere (SCV)"

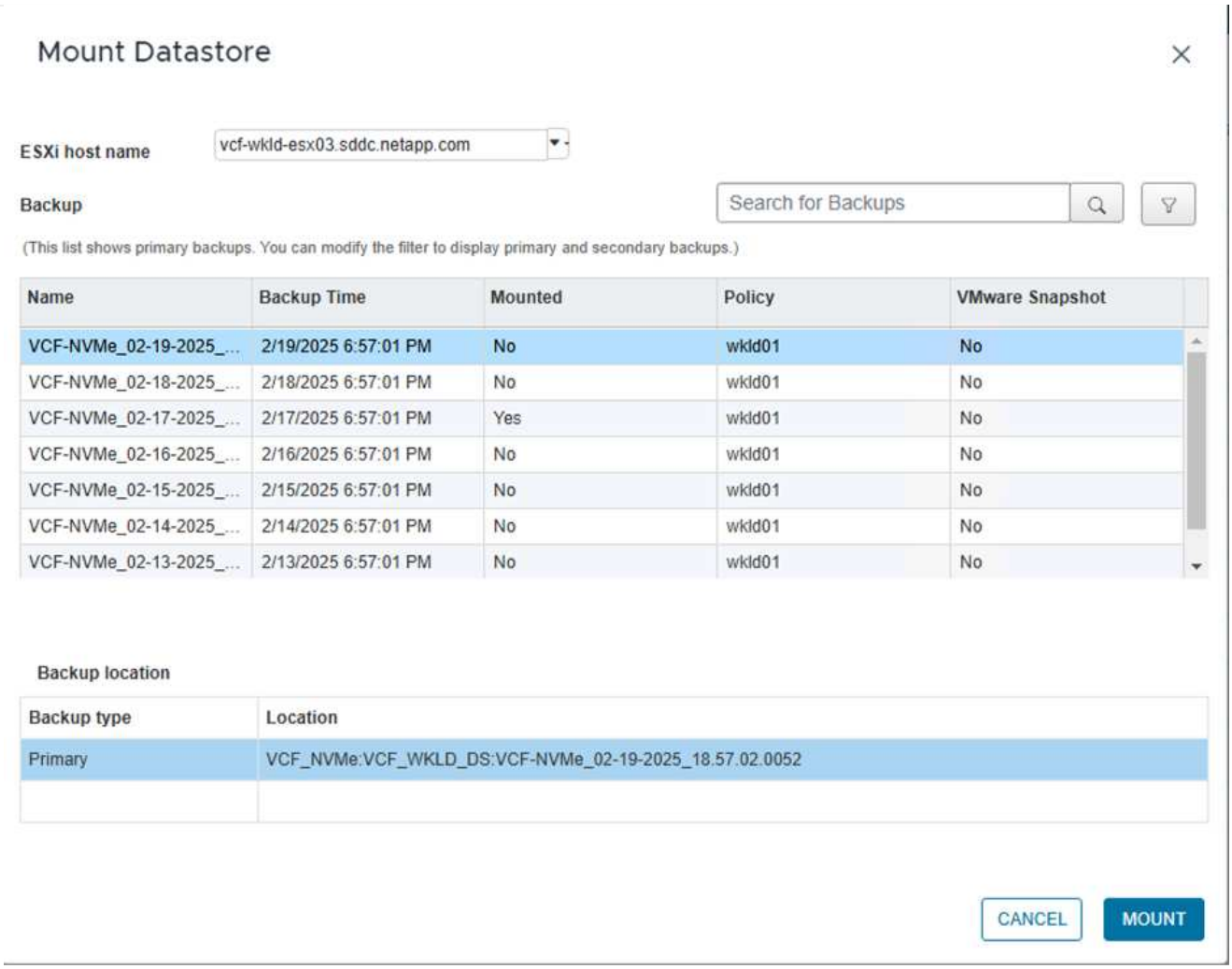
Restaurar máquinas virtuales, almacenes de datos, discos virtuales y archivos o carpetas

SCV proporciona capacidades integrales de copia de seguridad y restauración para entornos VMware. Para entornos VMFS, SCV utiliza operaciones de clonación y montaje junto con Storage VMotion para realizar operaciones de restauración. Esto garantiza una restauración eficiente y sin problemas de los datos. Para más detalles consultar"Cómo se realizan las operaciones de restauración."

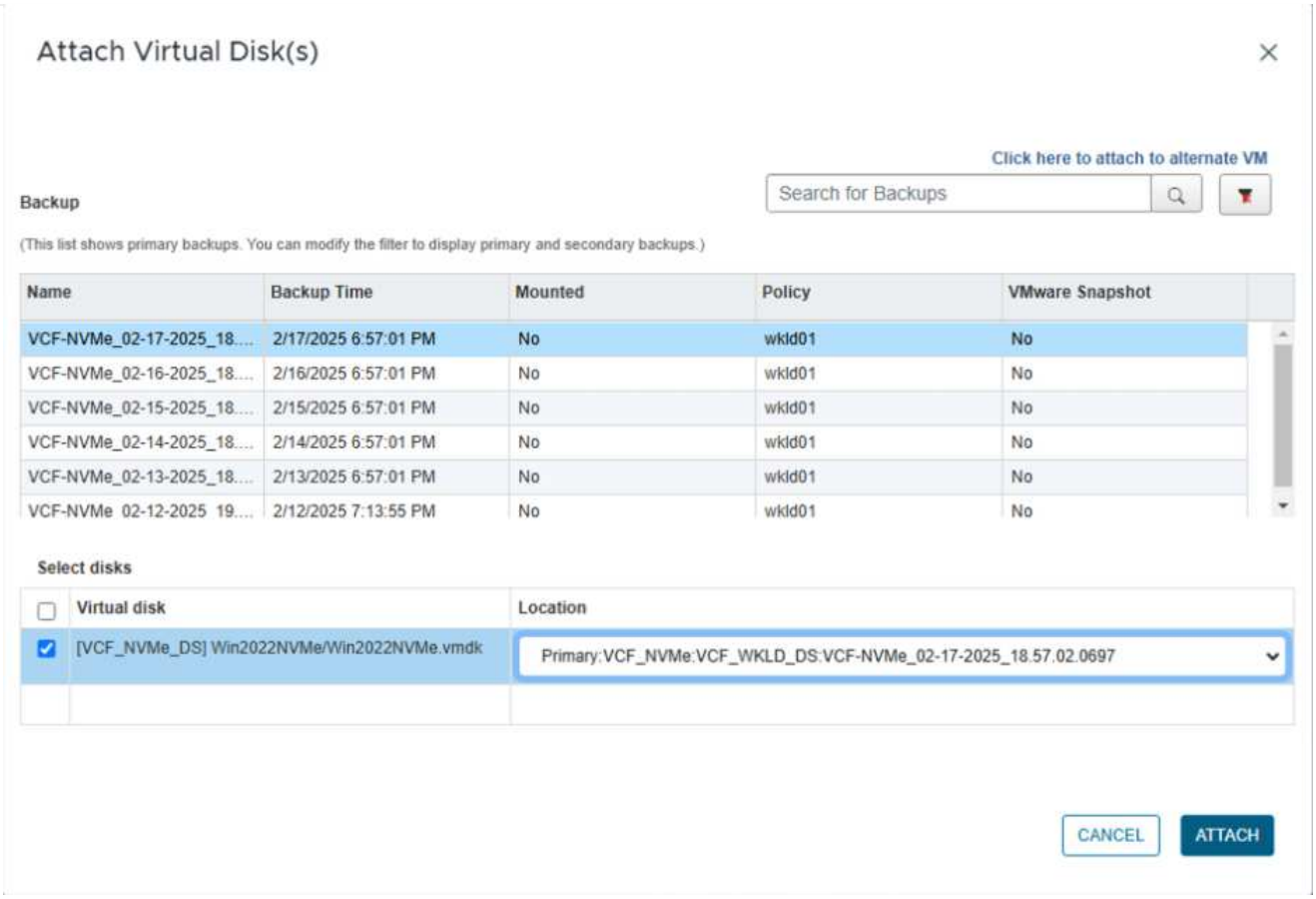
- Restauración de VM Puede restaurar la VM a su host original dentro del mismo vCenter Server o a un host ESXi alternativo administrado por el mismo vCenter Server.
  a. Haga clic con el botón derecho en una máquina virtual y seleccione SnapCenter Plug-in for VMware vSphere en la lista desplegable; luego, seleccione Restaurar en la lista desplegable secundaria para iniciar el asistente.
  b. En el Asistente de restauración, seleccione la instantánea de copia de seguridad que desea restaurar y seleccione Toda la máquina virtual en el campo Alcance de la restauración, seleccione la ubicación de restauración y luego ingrese la información de destino donde se debe montar la copia de seguridad. En la página Seleccionar ubicación, seleccione la ubicación para el almacén de datos restaurado. Revise la página Resumen y haga clic en Finalizar.



- Montar un almacén de datos Puede montar un almacén de datos tradicional desde una copia de seguridad si desea acceder a los archivos de la copia de seguridad. Puede montar la copia de seguridad en el mismo host ESXi donde se creó la copia de seguridad o en un host ESXi alternativo que tenga el mismo tipo de VM y configuraciones de host. Un almacén de datos puede montarse varias veces en un host.
  a. Haga clic con el botón derecho en un almacén de datos y seleccione SnapCenter Plug-in for VMware vSphere > Montar copia de seguridad.
  b. En la página Montar almacén de datos, seleccione una copia de seguridad y una ubicación de copia de seguridad (principal o secundaria) y, luego, haga clic en Montar.

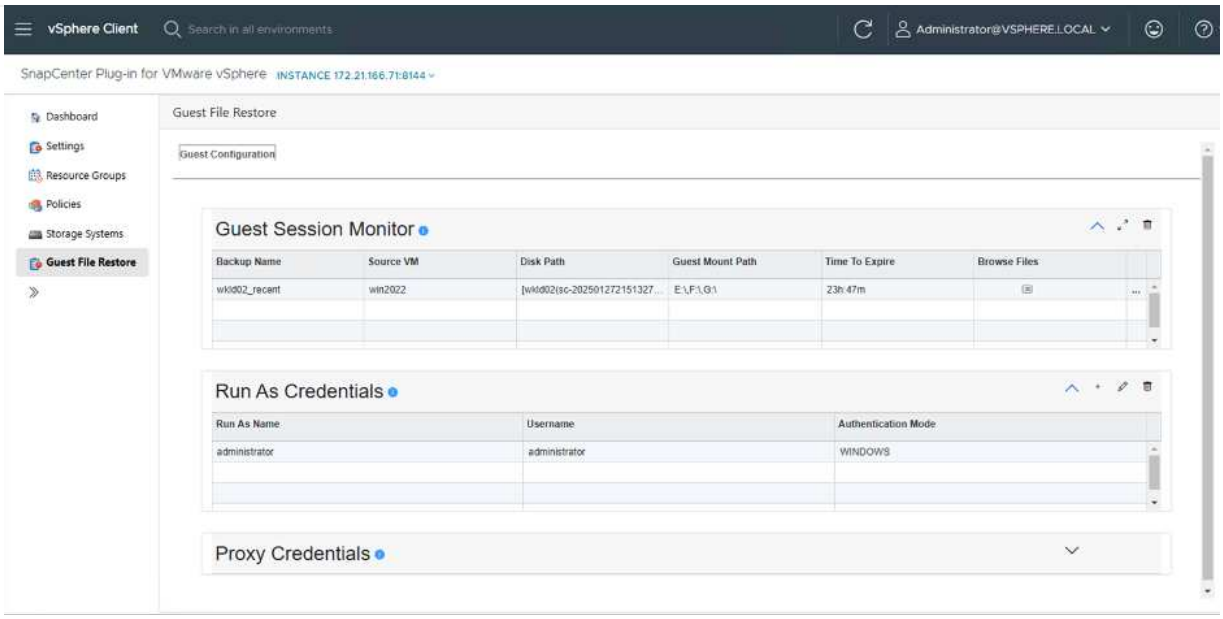


- Conectar un disco virtual Puede conectar uno o más VMDK desde una copia de seguridad a la VM principal, o a una VM alternativa en el mismo host ESXi, o a una VM alternativa en un host ESXi alternativo administrado por el mismo vCenter o un vCenter diferente en modo vinculado.
  a. Haga clic con el botón derecho en una máquina virtual, seleccione SnapCenter Plug-in for VMware vSphere > Conectar discos virtuales.
  b. En la ventana Conectar disco virtual, seleccione una copia de seguridad y seleccione uno o más discos que desee conectar y la ubicación desde donde desea conectarlos (principal o secundaria). De forma predeterminada, los discos virtuales seleccionados se conectan a la máquina virtual principal. Para conectar los discos virtuales seleccionados a una VM alternativa en el mismo host ESXi, seleccione Haga clic aquí para conectar a la VM alternativa y especifique la VM alternativa. Haga clic en Adjuntar.

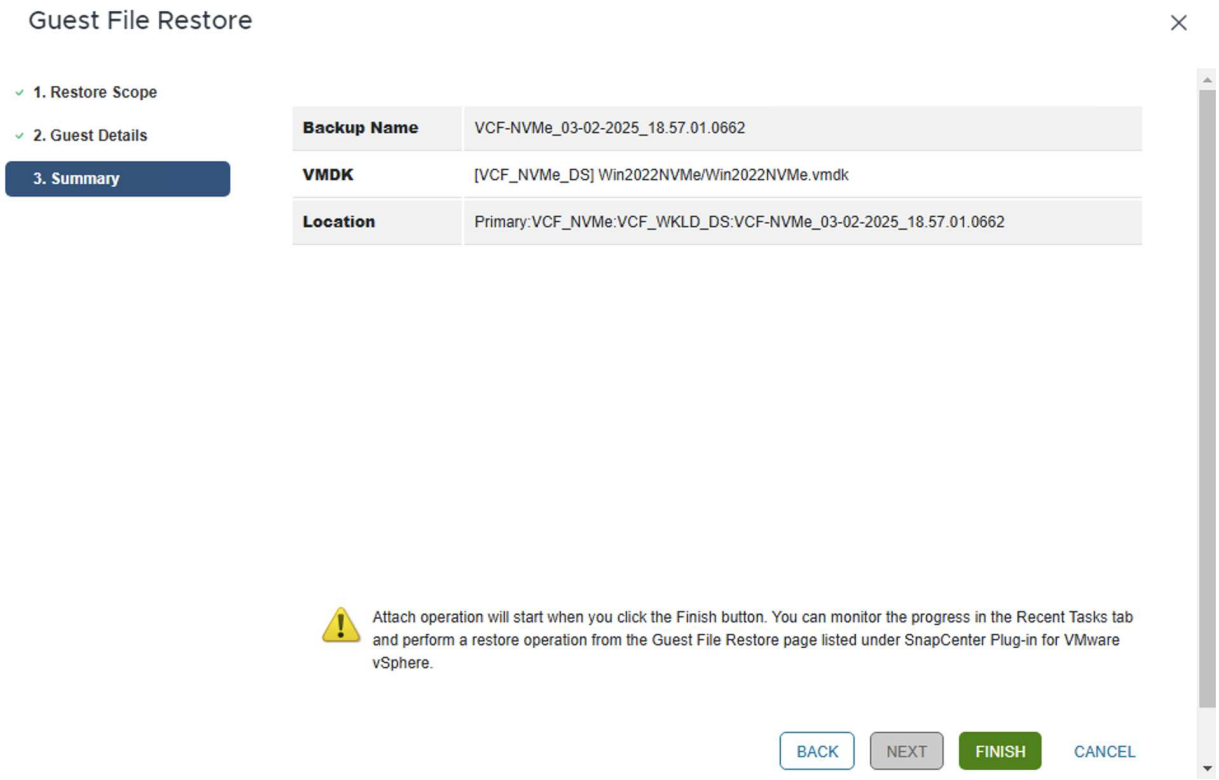


- Pasos para restaurar archivos y carpetas Es posible restaurar archivos y carpetas individuales en una sesión de restauración de archivos de invitado, que adjunta una copia de seguridad de un disco virtual y luego restaura los archivos o carpetas seleccionados. También se pueden restaurar archivos y carpetas. Para más detalles consultar"Restauración de archivos y carpetas de SnapCenter ."

  a. Cuando adjunta un disco virtual para operaciones de restauración de archivos o carpetas invitados, la máquina virtual de destino para la adjuntación debe tener credenciales configuradas antes de realizar la restauración. Desde el SnapCenter Plug-in for VMware vSphere , en complementos, seleccione la sección Restaurar archivos de invitado y ejecutar como credenciales e ingrese las credenciales de usuario. Para el nombre de usuario, debe ingresar “Administrador”.

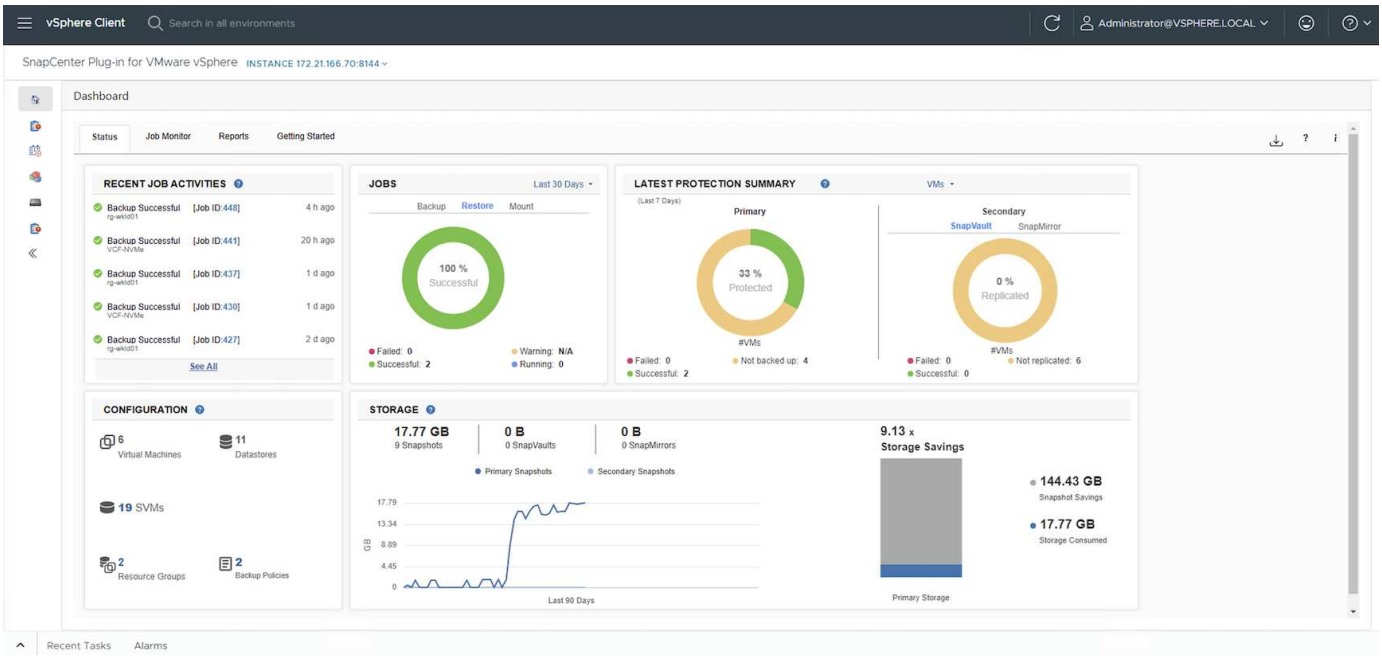


b. Haga clic con el botón derecho en la máquina virtual desde el cliente vSphere y seleccione SnapCenter Plug-in for VMware vSphere > Restaurar archivos invitados. En la página Ámbito de restauración, especifique el nombre de la copia de seguridad, el disco virtual VMDK y la ubicación: principal o secundaria. Haga clic en Resumen para confirmar.



Monitorear e informar

SCV proporciona sólidas capacidades de monitoreo y generación de informes para ayudar a los administradores a gestionar las operaciones de respaldo y restauración de manera eficiente. Puede ver información de estado, monitorear trabajos, descargar registros de trabajos, acceder a informes, para más detalles consultar"Complemento de SnapCenter para VMware vSphere Monitor and Report."



Al aprovechar el poder de NVMe sobre TCP y el SnapCenter Plug-in for VMware vSphere NetApp SnapCenter para VMware vSphere, las organizaciones pueden lograr protección de datos de alto rendimiento y recuperación ante desastres para los dominios de carga de trabajo de VMware Cloud Foundation. Este enfoque garantiza operaciones de respaldo y restauración rápidas y confiables, minimizando el tiempo de inactividad y protegiendo datos críticos.

Proteja los almacenes de datos de VMware con BlueXP

Obtenga información sobre cómo proteger los almacenes de datos de VMware mediante la BlueXP disaster recovery

Obtenga información sobre las soluciones de NetApp para recuperación ante desastres utilizando la BlueXP disaster recovery para VMware. Esto proporciona soluciones sólidas para la recuperación ante desastres mediante el uso de replicación a nivel de bloque desde un sitio principal a un sitio de recuperación ante desastres.

BlueXP DRaaS es un método eficaz y económico para proteger las cargas de trabajo contra fallas del sitio y problemas de integridad de los datos, incluidos ataques de ransomware. Además, NetApp BlueXP DRaaS mejora esta estrategia al proporcionar una solución de recuperación ante desastres administrada y basada en la nube, que garantiza una recuperación rápida y un tiempo de inactividad mínimo durante los desastres.

Consulte las siguientes soluciones para obtener detalles técnicos.

- "Recuperación ante desastres con BlueXP DRaaS para almacenes de datos VMFS"
- "Recuperación ante desastres con BlueXP DRaaS para almacenes de datos NFS"

Configure la protección de datos 3-2-1 para VMware con el complemento SnapCenter para VMware vSphere y la BlueXP backup and recovery

Configure una estrategia de protección de datos 3-2-1 para entornos VMware mediante el complemento SnapCenter para la BlueXP backup and recovery. Este procedimiento

incluye la configuración de copias de seguridad de máquinas virtuales y almacenes de datos en clústeres ONTAP primarios y secundarios, la configuración del complemento y BlueXP, y la administración de la replicación de datos en la nube o en un almacenamiento externo para una recuperación confiable.

La estrategia de respaldo 3-2-1 es un método de protección de datos aceptado por la industria, que proporciona un enfoque integral para salvaguardar datos valiosos. Esta estrategia es confiable y garantiza que incluso si ocurre algún desastre inesperado, todavía habrá una copia de los datos disponible.

Descripción general

La estrategia se compone de tres reglas fundamentales:

1. Conserve al menos tres copias de sus datos. Esto garantiza que incluso si se pierde o se corrompe una copia, todavía tendrá al menos dos copias restantes a las que recurrir.
2. Almacene dos copias de seguridad en diferentes medios o dispositivos de almacenamiento. La diversificación de los medios de almacenamiento ayuda a proteger contra fallas específicas del dispositivo o del medio. Si un dispositivo se daña o falla un tipo de medio, la otra copia de respaldo permanece intacta.
3. Por último, asegúrese de que al menos una copia de seguridad esté fuera del sitio. El almacenamiento externo funciona como medida de seguridad contra desastres localizados, como incendios o inundaciones, que podrían inutilizar las copias locales.

Este documento de solución cubre una solución de copias de seguridad 3-2-1 que utiliza el SnapCenter Plug-in for VMware vSphere (SCV) para crear copias de seguridad primarias y secundarias de nuestras máquinas virtuales locales y la BlueXP backup and recovery para máquinas virtuales para realizar una copia de seguridad de nuestros datos en el almacenamiento en la nube o StorageGRID.

Casos de uso

Esta solución aborda los siguientes casos de uso:

- Copia de seguridad y restauración de máquinas virtuales y almacenes de datos locales mediante el SnapCenter Plug-in for VMware vSphere.
- Copia de seguridad y restauración de máquinas virtuales y almacenes de datos locales, alojados en clústeres ONTAP y respaldados en almacenamiento de objetos mediante la BlueXP backup and recovery para máquinas virtuales.

Almacenamiento de datos NetApp ONTAP

ONTAP es la solución de almacenamiento líder en la industria de NetApp que ofrece almacenamiento unificado ya sea que acceda a través de protocolos SAN o NAS. La estrategia de respaldo 3-2-1 garantiza que los datos locales estén protegidos en más de un tipo de medio y NetApp ofrece plataformas que van desde flash de alta velocidad hasta medios de menor costo.

FAS	AFF C-Series	AFF A-Series	ASA A-Series
Hybrid flash storage	**Capacity all-flash storage**	**Performance all-flash storage**	**All-flash SAN storage**
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency Backup / Low-cost DR	Refresh of hybrid flash, Tier 1 @ 2-4ms latency Tier 2 workloads VMware datastores	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed

Para obtener más información sobre todas las plataformas de hardware de NetApp, consulte "Almacenamiento de datos de NetApp" .

Plugin de SnapCenter para VMware vSphere

El complemento SnapCenter para VMware vSphere es una oferta de protección de datos que está estrechamente integrada con VMware vSphere y permite una fácil gestión de copias de seguridad y restauraciones de máquinas virtuales. Como parte de esa solución, SnapMirror proporciona un método rápido y confiable para crear una segunda copia de seguridad inmutable de los datos de la máquina virtual en un clúster de almacenamiento ONTAP secundario. Con esta arquitectura instalada, las operaciones de restauración de máquinas virtuales se pueden iniciar fácilmente desde las ubicaciones de respaldo principales o secundarias.

SCV se implementa como un dispositivo virtual Linux mediante un archivo OVA. El complemento ahora utiliza una arquitectura de complemento remoto. El complemento remoto se ejecuta fuera del servidor vCenter y está alojado en el dispositivo virtual SCV.

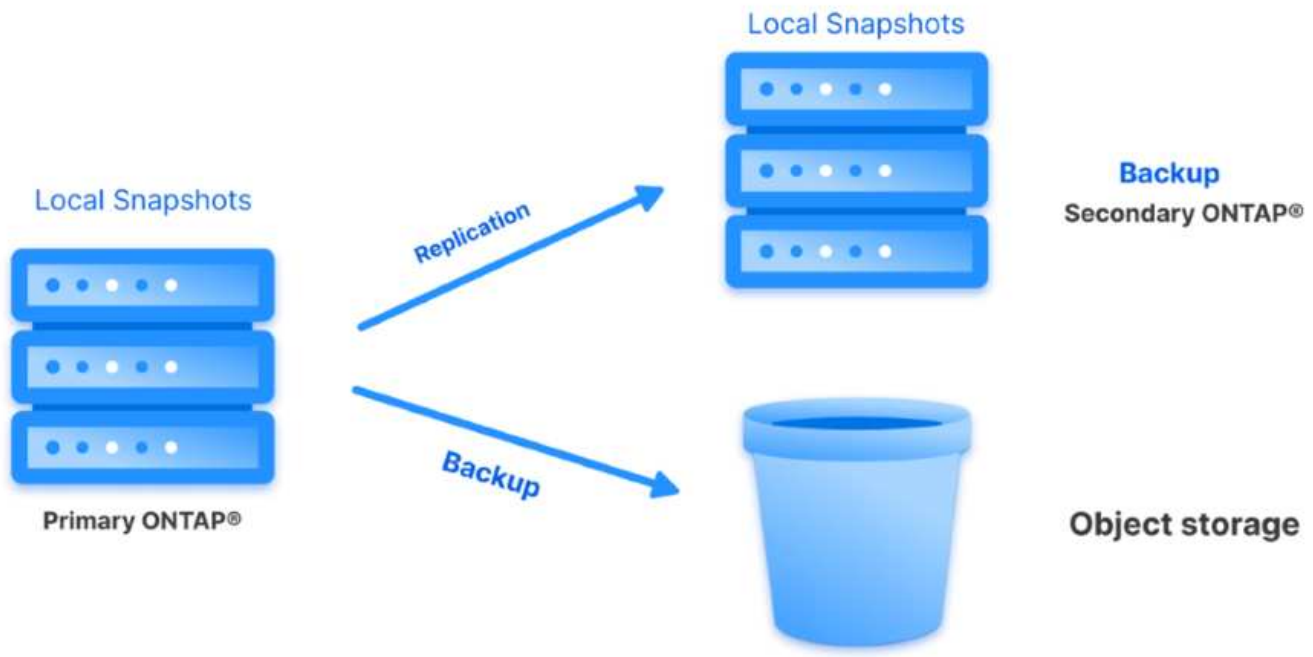
Para obtener información detallada sobre SCV, consulte "Documentación del SnapCenter Plug-in for VMware vSphere" .

BlueXP backup and recovery para máquinas virtuales

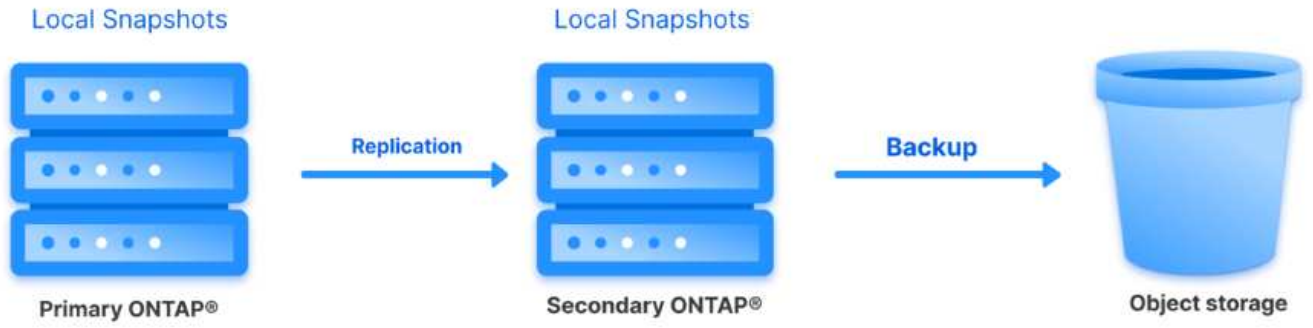
BlueXP backup and recovery es una herramienta basada en la nube para la gestión de datos que proporciona un único plano de control para una amplia gama de operaciones de respaldo y recuperación en entornos locales y en la nube. Parte de la suite de BlueXP backup and recovery NetApp BlueXP es una función que se integra con el complemento SnapCenter para VMware vSphere (en las instalaciones) para extender una copia de los datos al almacenamiento de objetos en la nube. Esto establece una tercera copia de los datos fuera del sitio que proviene de las copias de seguridad del almacenamiento primario o secundario. La BlueXP backup and recovery facilita la configuración de políticas de almacenamiento que transfieren copias de sus datos desde cualquiera de estas dos ubicaciones locales.

Al elegir entre las copias de seguridad primarias y secundarias como fuente en BlueXP Backup and Recovery, se implementará una de dos topologías:

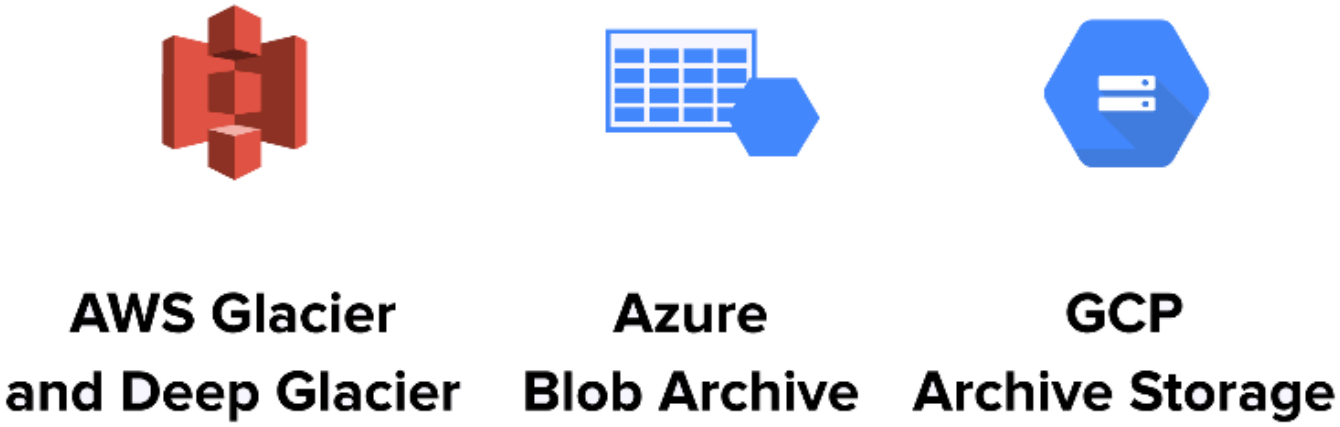
Topología de abanico: cuando el SnapCenter Plug-in for VMware vSphere inicia una copia de seguridad, inmediatamente se toma una instantánea local. Luego, SCV inicia una operación SnapMirror que replica la instantánea más reciente en el clúster ONTAP secundario. En BlueXP Backup and Recovery, una política especifica el clúster ONTAP principal como la fuente para una copia instantánea de los datos que se transferirán al almacenamiento de objetos en el proveedor de nube de su elección.



Topología en cascada: la creación de copias de datos primarias y secundarias mediante SCV es idéntica a la topología de abanico mencionada anteriormente. Sin embargo, esta vez se crea una política en BlueXP Backup and Recovery que especifica que la copia de seguridad en el almacenamiento de objetos se originará desde el clúster ONTAP secundario.



La BlueXP backup and recovery puede crear copias de seguridad de instantáneas de ONTAP locales en AWS Glacier, Azure Blob y almacenamiento de GCP Archive.



Además, puede utilizar NetApp StorageGRID como destino de respaldo de almacenamiento de objetos. Para obtener más información sobre StorageGRID , consulte "Página de inicio de StorageGRID" .

Descripción general de la implementación de la solución

Esta lista proporciona los pasos de alto nivel necesarios para configurar esta solución y ejecutar operaciones de copia de seguridad y restauración desde SCV y la BlueXP backup and recovery:

1. Configure la relación SnapMirror entre los clústeres ONTAP que se utilizarán para copias de datos primarias y secundarias.
2. Configurar el complemento SnapCenter para VMware vSphere.
   a. Agregar sistemas de almacenamiento
   b. Crear políticas de respaldo
   c. Crear grupos de recursos
   d. Ejecutar los primeros trabajos de copia de seguridad
3. Configurar la BlueXP backup and recovery para máquinas virtuales
   a. Añadir entorno de trabajo
   b. Descubra los dispositivos SCV y vCenter
   c. Crear políticas de respaldo
   d. Activar copias de seguridad
4. Restaurar máquinas virtuales desde el almacenamiento primario y secundario mediante SCV.
5. Restaure máquinas virtuales desde el almacenamiento de objetos mediante la copia de seguridad y restauración de BlueXP .

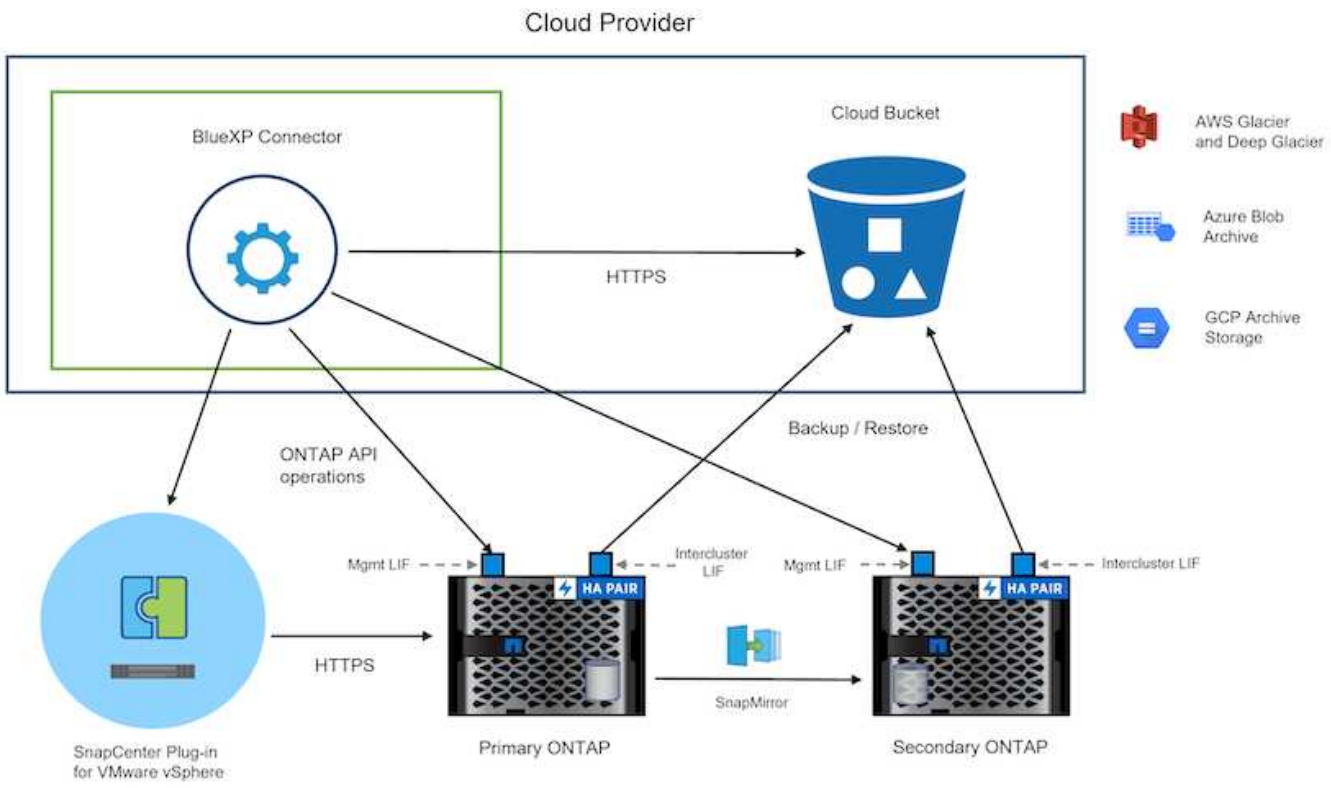
Prerrequisitos

El propósito de esta solución es demostrar la protección de datos de máquinas virtuales que se ejecutan en VMware vSphere, dominios de carga de trabajo VCF VI o dominios de administración VCF. Las máquinas virtuales de esta solución están alojadas en almacenes de datos NFS proporcionados por NetApp ONTAP. Esta solución asume que los siguientes componentes están configurados y listos para usar:

1. Clúster de almacenamiento ONTAP con almacenes de datos NFS o VMFS conectados a VMware vSphere. Se admiten almacenes de datos NFS y VMFS. Para esta solución se utilizaron almacenes de datos NFS.
2. Clúster de almacenamiento ONTAP secundario con relaciones SnapMirror establecidas para volúmenes utilizados para almacenes de datos NFS.
3. Conector BlueXP instalado para el proveedor de nube utilizado para copias de seguridad de almacenamiento de objetos.
4. Las máquinas virtuales que se respaldarán se encuentran en almacenes de datos NFS que residen en el clúster de almacenamiento ONTAP principal.
5. Conectividad de red entre el conector BlueXP y las interfaces de administración del clúster de almacenamiento ONTAP local.
6. Conectividad de red entre el conector BlueXP y la máquina virtual del dispositivo SCV local y entre el conector BlueXP y vCenter.
7. Conectividad de red entre los LIF entre clústeres de ONTAP locales y el servicio de almacenamiento de objetos.
8. DNS configurado para la administración de SVM en clústeres de almacenamiento ONTAP primarios y secundarios. Para obtener más información, consulte "Configurar DNS para la resolución del nombre de host" .

Arquitectura de alto nivel

La prueba/validación de esta solución se realizó en un laboratorio que puede o no coincidir con el entorno de implementación final.



Implementación de la solución

En esta solución, proporcionamos instrucciones detalladas para implementar y validar una solución que utiliza el SnapCenter Plug-in for VMware vSphere, junto con la BlueXP backup and recovery, para realizar la copia de seguridad y la recuperación de máquinas virtuales de Windows y Linux dentro de un clúster de VMware vSphere ubicado en un centro de datos local. Las máquinas virtuales en esta configuración se almacenan en almacenes de datos NFS alojados por un clúster de almacenamiento ONTAP A300. Además, un clúster de almacenamiento ONTAP A300 independiente sirve como destino secundario para los volúmenes replicados mediante SnapMirror. Además, se utilizaron el almacenamiento de objetos alojado en Amazon Web Services y Azure Blob como destinos para una tercera copia de los datos.

Revisaremos la creación de relaciones SnapMirror para copias secundarias de nuestras copias de seguridad administradas por SCV y la configuración de trabajos de copia de seguridad tanto en SCV como en la BlueXP backup and recovery.

Para obtener información detallada sobre el SnapCenter Plug-in for VMware vSphere, consulte "Documentación del SnapCenter Plug-in for VMware vSphere" .

Para obtener información detallada sobre la BlueXP backup and recovery, consulte "Documentación de BlueXP backup and recovery" .

Establecer relaciones SnapMirror entre clústeres ONTAP

El SnapCenter Plug-in for VMware vSphere utiliza la tecnología ONTAP SnapMirror para administrar el transporte de copias secundarias de SnapMirror y/o SnapVault a un clúster ONTAP secundario.

Las políticas de respaldo de SCV tienen la opción de utilizar relaciones SnapMirror o SnapVault . La principal diferencia es que al utilizar la opción SnapMirror , el programa de retención configurado para las copias de seguridad en la política será el mismo en las ubicaciones principal y secundaria. SnapVault está diseñado para archivar y al utilizar esta opción se puede establecer un programa de retención separado con la relación

SnapMirror para las copias de instantáneas en el clúster de almacenamiento ONTAP secundario.

La configuración de las relaciones de SnapMirror se puede realizar en BlueXP , donde muchos de los pasos están automatizados, o se puede realizar mediante el Administrador del sistema y la CLI de ONTAP . Todos estos métodos se analizan a continuación.

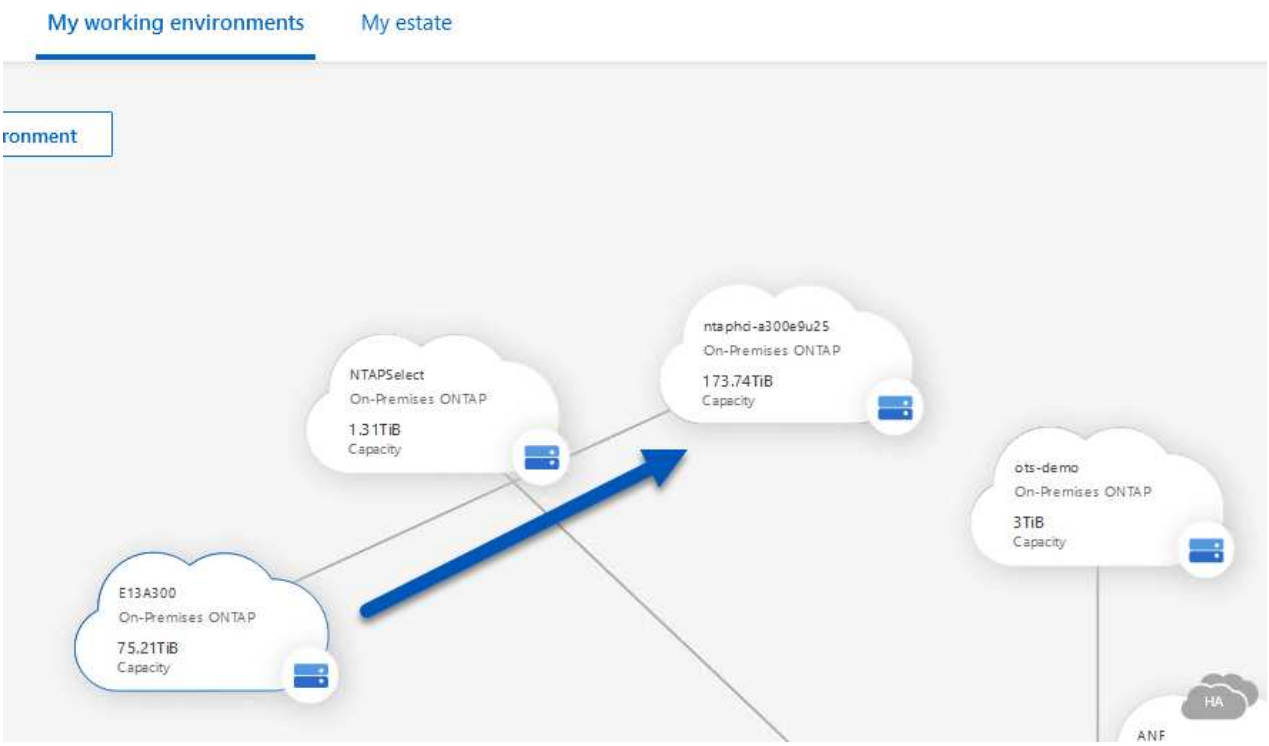
Establecer relaciones de SnapMirror con BlueXP

Los siguientes pasos deben completarse desde la consola web de BlueXP :

Configuración de replicación para sistemas de almacenamiento ONTAP primarios y secundarios

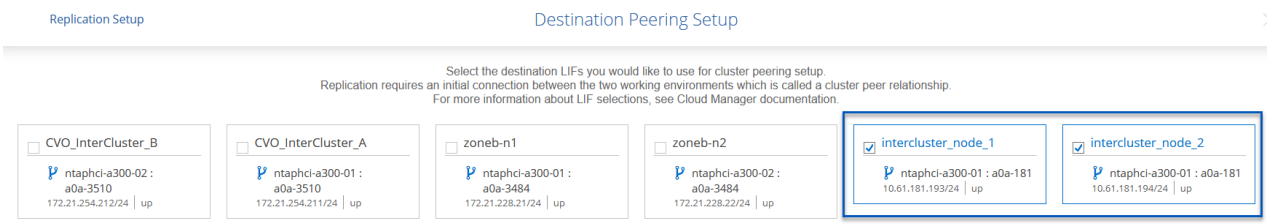
Comience iniciando sesión en la consola web de BlueXP y navegando hasta Canvas.

1. Arrastre y suelte el sistema de almacenamiento ONTAP de origen (principal) en el sistema de almacenamiento ONTAP de destino (secundario).

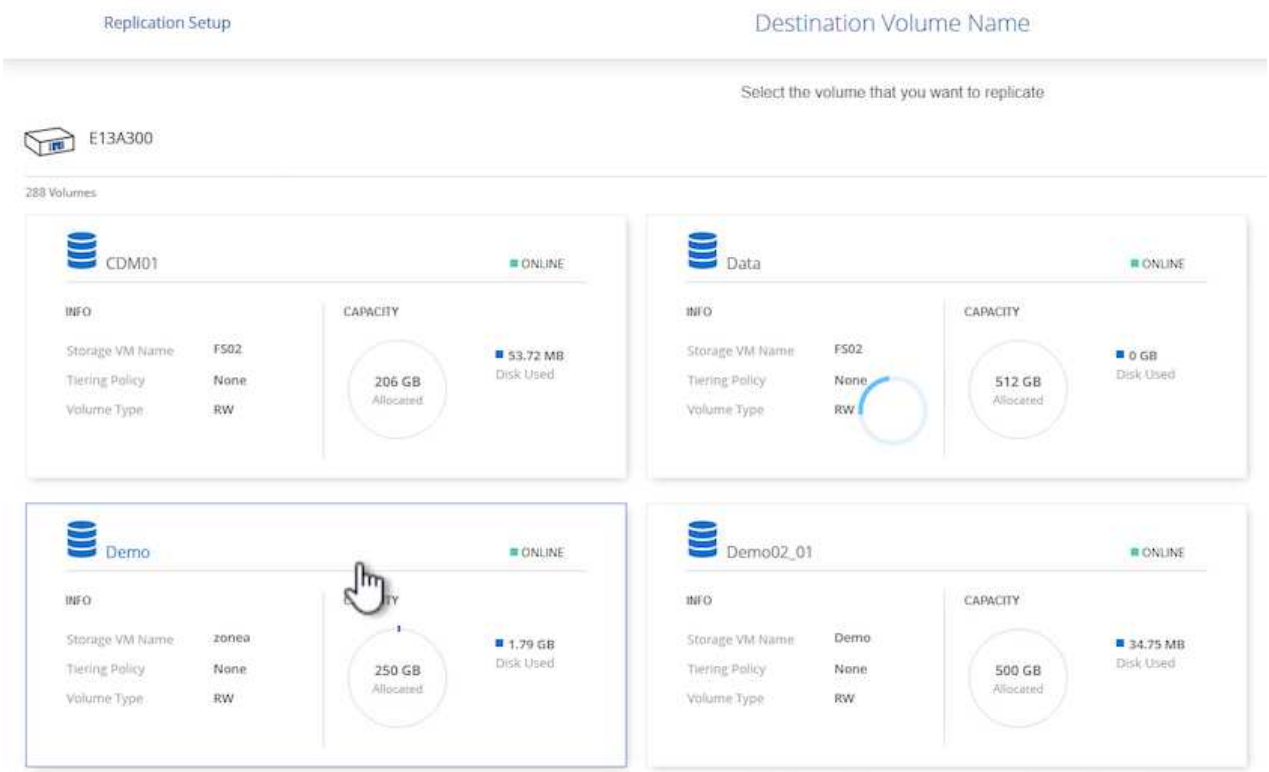


2. Desde el menú que aparece seleccione **Replicación**.

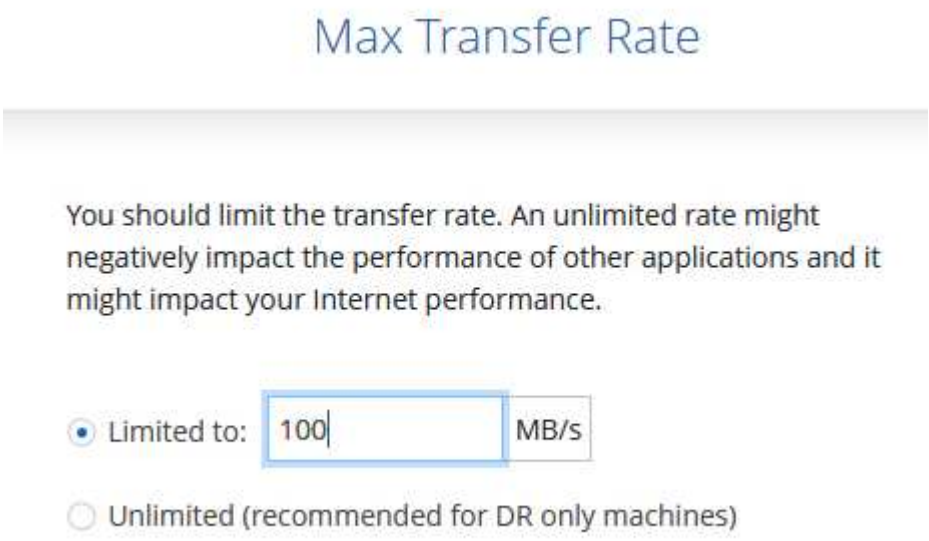
3. En la página **Configuración de emparejamiento de destino**, seleccione los LIF entre clústeres de destino que se utilizarán para la conexión entre sistemas de almacenamiento.



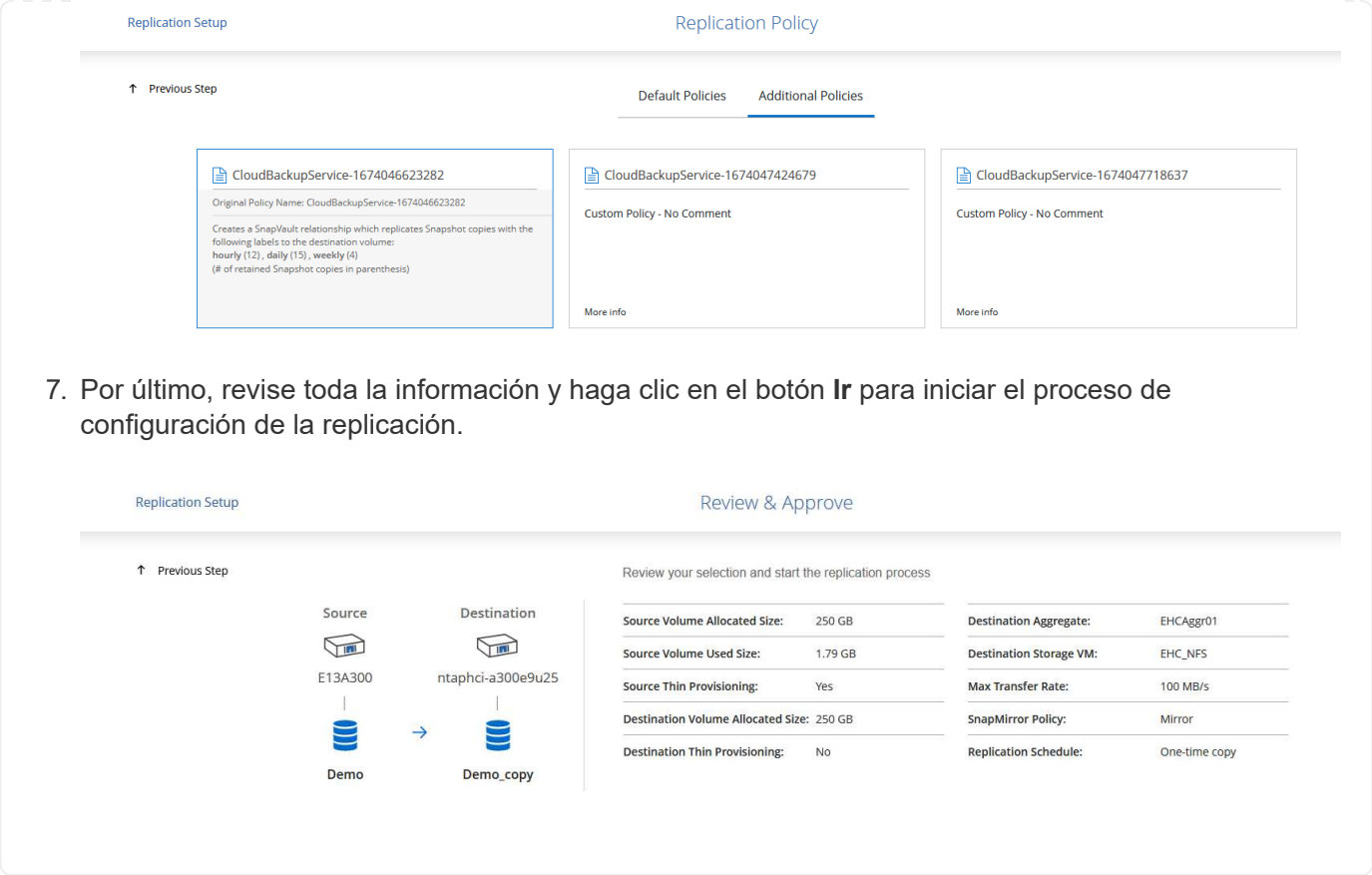
4. En la página **Nombre del volumen de destino**, primero seleccione el volumen de origen y luego complete el nombre del volumen de destino y seleccione el SVM de destino y el agregado. Haga clic en **Siguiente** para continuar.



5. Seleccione la velocidad de transferencia máxima para que se produzca la replicación.



6. Elija la política que determinará el programa de retención para las copias de seguridad secundarias. Esta política se puede crear de antemano (consulte el proceso manual a continuación en el paso **Crear una política de retención de instantáneas**) o se puede cambiar después del hecho si así se desea.



7. Por último, revise toda la información y haga clic en el botón **Ir** para iniciar el proceso de configuración de la replicación.

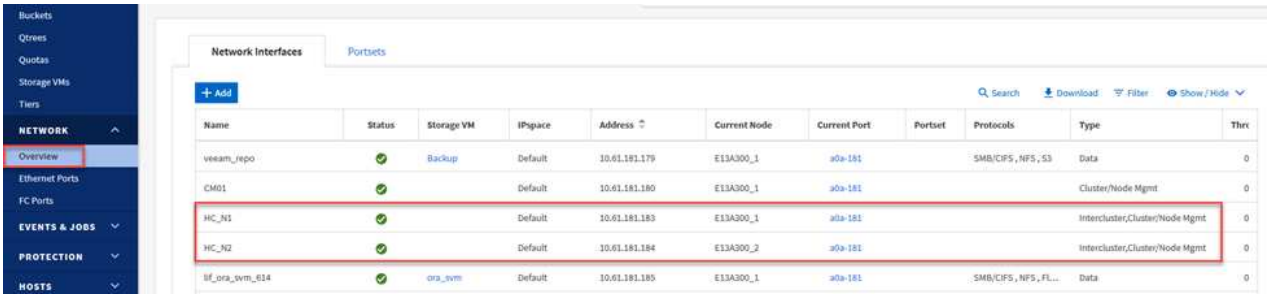
Establecer relaciones de SnapMirror con System Manager y ONTAP CLI

Todos los pasos necesarios para establecer relaciones de SnapMirror se pueden realizar con el Administrador del sistema o la CLI de ONTAP . La siguiente sección proporciona información detallada para ambos métodos:

Registrar las interfaces lógicas entre clústeres de origen y destino

Para los clústeres ONTAP de origen y destino, puede recuperar la información LIF entre clústeres desde el Administrador del sistema o desde la CLI.

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



2. Para recuperar las direcciones IP entre clústeres mediante la CLI, ejecute el siguiente comando:

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

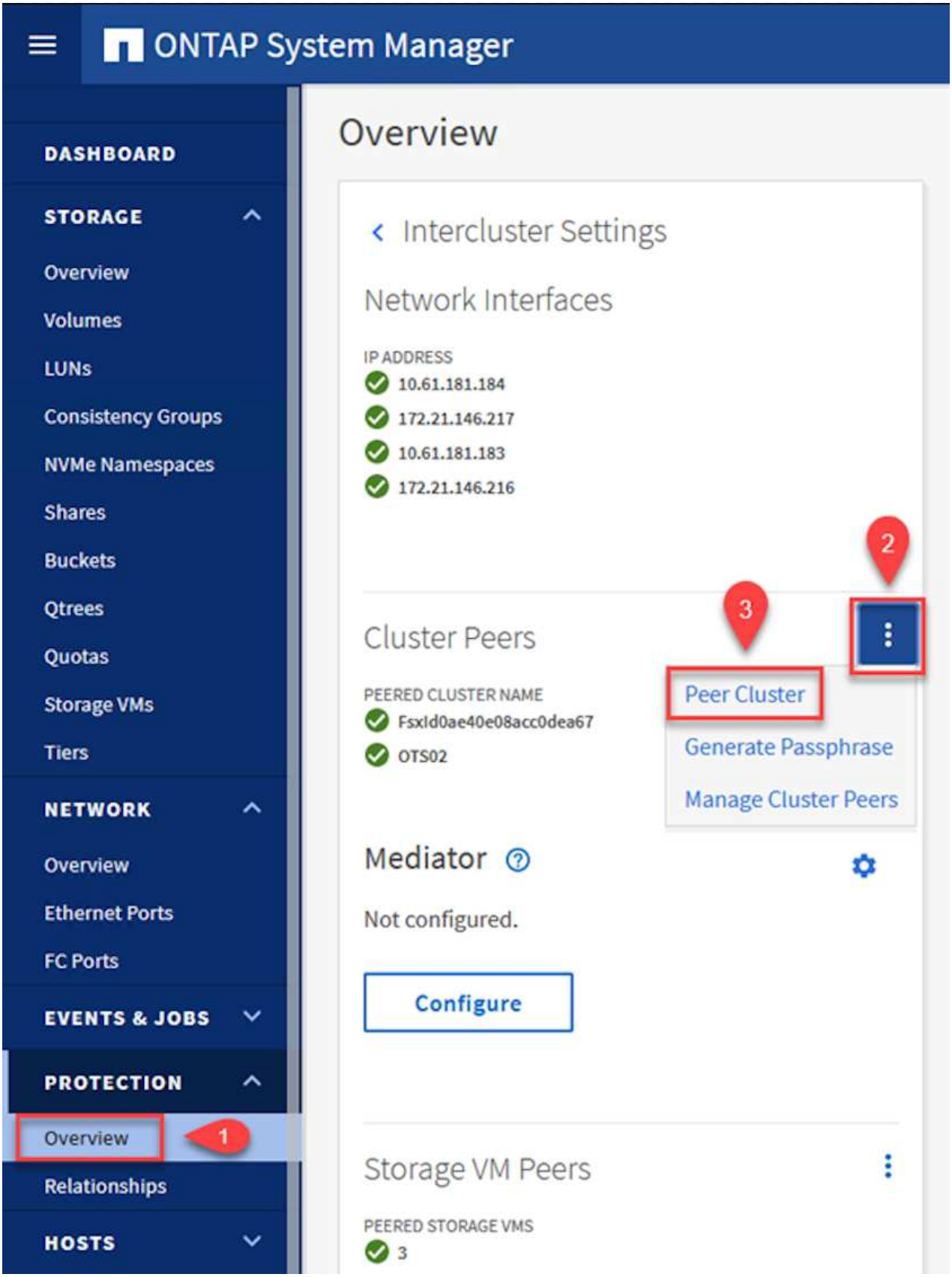
Establecer peering de clústeres entre clústeres ONTAP

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

1. Configure el peering en el clúster ONTAP de destino mediante el `cluster peer create` dominio. Cuando se le solicite, ingrese una frase de contraseña única que se utilizará más adelante en el clúster de origen para finalizar el proceso de creación.

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

2. En el clúster de origen, puede establecer la relación de pares del clúster mediante ONTAP System Manager o la CLI. Desde el Administrador del sistema ONTAP , navegue a Protección > Descripción general y seleccione Clúster de pares.

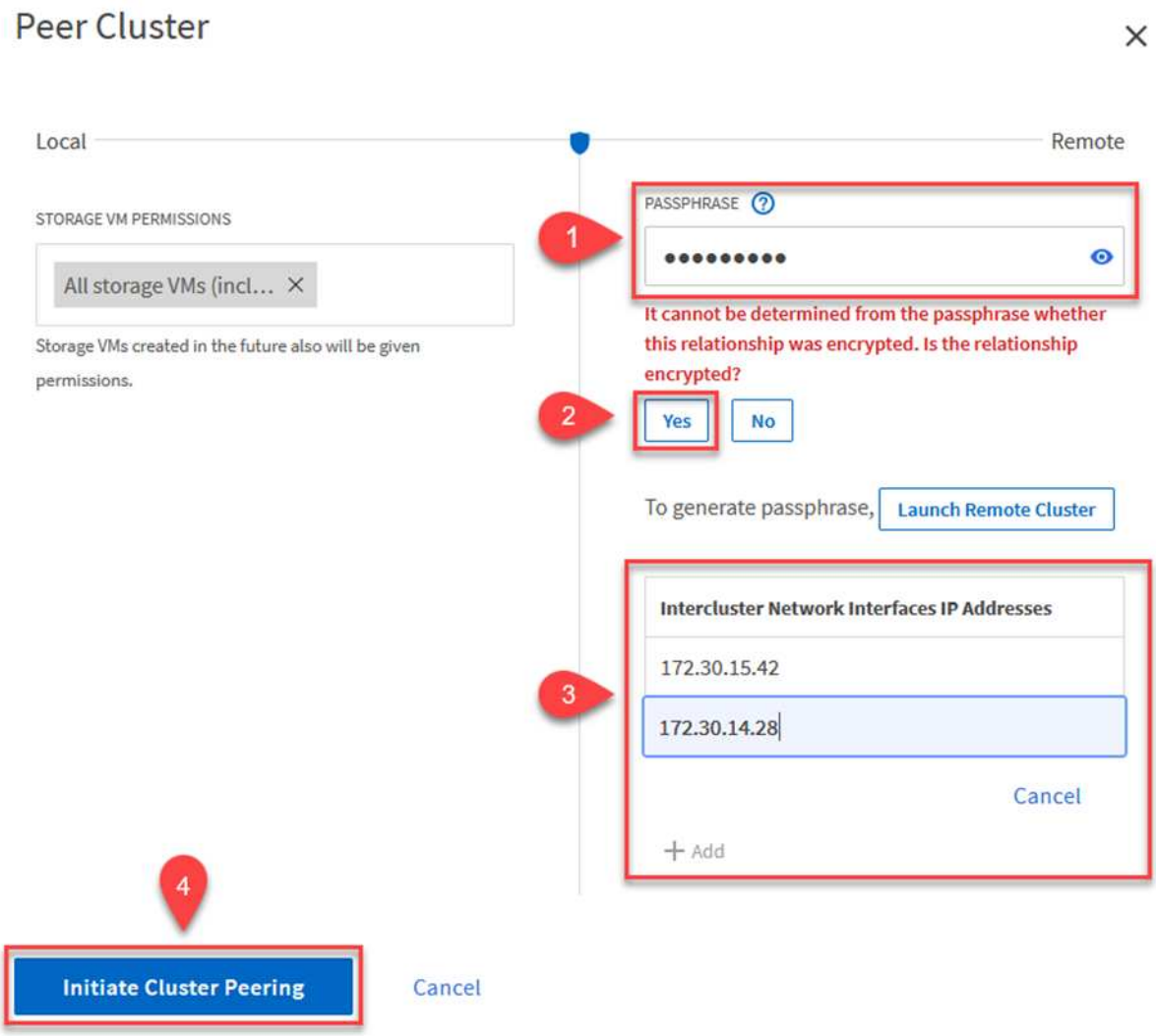


3. En el cuadro de diálogo Clúster de pares, complete la información requerida:
   a. Ingrese la frase de contraseña que se utilizó para establecer la relación de clúster de pares en el clúster ONTAP de destino.

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

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

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



4. Verifique el estado de la relación de pares del clúster desde el clúster ONTAP de destino con el siguiente comando:

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

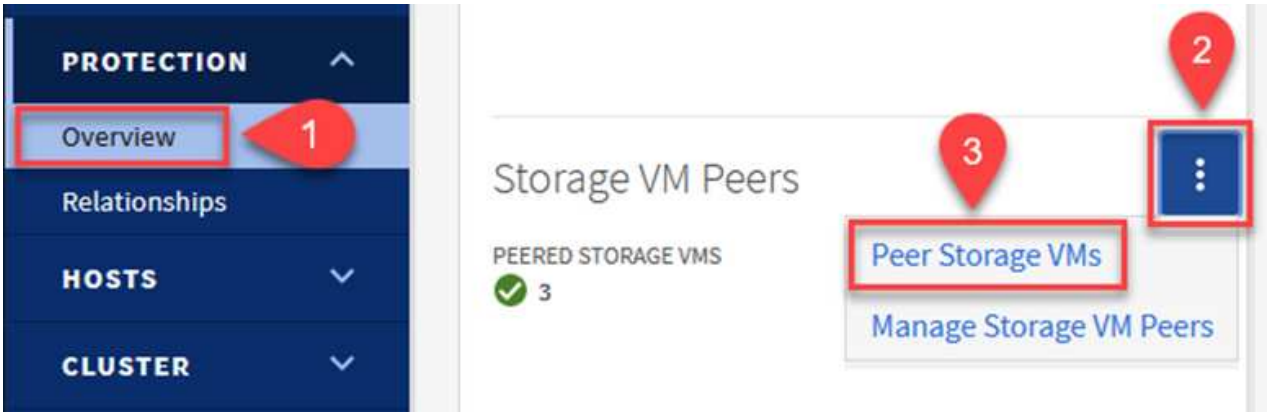
Establecer una relación de peering de SVM

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

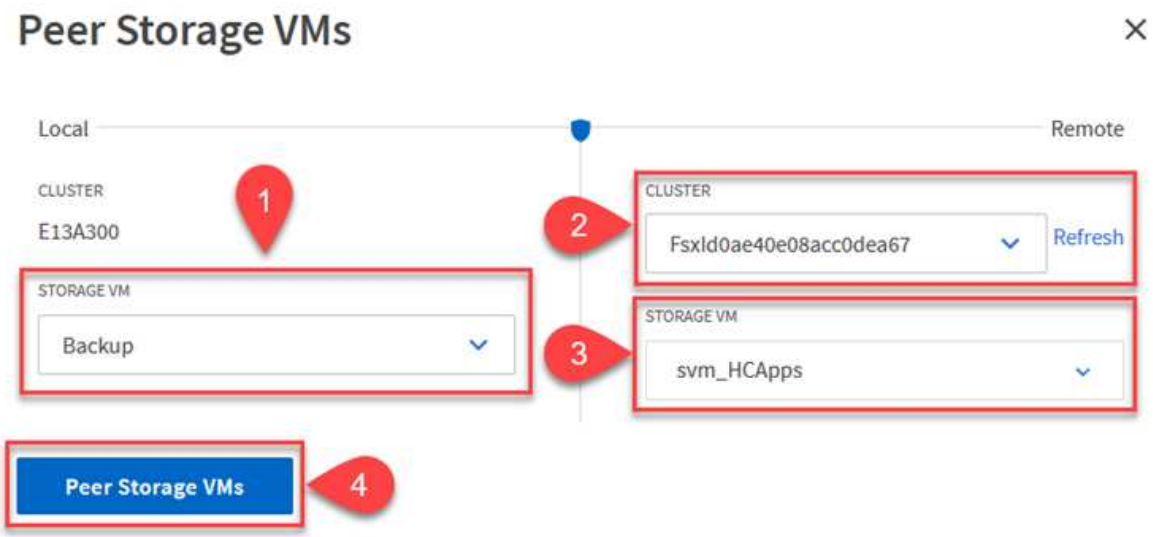
1. Desde el clúster ONTAP de destino, utilice el siguiente comando desde la CLI para crear la relación de pares de SVM:

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

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



4. En el cuadro de diálogo de la máquina virtual de almacenamiento de pares, complete los campos obligatorios:
   - La máquina virtual de almacenamiento de origen
   - El clúster de destino
   - La máquina virtual de almacenamiento de destino



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

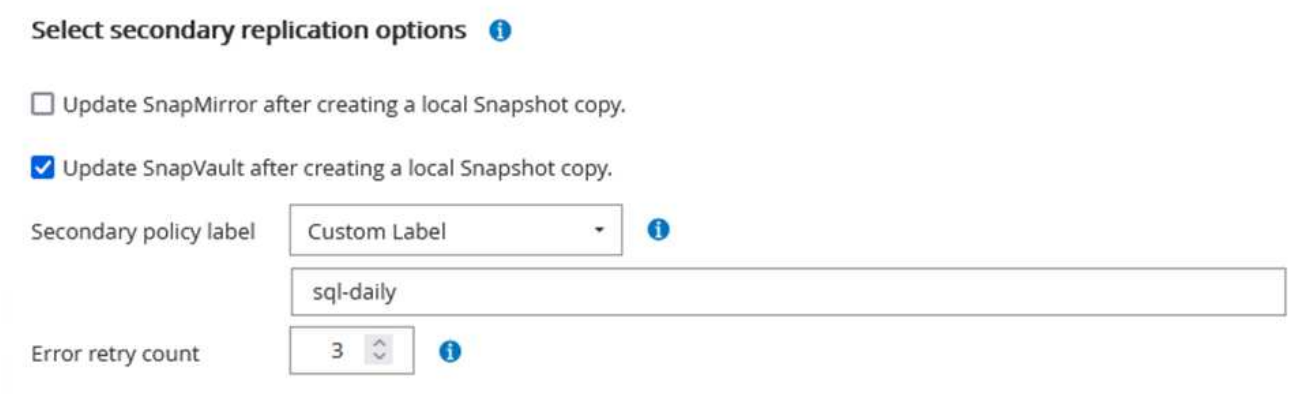
Crear una política de retención de instantáneas

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

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

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

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



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

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

1. Cree la política SnapMirror en el clúster FSx.

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

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

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

El siguiente script proporciona un ejemplo de una regla que podría agregarse a una política:

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

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

Crear volúmenes de destino

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

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

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

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

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

Inicializar las relaciones de SnapMirror

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

Para crear un volumen, ejecute el siguiente comando en el clúster ONTAP de destino:

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

Configurar el SnapCenter Plug-in for VMware vSphere

Una vez instalado, se puede acceder al SnapCenter Plug-in for VMware vSphere desde la interfaz de administración de vCenter Server Appliance. SCV administrará las copias de seguridad de los almacenes de datos NFS montados en los hosts ESXi y que contienen las máquinas virtuales Windows y Linux.

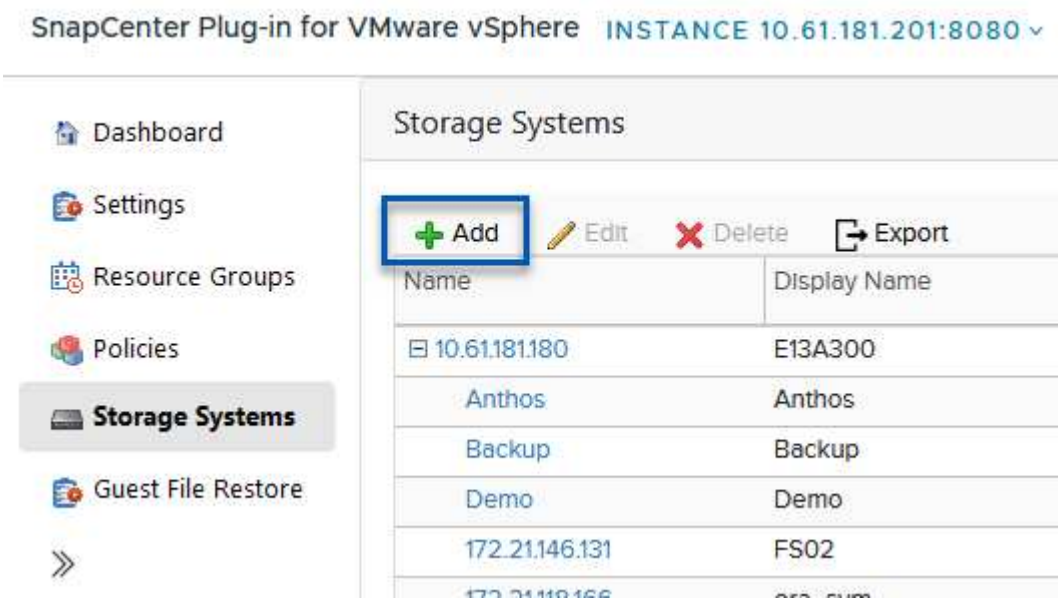
Revisar el "Flujo de trabajo de protección de datos" sección de la documentación de SCV para obtener más información sobre los pasos necesarios para configurar las copias de seguridad.

Para configurar copias de seguridad de sus máquinas virtuales y almacenes de datos, deberá completar los siguientes pasos desde la interfaz del complemento.

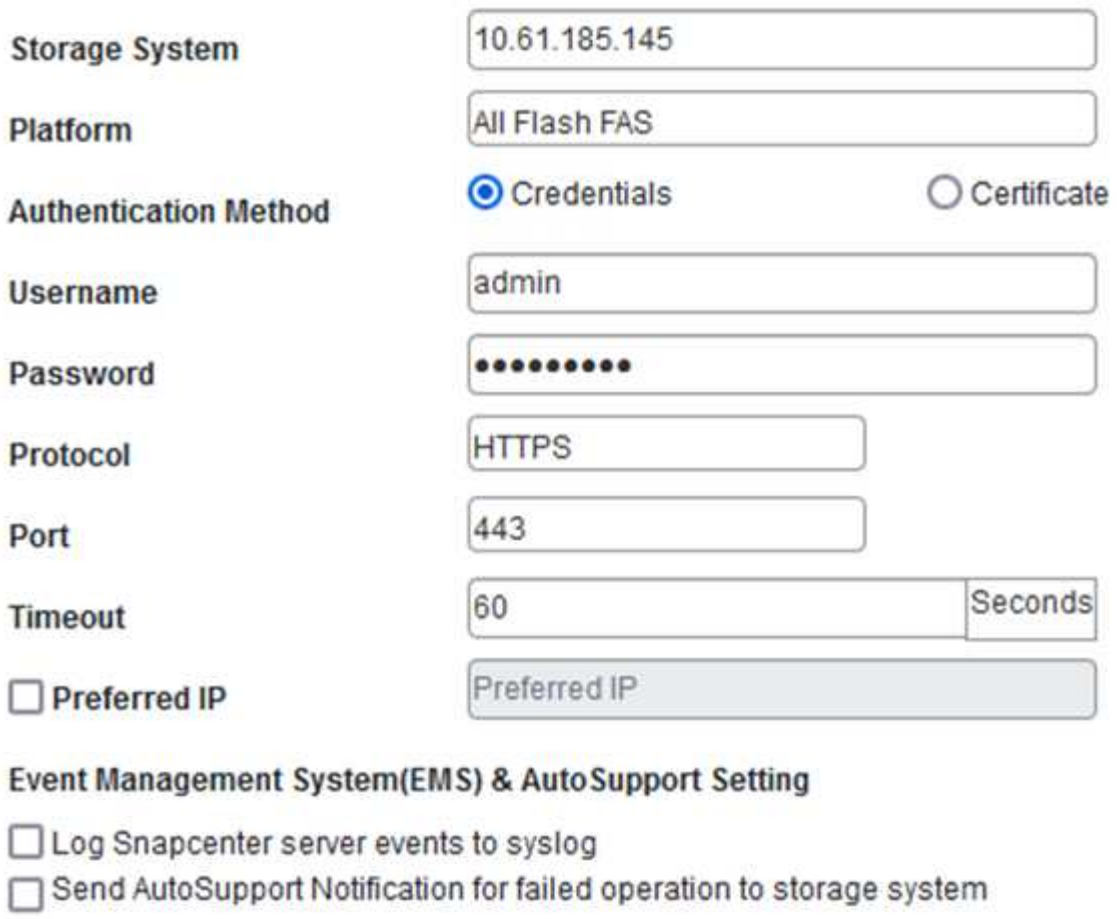
Sistemas de almacenamiento Discovery ONTAP

Descubra los clústeres de almacenamiento de ONTAP que se utilizarán para copias de seguridad primarias y secundarias.

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Sistemas de almacenamiento** en el menú de la izquierda y haga clic en el botón **Agregar**.



2. Complete las credenciales y el tipo de plataforma para el sistema de almacenamiento ONTAP principal y haga clic en **Agregar**.



3. Repita este procedimiento para el sistema de almacenamiento ONTAP secundario.

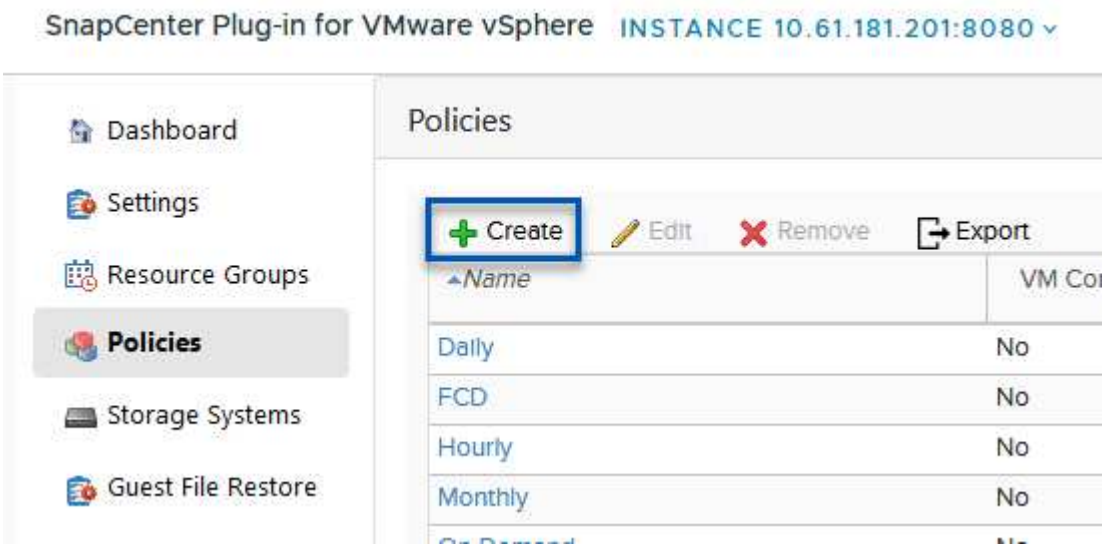
Crear políticas de respaldo de SCV

Las políticas especifican el período de retención, la frecuencia y las opciones de replicación para las copias de seguridad administradas por SCV.

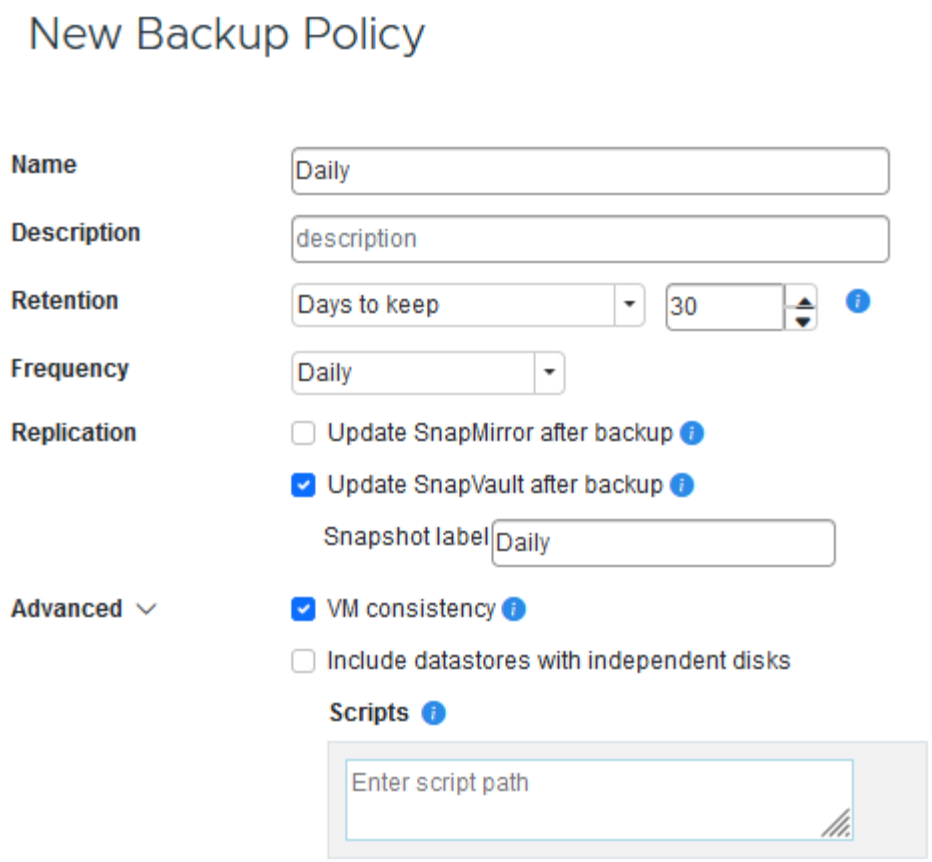
Revisar el "Crear políticas de respaldo para máquinas virtuales y almacenes de datos" sección de la documentación para obtener más información.

Para crear políticas de respaldo complete los siguientes pasos:

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Políticas** en el menú de la izquierda y haga clic en el botón **Crear**.



2. Especifique un nombre para la política, el período de retención, la frecuencia y las opciones de replicación, y la etiqueta de la instantánea.



> Al crear una política en el complemento SnapCenter , verá opciones para SnapMirror y SnapVault. Si elige SnapMirror, el programa de retención especificado en la política será el mismo para las instantáneas principales y secundarias. Si elige SnapVault, el programa de retención de la instantánea secundaria se basará en un programa separado implementado con la relación SnapMirror . Esto es útil cuando desea períodos de retención más largos para las copias de seguridad secundarias.

> Las etiquetas de instantáneas son útiles porque se pueden usar para implementar políticas con un período de retención específico para las copias de SnapVault replicadas en el clúster ONTAP secundario. Cuando se utiliza SCV con BlueXP Backup and Restore, el campo de etiqueta de instantánea debe estar en blanco o coincidir con la etiqueta especificada en la política de respaldo de BlueXP .

3. Repita el procedimiento para cada política requerida. Por ejemplo, políticas separadas para copias de seguridad diarias, semanales y mensuales.

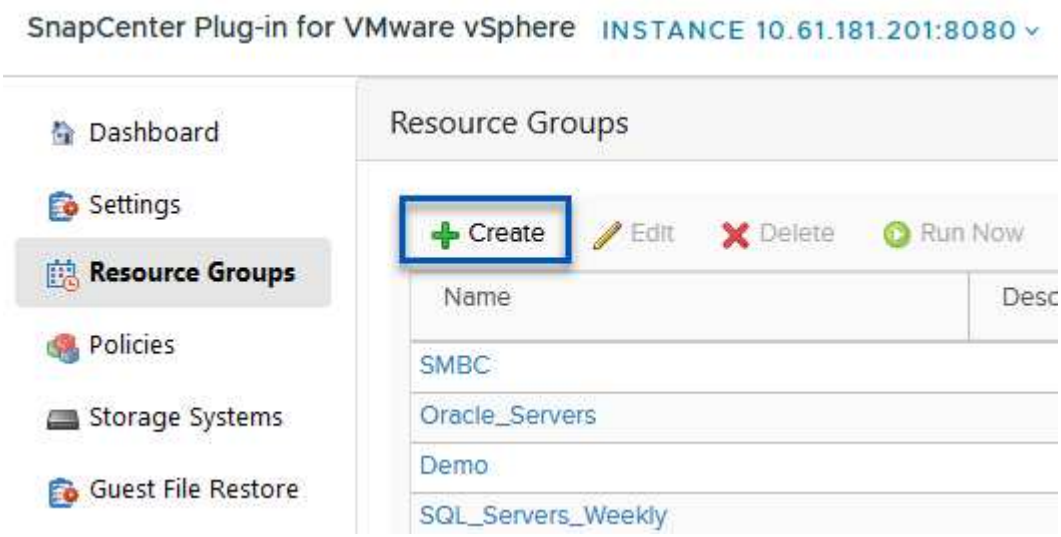
Crear grupos de recursos

Los grupos de recursos contienen los almacenes de datos y las máquinas virtuales que se incluirán en un trabajo de respaldo, junto con la política y el programa de respaldo asociados.

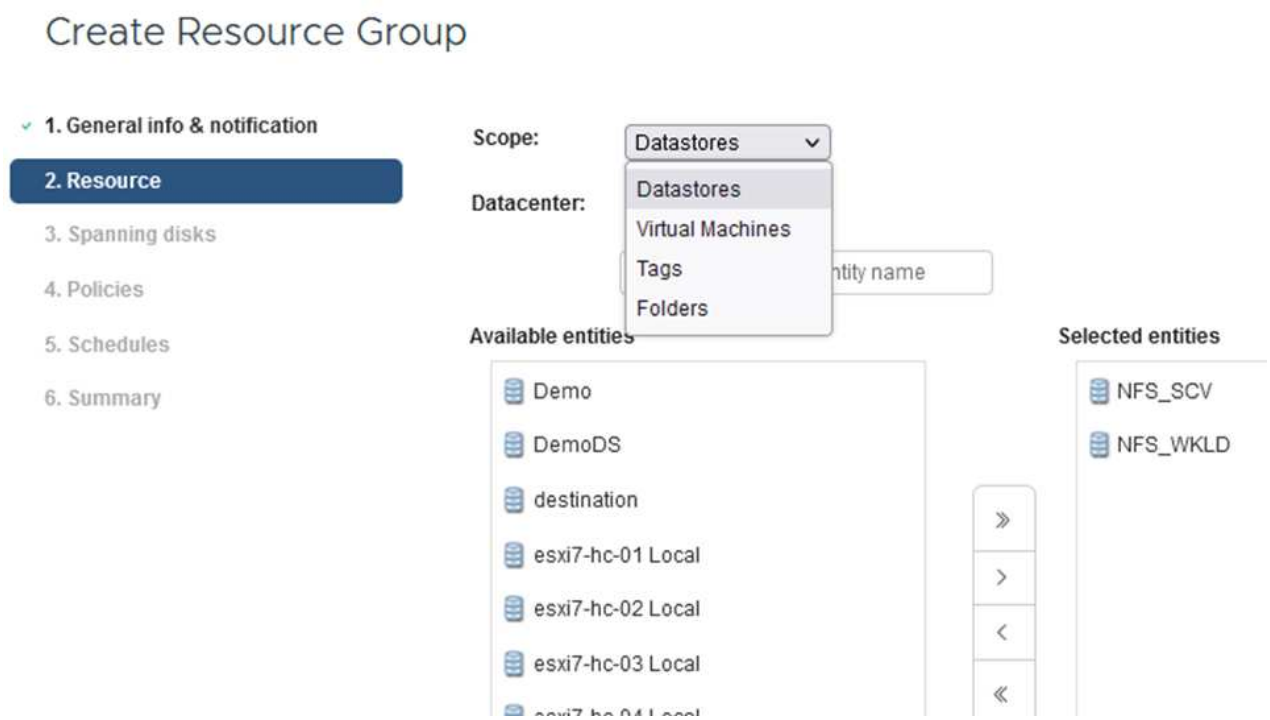
Revisar el "Crear grupos de recursos" sección de la documentación para obtener más información.

Para crear grupos de recursos, complete los siguientes pasos.

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Grupos de recursos** en el menú de la izquierda y haga clic en el botón **Crear**.

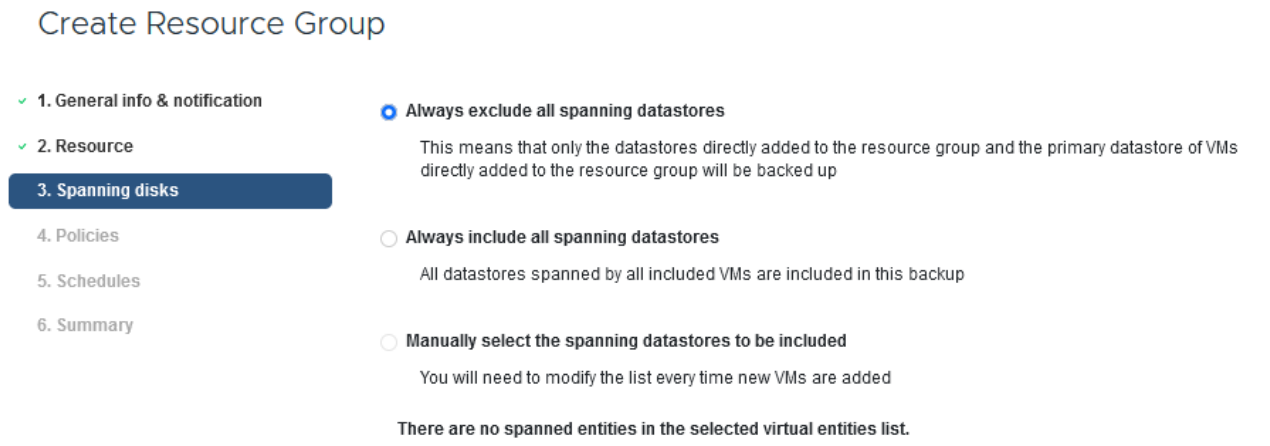


2. En el asistente Crear grupo de recursos, ingrese un nombre y una descripción para el grupo, así como la información necesaria para recibir notificaciones. Haga clic en **Siguiente**
3. En la página siguiente, seleccione los almacenes de datos y las máquinas virtuales que desee incluir en el trabajo de respaldo y luego haga clic en **Siguiente**.



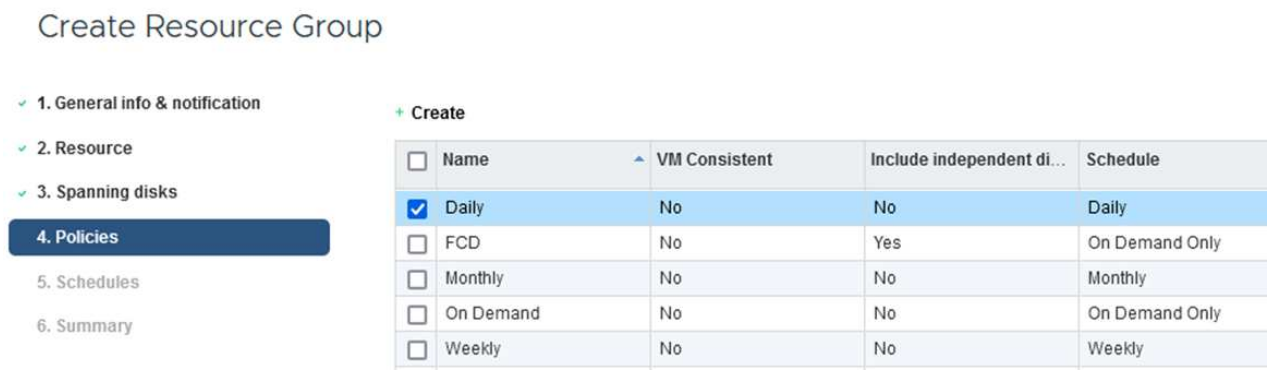
Tiene la opción de seleccionar máquinas virtuales específicas o almacenes de datos completos. Independientemente de lo que elija, se realiza un respaldo de todo el volumen (y del almacén de datos), ya que la copia de seguridad es el resultado de tomar una instantánea del volumen subyacente. En la mayoría de los casos, es más fácil elegir el almacén de datos completo. Sin embargo, si desea limitar la lista de máquinas virtuales disponibles al restaurar, puede elegir solo un subconjunto de máquinas virtuales para realizar una copia de seguridad.

4. Elija opciones para abarcar almacenes de datos para máquinas virtuales con VMDK que residen en múltiples almacenes de datos y luego haga clic en **Siguiente**.



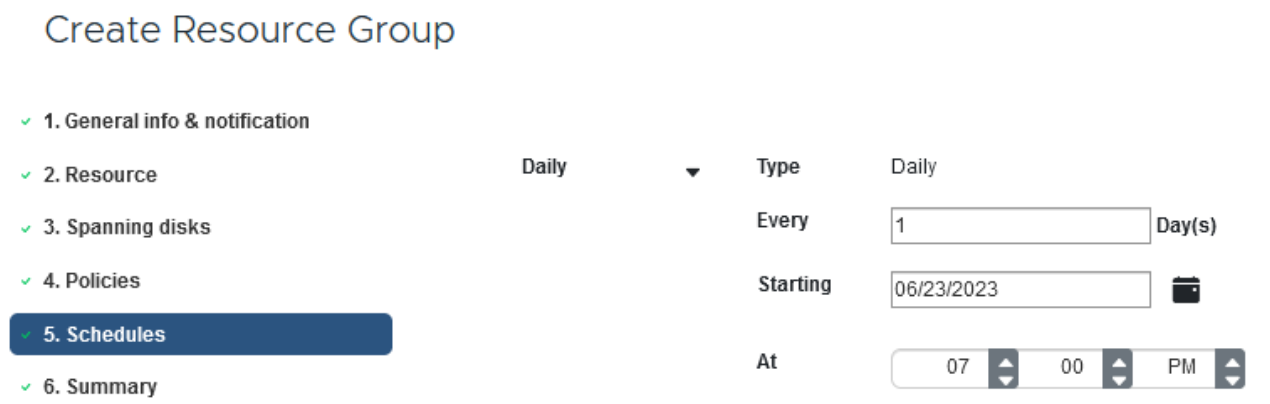
Actualmente, la BlueXP backup and recovery no admite la realización de copias de seguridad de máquinas virtuales con VMDK que abarquen varios almacenes de datos.

5. En la página siguiente, seleccione las políticas que se asociarán con el grupo de recursos y haga clic en **Siguiente**.



> Al realizar copias de seguridad de instantáneas administradas por SCV en un almacenamiento de objetos mediante la BlueXP backup and recovery, cada grupo de recursos solo se puede asociar con una única política.

6. Seleccione una programación que determinará en qué momentos se ejecutarán las copias de seguridad. Haga clic en **Siguiente**.

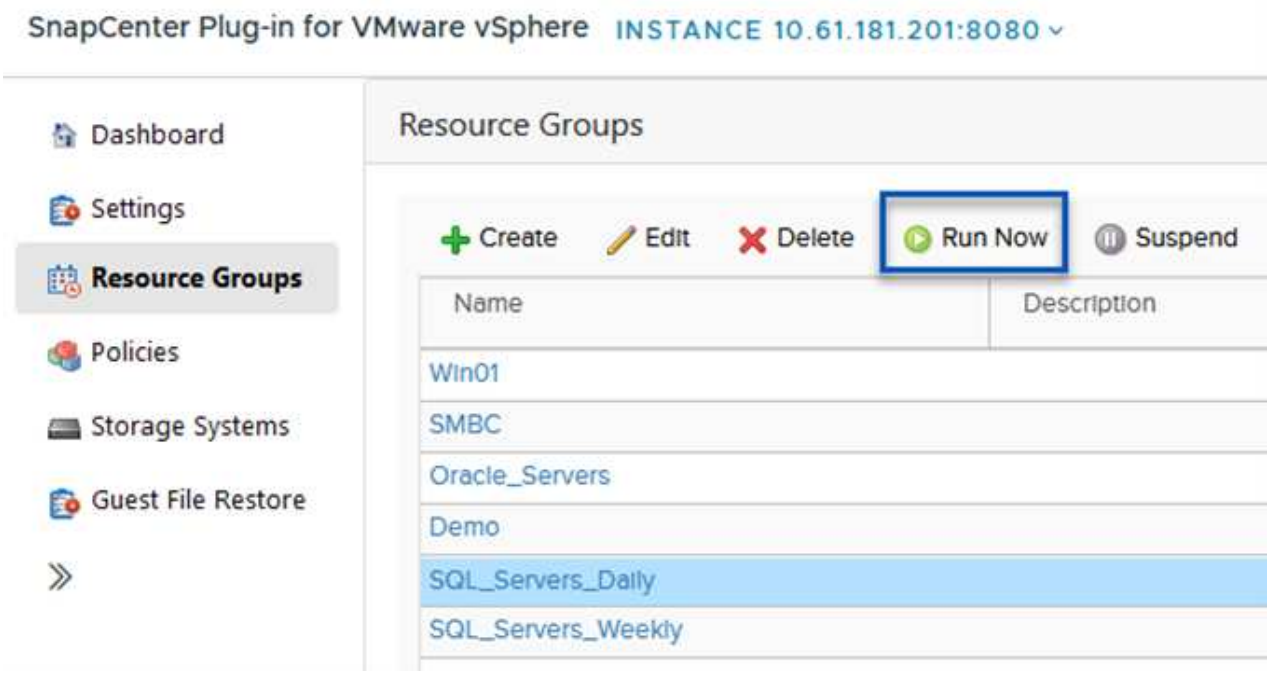


7. Por último, revise la página de resumen y luego haga clic en **Finalizar** para completar la creación del grupo de recursos.

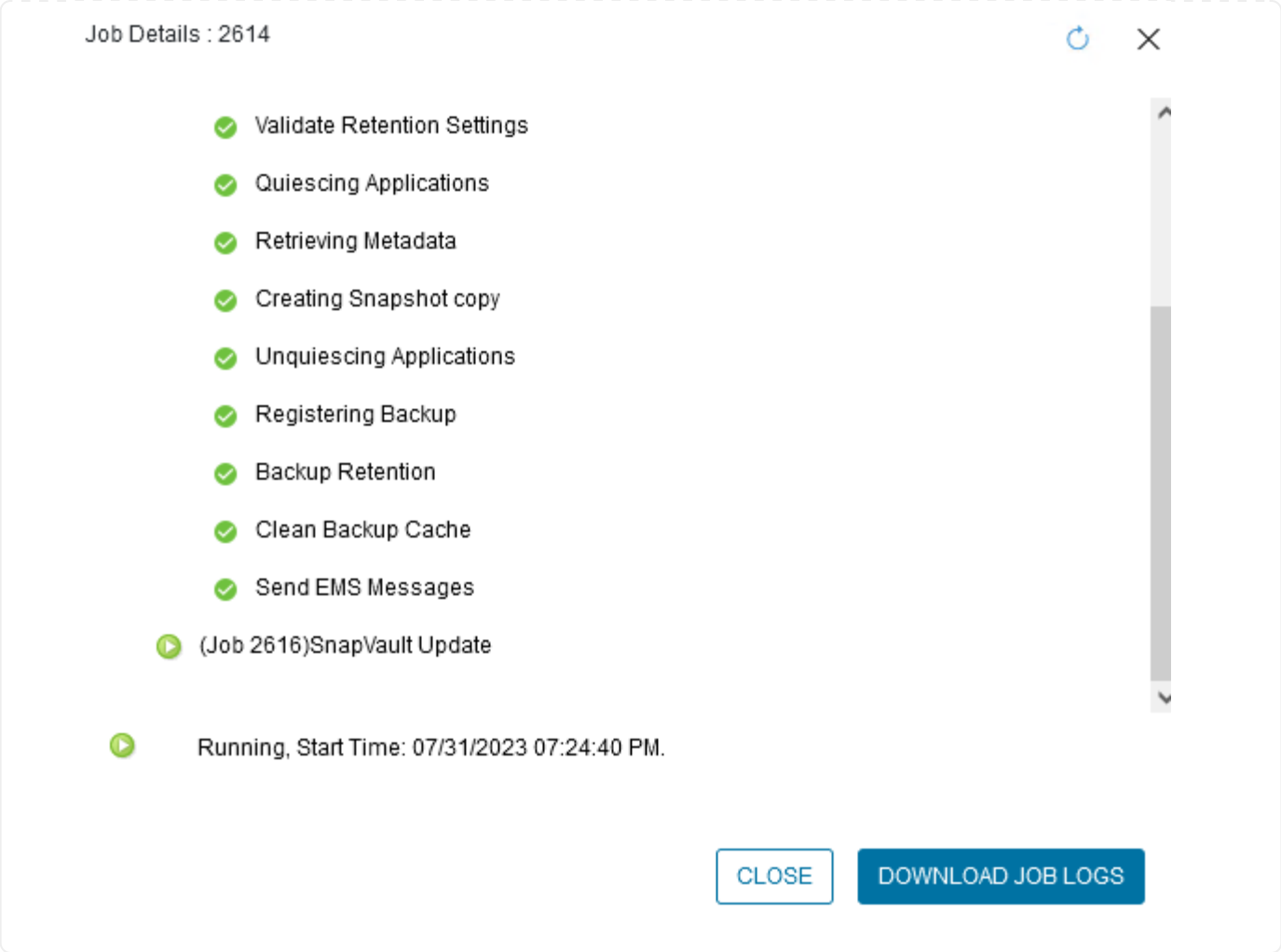
Ejecutar una tarea de respaldo

En este paso final, ejecute un trabajo de respaldo y supervise su progreso. Se debe completar con éxito al menos un trabajo de respaldo en SCV antes de que se puedan descubrir recursos desde BlueXP backup and recovery.

1. En el SnapCenter Plug-in for VMware vSphere, navegue hasta **Grupos de recursos** en el menú de la izquierda.
2. Para iniciar un trabajo de respaldo, seleccione el grupo de recursos deseado y haga clic en el botón **Ejecutar ahora**.



3. Para supervisar el trabajo de respaldo, navegue hasta **Panel de control** en el menú de la izquierda. En **Actividades laborales recientes**, haga clic en el número de identificación del trabajo para monitorear el progreso del trabajo.



Configurar copias de seguridad en el almacenamiento de objetos en la BlueXP backup and recovery

Para que BlueXP administre la infraestructura de datos de manera efectiva, requiere la instalación previa de un Conector. El conector ejecuta las acciones involucradas en el descubrimiento de recursos y la gestión de operaciones de datos.

Para obtener más información sobre el conector BlueXP , consulte "Aprenda sobre los conectores" en la documentación de BlueXP .

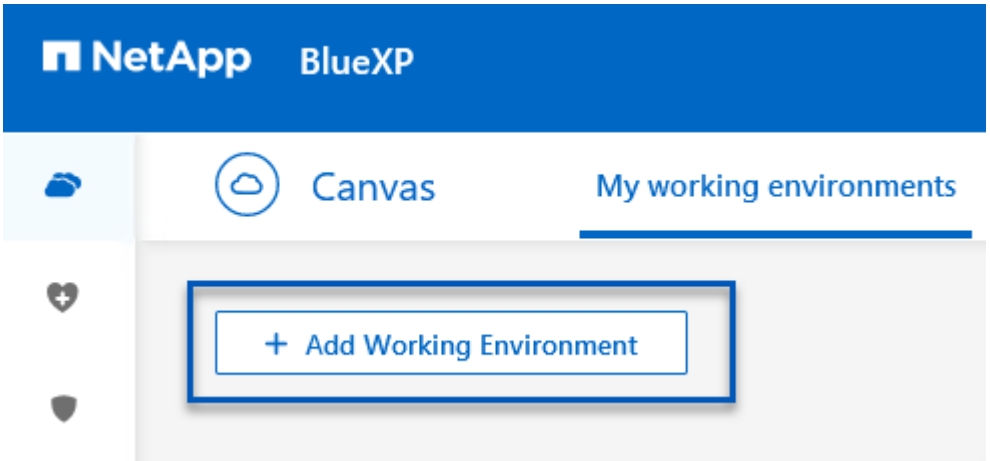
Una vez instalado el conector para el proveedor de nube que se utilice, será posible ver una representación gráfica del almacenamiento de objetos desde el Canvas.

Para configurar la BlueXP backup and recovery para realizar copias de seguridad de los datos administrados por SCV en las instalaciones, complete los siguientes pasos:

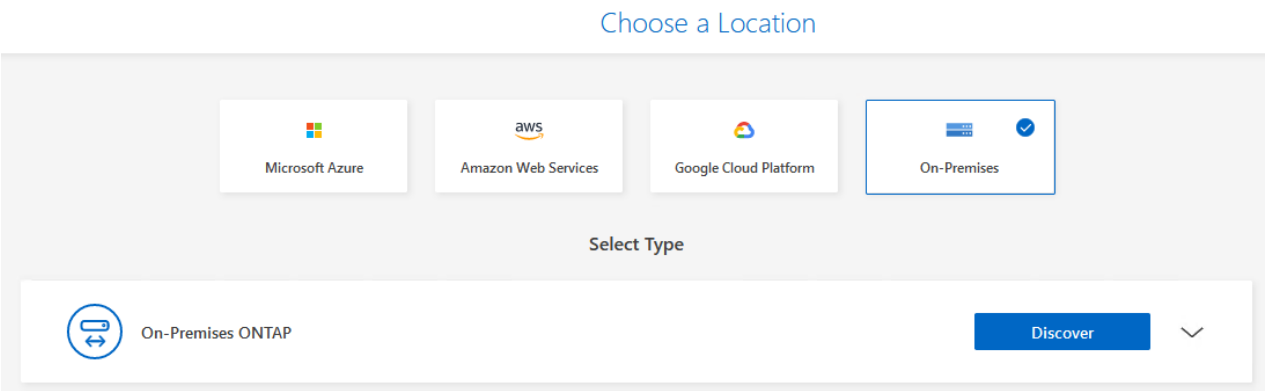
Añadir entornos de trabajo al Canvas

El primer paso es agregar los sistemas de almacenamiento ONTAP locales a BlueXP

1. Desde el lienzo, seleccione **Agregar entorno de trabajo** para comenzar.



2. Seleccione **En las instalaciones** de la selección de ubicaciones y luego haga clic en el botón **Descubrir**.



3. Complete las credenciales para el sistema de almacenamiento ONTAP y haga clic en el botón **Descubrir** para agregar el entorno de trabajo.

ONTAP Cluster IP

10.61.181.180

User Name

admin

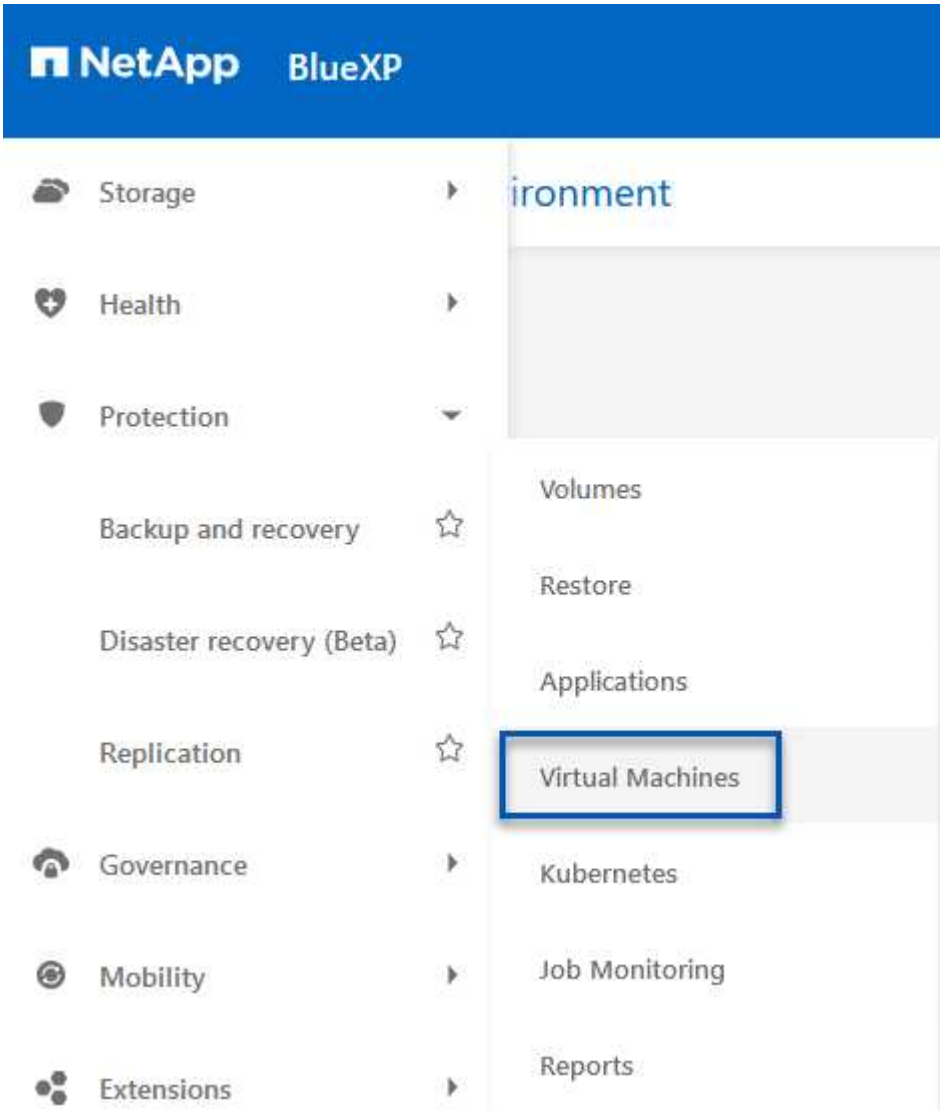
Password

••••••••••

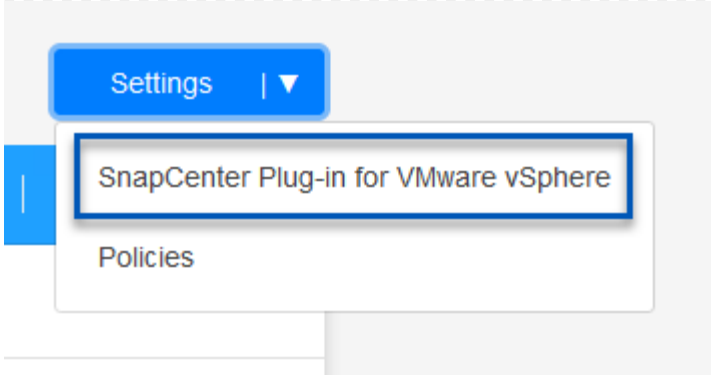
Descubra el dispositivo SCV local y vCenter

Para descubrir el almacén de datos local y los recursos de la máquina virtual, agregue información para el agente de datos SCV y credenciales para el dispositivo de administración de vCenter.

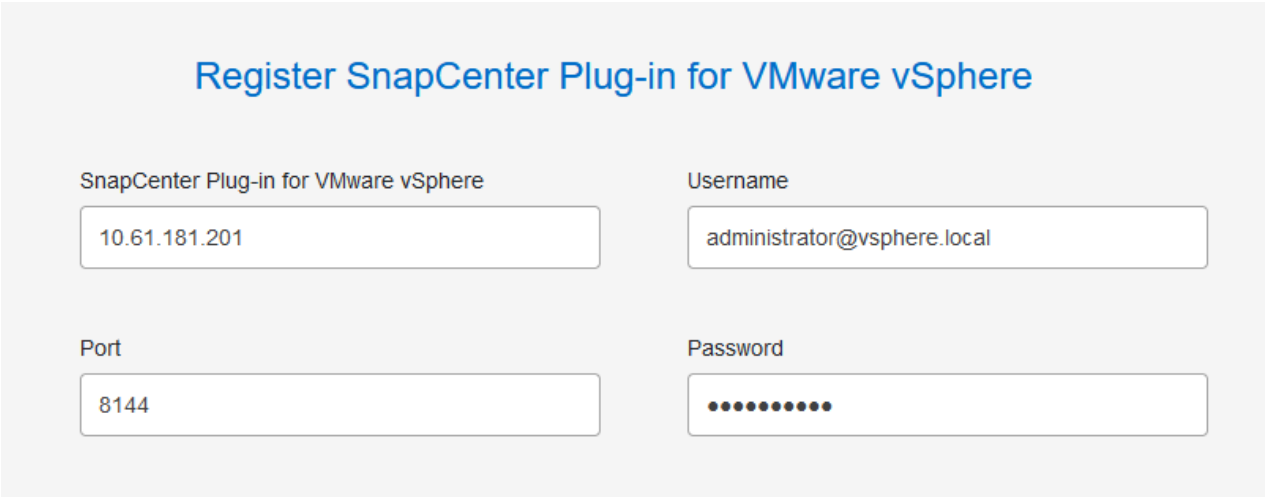
1. Desde el menú izquierdo de BlueXP , seleccione **Protección > Copia de seguridad y recuperación > Máquinas virtuales**



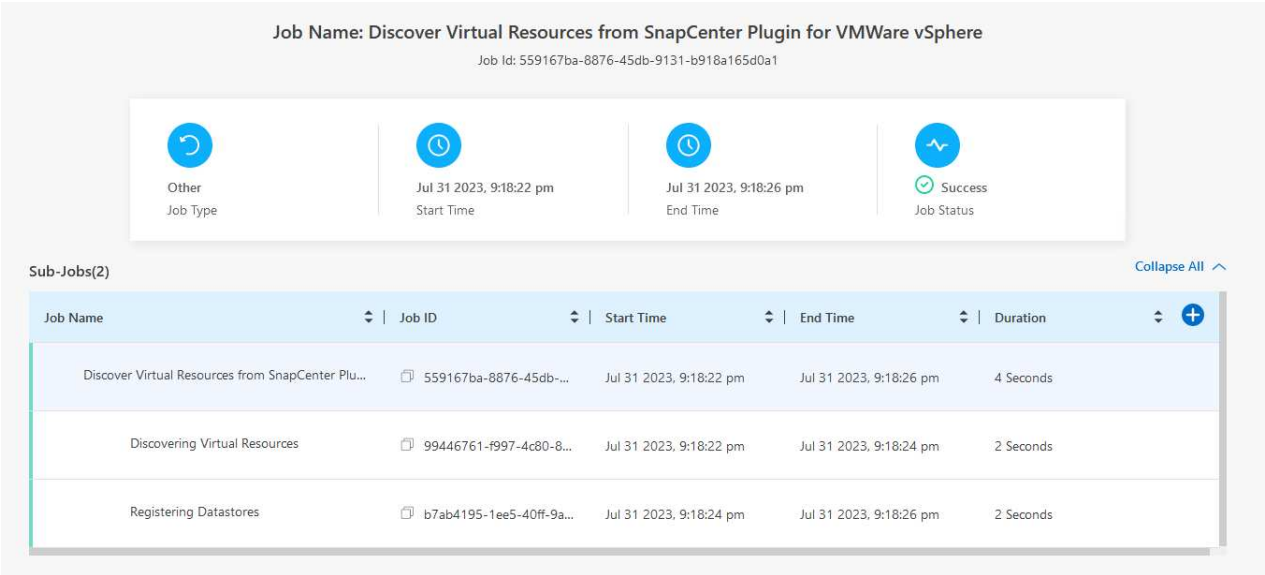
2. Desde la pantalla principal de Máquinas Virtuales acceda al menú desplegable **Configuración** y seleccione * SnapCenter Plug-in for VMware vSphere*.



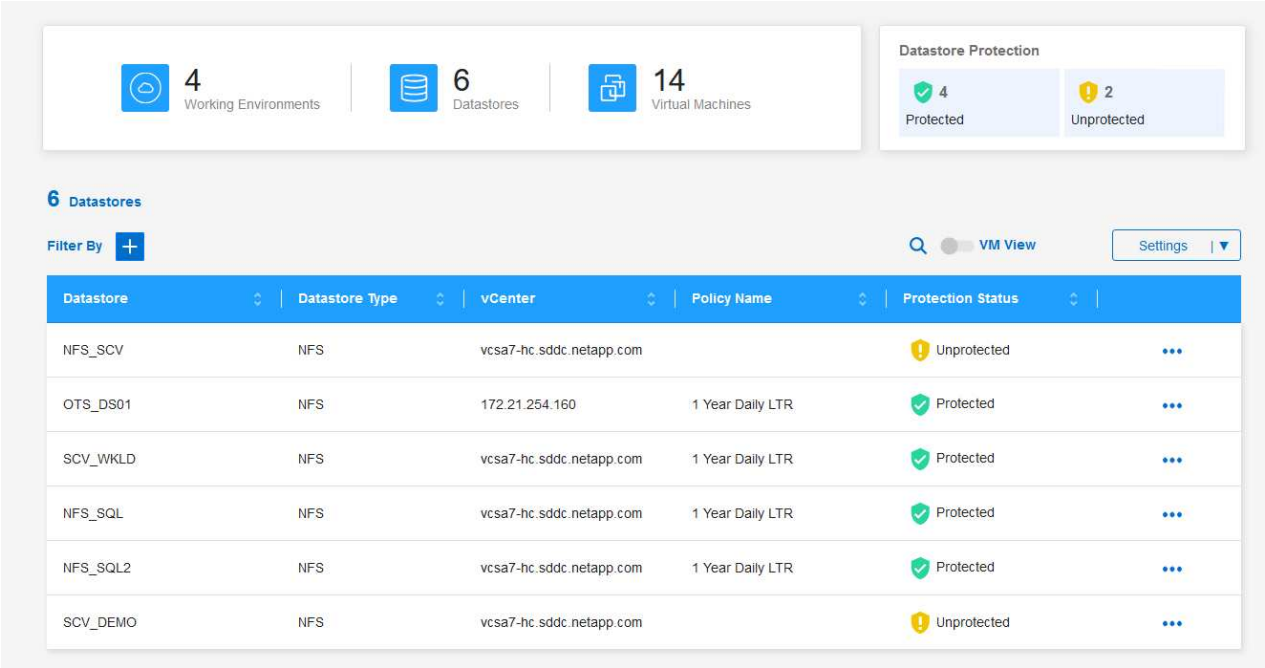
3. Haga clic en el botón **Registrar** y luego ingrese la dirección IP y el número de puerto para el dispositivo de complemento SnapCenter y el nombre de usuario y la contraseña para el dispositivo de administración de vCenter. Haga clic en el botón **Registrarse** para comenzar el proceso de descubrimiento.



4. El progreso de los trabajos se puede monitorear desde la pestaña Monitoreo de trabajos.



5. Una vez que se complete el descubrimiento, podrá ver los almacenes de datos y las máquinas virtuales en todos los dispositivos SCV descubiertos.

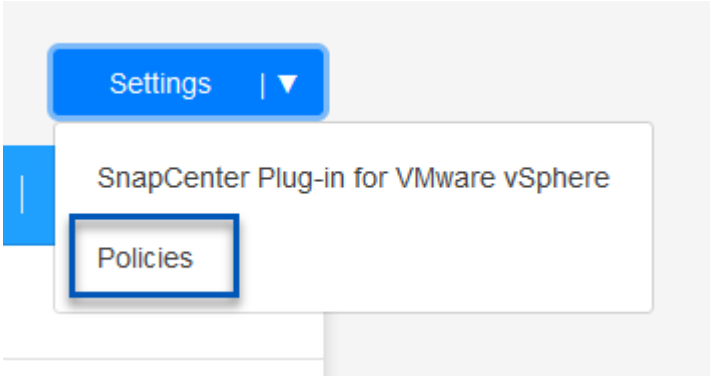

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV
NFS
vcsa7-hc.sddc.netapp.com
Unprotected
OTS_DS01
NFS
172.21.254.160
1 Year Daily LTR
Protected
SCV_WKLD
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL2
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
SCV_DEMO
NFS
vcsa7-hc.sddc.netapp.com
Unprotected

Crear políticas de copia de seguridad de BlueXP

En la BlueXP backup and recovery para máquinas virtuales, cree políticas para especificar el período de retención, la fuente de la copia de seguridad y la política de archivo.

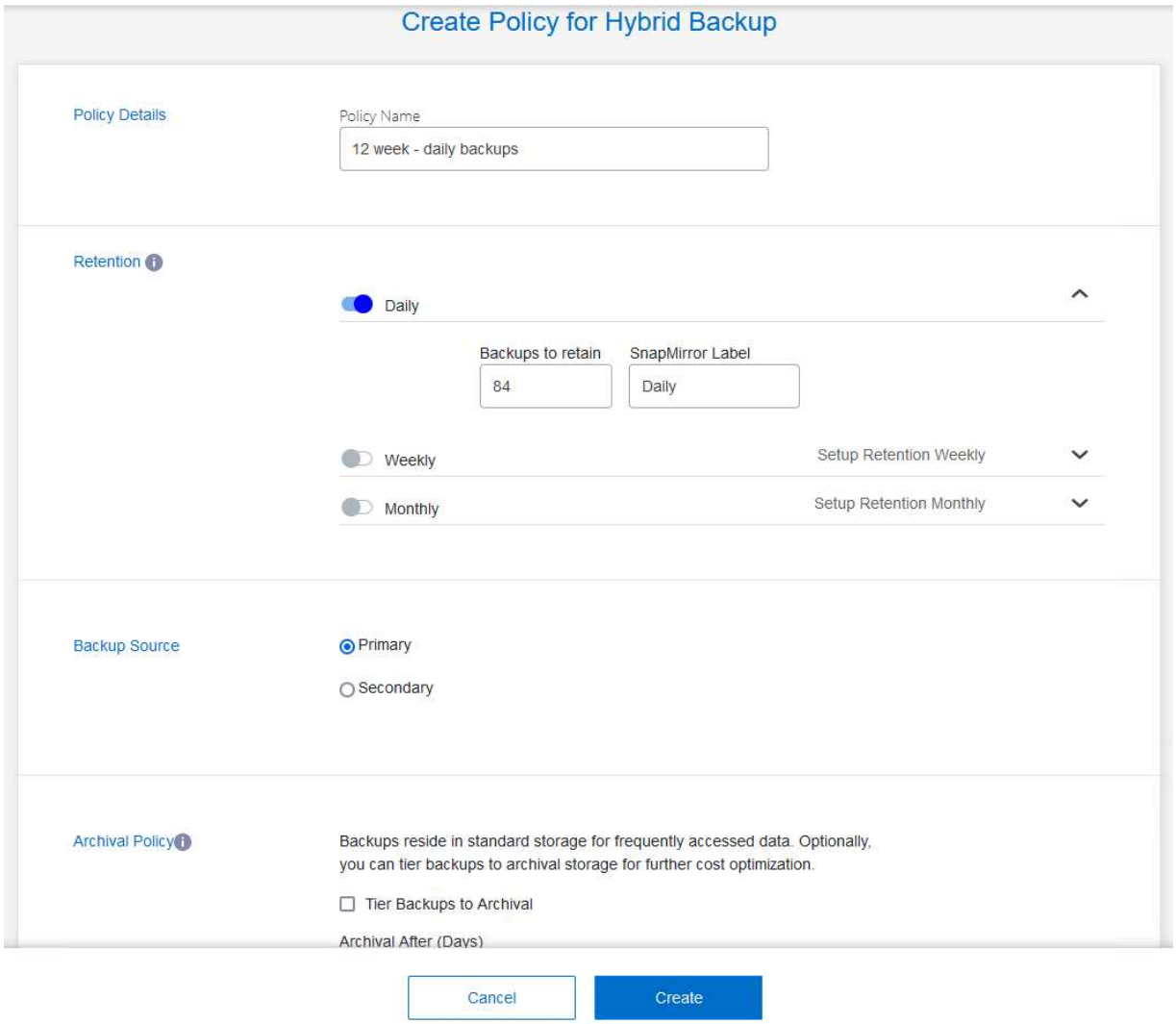
Para obtener más información sobre la creación de políticas, consulte "Crear una política para realizar copias de seguridad de almacenes de datos" .

1. Desde la página principal de BlueXP backup and recovery para máquinas virtuales, acceda al menú desplegable **Configuración** y seleccione **Políticas**.



2. Haga clic en **Crear política** para acceder a la ventana **Crear política para copia de seguridad híbrida**.

   a. Agregar un nombre para la política
   b. Seleccione el período de retención deseado
   c. Seleccione si las copias de seguridad se obtendrán del sistema de almacenamiento ONTAP local primario o secundario
   d. De manera opcional, especifique después de qué período de tiempo las copias de seguridad se almacenarán en niveles en el almacenamiento de archivo para obtener ahorros de costos adicionales.



La etiqueta SnapMirror ingresada aquí se utiliza para identificar a qué copias de seguridad se aplicará la política. El nombre de la etiqueta debe coincidir con el nombre de la etiqueta en la política SCV local correspondiente.

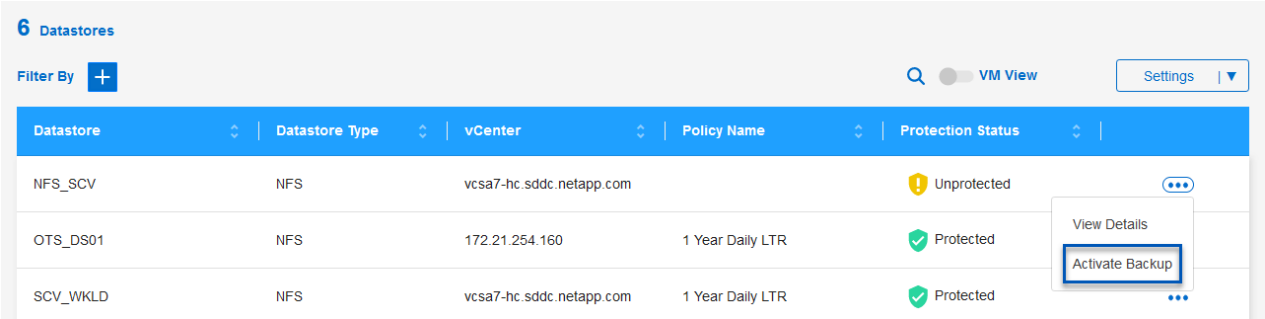
3. Haga clic en **Crear** para completar la creación de la política.

Copia de seguridad de almacenes de datos en Amazon Web Services

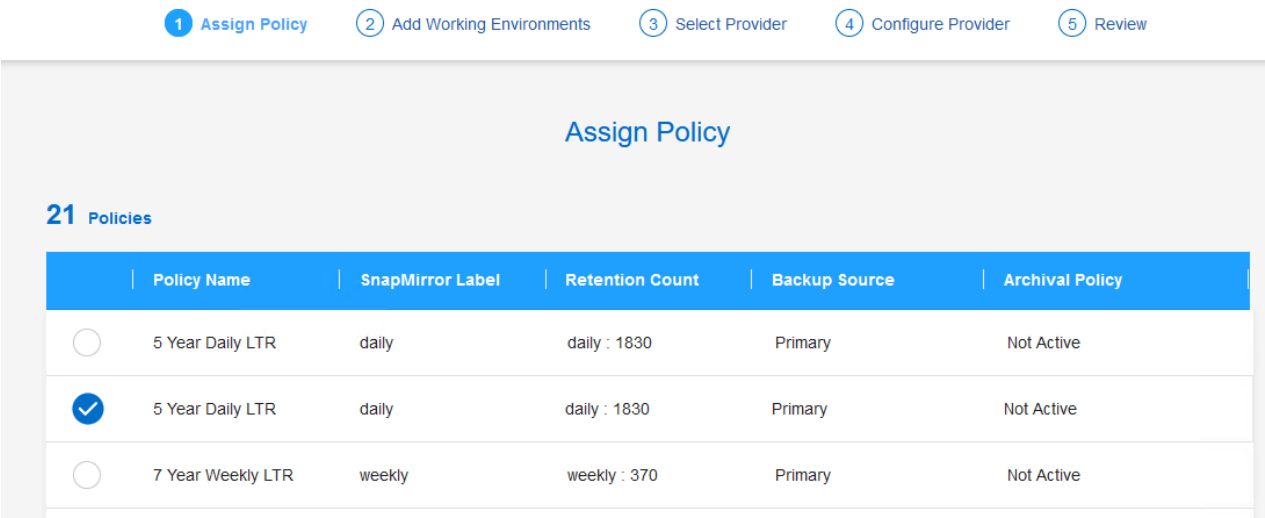
El paso final es activar la protección de datos para los almacenes de datos individuales y las máquinas virtuales. Los siguientes pasos describen cómo activar las copias de seguridad en AWS.

Para obtener más información, consulte "Realizar copias de seguridad de almacenes de datos en Amazon Web Services" .

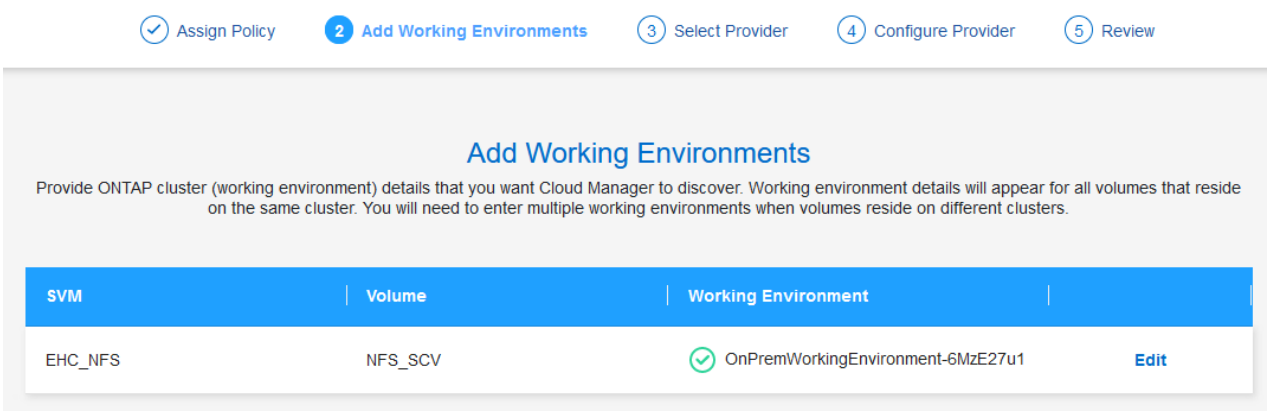
1. Desde la página principal de BlueXP backup and recovery para máquinas virtuales, acceda al menú desplegable de configuración del almacén de datos del cual se realizará la copia de seguridad y seleccione **Activar copia de seguridad**.



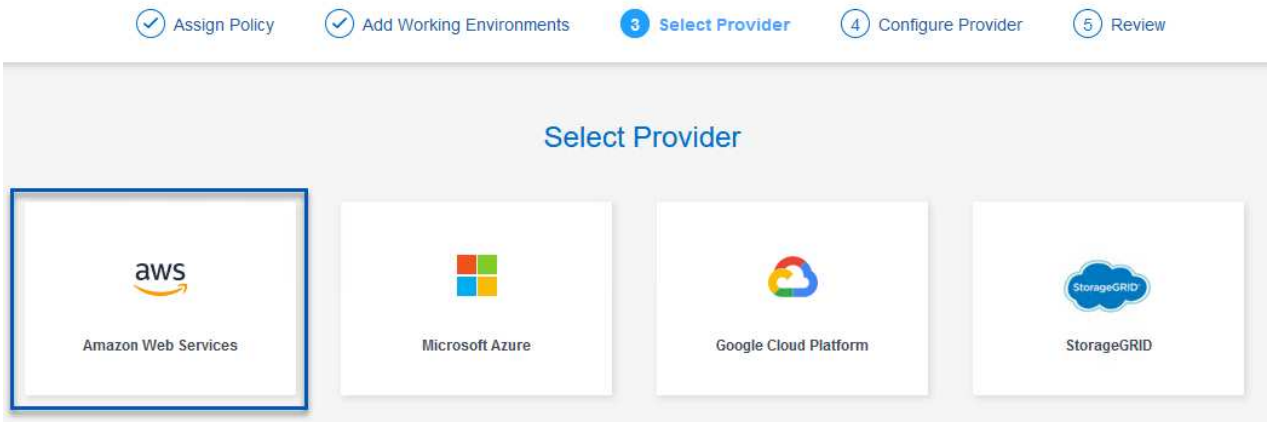
2. Asigne la política que se utilizará para la operación de protección de datos y haga clic en **Siguiente**.



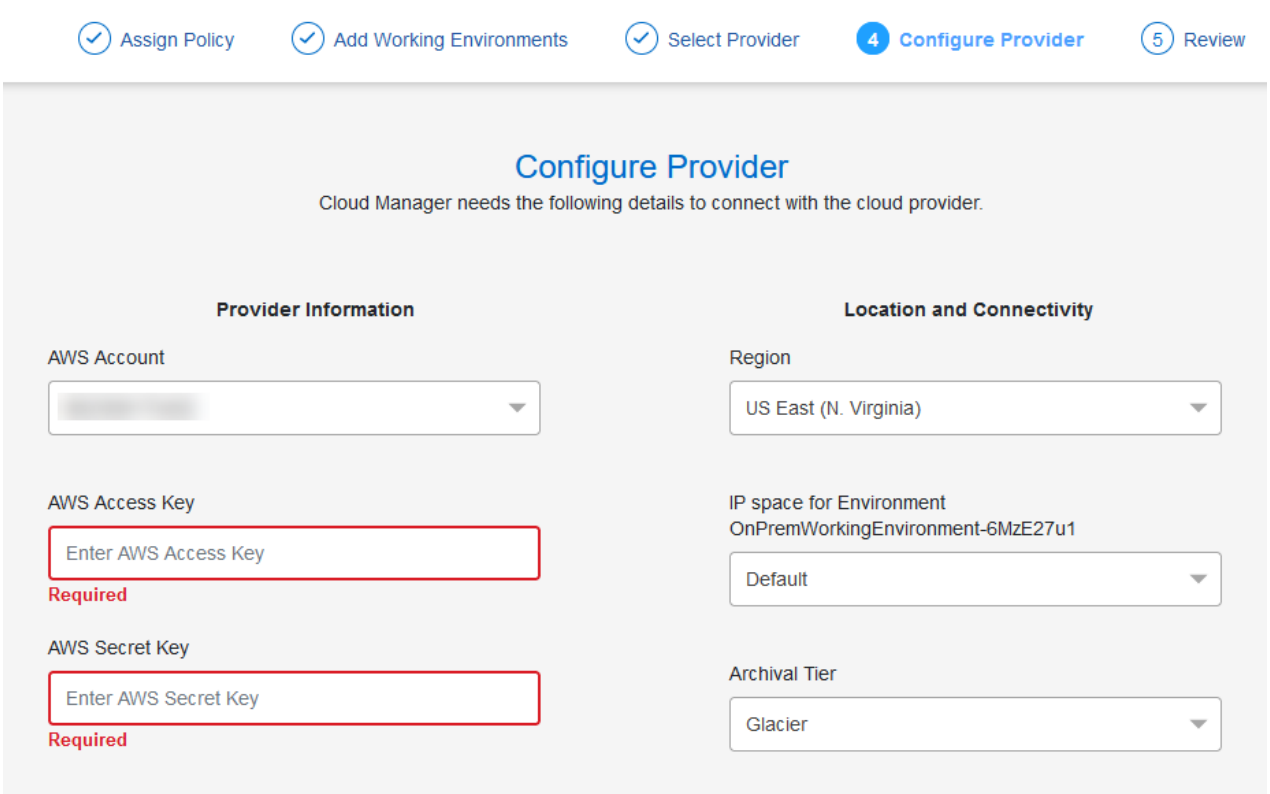
3. En la página **Agregar entornos de trabajo**, el almacén de datos y el entorno de trabajo deben aparecer con una marca de verificación si el entorno de trabajo se ha descubierto previamente. Si el entorno de trabajo no ha sido descubierto previamente puedes agregarlo aquí. Haga clic en **Siguiente** para continuar.



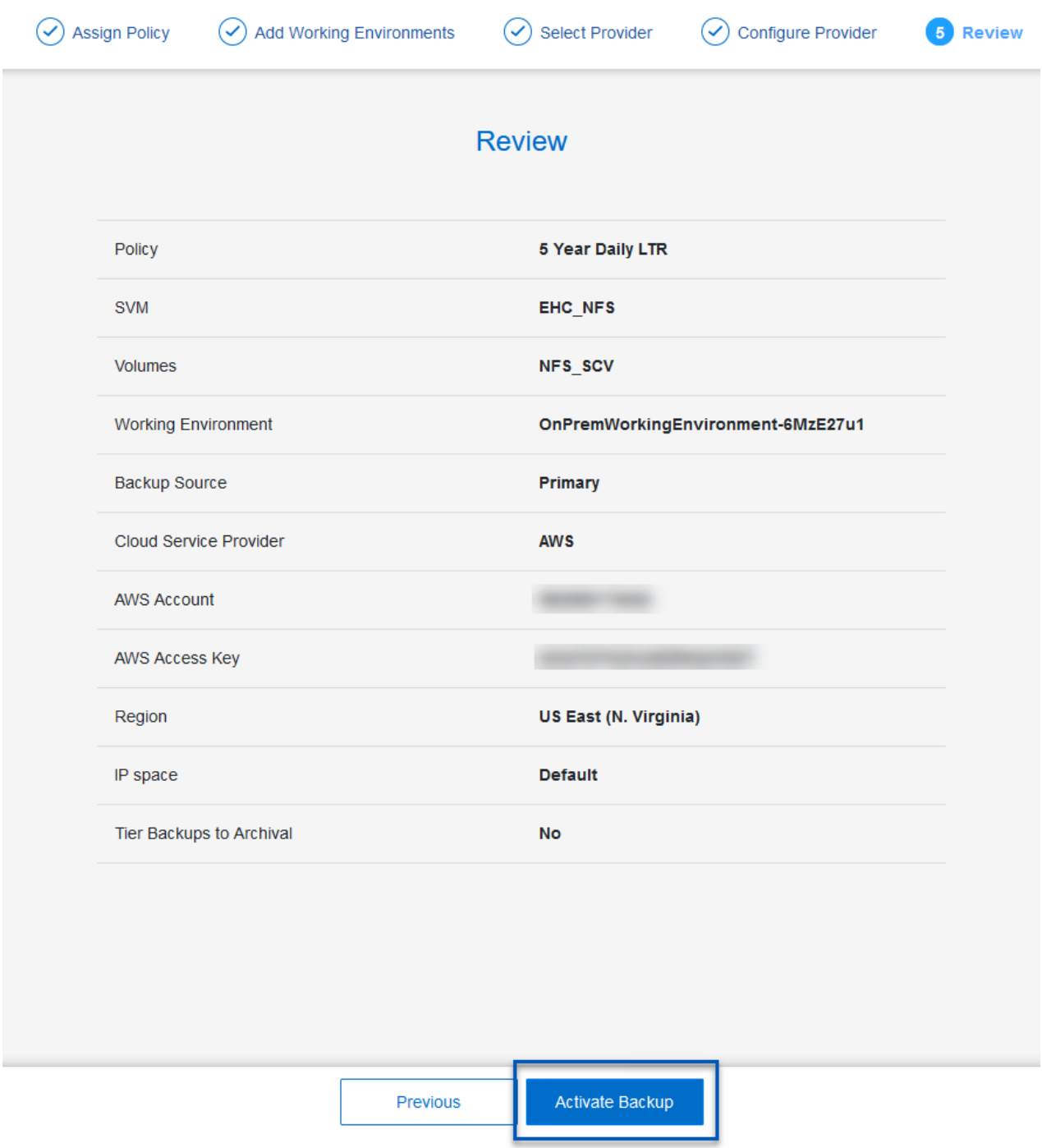
4. En la página **Seleccionar proveedor**, haga clic en AWS y luego haga clic en el botón **Siguiente** para continuar.



5. Complete la información de credenciales específicas del proveedor para AWS, incluida la clave de acceso y la clave secreta de AWS, la región y el nivel de archivo que se utilizará. Además, seleccione el espacio de IP de ONTAP para el sistema de almacenamiento de ONTAP local. Haga clic en **Siguiente**.



6. Por último, revise los detalles del trabajo de respaldo y haga clic en el botón **Activar respaldo** para iniciar la protección de datos del almacén de datos.



En este punto es posible que la transferencia de datos no comience inmediatamente. El BlueXP backup and recovery escanea cada hora en busca de instantáneas pendientes y luego las transfiere al almacenamiento de objetos.

Restaurar máquinas virtuales en caso de pérdida de datos

Garantizar la protección de sus datos es solo un aspecto de la protección integral de datos. Igualmente crucial es la capacidad de restaurar rápidamente los datos desde cualquier ubicación en caso de pérdida de datos o de un ataque de ransomware. Esta capacidad es vital para mantener operaciones comerciales sin problemas y alcanzar los objetivos del punto de recuperación.

NetApp ofrece una estrategia 3-2-1 altamente adaptable, que proporciona un control personalizado sobre los cronogramas de retención en las ubicaciones de almacenamiento primario, secundario y de objetos. Esta estrategia proporciona la flexibilidad de adaptar los enfoques de protección de datos a necesidades específicas.

Esta sección proporciona una descripción general del proceso de restauración de datos tanto del SnapCenter Plug-in for VMware vSphere como de la BlueXP backup and recovery para máquinas virtuales.

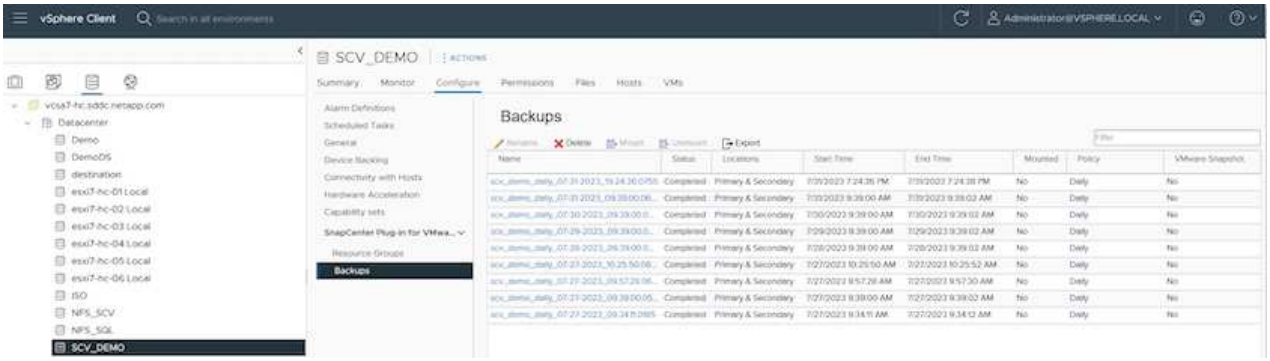
Restauración de máquinas virtuales desde el SnapCenter Plug-in for VMware vSphere

Para esta solución, las máquinas virtuales se restauraron en ubicaciones originales y alternativas. No todos los aspectos de las capacidades de restauración de datos de SCV estarán cubiertos en esta solución. Para obtener información detallada sobre todo lo que SCV tiene para ofrecer, consulte el "Restaurar máquinas virtuales a partir de copias de seguridad" en la documentación del producto.

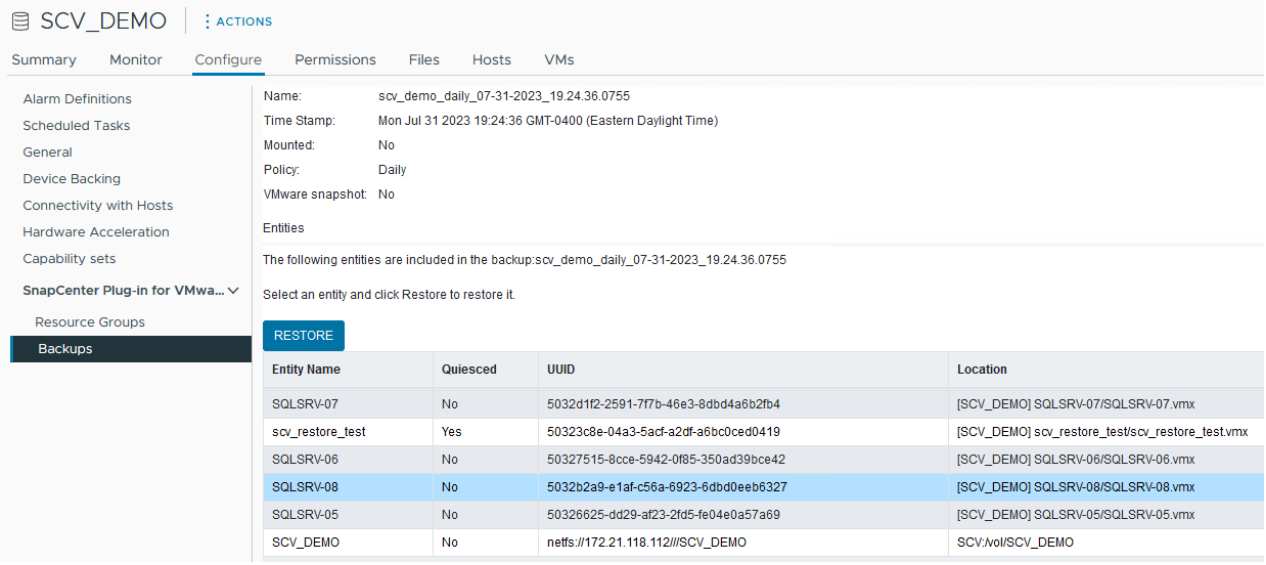
Restaurar máquinas virtuales desde SCV

Complete los siguientes pasos para restaurar una máquina virtual desde el almacenamiento primario o secundario.

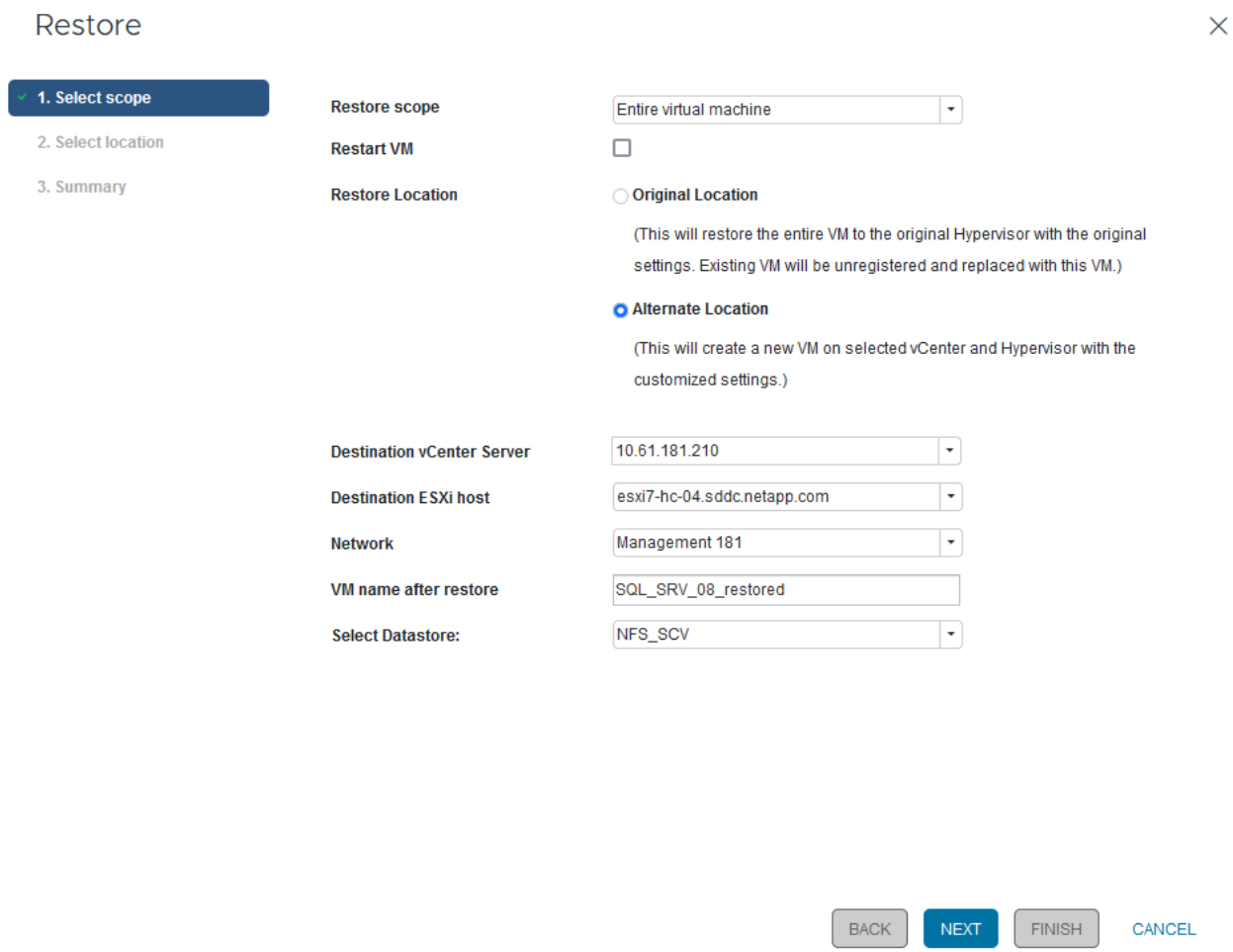
1. Desde el cliente vCenter, navegue a **Inventario > Almacenamiento** y haga clic en el almacén de datos que contiene las máquinas virtuales que desea restaurar.
2. Desde la pestaña **Configurar** haga clic en **Copias de seguridad** para acceder a la lista de copias de seguridad disponibles.



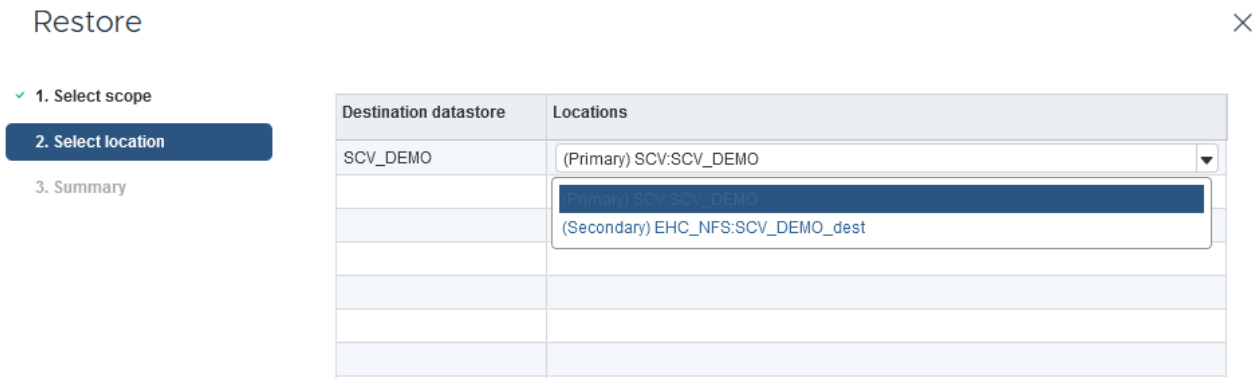
3. Haga clic en una copia de seguridad para acceder a la lista de máquinas virtuales y luego seleccione una máquina virtual para restaurar. Haga clic en **Restaurar**.



4. Desde el asistente de restauración, seleccione restaurar toda la máquina virtual o un VMDK específico. Seleccione instalar en la ubicación original o en una ubicación alternativa, proporcione el nombre de la máquina virtual después de la restauración y el almacén de datos de destino. Haga clic en **Siguiente**.



5. Elija realizar la copia de seguridad desde la ubicación de almacenamiento principal o secundaria.



6. Por último, revise un resumen del trabajo de respaldo y haga clic en Finalizar para comenzar el proceso de restauración.

Restauración de máquinas virtuales desde BlueXP backup and recovery para máquinas virtuales

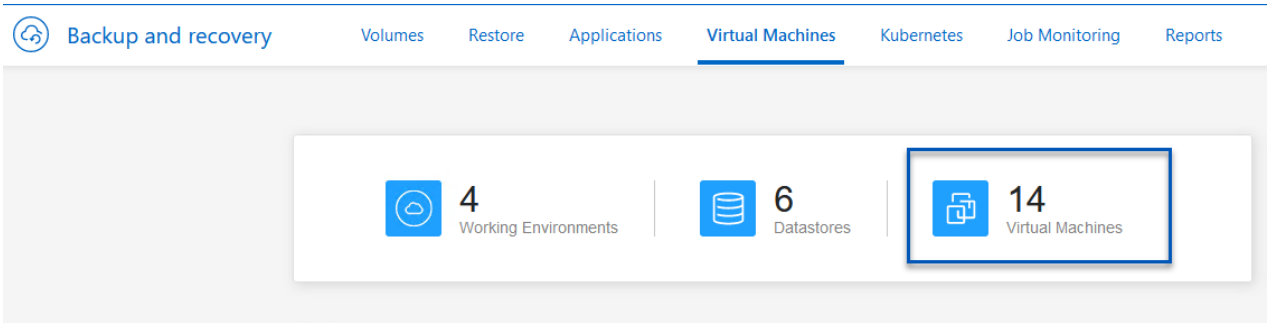
La BlueXP backup and recovery para máquinas virtuales permite restaurar máquinas virtuales a su ubicación original. Se accede a las funciones de restauración a través de la consola web de BlueXP .

Para obtener más información, consulte "Restaurar datos de máquinas virtuales desde la nube" .

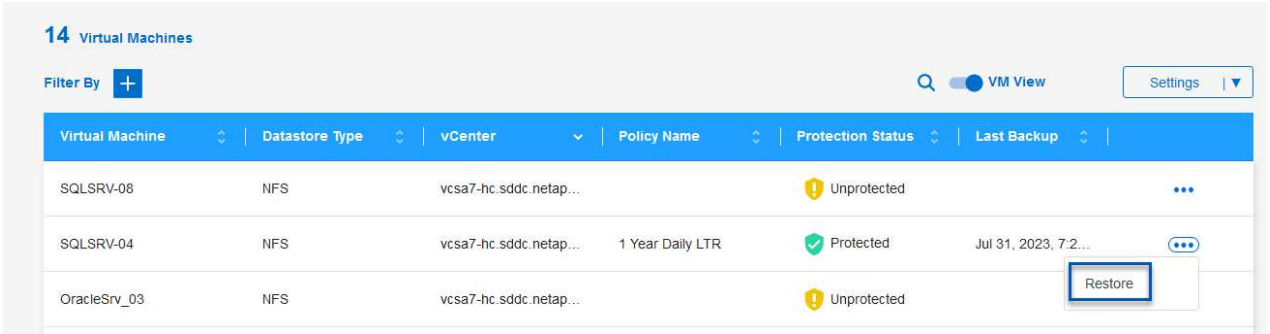
Restaurar máquinas virtuales desde la BlueXP backup and recovery

Para restaurar una máquina virtual desde la BlueXP backup and recovery, complete los siguientes pasos.

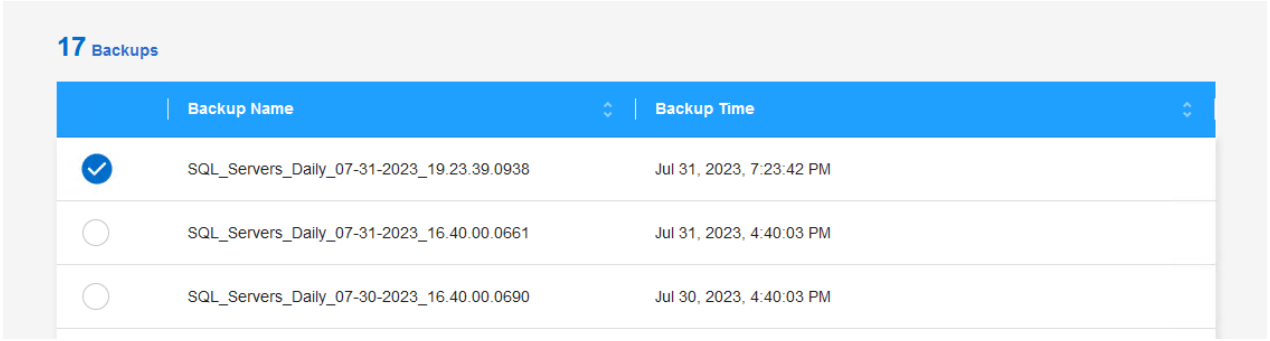
1. Vaya a **Protección > Copia de seguridad y recuperación > Máquinas virtuales** y haga clic en Máquinas virtuales para ver la lista de máquinas virtuales disponibles para restaurar.



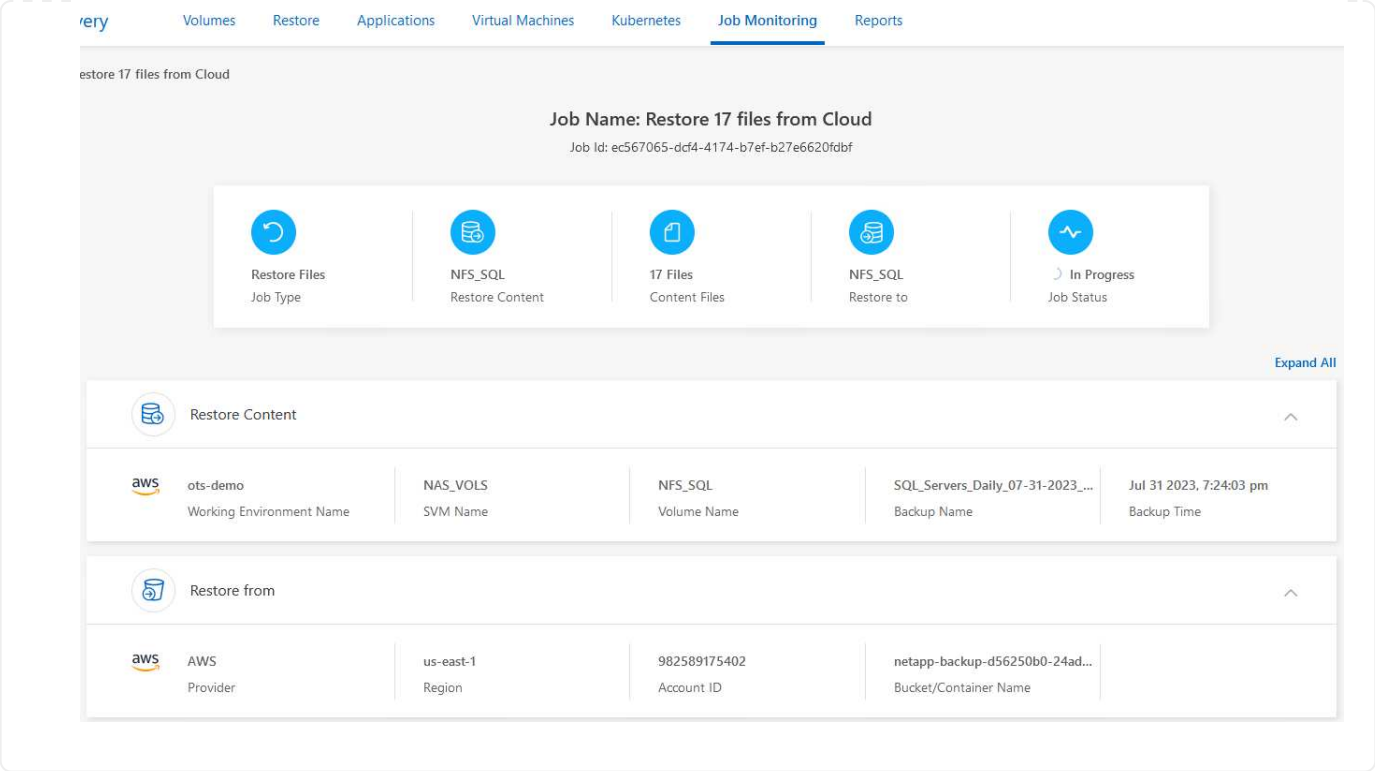
2. Acceda al menú desplegable de configuración de la máquina virtual que se restaurará y seleccione



3. Seleccione la copia de seguridad que desea restaurar y haga clic en **Siguiente**.



4. Revise un resumen del trabajo de respaldo y haga clic en **Restaurar** para iniciar el proceso de restauración.
5. Supervise el progreso del trabajo de restauración desde la pestaña **Supervisión del trabajo**.



Conclusión

La estrategia de respaldo 3-2-1, cuando se implementa con el SnapCenter Plug-in for VMware vSphere y la BlueXP backup and recovery para máquinas virtuales, ofrece una solución sólida, confiable y rentable para la protección de datos. Esta estrategia no solo garantiza la redundancia y la accesibilidad de los datos, sino que también proporciona la flexibilidad de restaurar datos desde cualquier ubicación y desde sistemas de almacenamiento ONTAP locales y almacenamiento de objetos basado en la nube.

El caso de uso presentado en esta documentación se centra en tecnologías de protección de datos probadas que resaltan la integración entre NetApp, VMware y los principales proveedores de nube. El SnapCenter Plug-in for VMware vSphere proporciona una integración perfecta con VMware vSphere, lo que permite una gestión eficiente y centralizada de las operaciones de protección de datos. Esta integración optimiza los procesos de respaldo y recuperación de máquinas virtuales, lo que permite una fácil programación, monitoreo y operaciones de restauración flexibles dentro del ecosistema VMware. La BlueXP backup and recovery para máquinas virtuales ofrece una solución única (1) en 3-2-1 al brindar copias de seguridad seguras y con espacio de aire de los datos de las máquinas virtuales en un almacenamiento de objetos basado en la nube. La interfaz intuitiva y el flujo de trabajo lógico proporcionan una plataforma segura para el archivo a largo plazo de datos críticos.

Información adicional

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

- "Documentación del SnapCenter Plug-in for VMware vSphere"
- "Documentación de BlueXP"

Configurar la recuperación ante desastres para almacenes de datos VMFS mediante la BlueXP disaster recovery

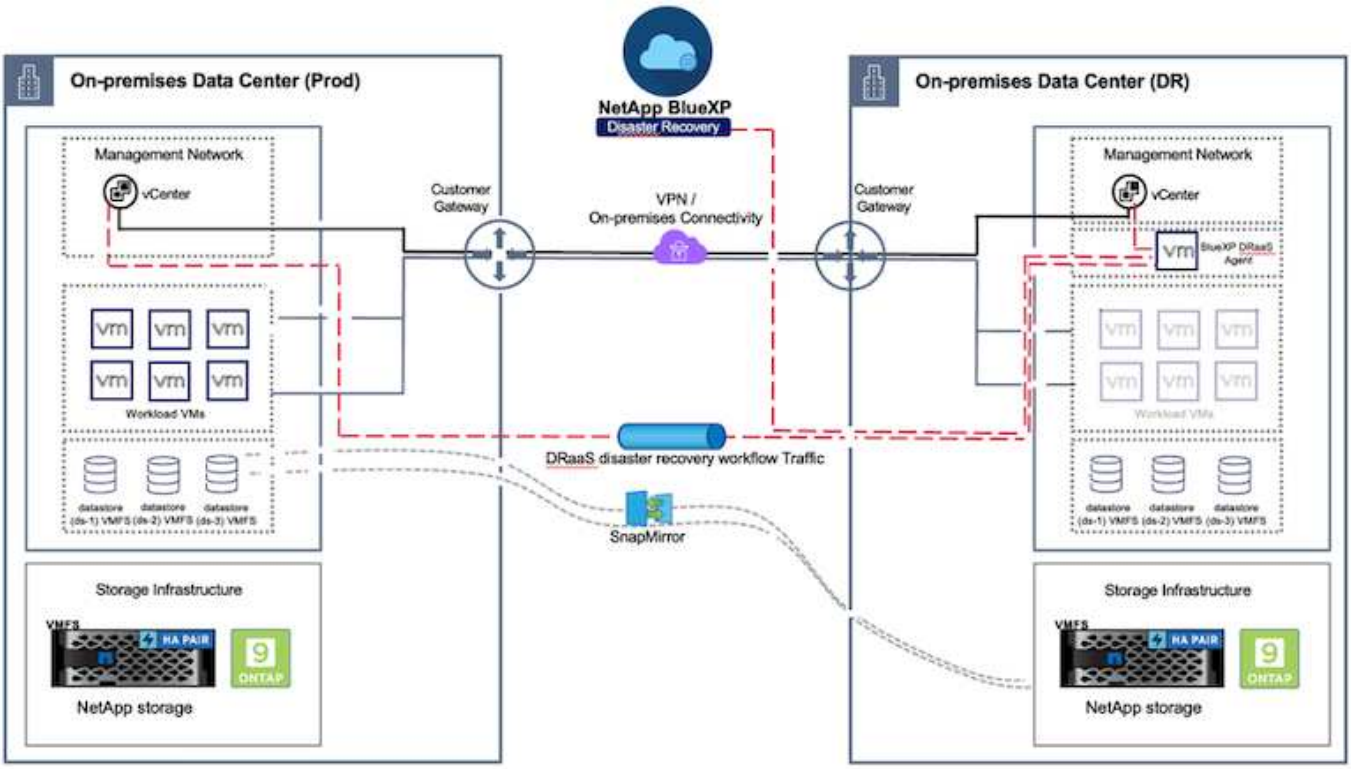
En este caso de uso, describimos el procedimiento para configurar la recuperación ante desastres mediante la BlueXP disaster recovery para máquinas virtuales VMware locales que utilizan almacenes de datos del sistema de archivos de máquina virtual VMware (VMFS). Este procedimiento incluye la configuración de la cuenta y el conector de BlueXP , el establecimiento de la replicación de SnapMirror entre sistemas ONTAP , la integración con VMware vCenter y la automatización de las operaciones de conmutación por error y recuperación.

La recuperación ante desastres mediante la replicación a nivel de bloque desde el sitio de producción al sitio de recuperación ante desastres es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos, como ataques de ransomware. Con la replicación SnapMirror de NetApp , las cargas de trabajo de VMware que se ejecutan en sistemas ONTAP locales que utilizan un almacén de datos VMFS se pueden replicar en otro sistema de almacenamiento ONTAP en un centro de datos de recuperación designado donde reside VMware.

Introducción

Esta sección del documento describe la configuración de BlueXP DRaaS para configurar la recuperación ante desastres de las máquinas virtuales VMware locales en otro sitio designado. Como parte de esta configuración, la cuenta BlueXP , el conector BlueXP y las matrices ONTAP agregadas dentro del espacio de trabajo de BlueXP son necesarias para habilitar la comunicación desde VMware vCenter al almacenamiento ONTAP . Además, este documento detalla cómo configurar la replicación entre sitios y cómo configurar y probar un plan de recuperación. La última sección tiene instrucciones para realizar una conmutación por error completa del sitio y cómo realizar una conmutación por error cuando el sitio principal se recupera y se compra en línea.

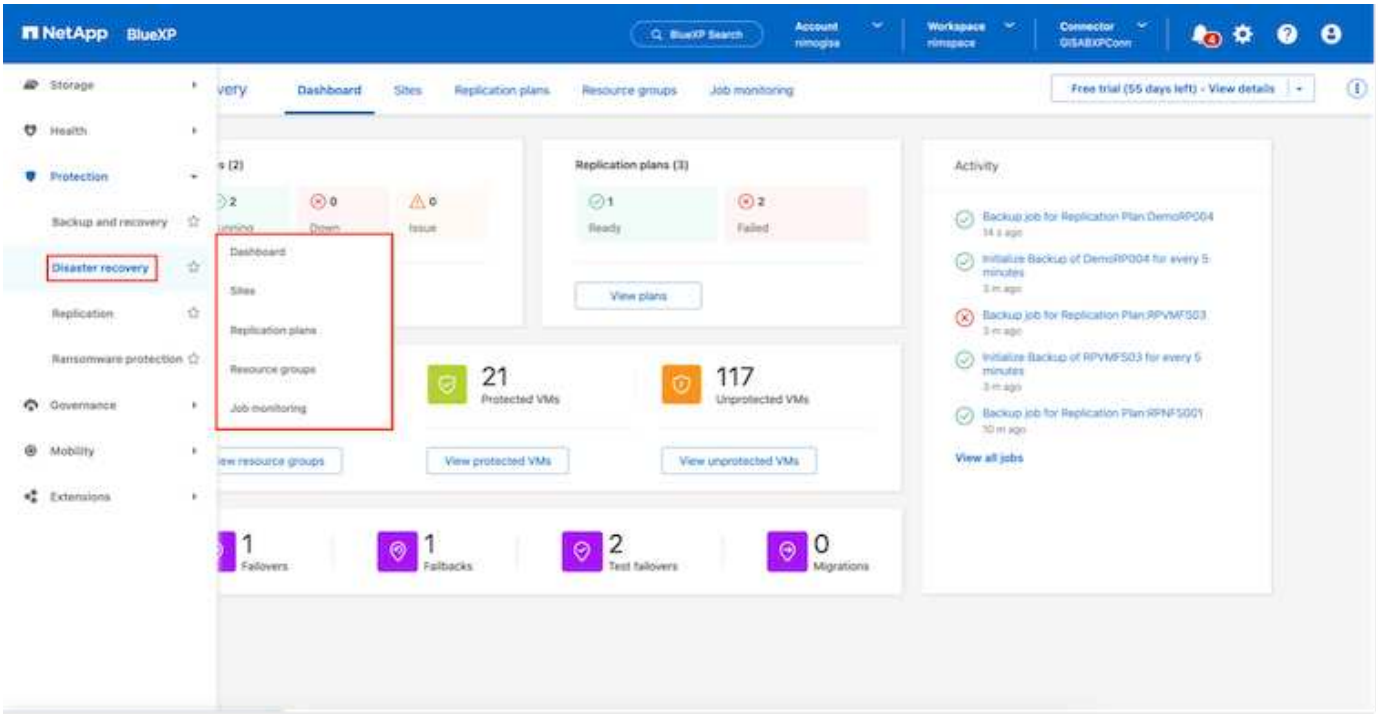
Al utilizar el servicio de BlueXP disaster recovery , que está integrado en la consola BlueXP de NetApp , los clientes pueden descubrir sus VMware vCenters locales junto con el almacenamiento ONTAP , crear agrupaciones de recursos, crear un plan de recuperación ante desastres, asociarlo con grupos de recursos y probar o ejecutar conmutación por error y recuperación. SnapMirror proporciona replicación de bloques a nivel de almacenamiento para mantener los dos sitios actualizados con cambios incrementales, lo que da como resultado un RPO de hasta 5 minutos. También es posible simular procedimientos de DR como un simulacro regular sin afectar la producción ni los almacenes de datos replicados ni incurrir en costos de almacenamiento adicionales. La BlueXP disaster recovery aprovecha la tecnología FlexClone de ONTAP para crear una copia que ahorra espacio del almacén de datos VMFS a partir de la última instantánea replicada en el sitio de recuperación ante desastres. Una vez completada la prueba de DR, los clientes pueden simplemente eliminar el entorno de prueba, nuevamente sin ningún impacto en los recursos de producción replicados reales. Cuando existe una necesidad (planificada o no planificada) de una conmutación por error real, con unos pocos clics, el servicio de BlueXP disaster recovery orquestará todos los pasos necesarios para activar automáticamente las máquinas virtuales protegidas en el sitio de recuperación ante desastres designado. El servicio también revertirá la relación de SnapMirror con el sitio principal y replicará cualquier cambio del secundario al principal para una operación de conmutación por error, cuando sea necesario. Todo esto se puede lograr con una fracción del costo en comparación con otras alternativas conocidas.



Empezando

Para comenzar con la BlueXP disaster recovery, utilice la consola de BlueXP y luego acceda al servicio.

1. Inicie sesión en BlueXP.
2. Desde la navegación izquierda de BlueXP , seleccione Protección > Recuperación ante desastres.
3. Aparece el panel de BlueXP disaster recovery .

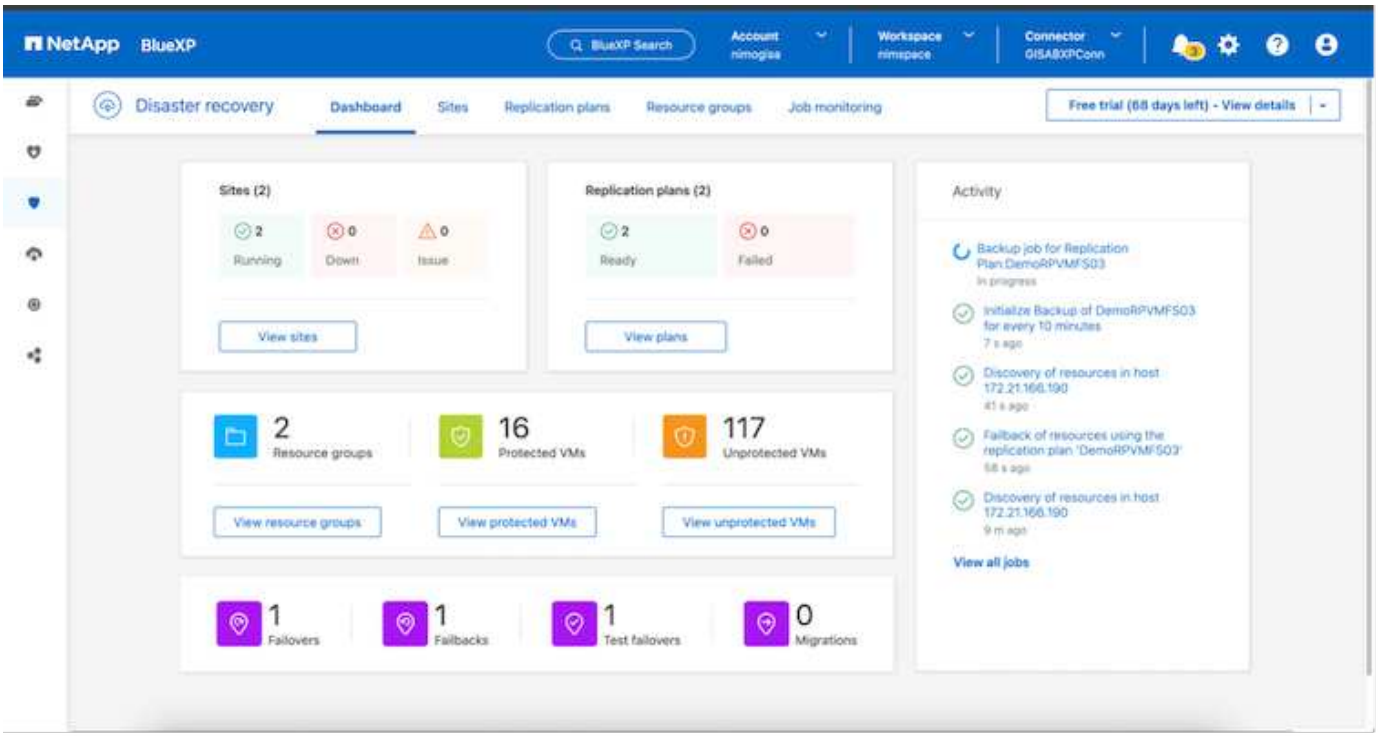


Antes de configurar el plan de recuperación ante desastres, asegúrese de que se cumplan los siguientes requisitos previos:

- El conector BlueXP está configurado en NetApp BlueXP. El conector debe implementarse en AWS VPC.
- La instancia del conector BlueXP tiene conectividad con el vCenter de origen y destino y con los sistemas de almacenamiento.
- Los sistemas de almacenamiento NetApp locales que alojan almacenes de datos VMFS para VMware se agregan en BlueXP.
- La resolución de DNS debe estar vigente cuando se utilizan nombres DNS. De lo contrario, utilice direcciones IP para vCenter.
- La replicación de SnapMirror está configurada para los volúmenes de almacén de datos basados en VMFS designados.

Una vez establecida la conectividad entre los sitios de origen y destino, continúe con los pasos de configuración, que deberían tomar entre 3 y 5 minutos.

NetApp recomienda implementar el conector BlueXP en el sitio de recuperación ante desastres o en un tercer sitio, para que el conector BlueXP pueda comunicarse a través de la red con los recursos de origen y destino durante interrupciones reales o desastres naturales.

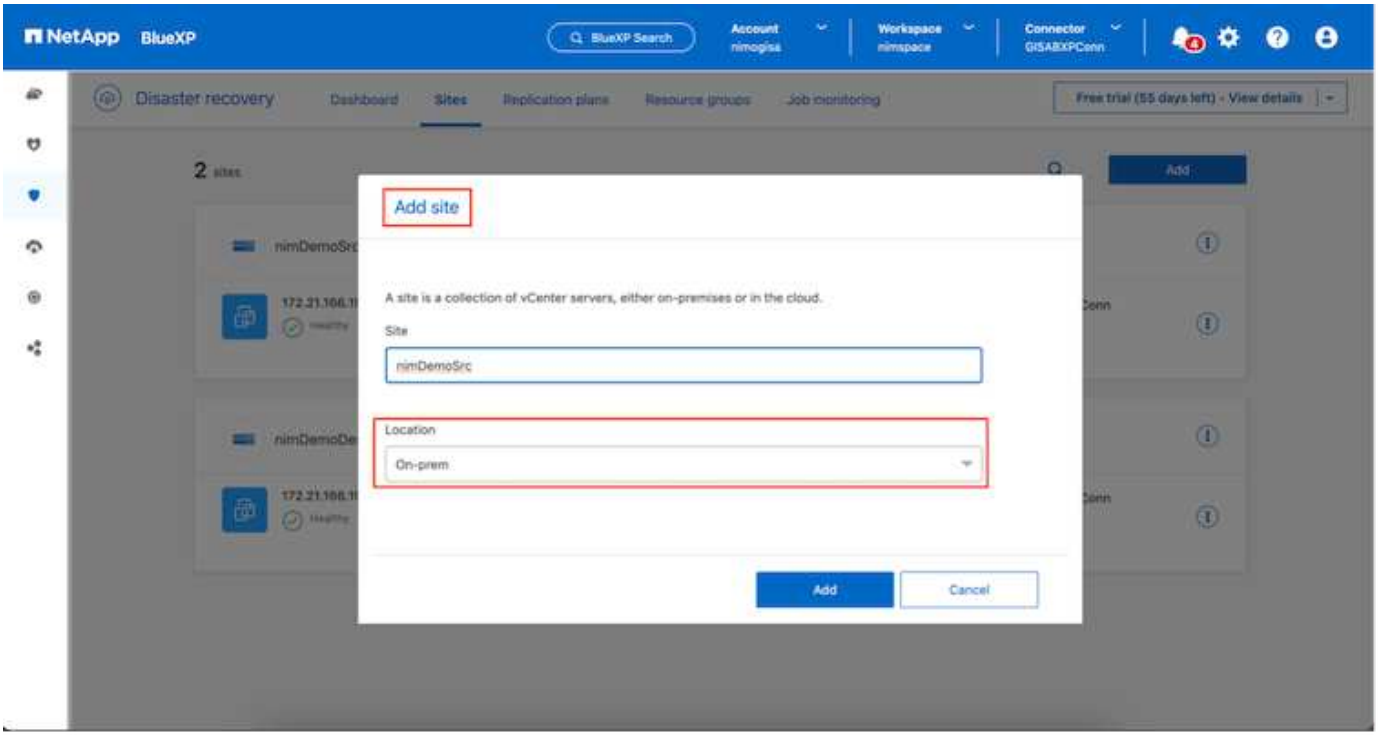


La compatibilidad con almacenes de datos VMFS locales a locales se encuentra en versión preliminar tecnológica al momento de escribir este documento. Esta capacidad es compatible con almacenes de datos VMFS basados en protocolos FC e ISCSI.

Configuración de BlueXP disaster recovery

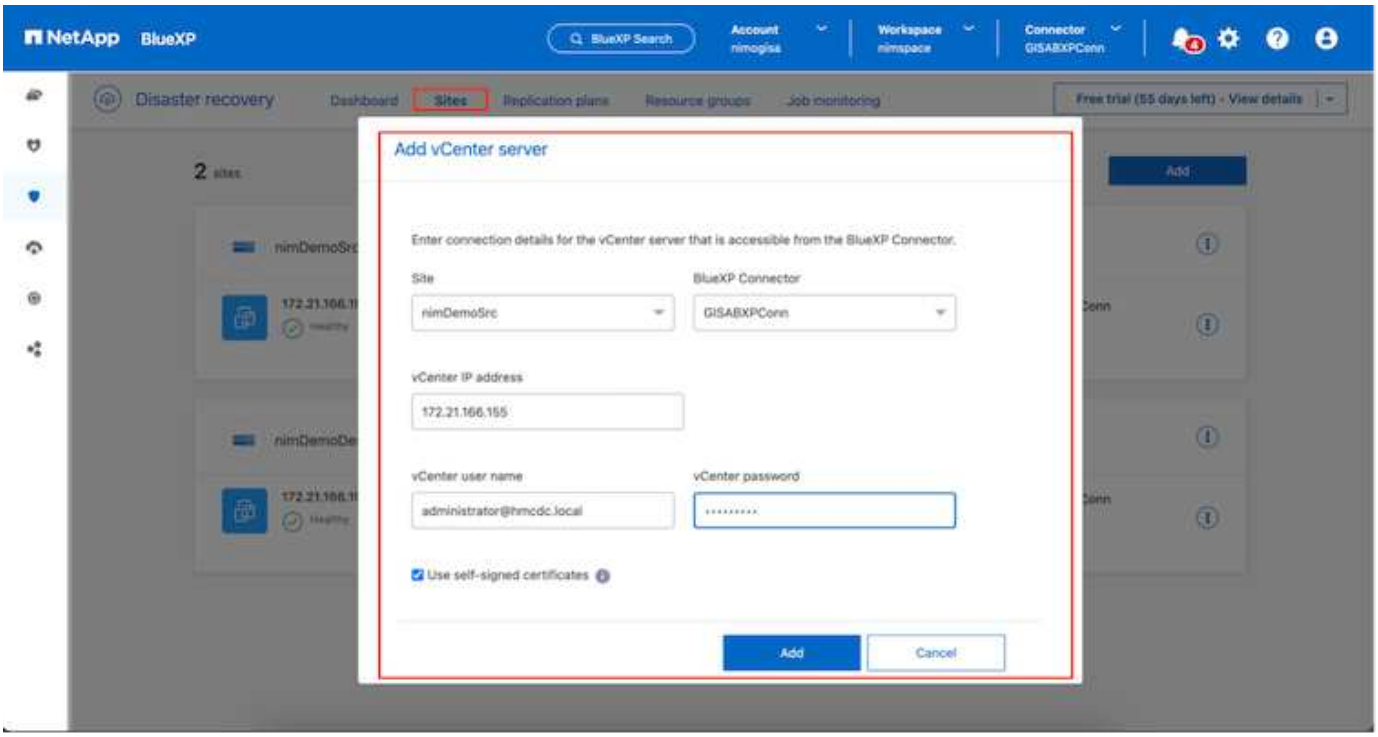
El primer paso para prepararse para la recuperación ante desastres es descubrir y agregar los recursos de almacenamiento y vCenter locales a la BlueXP disaster recovery.

Asegúrese de que los sistemas de almacenamiento ONTAP se agreguen al entorno de trabajo dentro del lienzo. Abra la consola BlueXP y seleccione **Protección > Recuperación ante desastres** en la navegación izquierda. Seleccione **Descubrir servidores vCenter** o utilice el menú superior, seleccione **Sitios > Agregar > Agregar vCenter**.

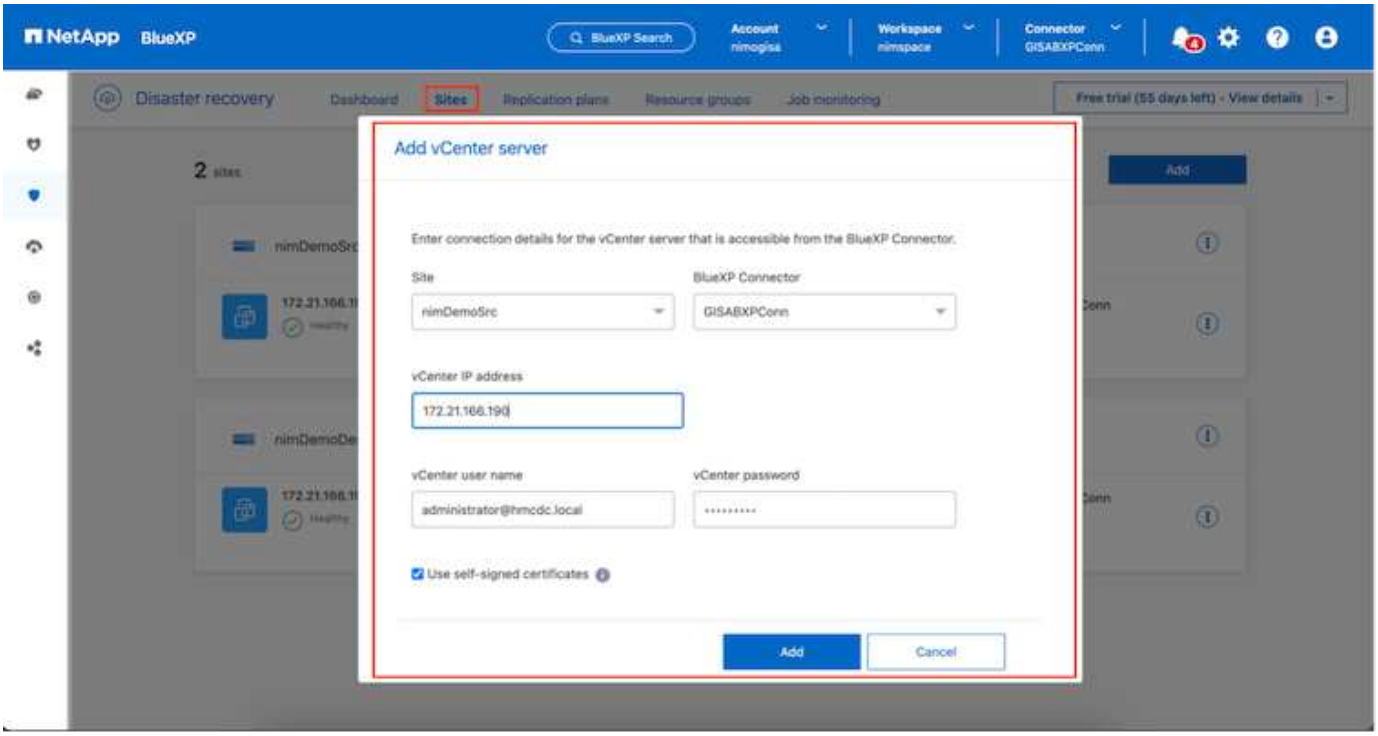


Agregue las siguientes plataformas:

- **Fuente**. vCenter local.



- **Destino**. Centro de datos SDDC de VMC.



Una vez que se agregan los vCenters, se activa el descubrimiento automático.

Configuración de la replicación de almacenamiento entre el sitio de origen y el de destino

SnapMirror utiliza instantáneas de ONTAP para administrar la transferencia de datos de una ubicación a otra. Inicialmente, se copia una copia completa basada en una instantánea del volumen de origen al destino para realizar una sincronización de línea base. A medida que se producen cambios en los datos en la fuente, se crea una nueva instantánea y se compara con la instantánea de referencia. Luego, los bloques que se han modificado se replican en el destino, y la instantánea más nueva se convierte en la línea de base actual, o la instantánea común más nueva. Esto permite que el proceso se repita y que se envíen actualizaciones incrementales al destino.

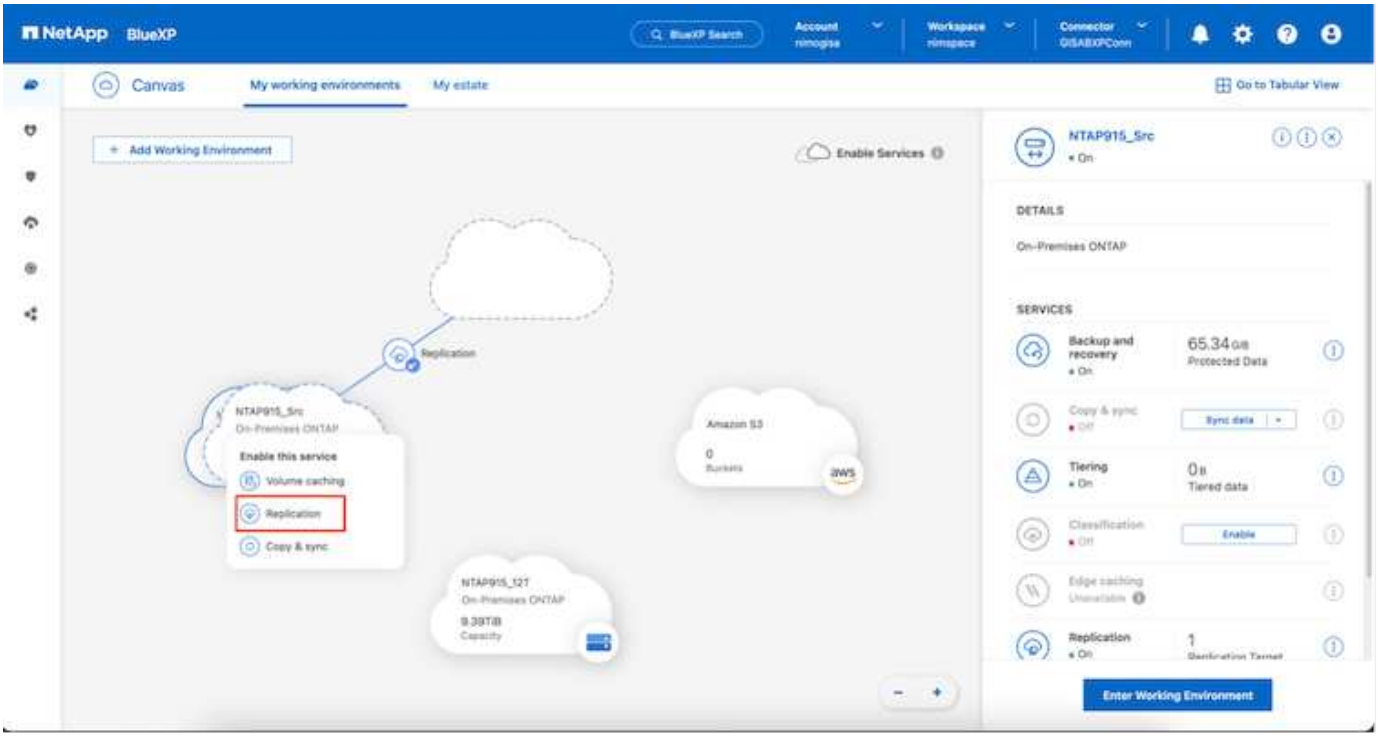
Cuando se establece una relación SnapMirror , el volumen de destino está en un estado de solo lectura en línea y, por lo tanto, aún es accesible. SnapMirror trabaja con bloques físicos de almacenamiento, en lugar de a nivel de archivos u otro nivel lógico. Esto significa que el volumen de destino es una réplica idéntica del de origen, incluidas instantáneas, configuraciones de volumen, etc. Si el volumen de origen utiliza funciones de eficiencia de espacio de ONTAP , como compresión de datos y deduplicación de datos, el volumen replicado conservará estas optimizaciones.

Al romper la relación de SnapMirror , el volumen de destino se puede escribir y normalmente se utiliza para realizar una conmutación por error cuando se utiliza SnapMirror para sincronizar datos con un entorno de recuperación ante desastres. SnapMirror es lo suficientemente sofisticado para permitir que los datos modificados en el sitio de conmutación por error se resincronicen de manera eficiente con el sistema principal, en caso de que más tarde vuelva a estar en línea, y luego permitir que se restablezca la relación original de SnapMirror .

Cómo configurarlo para VMware Disaster Recovery

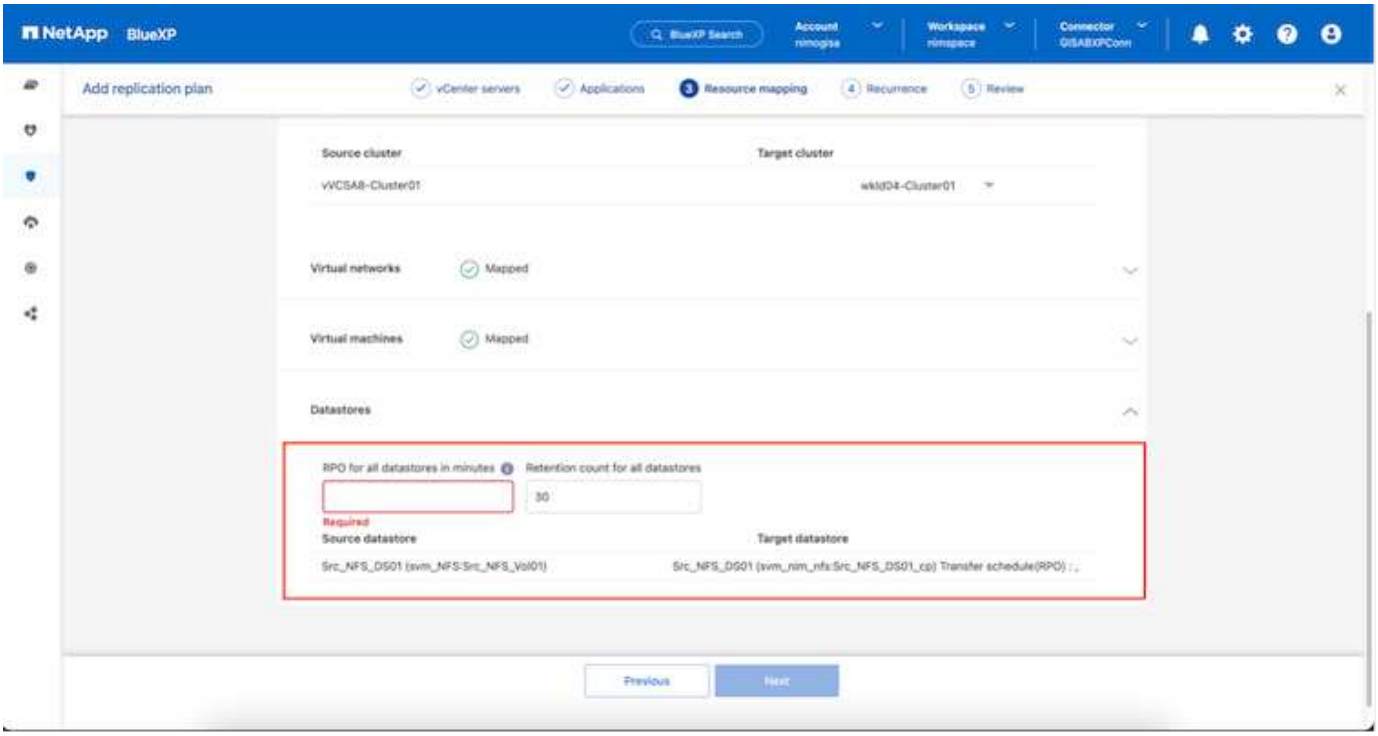
El proceso para crear la replicación de SnapMirror sigue siendo el mismo para cualquier aplicación. El proceso puede ser manual o automatizado. La forma más sencilla es aprovechar BlueXP para configurar la replicación

de SnapMirror mediante el simple arrastrar y soltar del sistema ONTAP de origen en el entorno al destino para activar el asistente que lo guía a través del resto del proceso.



BlueXP DRaaS también puede automatizar lo mismo siempre que se cumplan los dos criterios siguientes:

- Los clústeres de origen y destino tienen una relación de pares.
- El SVM de origen y el SVM de destino tienen una relación de pares.

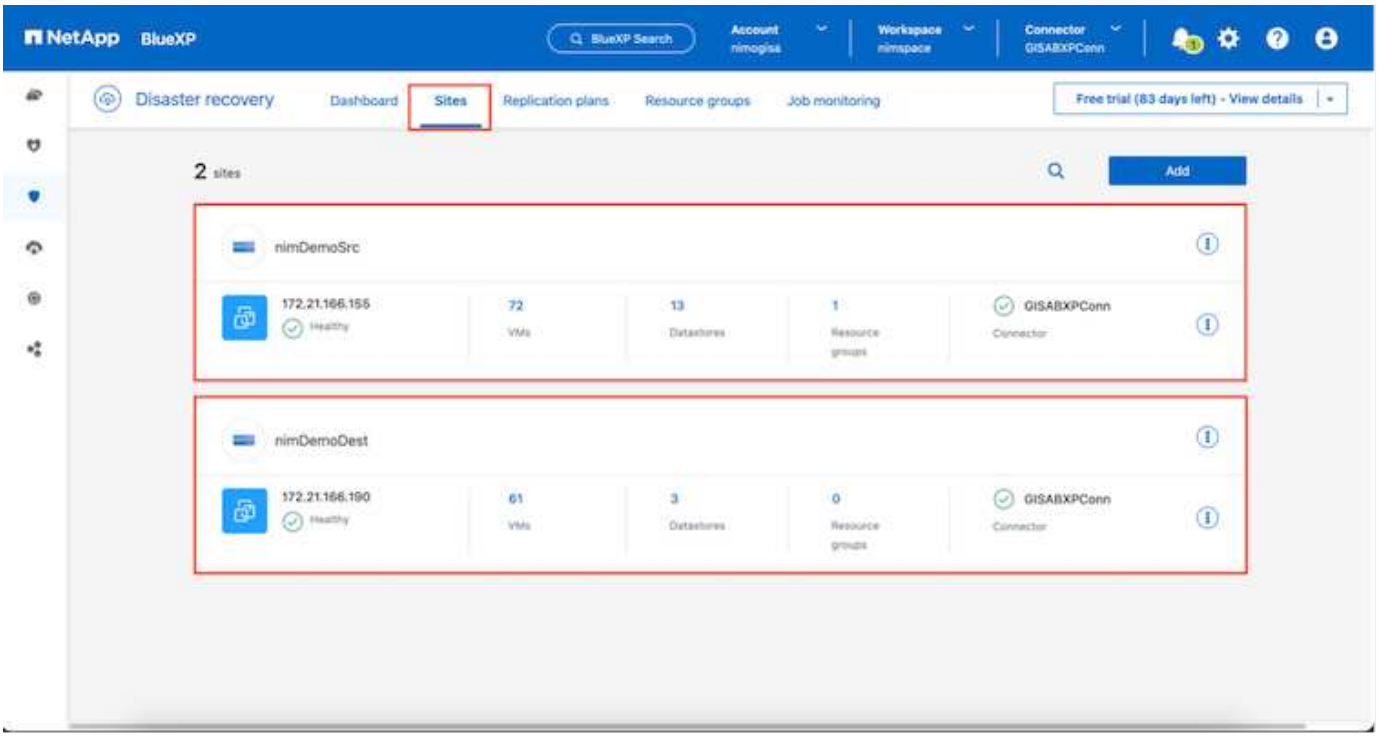


Si la relación SnapMirror ya está configurada para el volumen a través de CLI, BlueXP DRaaS retoma la relación y continúa con el resto de las operaciones del flujo de trabajo.

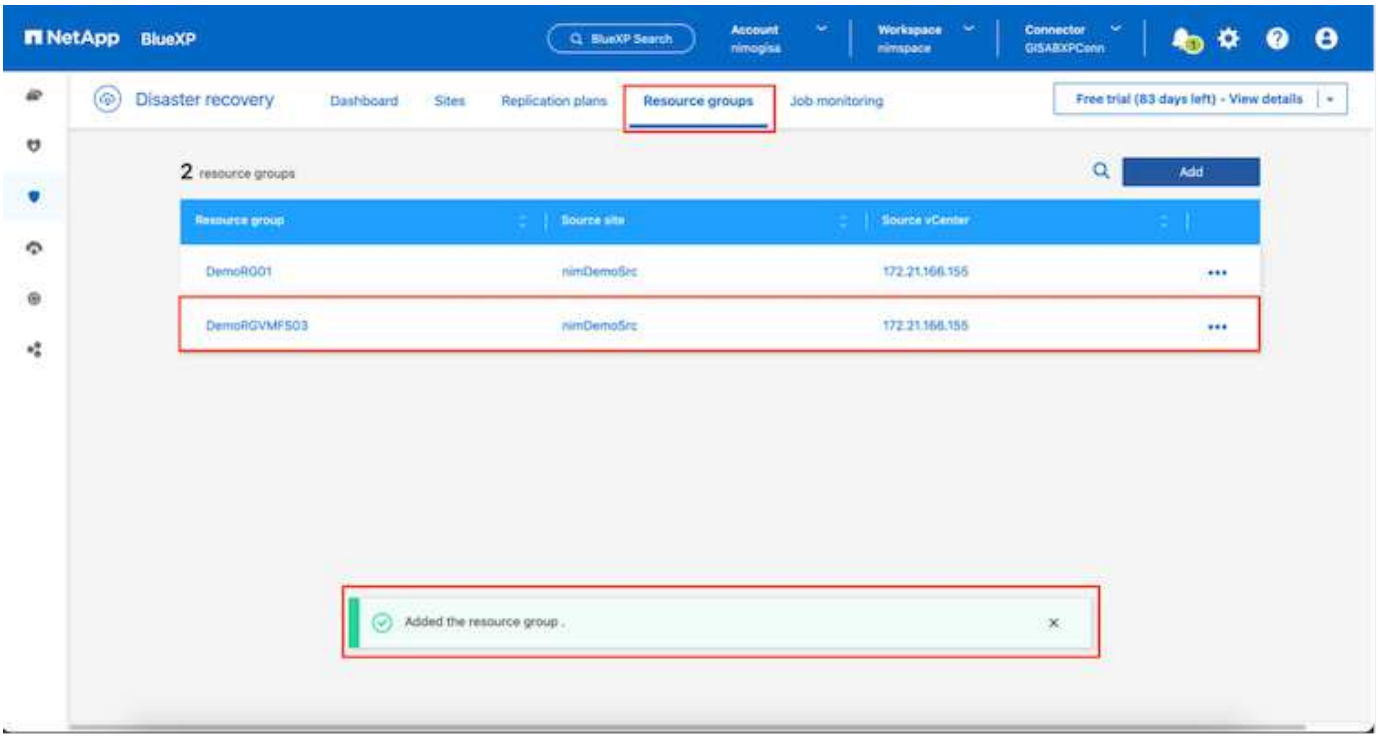
Además de los enfoques anteriores, la replicación de SnapMirror también se puede crear a través de ONTAP CLI o el Administrador del sistema. Independientemente del enfoque utilizado para sincronizar los datos mediante SnapMirror, BlueXP DRaaS organiza el flujo de trabajo para lograr operaciones de recuperación ante desastres fluidas y eficientes.

¿Qué puede hacer por usted la BlueXP disaster recovery ?

Una vez agregados los sitios de origen y destino, la BlueXP disaster recovery realiza un descubrimiento profundo automático y muestra las máquinas virtuales junto con los metadatos asociados. La BlueXP disaster recovery también detecta automáticamente las redes y los grupos de puertos utilizados por las máquinas virtuales y los completa.

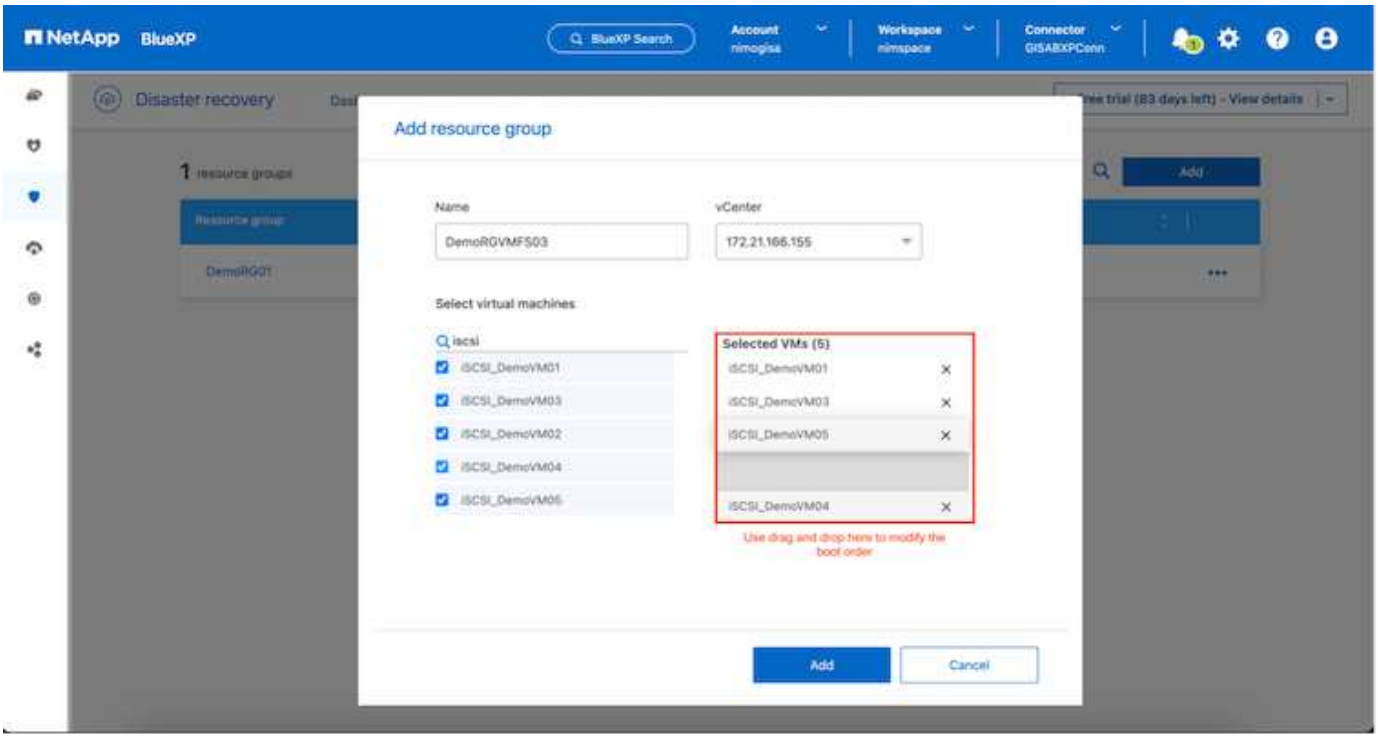


Una vez agregados los sitios, las máquinas virtuales se pueden agrupar en grupos de recursos. Los grupos de recursos de BlueXP disaster recovery le permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque y los retrasos de arranque que se pueden ejecutar durante la recuperación. Para comenzar a crear grupos de recursos, navegue a **Grupos de recursos** y haga clic en **Crear nuevo grupo de recursos**.

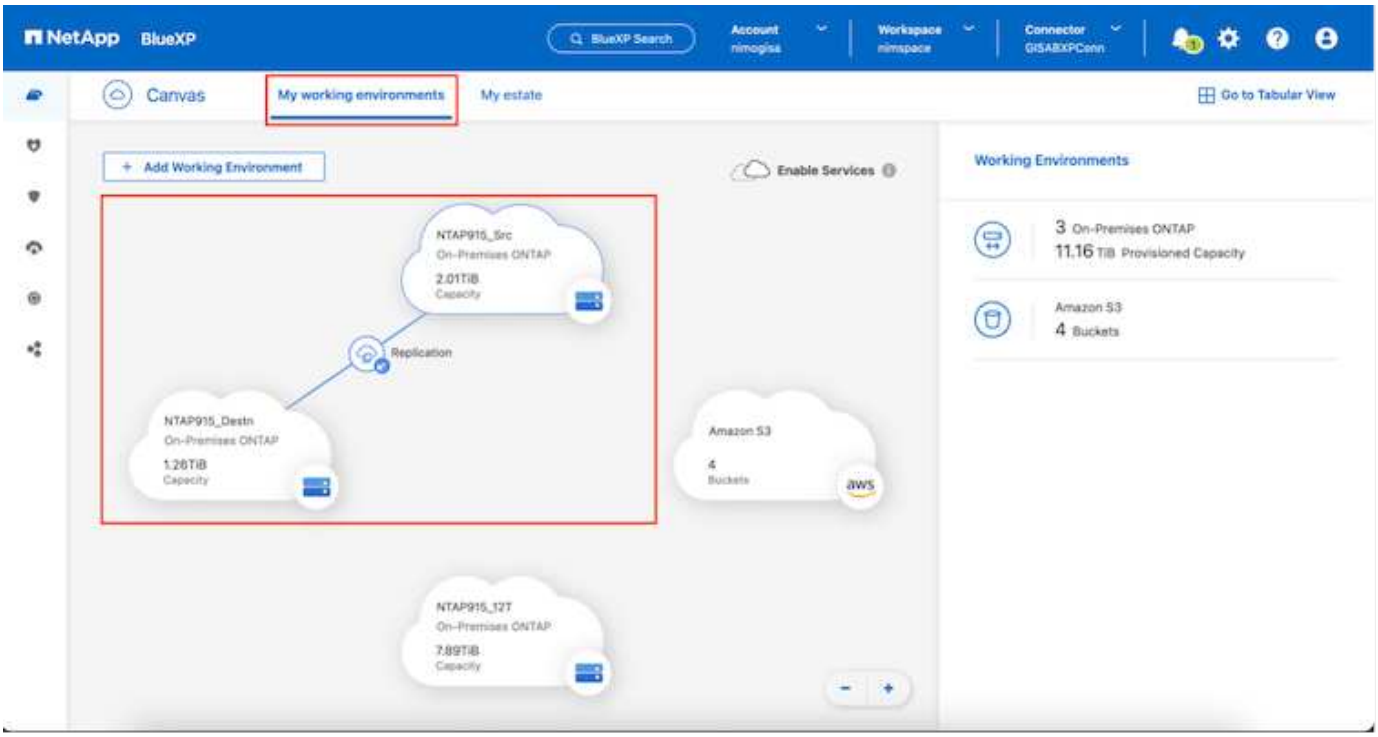


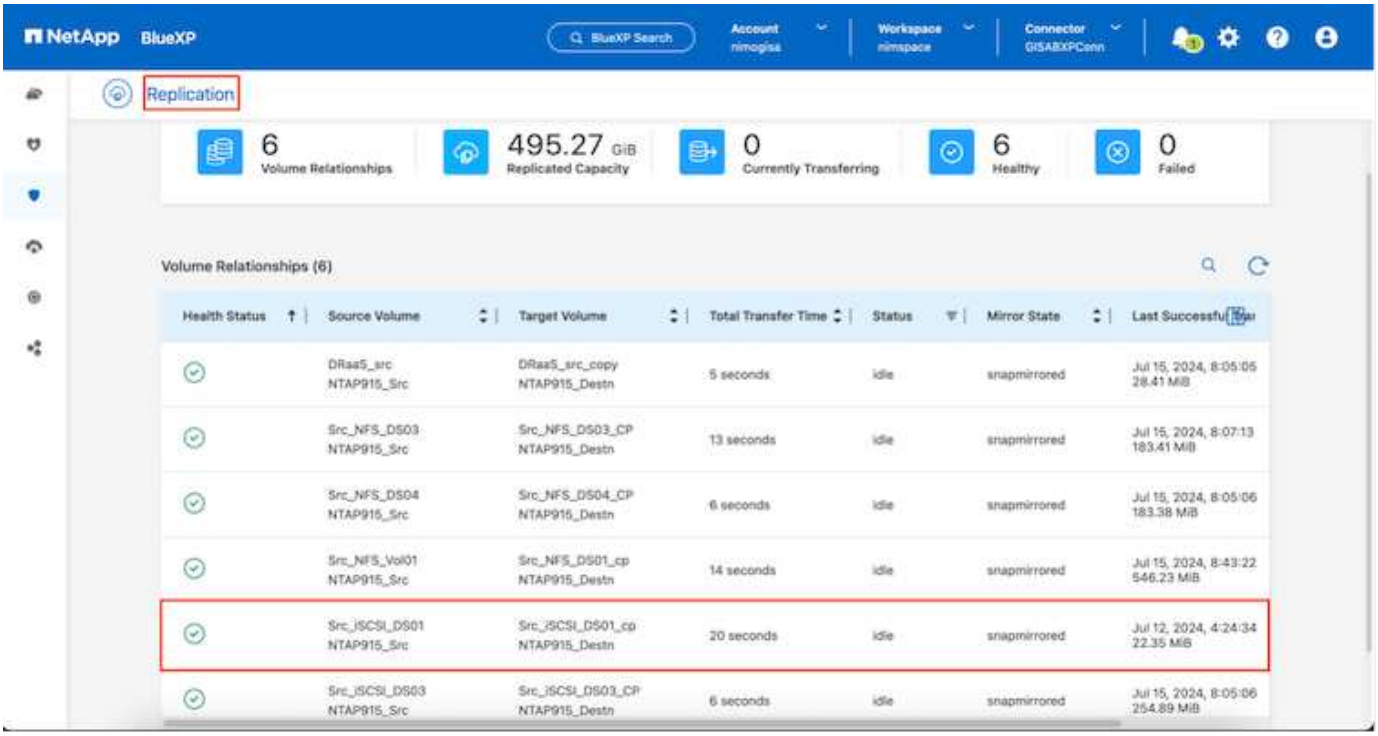
El grupo de recursos también se puede crear mientras se crea un plan de replicación.

El orden de arranque de las máquinas virtuales se puede definir o modificar durante la creación de grupos de recursos mediante un simple mecanismo de arrastrar y soltar.



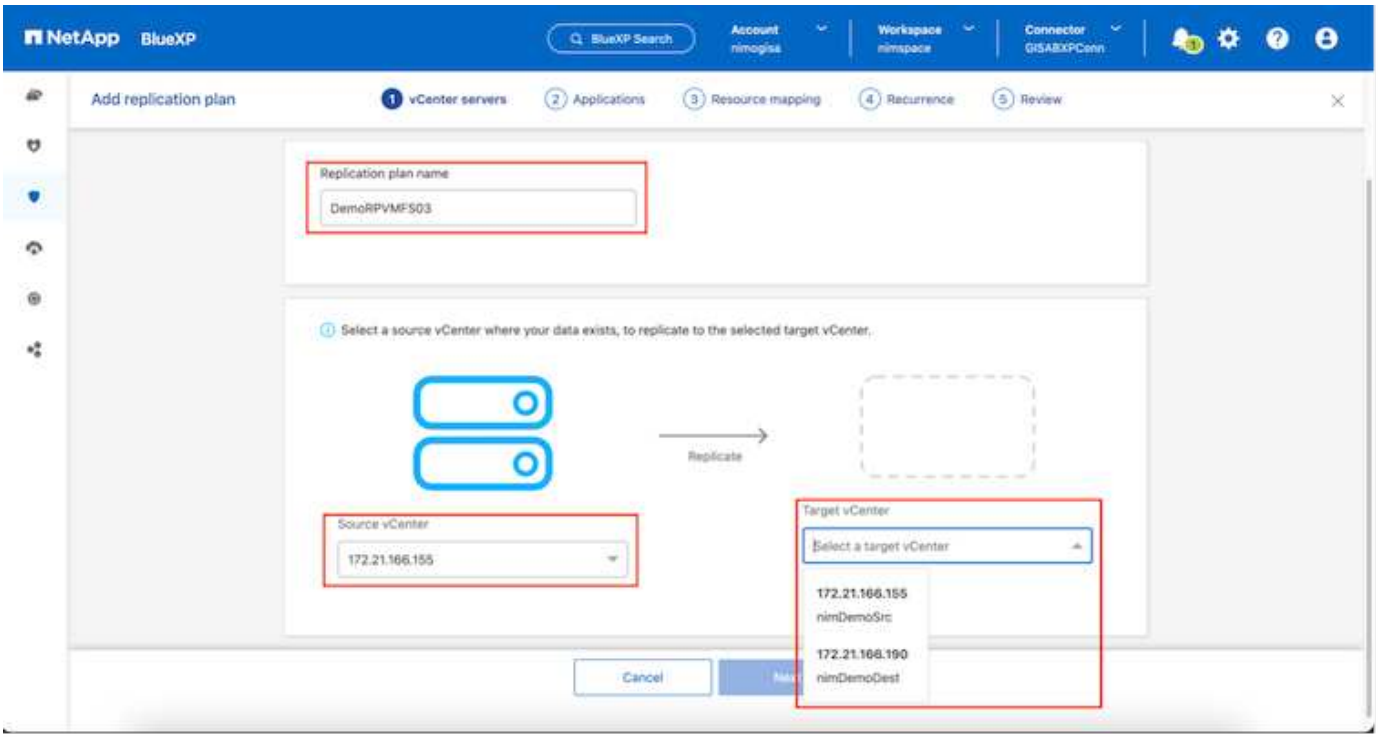
Una vez creados los grupos de recursos, el siguiente paso es crear el plan de ejecución o un plan para recuperar máquinas virtuales y aplicaciones en caso de desastre. Como se menciona en los requisitos previos, la replicación de SnapMirror se puede configurar de antemano o DRaaS puede configurarla utilizando el RPO y el recuento de retención especificados durante la creación del plan de replicación.



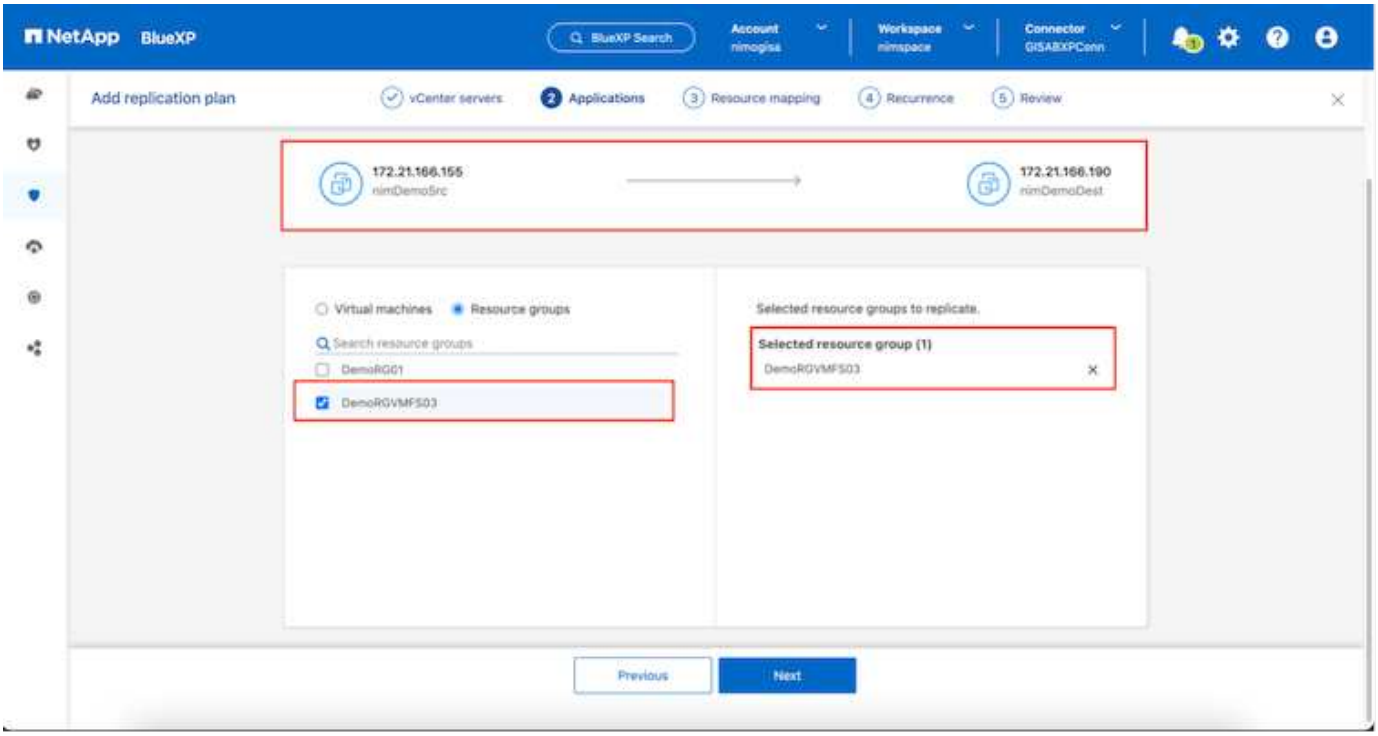


Configure el plan de replicación seleccionando las plataformas vCenter de origen y destino en el menú desplegable y elija los grupos de recursos que se incluirán en el plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones y el mapeo de clústeres y redes. Para definir el plan de recuperación, navegue a la pestaña **Plan de replicación** y haga clic en **Agregar plan**.

Primero, seleccione el vCenter de origen y luego seleccione el vCenter de destino.



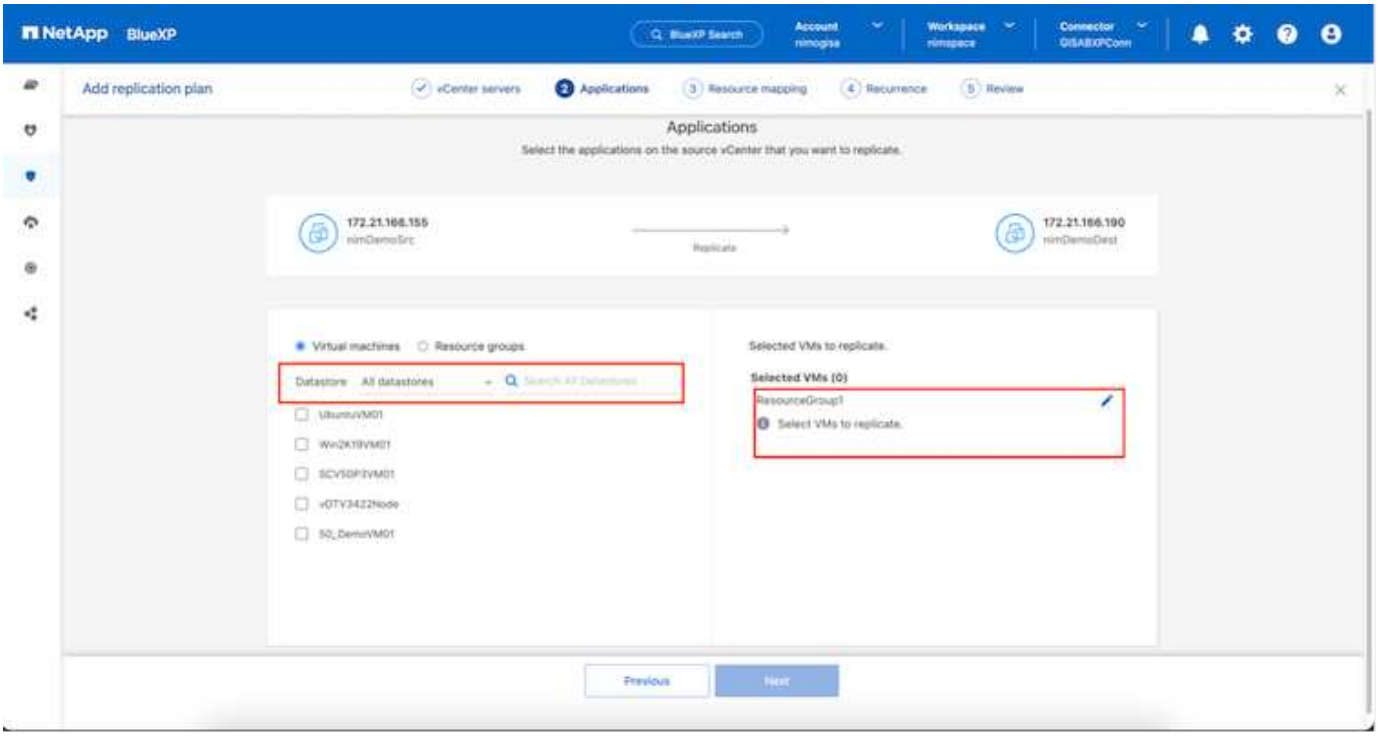
El siguiente paso es seleccionar los grupos de recursos existentes. Si no se crean grupos de recursos, el asistente ayuda a agrupar las máquinas virtuales necesarias (básicamente, crea grupos de recursos funcionales) en función de los objetivos de recuperación. Esto también ayuda a definir la secuencia de operaciones de cómo se deben restaurar las máquinas virtuales de la aplicación.



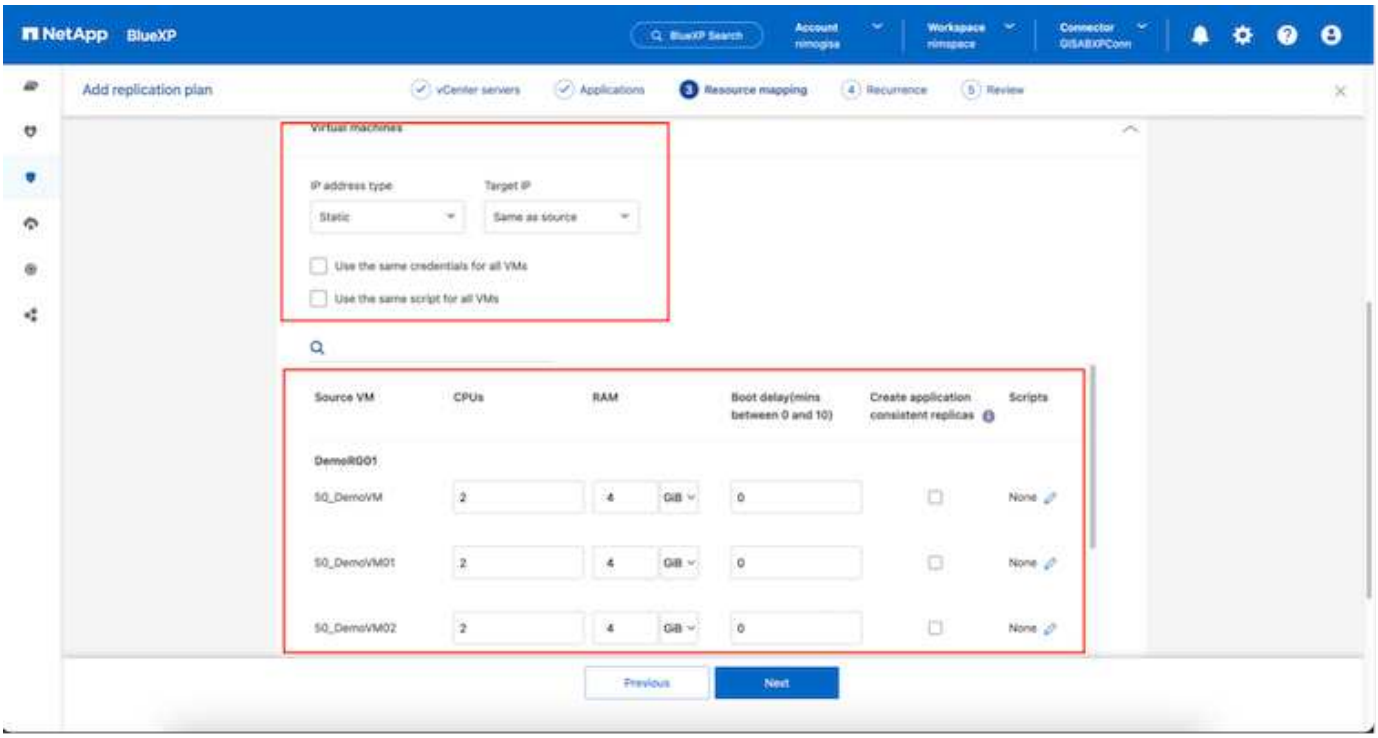
El grupo de recursos permite establecer el orden de arranque mediante la funcionalidad de arrastrar y soltar. Se puede utilizar para modificar fácilmente el orden en que se encenderán las máquinas virtuales durante el proceso de recuperación.

Cada máquina virtual dentro de un grupo de recursos se inicia en secuencia según el orden. Se inician dos grupos de recursos en paralelo.

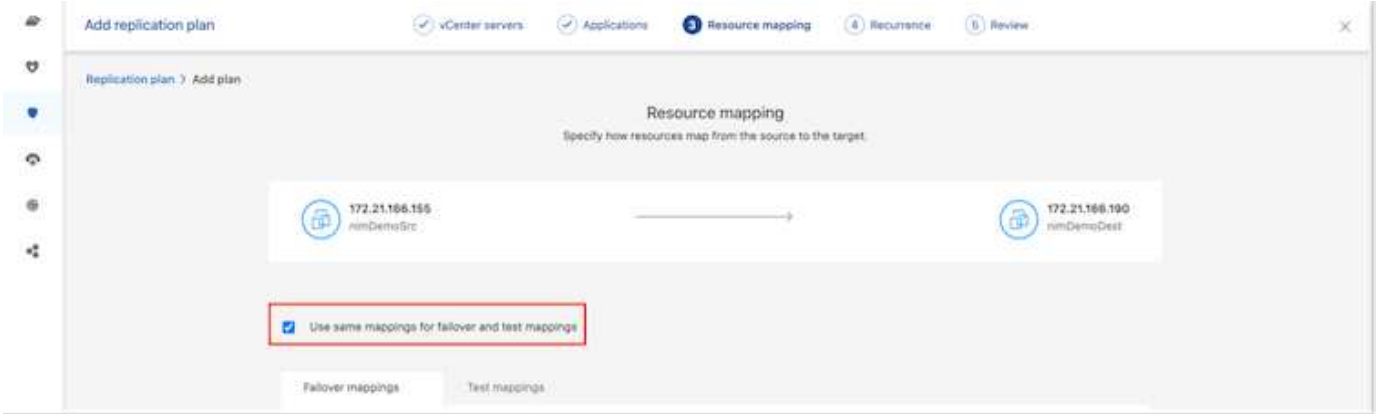
La siguiente captura de pantalla muestra la opción para filtrar máquinas virtuales o almacenes de datos específicos según los requisitos organizativos si no se crean grupos de recursos de antemano.



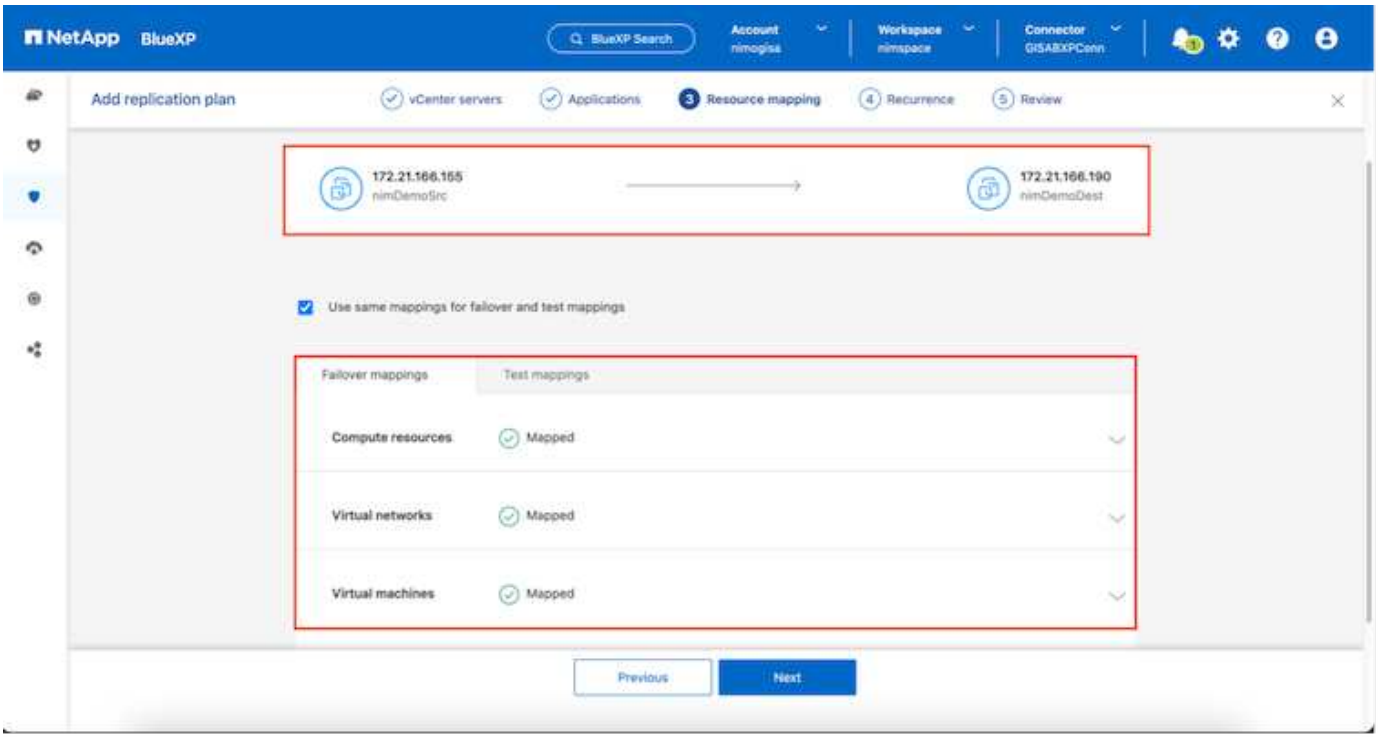
Una vez seleccionados los grupos de recursos, cree las asignaciones de conmutación por error. En este paso, especifique cómo se asignan los recursos del entorno de origen al destino. Esto incluye recursos computacionales y redes virtuales. Personalización de IP, scripts previos y posteriores, retrasos en el arranque, consistencia de la aplicación, etc. Para obtener información detallada, consulte"Crear un plan de replicación" .



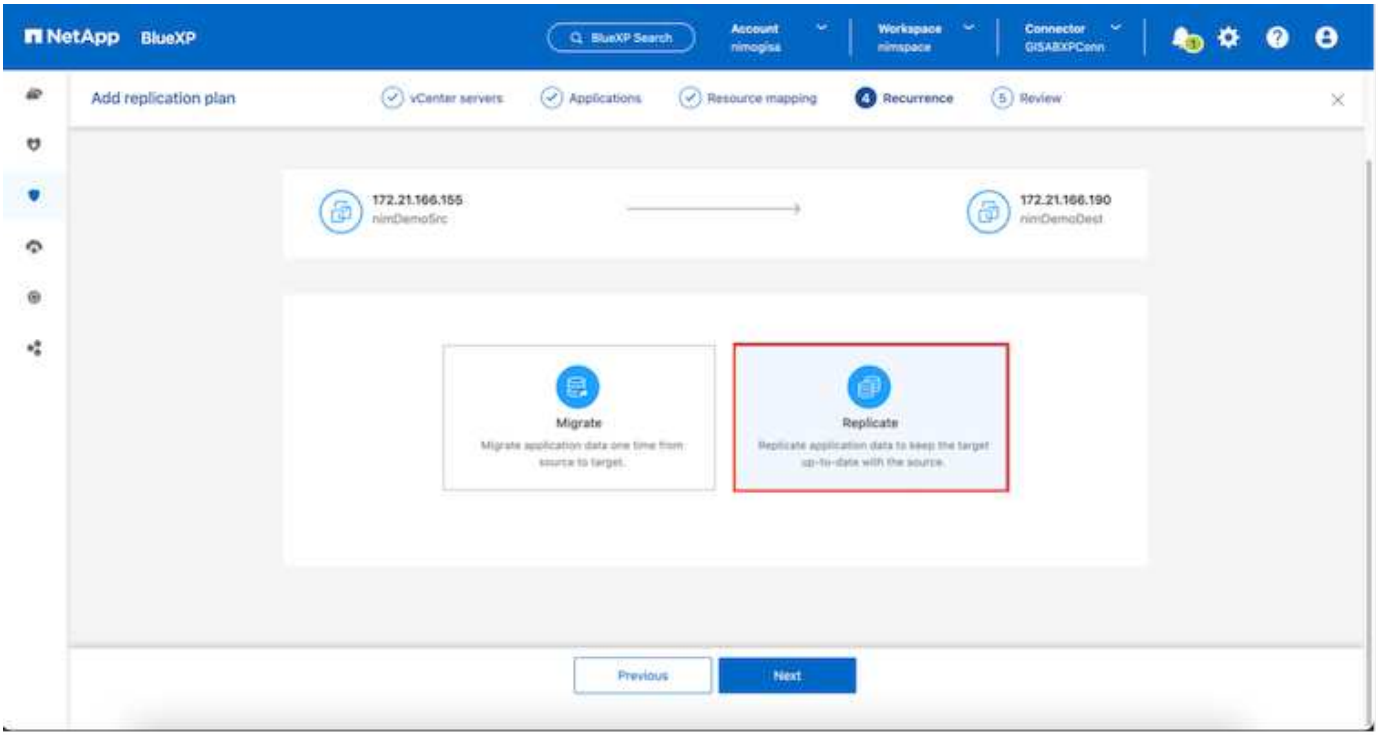
De forma predeterminada, se utilizan los mismos parámetros de mapeo para las operaciones de prueba y de conmutación por error. Para aplicar diferentes asignaciones para el entorno de prueba, seleccione la opción Asignación de prueba después de desmarcar la casilla de verificación como se muestra a continuación:



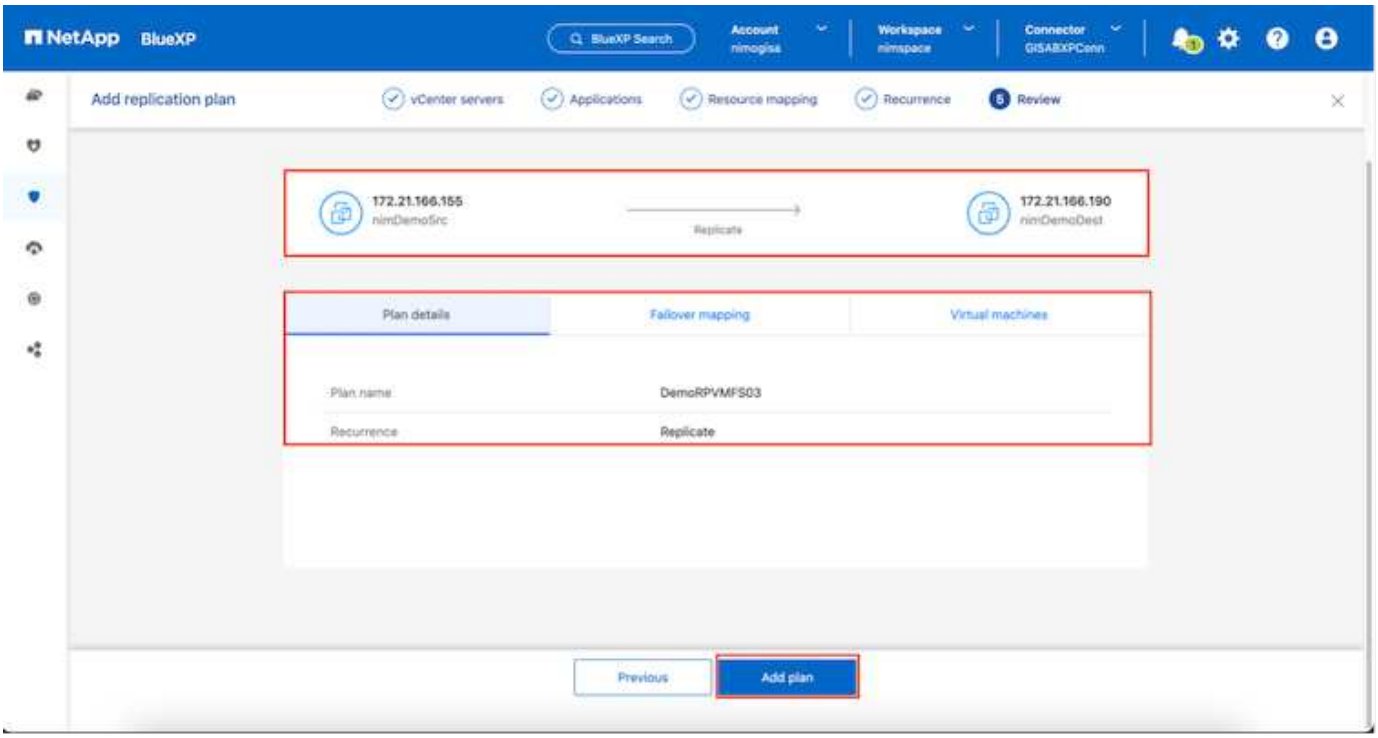
Una vez completado el mapeo de recursos, haga clic en Siguiente.

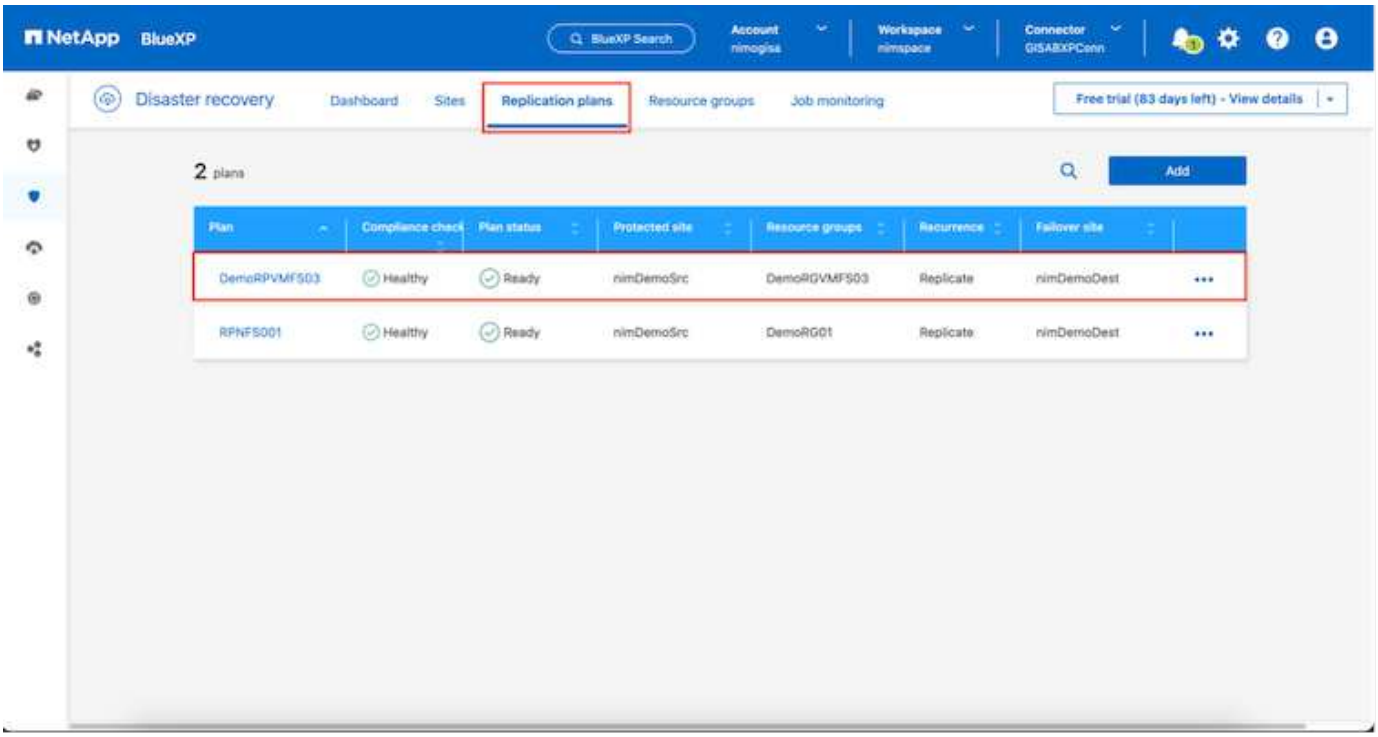


Seleccione el tipo de recurrencia. En palabras simples, seleccione la opción Migrar (migración única mediante conmutación por error) o replicación continua recurrente. En este tutorial, se selecciona la opción Replicar.

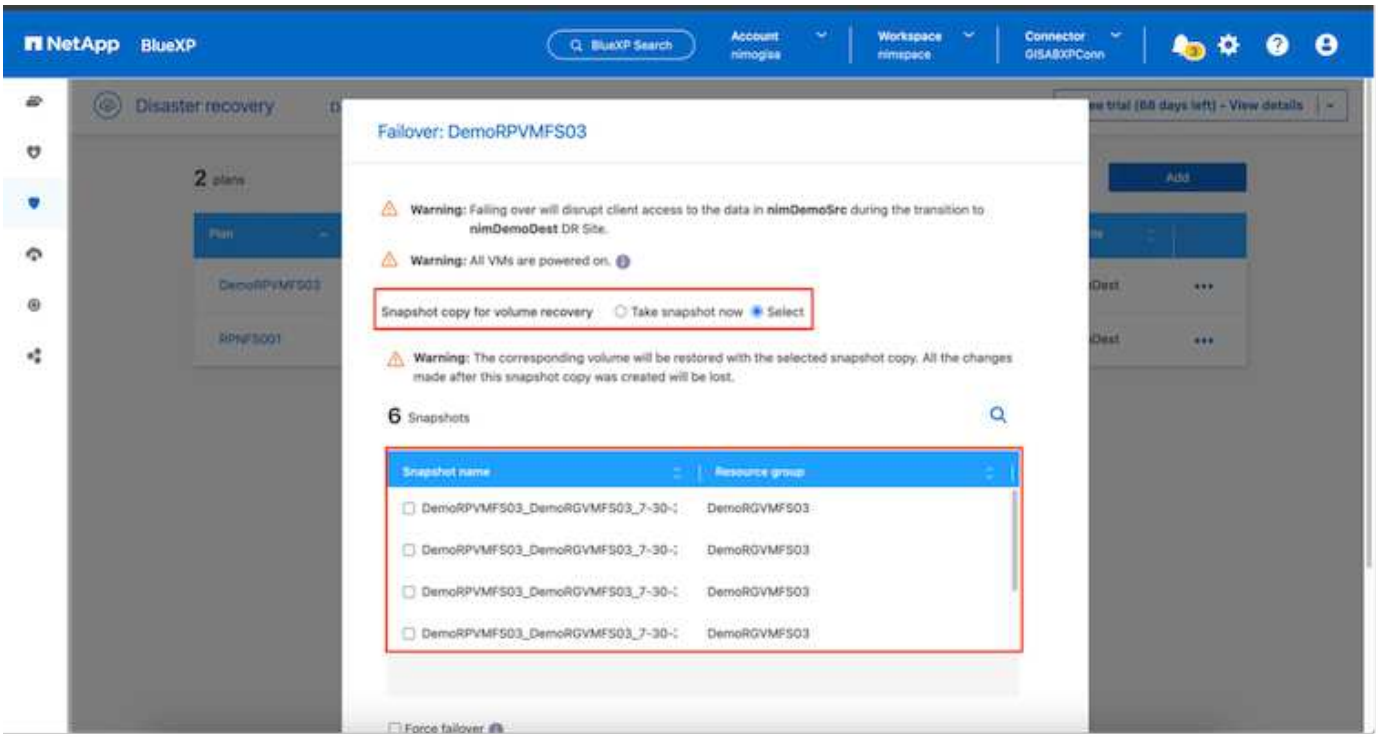


Una vez hecho esto, revise los mapeos creados y luego haga clic en Agregar plan.

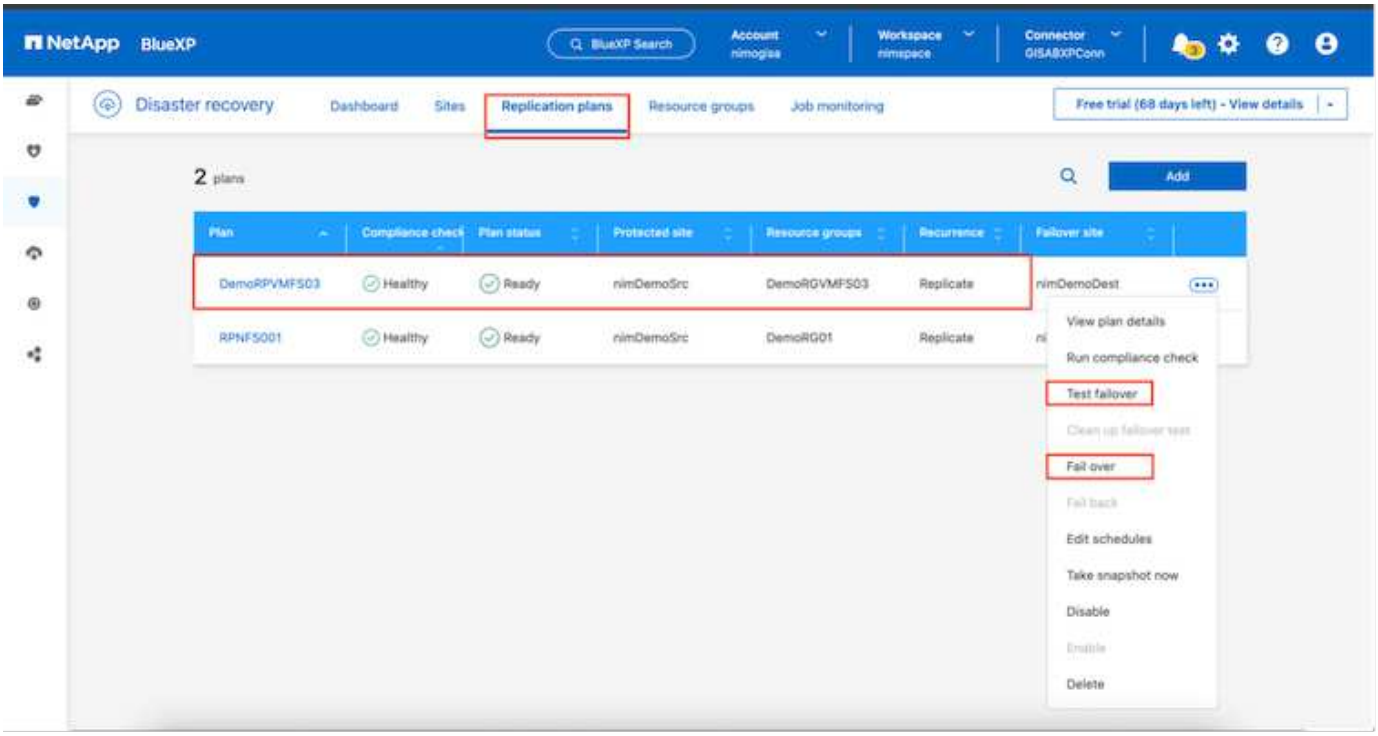




Una vez creado el plan de replicación, se puede realizar una conmutación por error según los requisitos seleccionando la opción de conmutación por error, la opción de conmutación por error de prueba o la opción de migración. La BlueXP disaster recovery garantiza que el proceso de replicación se ejecute según el plan cada 30 minutos. Durante las opciones de conmutación por error y conmutación por error de prueba, puede utilizar la copia de instantánea de SnapMirror más reciente o puede seleccionar una copia de instantánea específica de una copia de instantánea de un momento determinado (según la política de retención de SnapMirror). La opción de punto en el tiempo puede ser muy útil si hay un evento de corrupción como ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. La BlueXP disaster recovery muestra todos los puntos de recuperación disponibles.



Para activar o probar la conmutación por error con la configuración especificada en el plan de replicación, haga clic en **Conmutación por error** o **Probar conmutación por error**.

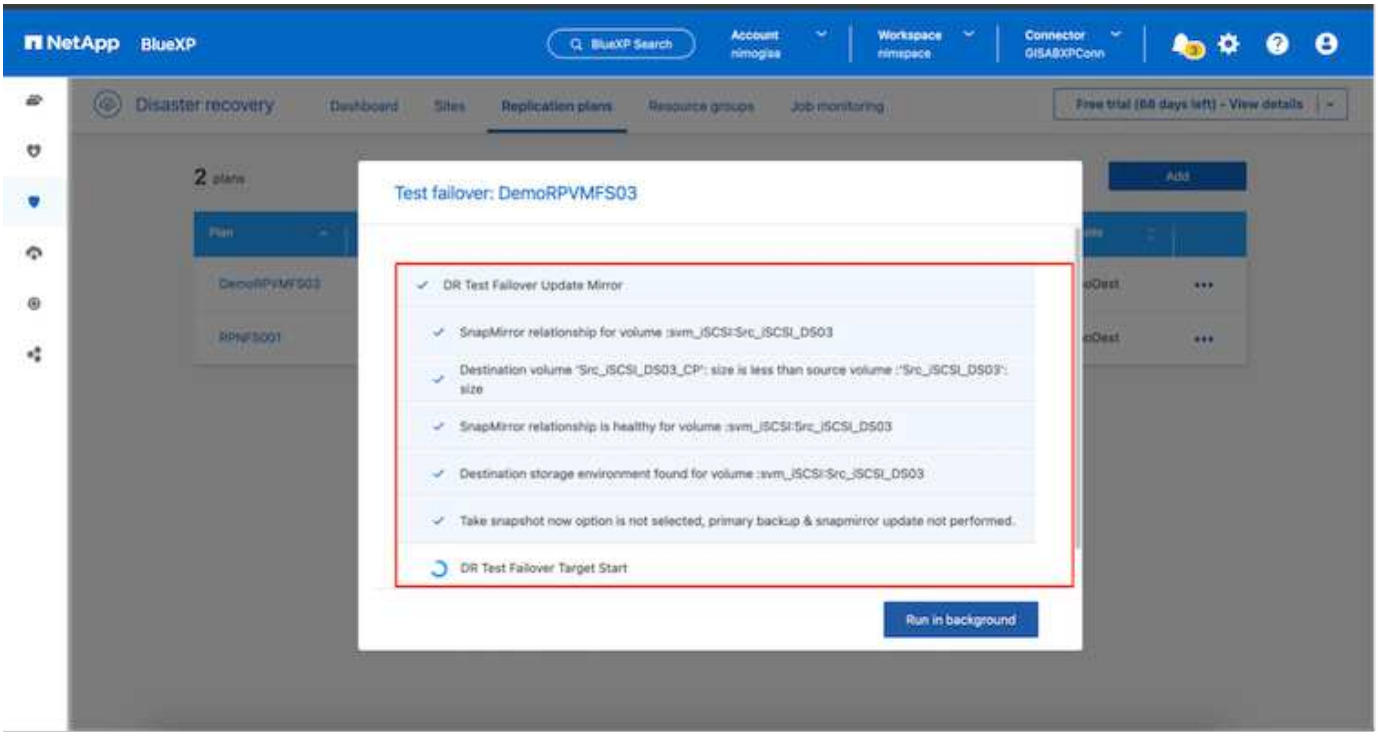


¿Qué sucede durante una operación de conmutación por error o de prueba?

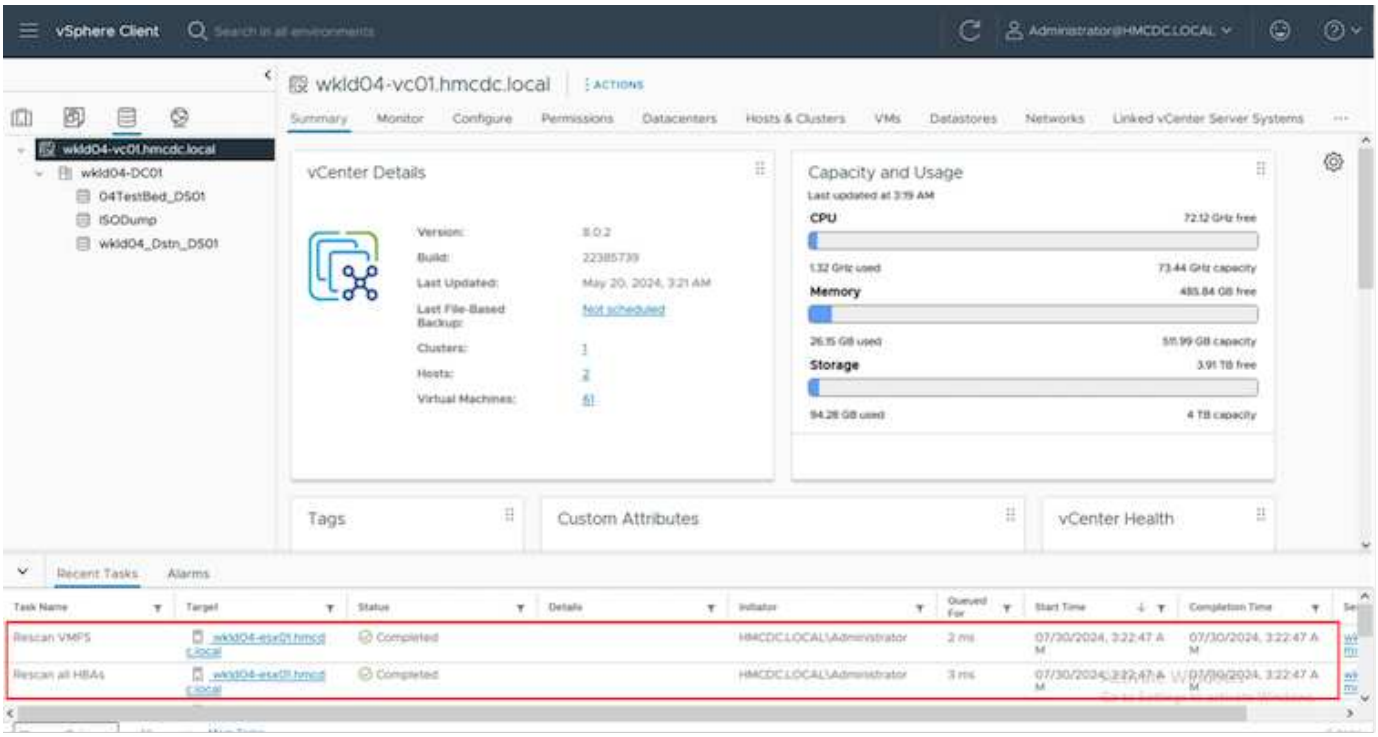
Durante una operación de conmutación por error de prueba, la BlueXP disaster recovery crea un volumen FlexClone en el sistema de almacenamiento ONTAP de destino utilizando la última copia de instantánea o una instantánea seleccionada del volumen de destino.

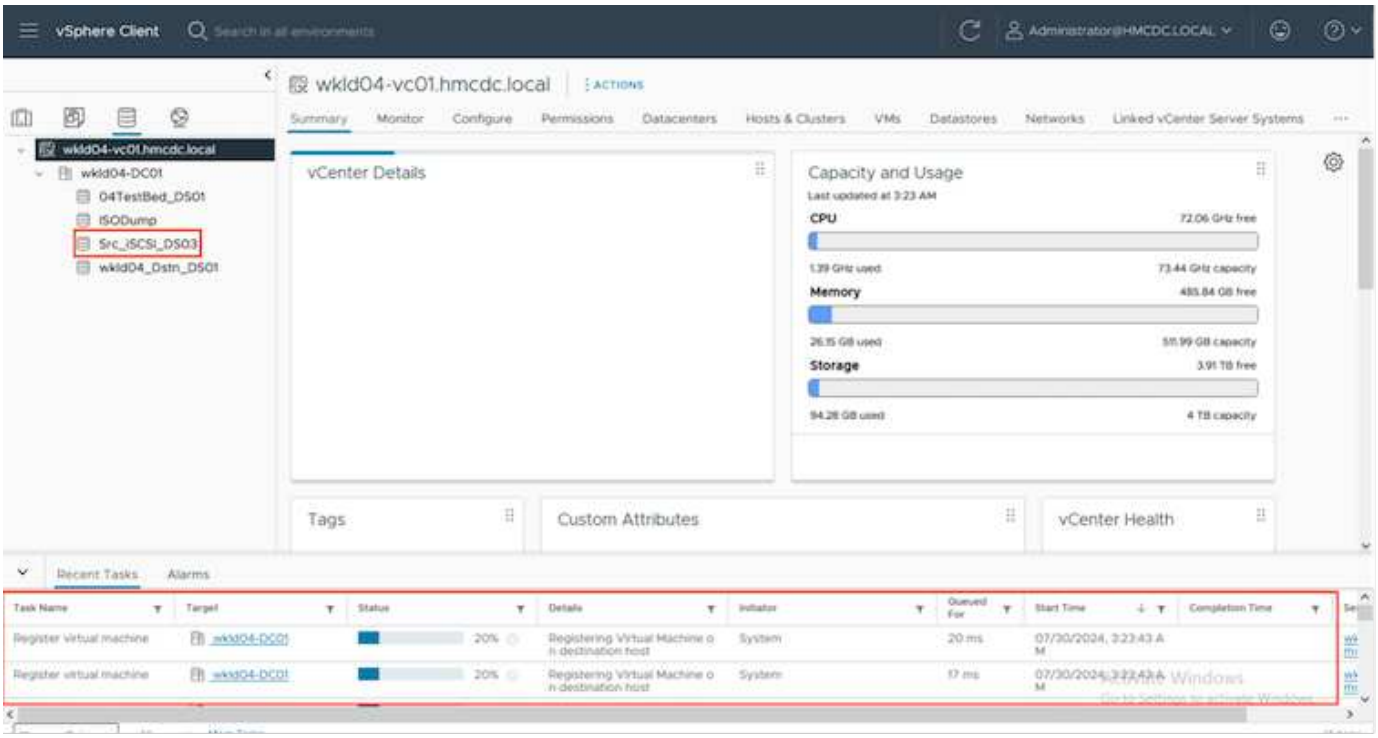
Una operación de conmutación por error de prueba crea un volumen clonado en el sistema de almacenamiento ONTAP de destino.

Ejecutar una operación de recuperación de prueba no afecta la replicación de SnapMirror .



Durante el proceso, la BlueXP disaster recovery no asigna el volumen de destino original. En lugar de ello, crea un nuevo volumen FlexClone a partir de la instantánea seleccionada y un almacén de datos temporal que respalda el volumen FlexClone se asigna a los hosts ESXi.

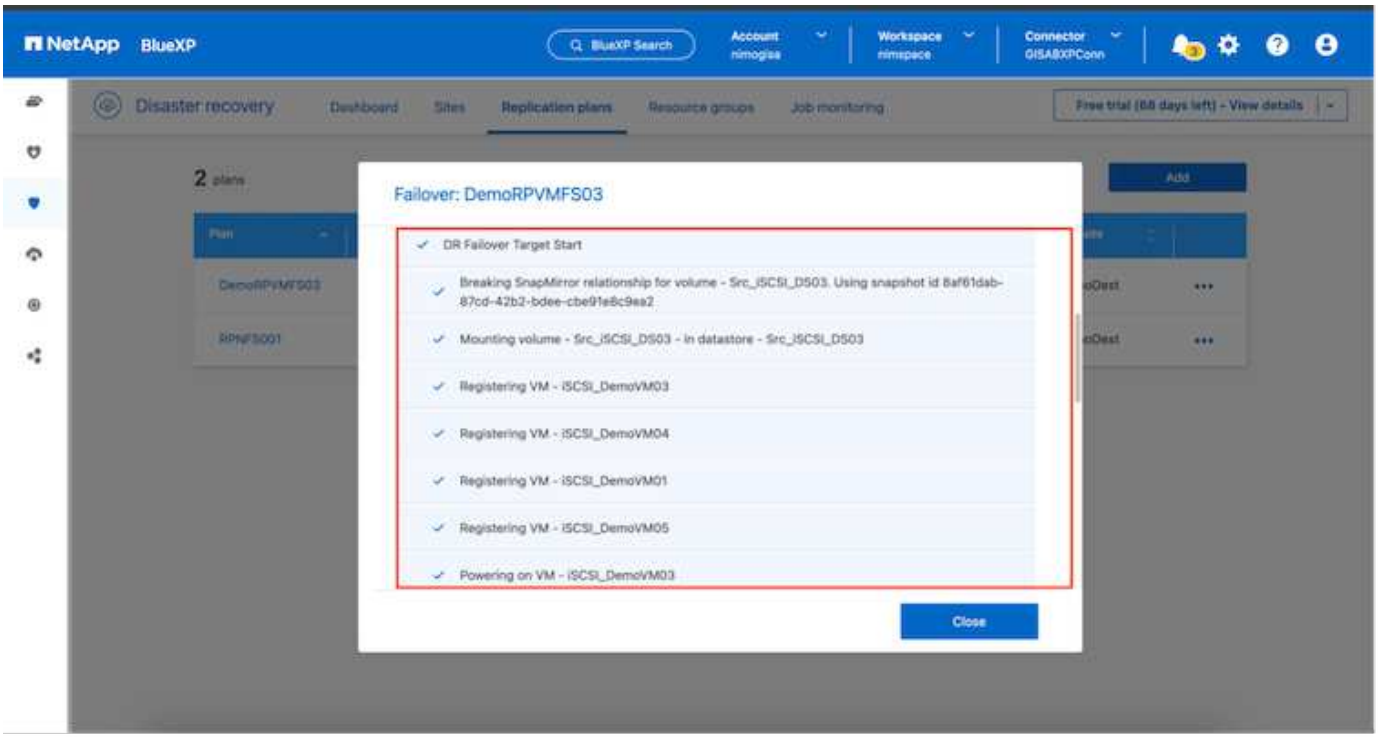




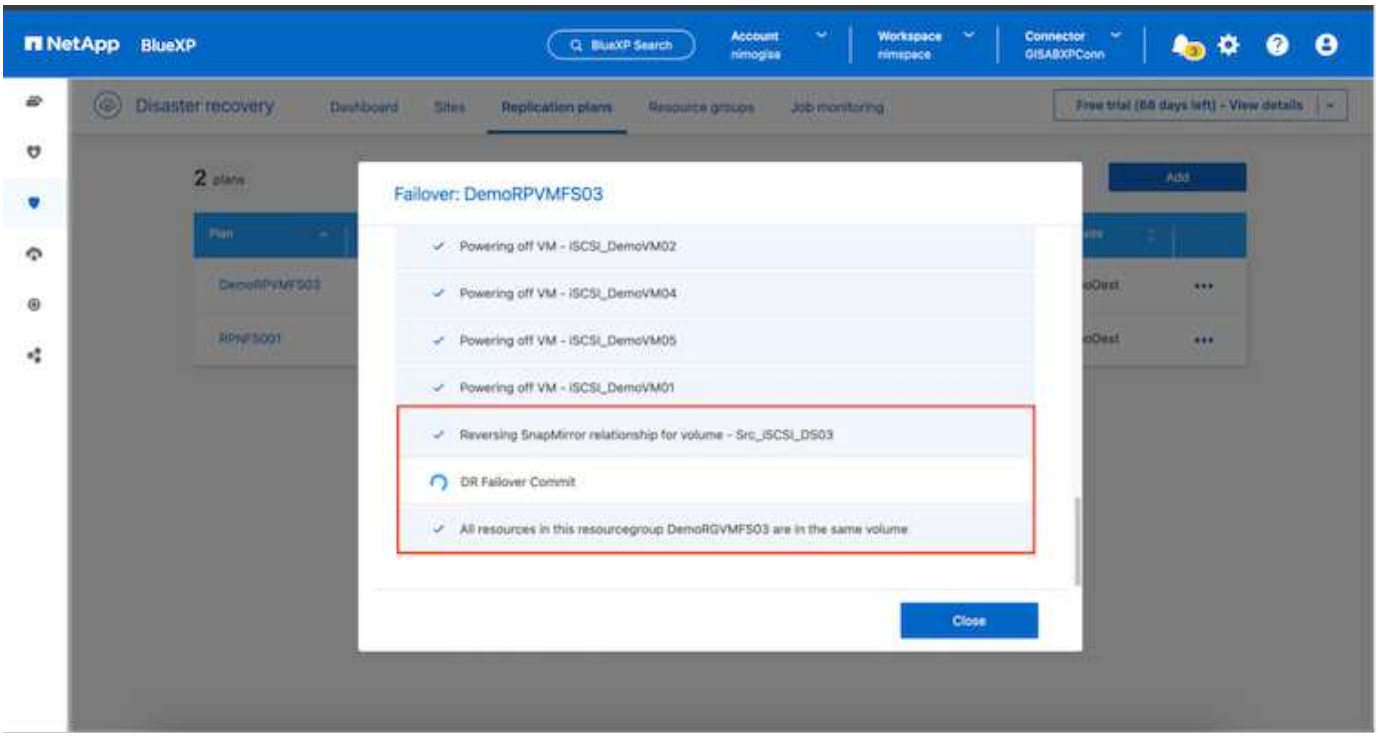
Cuando se completa la operación de conmutación por error de prueba, se puede activar la operación de limpieza utilizando **"Limpiar prueba de conmutación por error"**. Durante esta operación, la BlueXP disaster recovery destruye el volumen FlexClone que se utilizó en la operación.

En caso de que ocurra un desastre real, la BlueXP disaster recovery realiza los siguientes pasos:

1. Rompe la relación SnapMirror entre los sitios.
2. Monta el volumen del almacén de datos VMFS después de la renovación para su uso inmediato.
3. Registrar las máquinas virtuales
4. Encender las máquinas virtuales



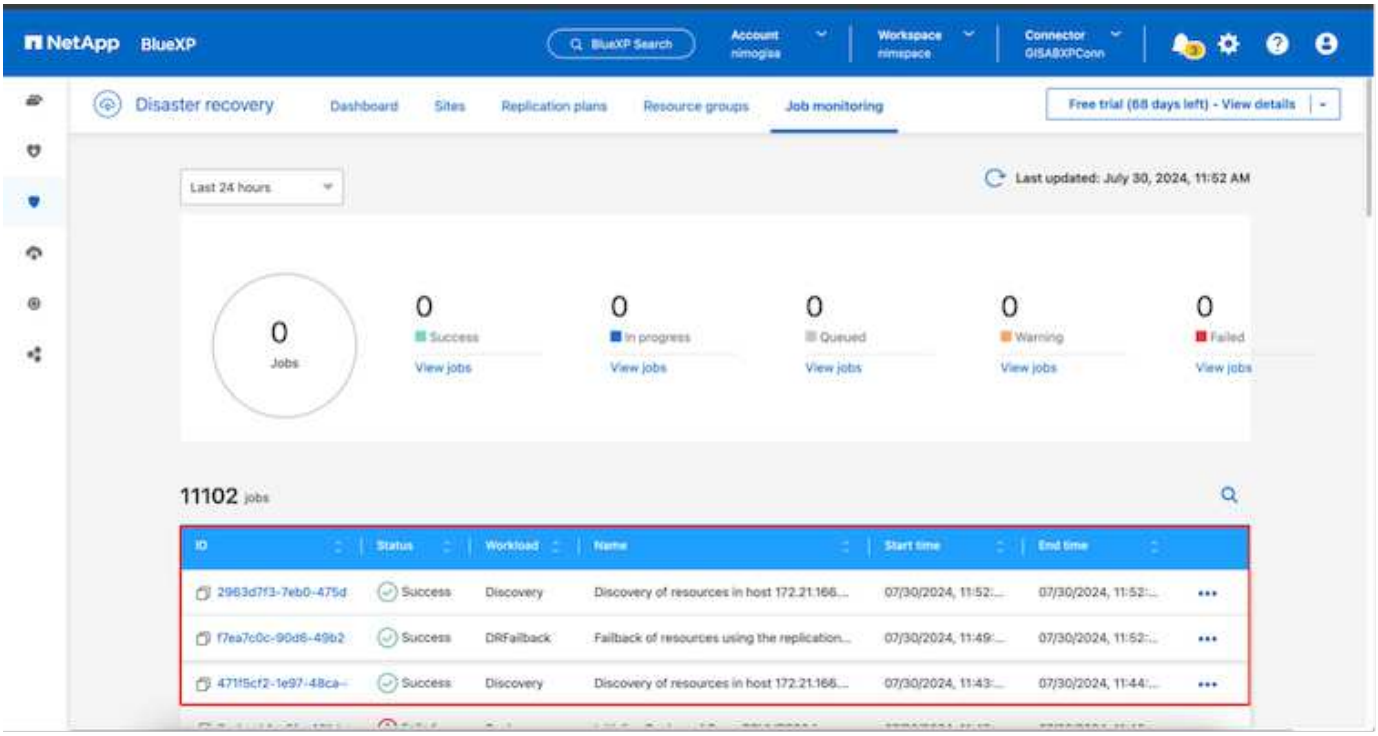
Una vez que el sitio principal está en funcionamiento, la BlueXP disaster recovery permite la resincronización inversa para SnapMirror y habilita la conmutación por recuperación, que nuevamente se puede realizar con el clic de un botón.



Y si se elige la opción de migrar, se considera como un evento de conmutación por error planificado. En este caso, se activa un paso adicional que consiste en apagar las máquinas virtuales en el sitio de origen. El resto de los pasos siguen siendo los mismos que en el evento de conmutación por error.

Desde BlueXP o la CLI de ONTAP , puede supervisar el estado de salud de la replicación para los volúmenes de almacén de datos adecuados, y el estado de una conmutación por error o de una conmutación por error de

prueba se puede rastrear a través de la Supervisión de trabajos.



Esto proporciona una solución poderosa para gestionar un plan de recuperación ante desastres personalizado y adaptado. La conmutación por error se puede realizar de forma planificada o con solo hacer clic en un botón cuando ocurre un desastre y se toma la decisión de activar el sitio de recuperación ante desastres.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado o utilizar el"simulador de soluciones" .

Configurar la recuperación ante desastres para almacenes de datos NFS mediante la BlueXP disaster recovery

En este caso de uso, describimos el procedimiento para configurar la recuperación ante desastres mediante la BlueXP disaster recovery para máquinas virtuales VMware locales que utilizan almacenes de datos NFS. Este procedimiento incluye configurar la cuenta y el conector de BlueXP , agregar matrices ONTAP para habilitar la comunicación entre VMware vCenter y el almacenamiento ONTAP , configurar la replicación entre sitios y crear y probar planes de recuperación.

La implementación de la recuperación ante desastres a través de la replicación a nivel de bloque desde el sitio de producción al sitio de recuperación ante desastres es un método resiliente y rentable para proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos, como ataques de ransomware. Al utilizar la replicación SnapMirror de NetApp , las cargas de trabajo de VMware que se ejecutan en sistemas ONTAP locales con almacén de datos NFS se pueden replicar a otro sistema de almacenamiento ONTAP ubicado en un centro de datos de recuperación designado donde también se implementa VMware.

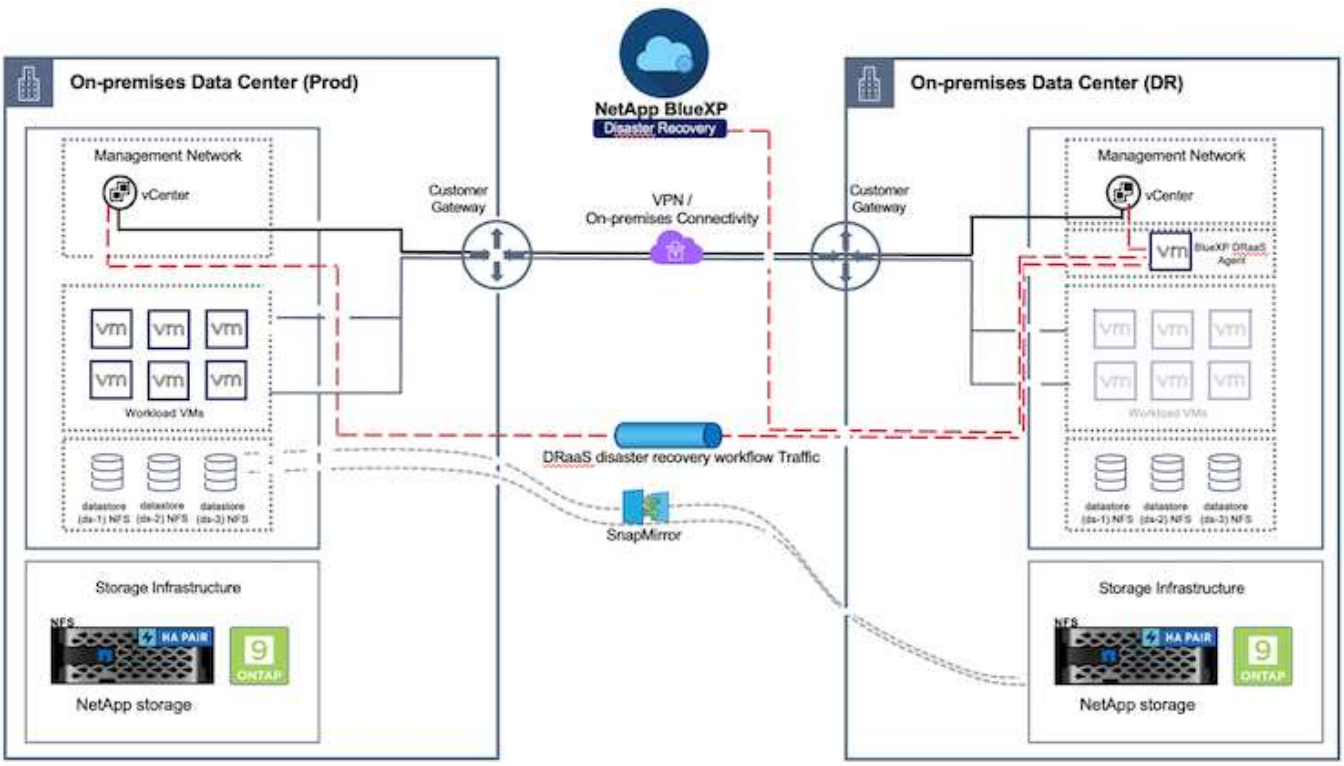
Introducción

Esta sección del documento describe la configuración de BlueXP DRaaS para configurar la recuperación ante desastres de las máquinas virtuales VMware locales en otro sitio designado. Como parte de esta

configuración, la cuenta BlueXP , el conector BlueXP y las matrices ONTAP agregadas dentro del espacio de trabajo de BlueXP son necesarias para habilitar la comunicación desde VMware vCenter al almacenamiento ONTAP . Además, este documento detalla cómo configurar la replicación entre sitios y cómo configurar y probar un plan de recuperación. La última sección tiene instrucciones para realizar una conmutación por error completa del sitio y cómo realizar una conmutación por error cuando el sitio principal se recupera y se compra en línea.

Al utilizar el servicio de BlueXP disaster recovery , integrado en la consola BlueXP de NetApp , las empresas pueden descubrir fácilmente sus VMware vCenters locales y su almacenamiento ONTAP . Las organizaciones pueden luego crear agrupaciones de recursos, crear un plan de recuperación ante desastres, asociarlo con grupos de recursos y probar o ejecutar conmutación por error y conmutación por recuperación. SnapMirror proporciona replicación de bloques a nivel de almacenamiento para mantener los dos sitios actualizados con cambios incrementales, lo que da como resultado un objetivo de punto de recuperación (RPO) de hasta 5 minutos. Además, es posible simular procedimientos de recuperación ante desastres sin afectar la producción ni incurrir en costos de almacenamiento adicionales.

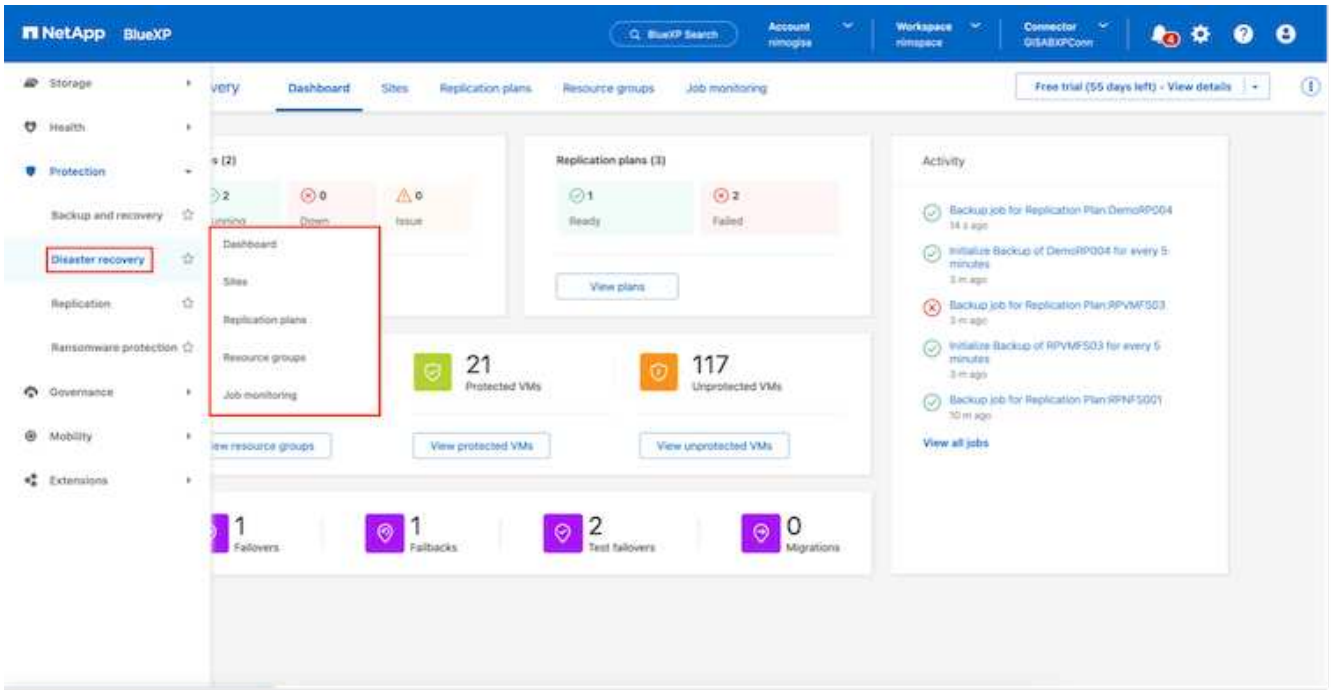
La BlueXP disaster recovery aprovecha la tecnología FlexClone de ONTAP para crear una copia que ahorra espacio del almacén de datos NFS a partir de la última instantánea replicada en el sitio de recuperación ante desastres. Después de completar la prueba de recuperación ante desastres, los clientes pueden eliminar fácilmente el entorno de prueba sin afectar los recursos de producción replicados reales. En caso de una conmutación por error real, el servicio de BlueXP disaster recovery organiza todos los pasos necesarios para activar automáticamente las máquinas virtuales protegidas en el sitio de recuperación ante desastres designado con solo unos pocos clics. El servicio también revertirá la relación de SnapMirror con el sitio principal y replicará cualquier cambio del secundario al principal para una operación de conmutación por error, cuando sea necesario. Todas estas capacidades tienen un costo mucho menor que el de otras alternativas conocidas.



Empezando

Para comenzar con la BlueXP disaster recovery, utilice la consola de BlueXP y luego acceda al servicio.

1. Inicie sesión en BlueXP.
2. Desde la navegación izquierda de BlueXP , seleccione Protección > Recuperación ante desastres.
3. Aparece el panel de BlueXP disaster recovery .

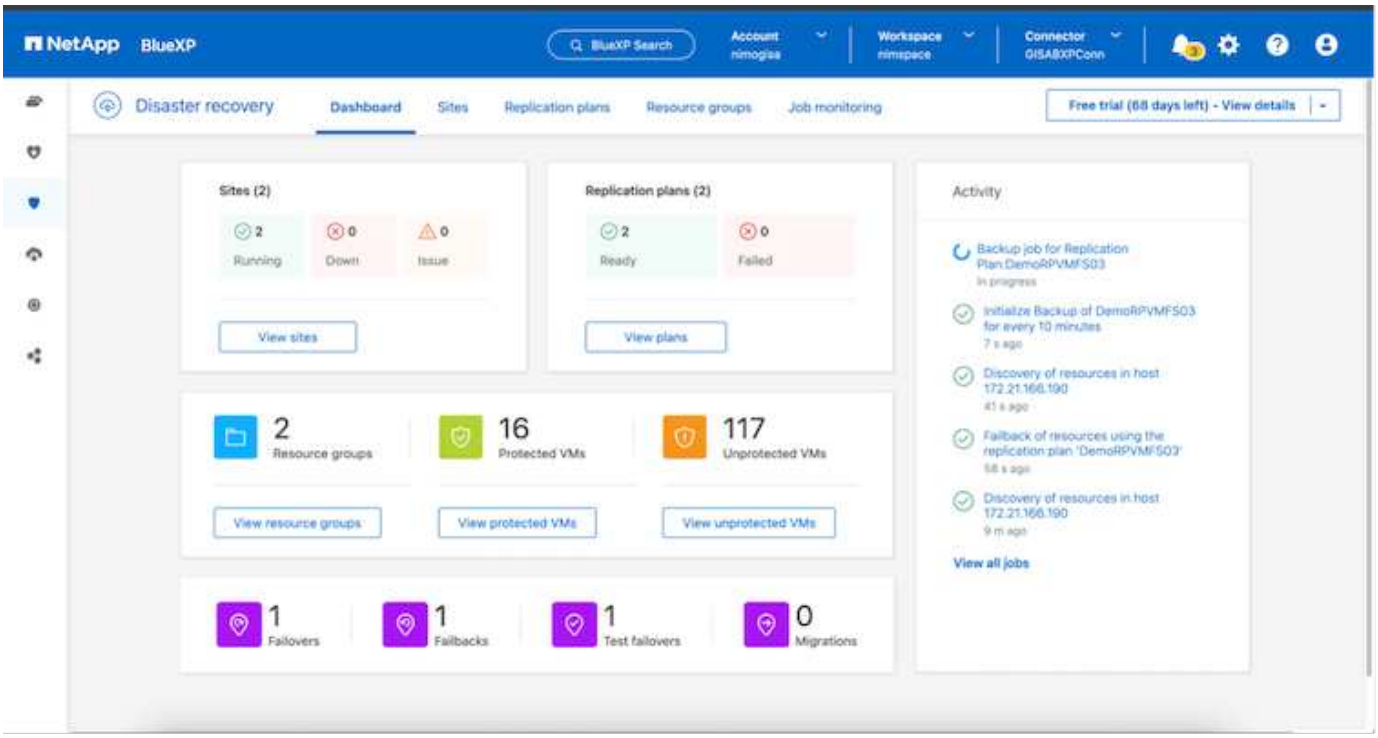


Antes de configurar el plan de recuperación ante desastres, asegúrese de que se cumplan los siguientes requisitos previos:

- El conector BlueXP está configurado en NetApp BlueXP.
- La instancia del conector BlueXP tiene conectividad con el vCenter de origen y destino y con los sistemas de almacenamiento.
- Clúster NetApp Data ONTAP para proporcionar almacenes de datos NFS.
- Los sistemas de almacenamiento NetApp locales que alojan almacenes de datos NFS para VMware se agregan en BlueXP.
- La resolución de DNS debe estar vigente cuando se utilizan nombres DNS. De lo contrario, utilice direcciones IP para vCenter.
- La replicación de SnapMirror está configurada para los volúmenes de almacén de datos basados en NFS designados.
- Asegúrese de que el entorno tenga versiones compatibles de vCenter Server y servidores ESXi.

Una vez establecida la conectividad entre los sitios de origen y destino, proceda con los pasos de configuración, que deberían tomar un par de clics y entre 3 y 5 minutos.

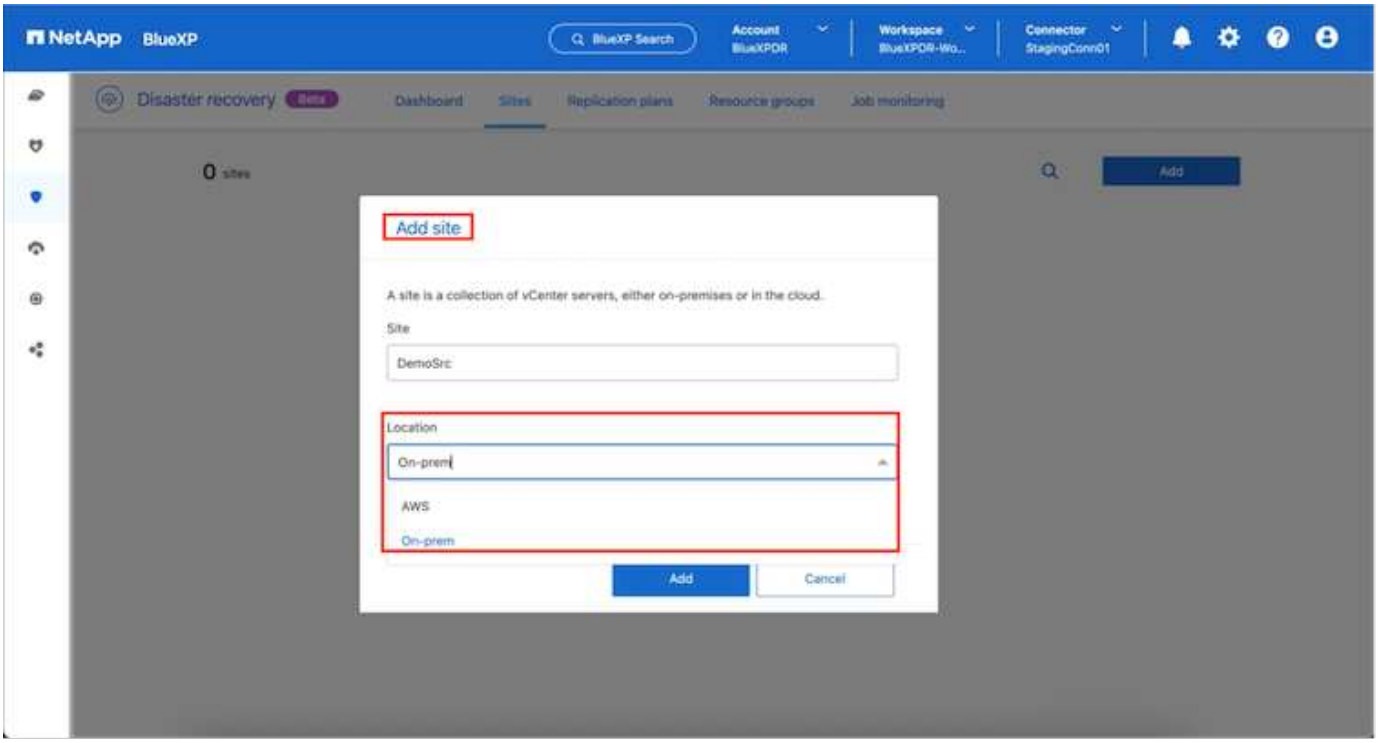
> NetApp recomienda implementar el conector BlueXP en el sitio de destino o en un tercer sitio, para que el conector BlueXP pueda comunicarse a través de la red con los recursos de origen y destino.



Configuración de BlueXP disaster recovery

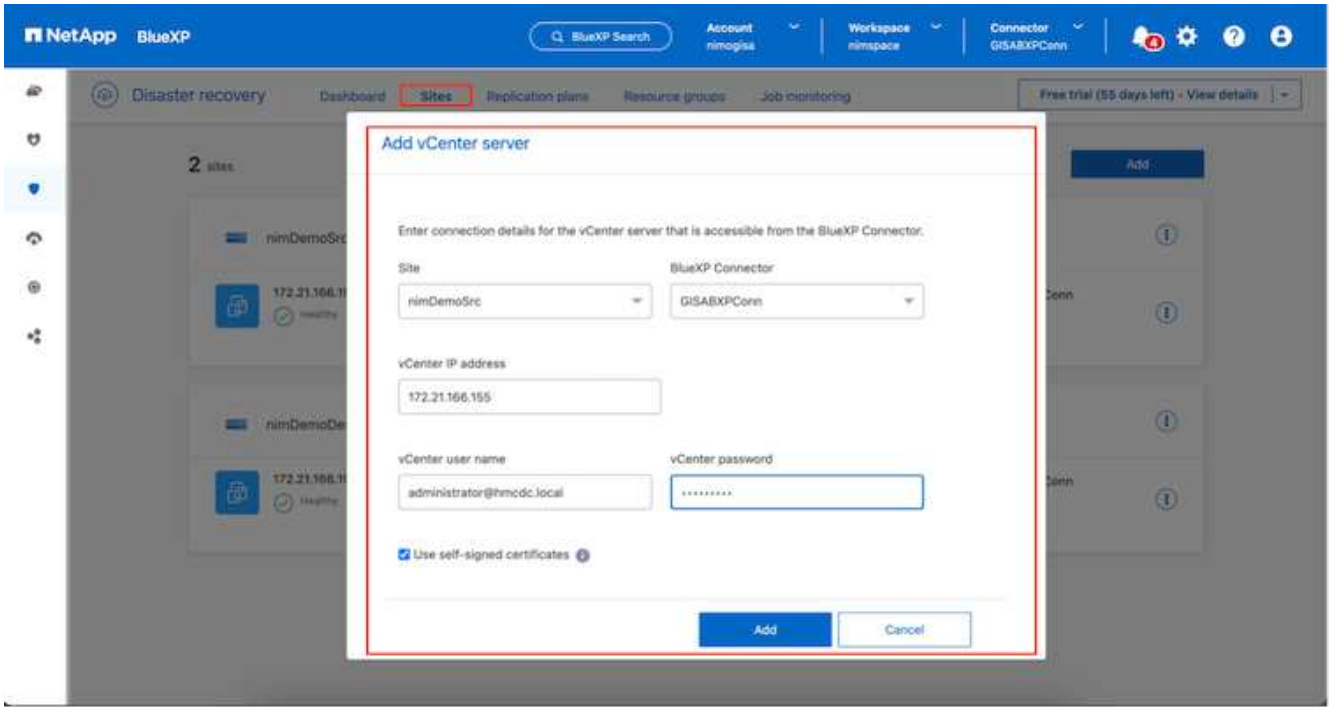
El primer paso para prepararse para la recuperación ante desastres es descubrir y agregar los recursos de almacenamiento y vCenter locales a la BlueXP disaster recovery.

Abra la consola BlueXP y seleccione **Protección > Recuperación ante desastres** en la navegación izquierda. Seleccione **Descubrir servidores vCenter** o utilice el menú superior, seleccione **Sitios > Agregar > Agregar vCenter**.

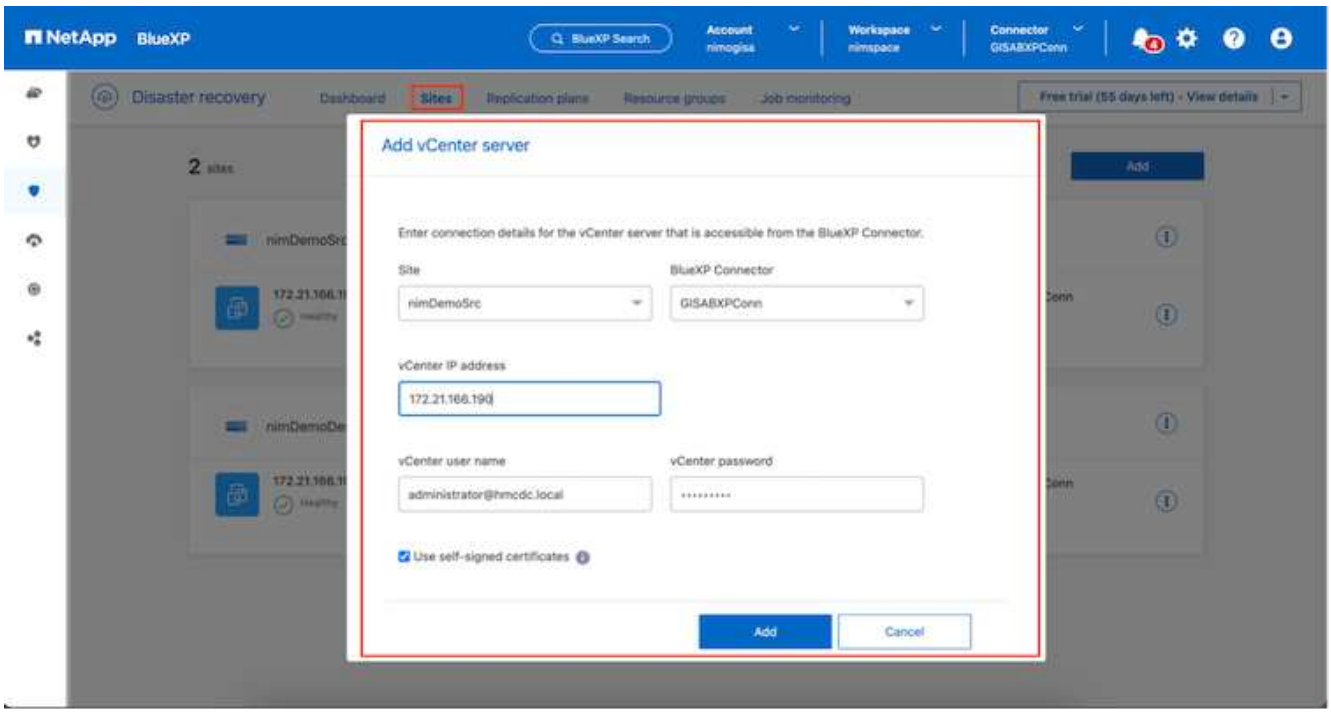


Agregue las siguientes plataformas:

- **Fuente**. vCenter local.



- **Destino**. Centro de datos SDDC de VMC.



Una vez que se agregan los vCenters, se activa el descubrimiento automático.

Configuración de la replicación de almacenamiento entre la matriz del sitio de origen y la matriz del sitio de destino

SnapMirror proporciona replicación de datos en un entorno NetApp . Basada en la tecnología NetApp Snapshot, la replicación de SnapMirror es extremadamente eficiente porque replica solo los bloques que se

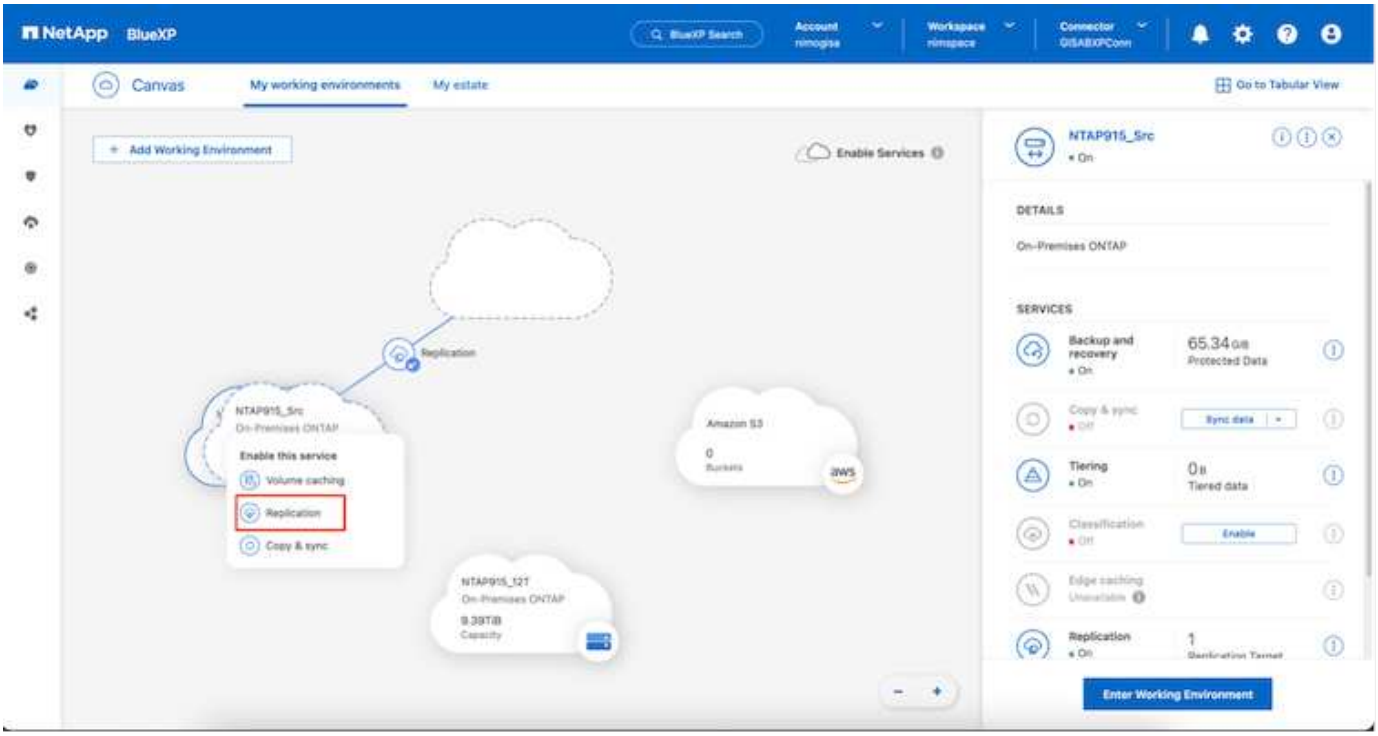
han modificado o agregado desde la actualización anterior. SnapMirror se configura fácilmente mediante NetApp OnCommand System Manager o la CLI de ONTAP . BlueXP DRaaS también crea la relación SnapMirror siempre que el peering de clúster y SVM esté configurado de antemano.

Para los casos en los que el almacenamiento principal no se pierde por completo, SnapMirror proporciona un medio eficiente para resincronizar los sitios primarios y de recuperación ante desastres. SnapMirror puede resincronizar los dos sitios, transfiriendo únicamente datos modificados o nuevos al sitio principal desde el sitio de recuperación ante desastres, simplemente invirtiendo las relaciones de SnapMirror . Esto significa que los planes de replicación en BlueXP DRaaS se pueden resincronizar en cualquier dirección después de una conmutación por error sin tener que volver a copiar todo el volumen. Si una relación se vuelve a sincronizar en la dirección inversa, solo los datos nuevos que se escribieron desde la última sincronización exitosa de la copia de la instantánea se envían de regreso al destino.

> Si la relación SnapMirror ya está configurada para el volumen a través de CLI o el Administrador del sistema, BlueXP DRaaS retoma la relación y continúa con el resto de las operaciones del flujo de trabajo.

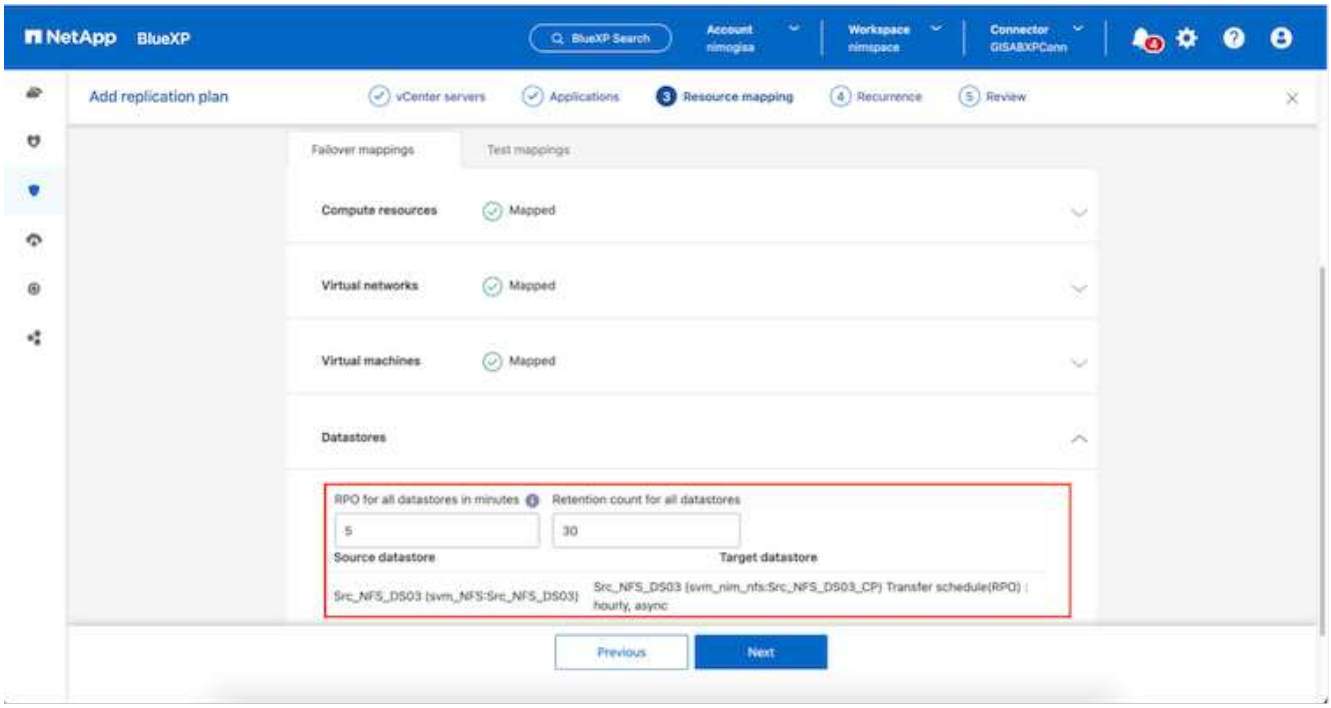
Cómo configurarlo para VMware Disaster Recovery

El proceso para crear la replicación de SnapMirror sigue siendo el mismo para cualquier aplicación. El proceso puede ser manual o automatizado. La forma más sencilla es aprovechar BlueXP para configurar la replicación de SnapMirror mediante el simple arrastrar y soltar del sistema ONTAP de origen en el entorno al destino para activar el asistente que lo guía a través del resto del proceso.



BlueXP DRaaS también puede automatizar lo mismo siempre que se cumplan los dos criterios siguientes:

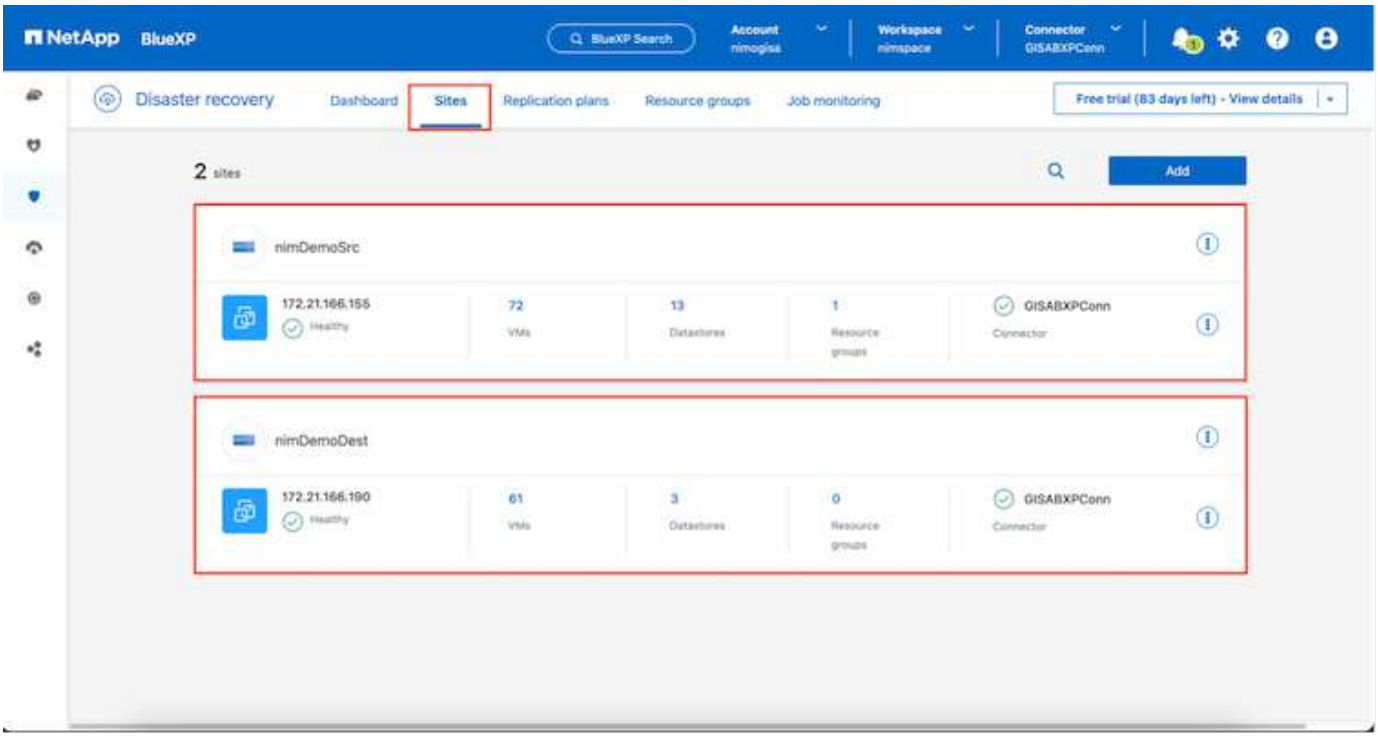
- Los clústeres de origen y destino tienen una relación de pares.
- El SVM de origen y el SVM de destino tienen una relación de pares.



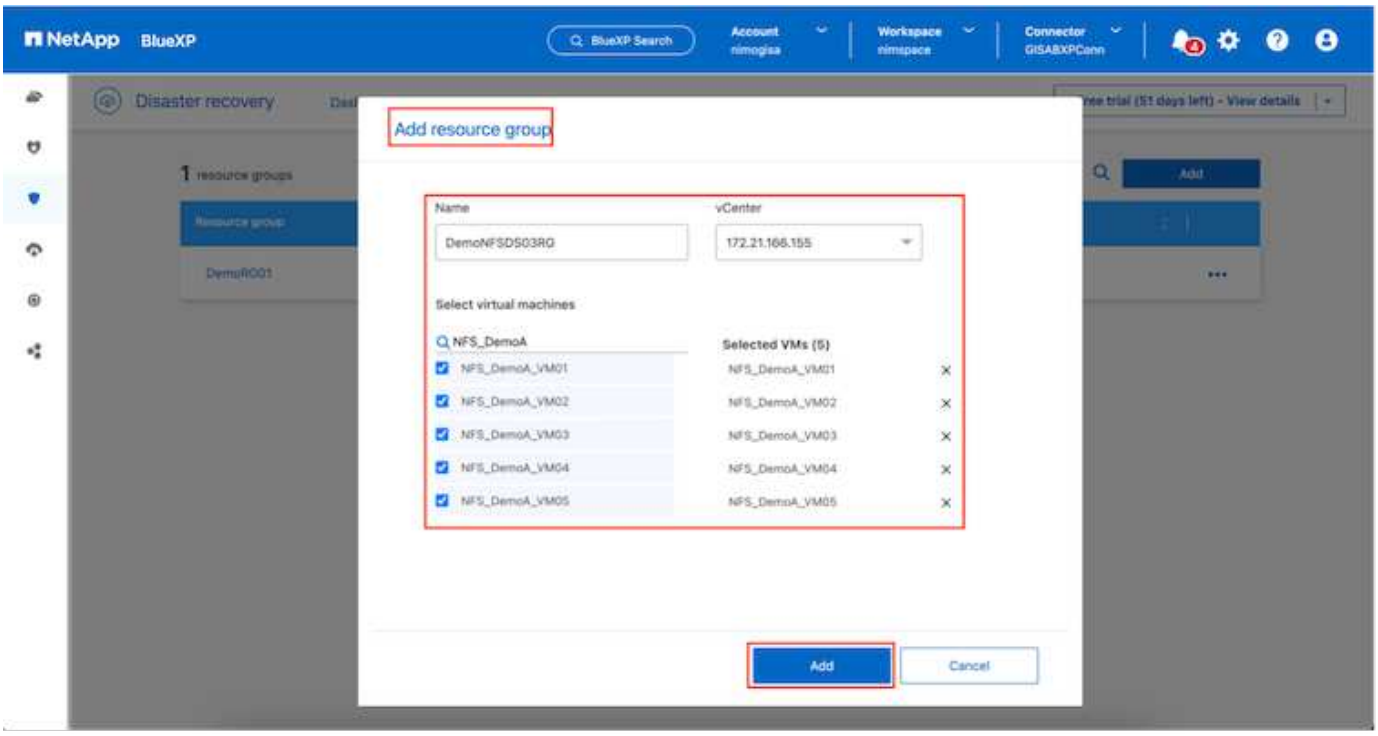
Si la relación SnapMirror ya está configurada para el volumen a través de CLI, BlueXP DRaaS retoma la relación y continúa con el resto de las operaciones del flujo de trabajo.

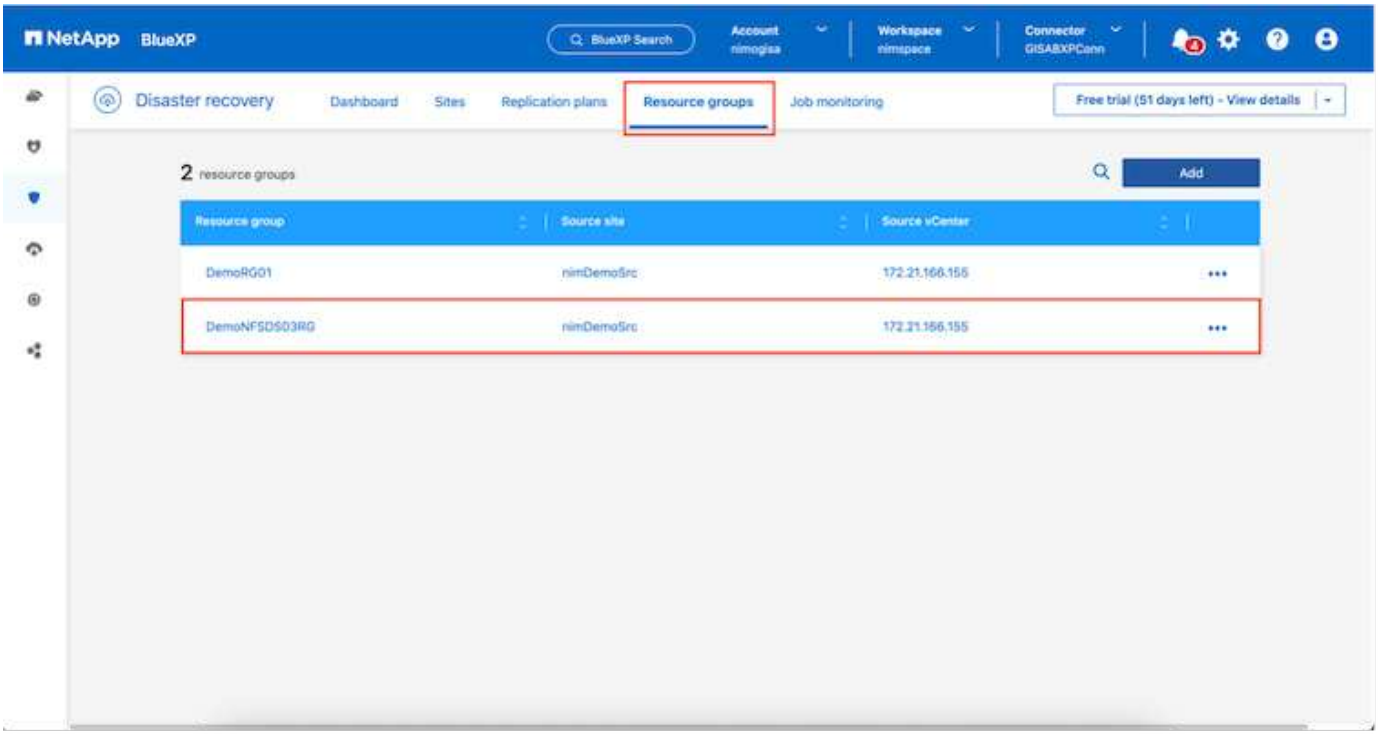
¿Qué puede hacer por usted la BlueXP disaster recovery ?

Una vez agregados los sitios de origen y destino, la BlueXP disaster recovery realiza un descubrimiento profundo automático y muestra las máquinas virtuales junto con los metadatos asociados. La BlueXP disaster recovery también detecta automáticamente las redes y los grupos de puertos utilizados por las máquinas virtuales y los completa.



Una vez agregados los sitios, las máquinas virtuales se pueden agrupar en grupos de recursos. Los grupos de recursos de BlueXP disaster recovery le permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque y los retrasos de arranque que se pueden ejecutar durante la recuperación. Para comenzar a crear grupos de recursos, navegue a **Grupos de recursos** y haga clic en **Crear nuevo grupo de recursos**.

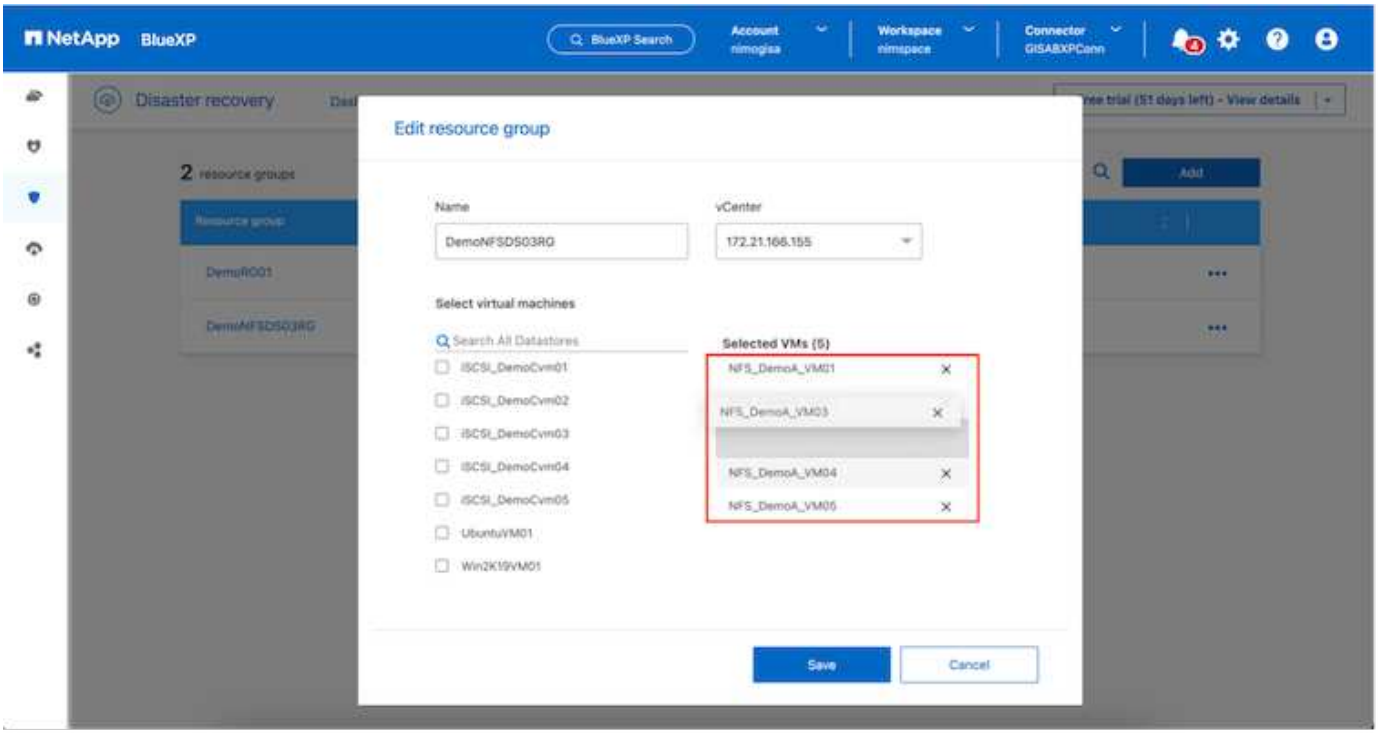




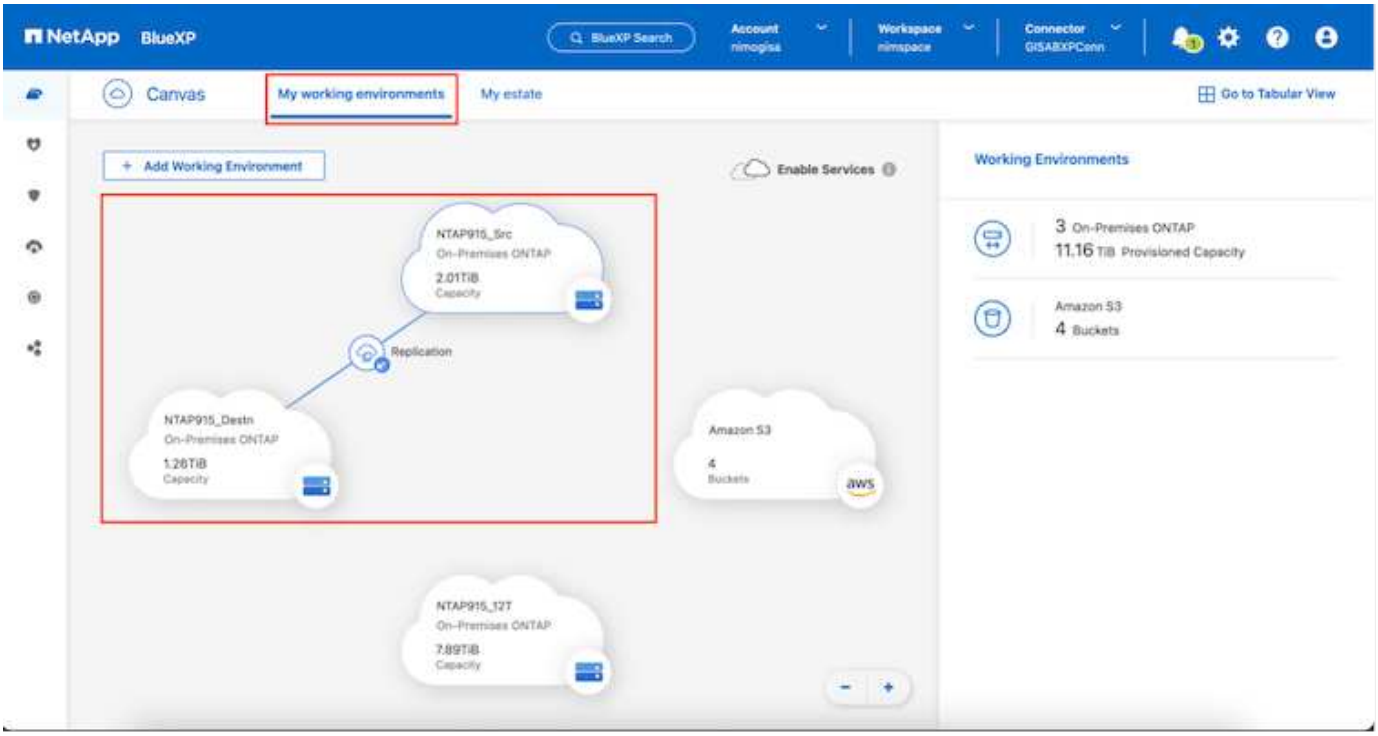
El grupo de recursos también se puede crear mientras se crea un plan de replicación.

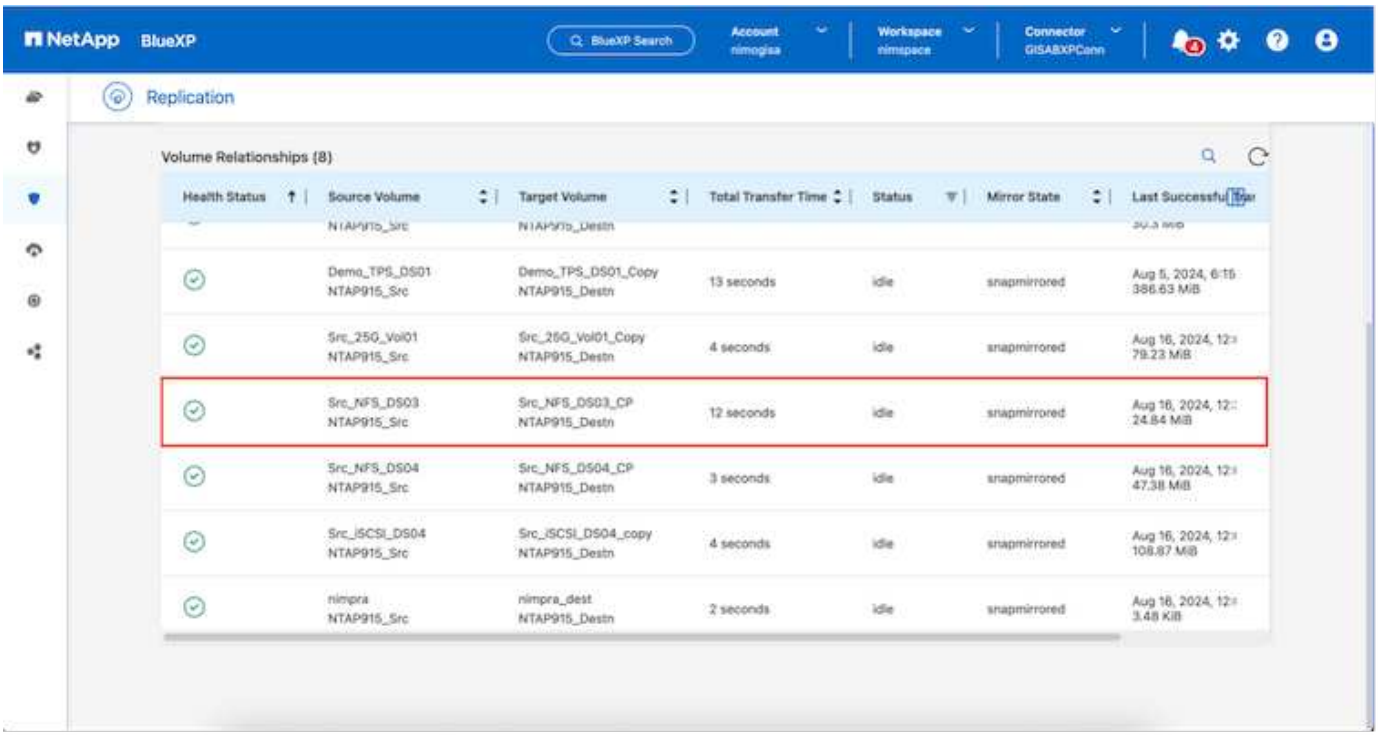
El orden de arranque de las máquinas virtuales se puede definir o modificar durante la creación de grupos de

recursos mediante un simple mecanismo de arrastrar y soltar.



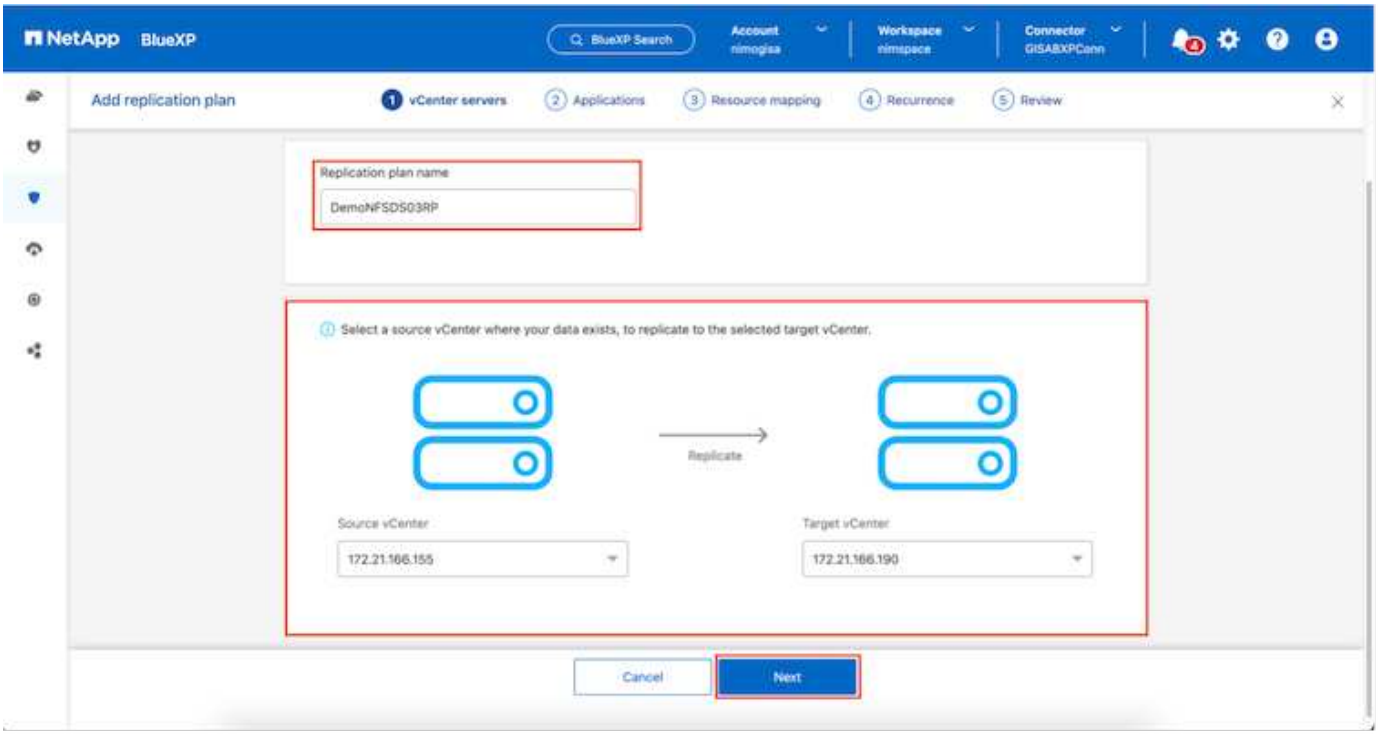
Una vez creados los grupos de recursos, el siguiente paso es crear el plan de ejecución o un plan para recuperar máquinas virtuales y aplicaciones en caso de desastre. Como se menciona en los requisitos previos, la replicación de SnapMirror se puede configurar de antemano o DRaaS puede configurarla utilizando el RPO y el recuento de retención especificados durante la creación del plan de replicación.





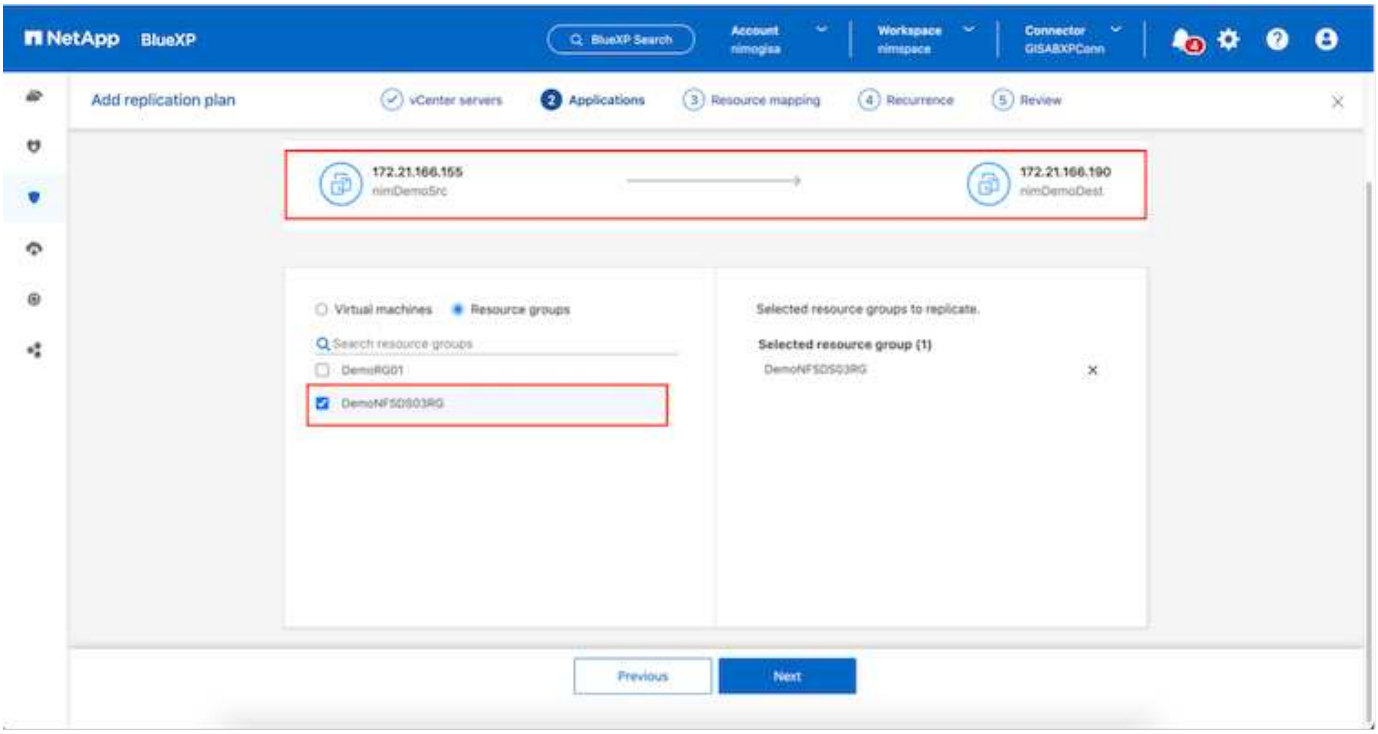
Configure el plan de replicación seleccionando las plataformas vCenter de origen y destino en el menú desplegable y elija los grupos de recursos que se incluirán en el plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones y el mapeo de clústeres y redes. Para definir el plan de recuperación, navegue a la pestaña **Plan de replicación** y haga clic en **Agregar plan**.

Primero, seleccione el vCenter de origen y luego seleccione el vCenter de destino.



El siguiente paso es seleccionar los grupos de recursos existentes. Si no se crean grupos de recursos, el asistente ayuda a agrupar las máquinas virtuales necesarias (básicamente, crea grupos de recursos funcionales) en función de los objetivos de recuperación. Esto también ayuda a definir la secuencia de

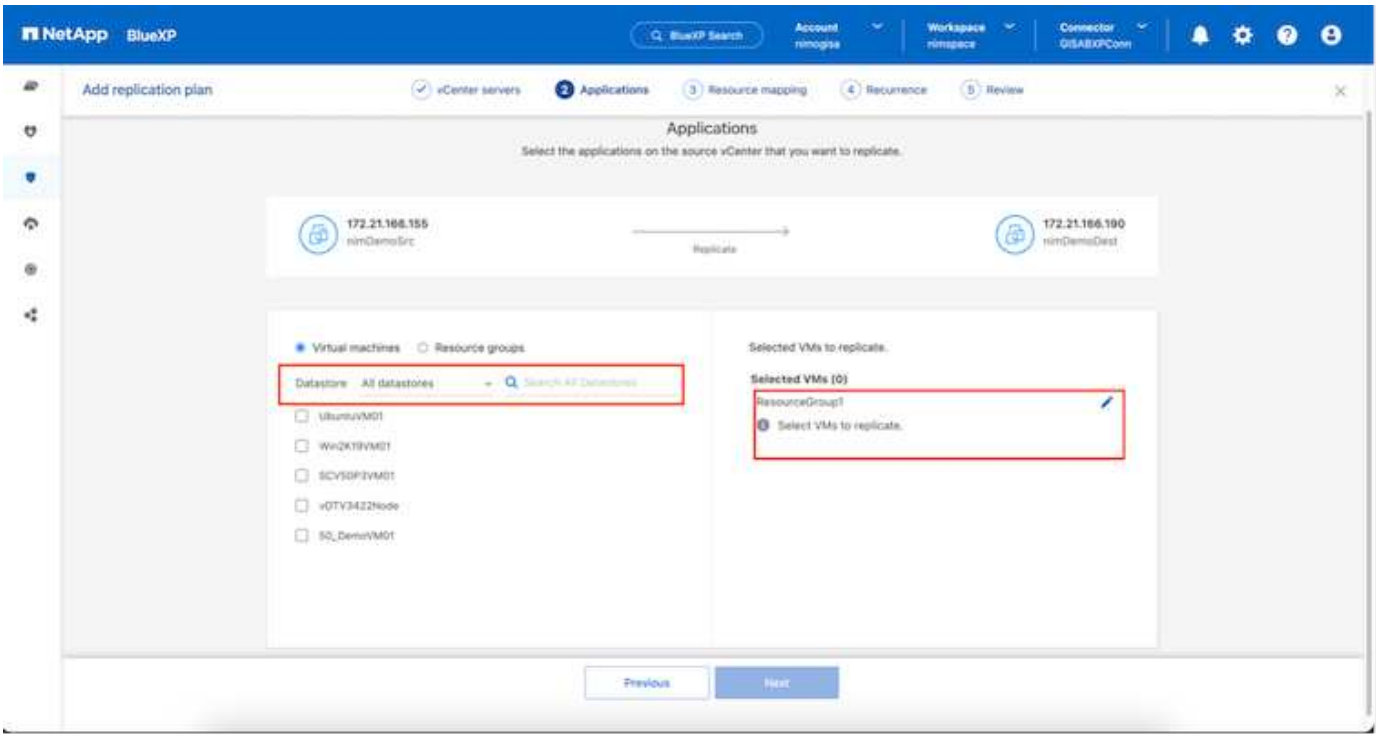
operaciones de cómo se deben restaurar las máquinas virtuales de la aplicación.



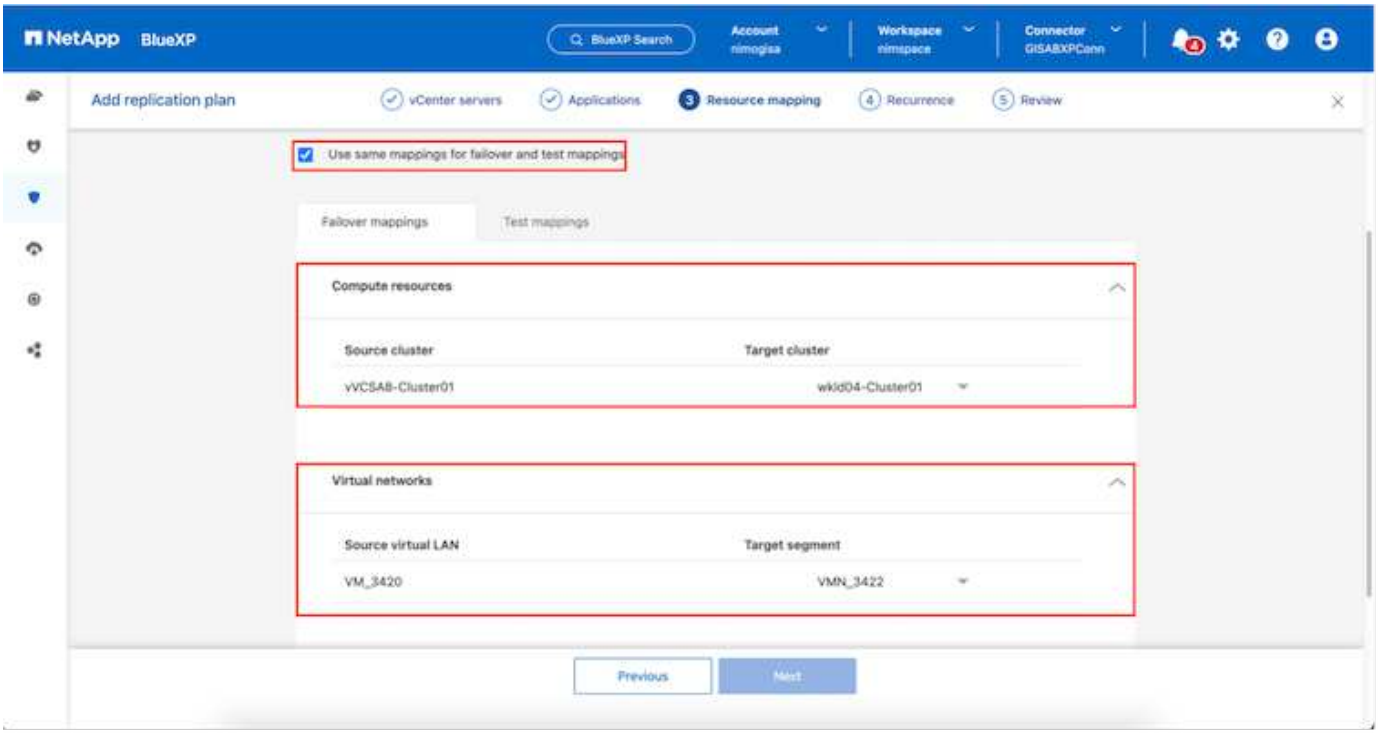
El grupo de recursos permite establecer el orden de arranque mediante la funcionalidad de arrastrar y soltar. Se puede utilizar para modificar fácilmente el orden en que se encenderán las máquinas virtuales durante el proceso de recuperación.

Cada máquina virtual dentro de un grupo de recursos se inicia en secuencia según el orden. Se inician dos grupos de recursos en paralelo.

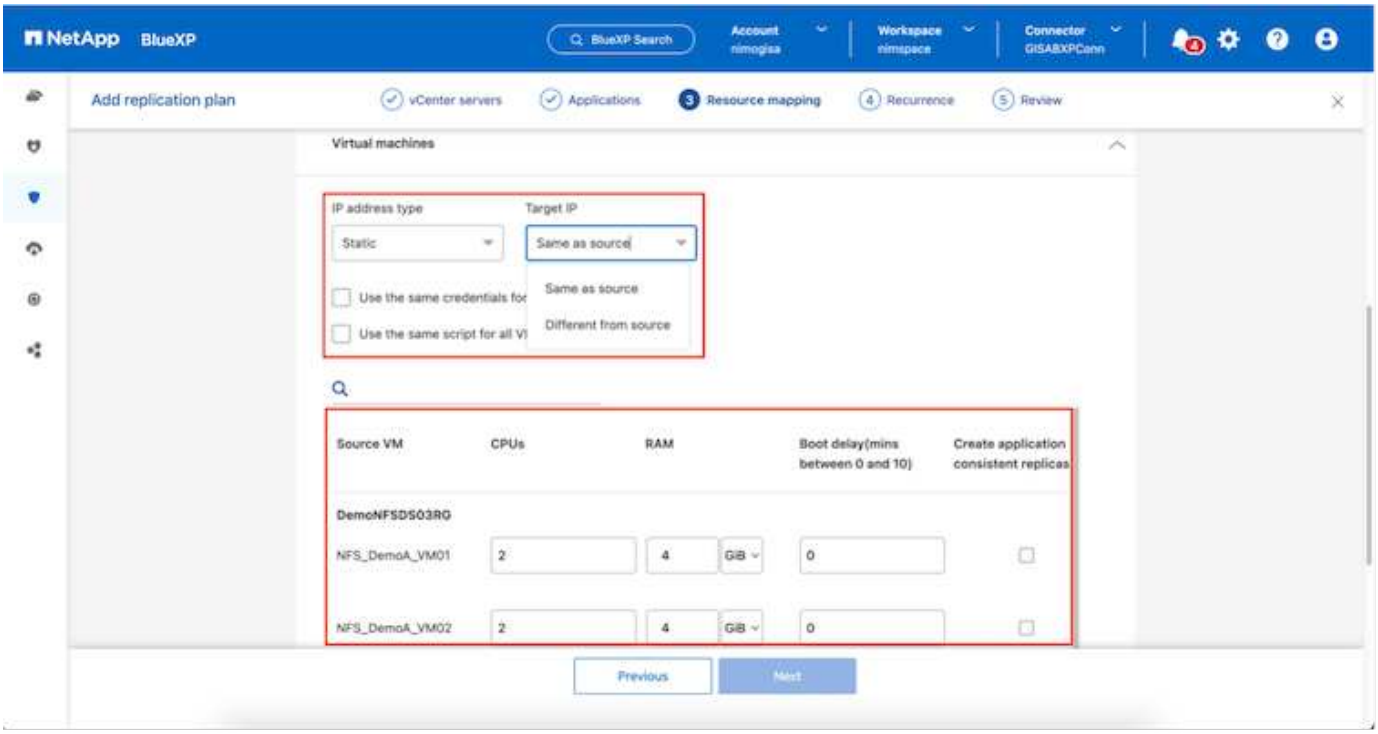
La siguiente captura de pantalla muestra la opción para filtrar máquinas virtuales o almacenes de datos específicos según los requisitos organizativos si no se crean grupos de recursos de antemano.



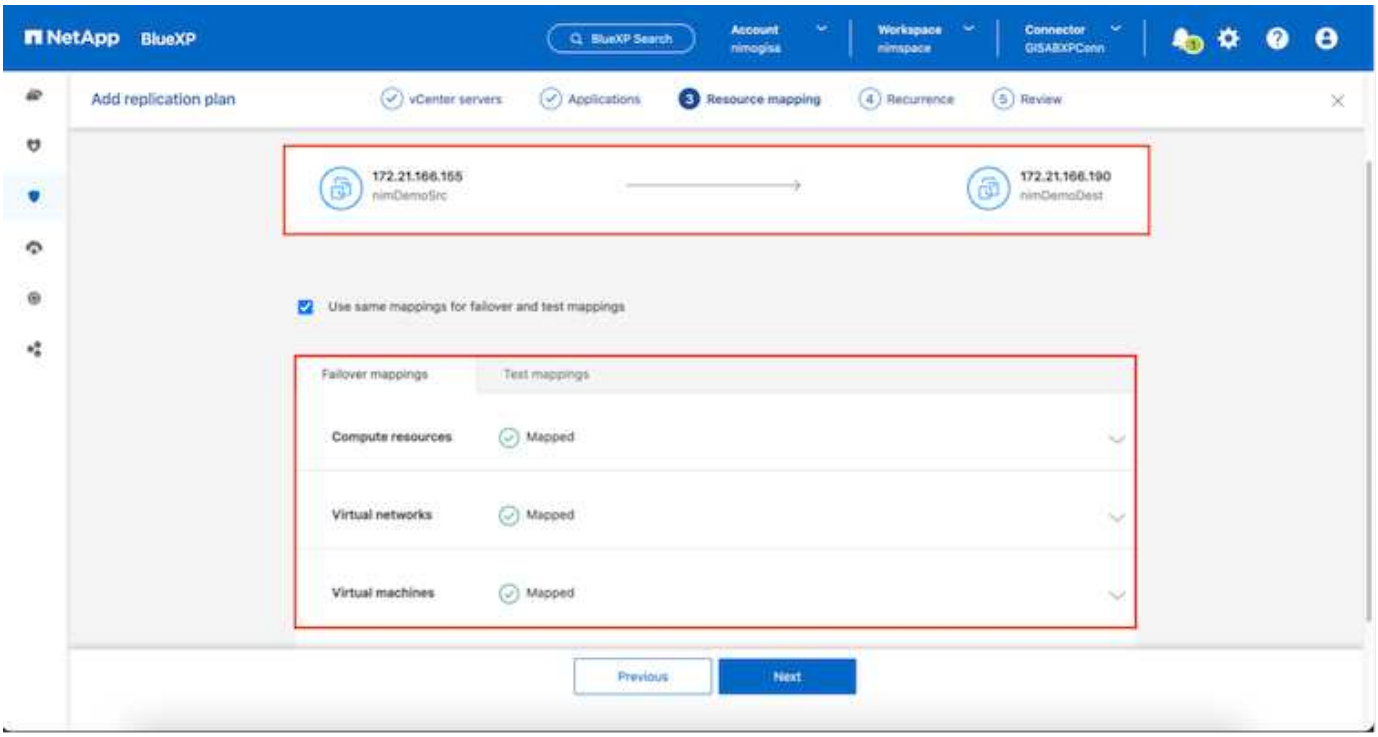
Una vez seleccionados los grupos de recursos, cree las asignaciones de conmutación por error. En este paso, especifique cómo se asignan los recursos del entorno de origen al destino. Esto incluye recursos computacionales y redes virtuales. Personalización de IP, scripts previos y posteriores, retrasos en el arranque, consistencia de la aplicación, etc. Para obtener información detallada, consulte"Crear un plan de replicación" .



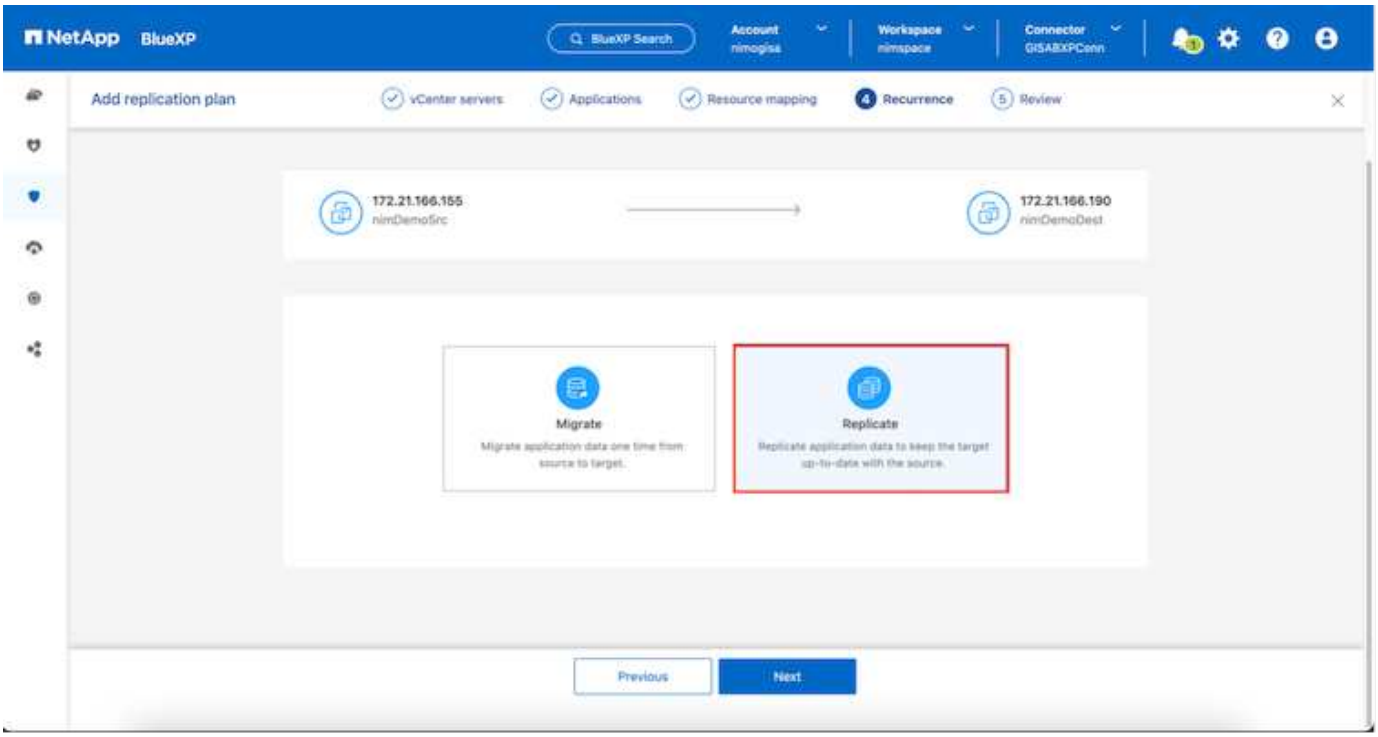
De forma predeterminada, se utilizan los mismos parámetros de mapeo para las operaciones de prueba y de conmutación por error. Para configurar diferentes asignaciones para el entorno de prueba, seleccione la opción Asignación de prueba después de desmarcar la casilla de verificación como se muestra a continuación:



Una vez completado el mapeo de recursos, haga clic en Siguiente.

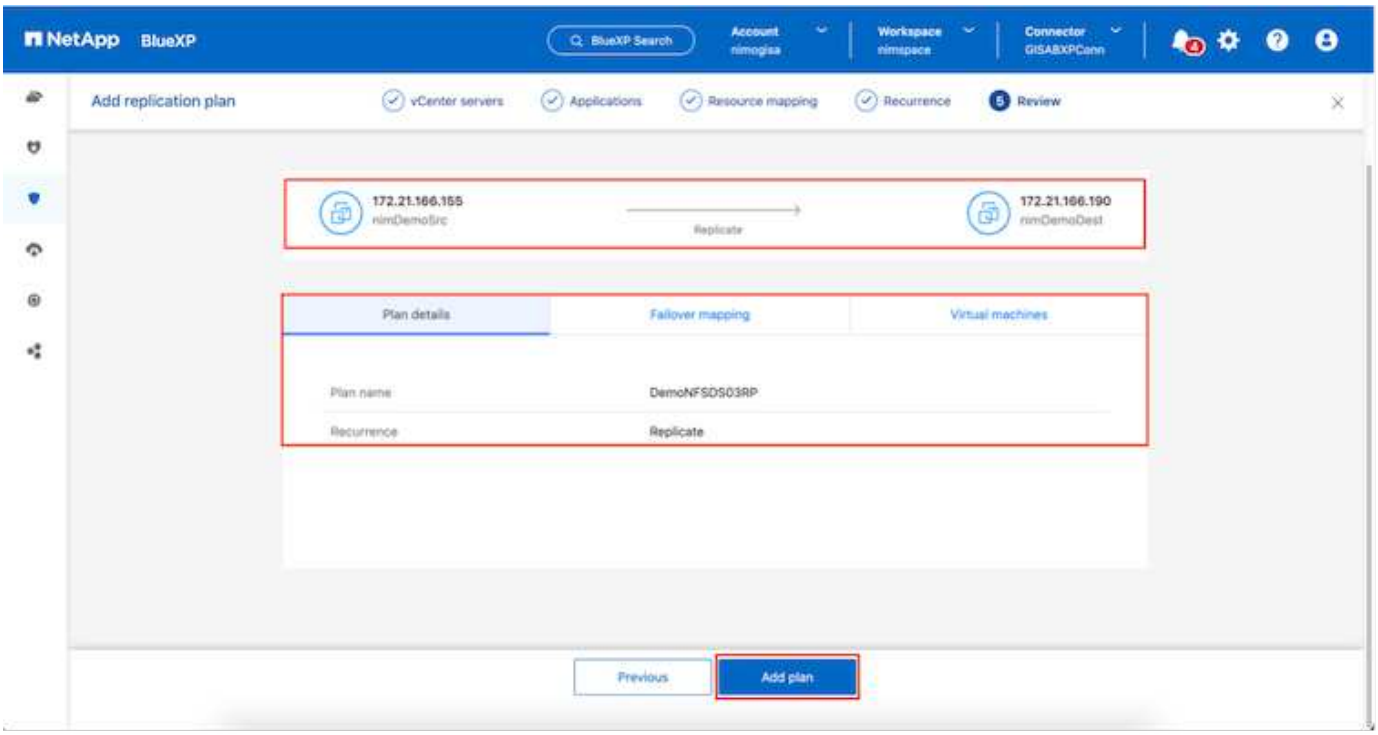


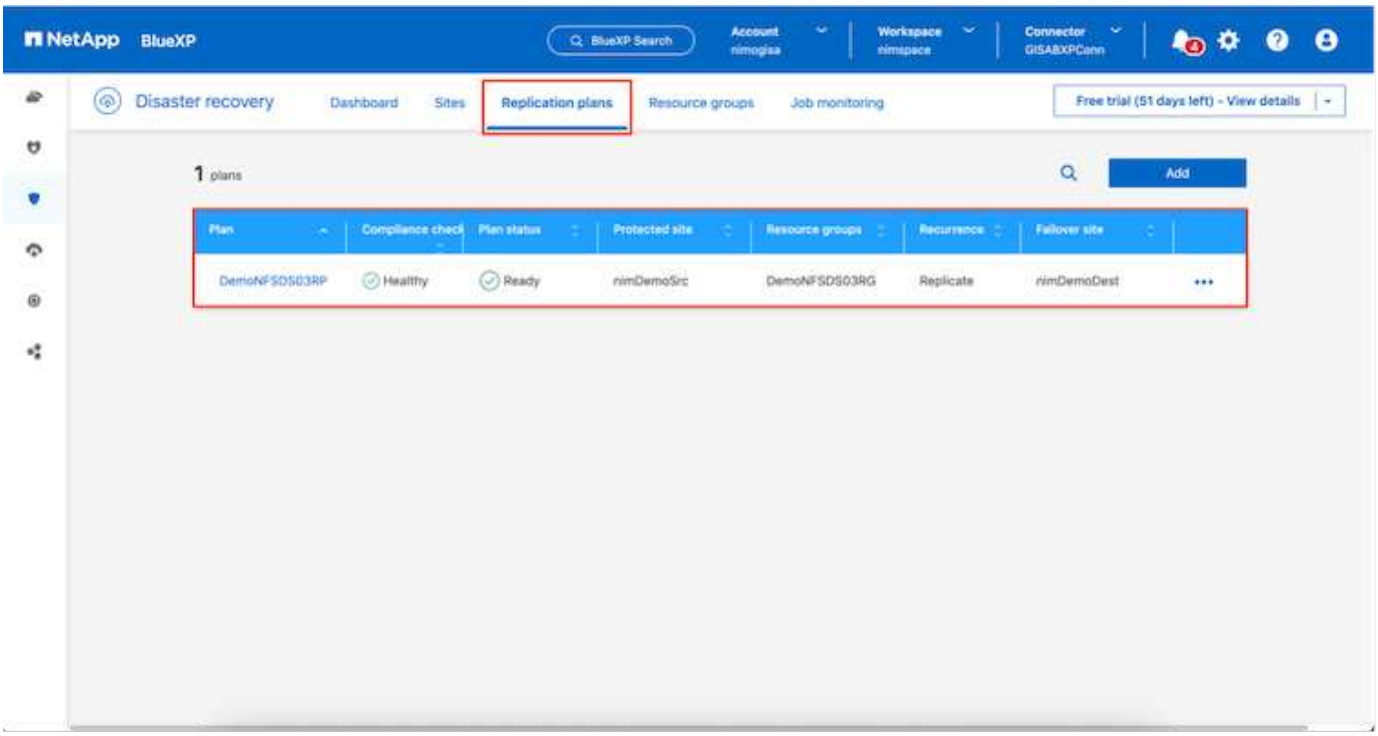
Seleccione el tipo de recurrencia. En palabras simples, seleccione la opción Migrar (migración única mediante conmutación por error) o replicación continua recurrente. En este tutorial, se selecciona la opción Replicar.



Una vez hecho esto, revise los mapeos creados y luego haga clic en **Agregar plan**.

> Se pueden incluir máquinas virtuales de diferentes volúmenes y SVM en un plan de replicación. Dependiendo de la ubicación de la VM (ya sea en el mismo volumen o en un volumen separado dentro de la misma SVM, volúmenes separados en diferentes SVM), la BlueXP disaster recovery crea una instantánea de grupo de consistencia.



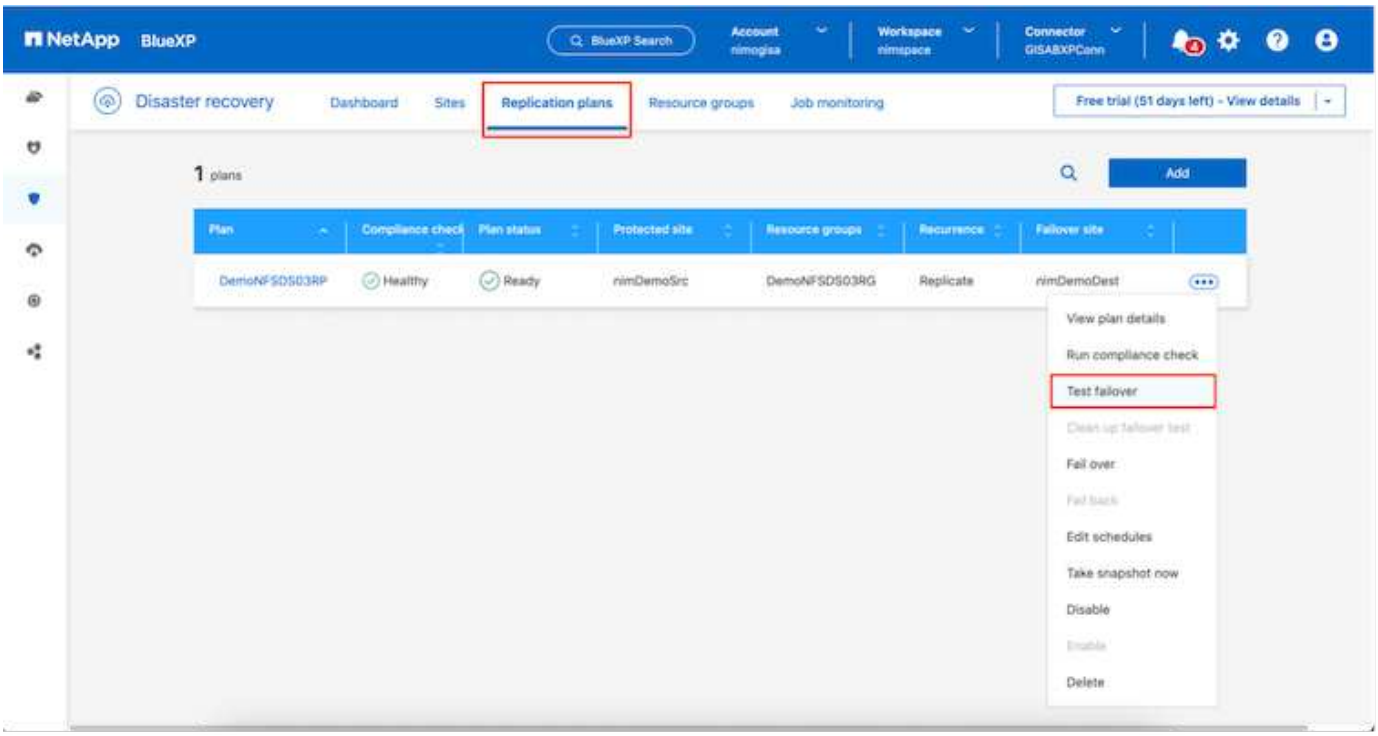


BlueXP DRaaS consta de los siguientes flujos de trabajo:

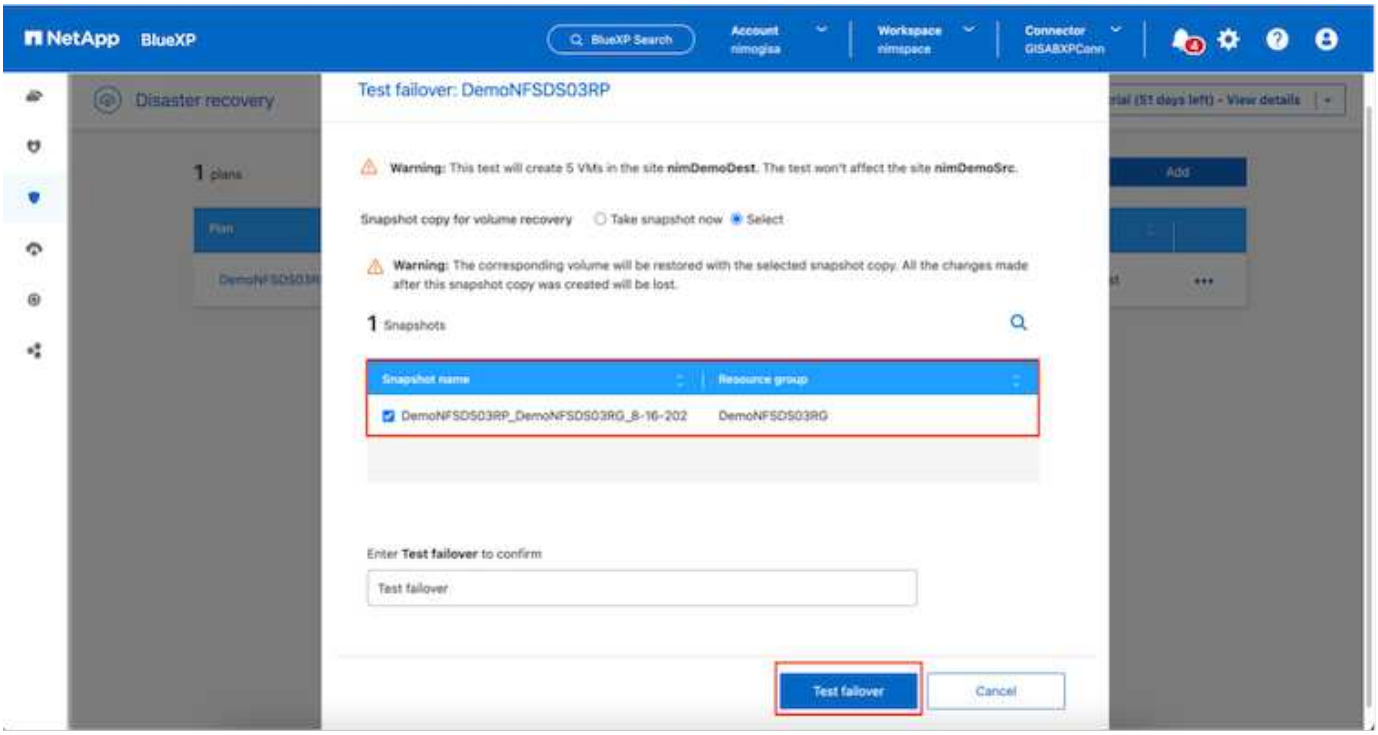
- Conmutación por error de prueba (incluidas simulaciones automatizadas periódicas)
- Prueba de conmutación por error de limpieza
- Conmutación por error
- Recuperación por recuperación

Prueba de conmutación por error

La conmutación por error de prueba en BlueXP DRaaS es un procedimiento operativo que permite a los administradores de VMware validar completamente sus planes de recuperación sin interrumpir sus entornos de producción.



BlueXP DRaaS incorpora la capacidad de seleccionar la instantánea como una capacidad opcional en la operación de conmutación por error de prueba. Esta capacidad permite al administrador de VMware verificar que cualquier cambio realizado recientemente en el entorno se replique en el sitio de destino y, por lo tanto, esté presente durante la prueba. Estos cambios incluyen parches para el sistema operativo invitado de la máquina virtual.

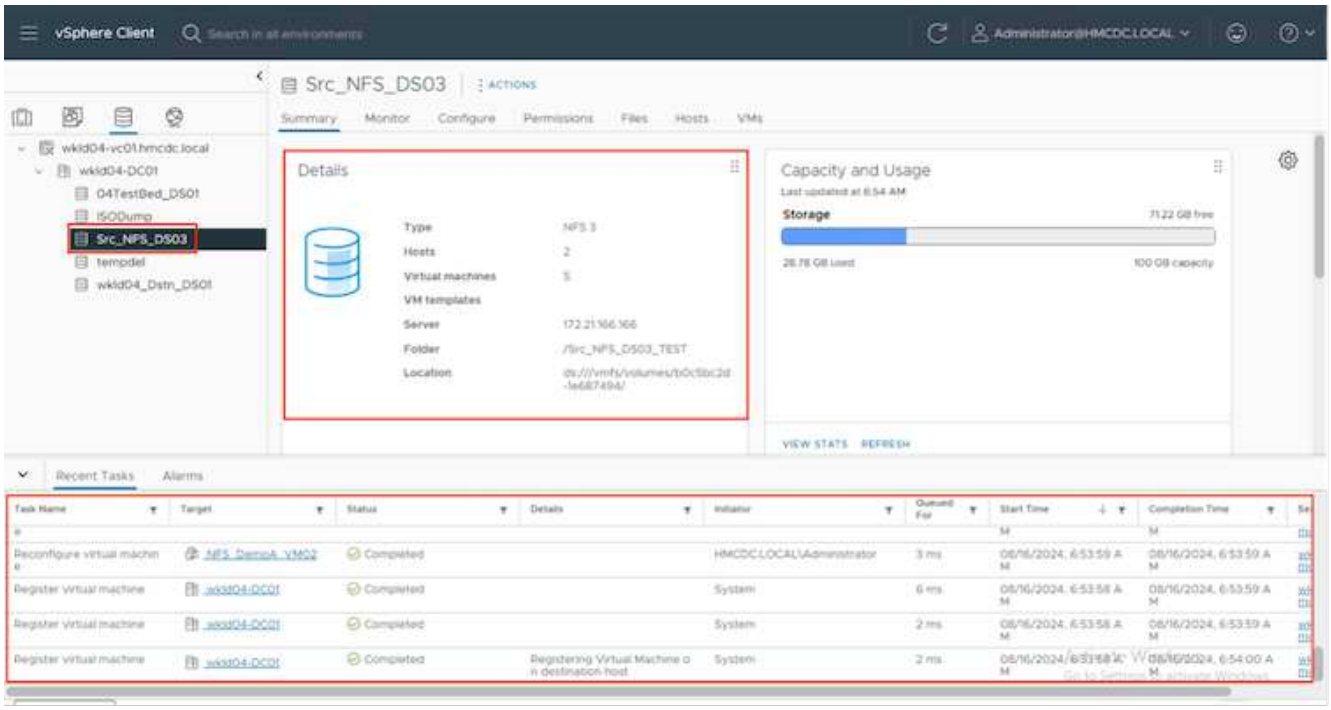


Cuando el administrador de VMware ejecuta una operación de conmutación por error de prueba, BlueXP DRaaS automatiza las siguientes tareas:

- Activar relaciones de SnapMirror para actualizar el almacenamiento en el sitio de destino con cualquier

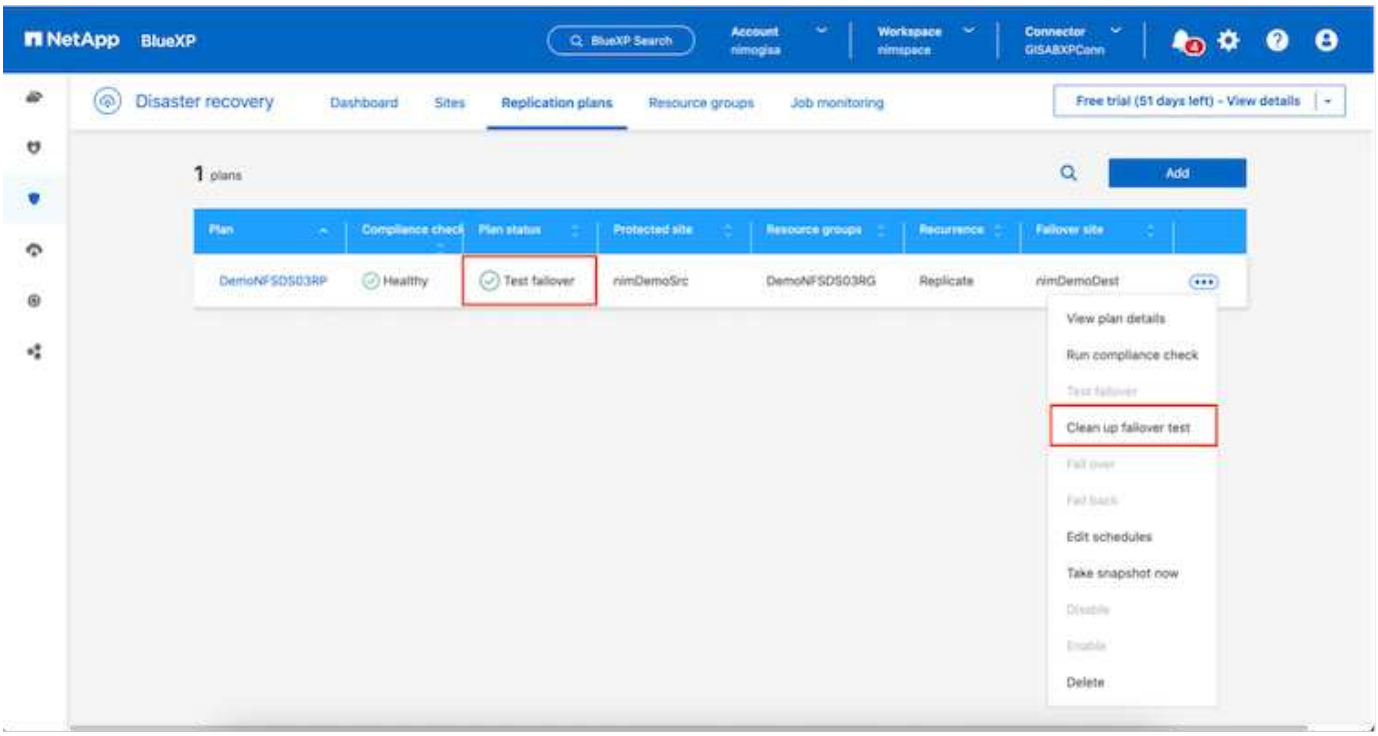
cambio reciente que se haya realizado en el sitio de producción.

- Creación de volúmenes NetApp FlexClone de los volúmenes FlexVol en la matriz de almacenamiento DR.
- Conexión de los almacenes de datos NFS en los volúmenes FlexClone a los hosts ESXi en el sitio de recuperación ante desastres.
- Conectar los adaptadores de red de la máquina virtual a la red de prueba especificada durante la asignación.
- Reconfigurar la configuración de red del sistema operativo invitado de la máquina virtual según lo definido para la red en el sitio de recuperación ante desastres.
- Ejecutar cualquier comando personalizado que se haya almacenado en el plan de replicación.
- Encender las máquinas virtuales en el orden definido en el plan de replicación.



Operación de prueba de conmutación por error de limpieza

La operación de prueba de conmutación por error de limpieza se produce después de que se haya completado la prueba del plan de replicación y el administrador de VMware responda al mensaje de limpieza.



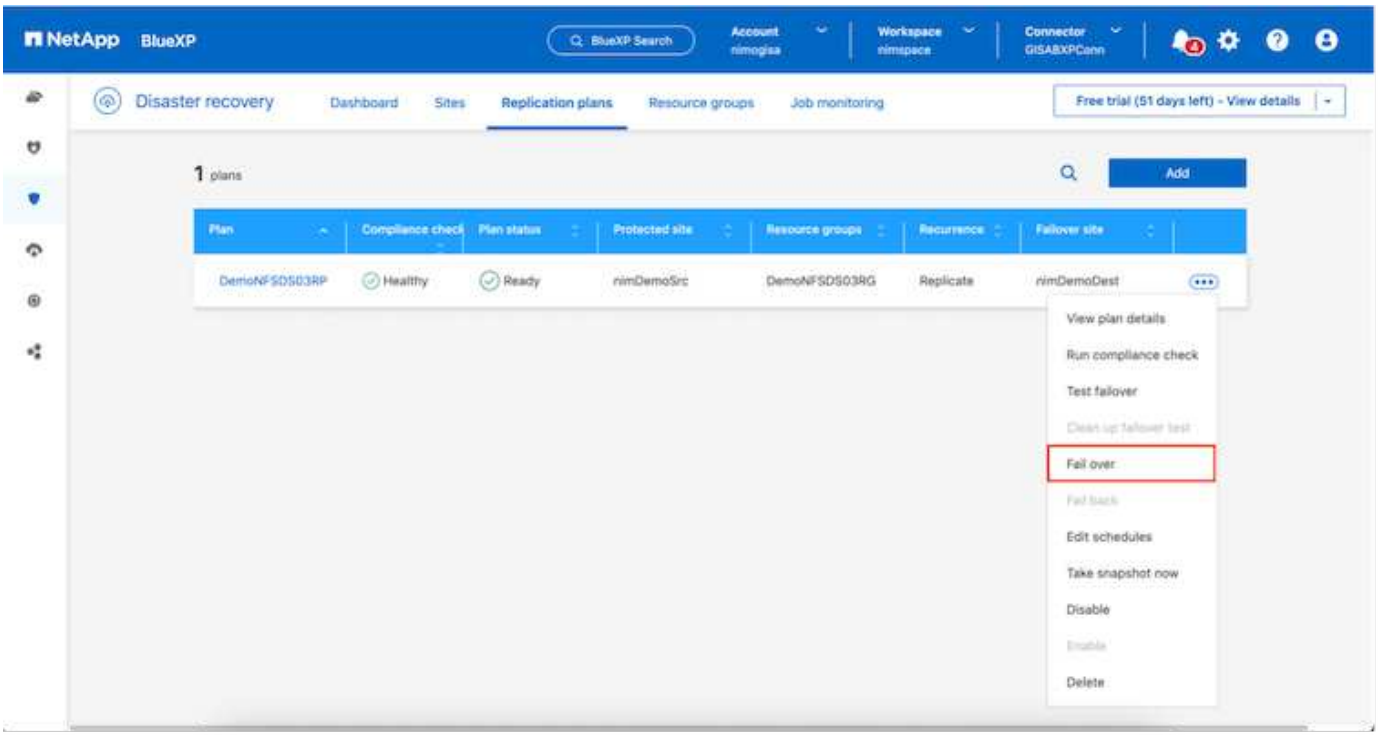
Esta acción restablecerá las máquinas virtuales (VM) y el estado del plan de replicación al estado listo.

Cuando el administrador de VMware realiza una operación de recuperación, BlueXP DRaaS completa el siguiente proceso:

1. Apaga cada VM recuperada en la copia FlexClone que se utilizó para la prueba.
2. Elimina el volumen FlexClone que se utilizó para presentar las máquinas virtuales recuperadas durante la prueba.

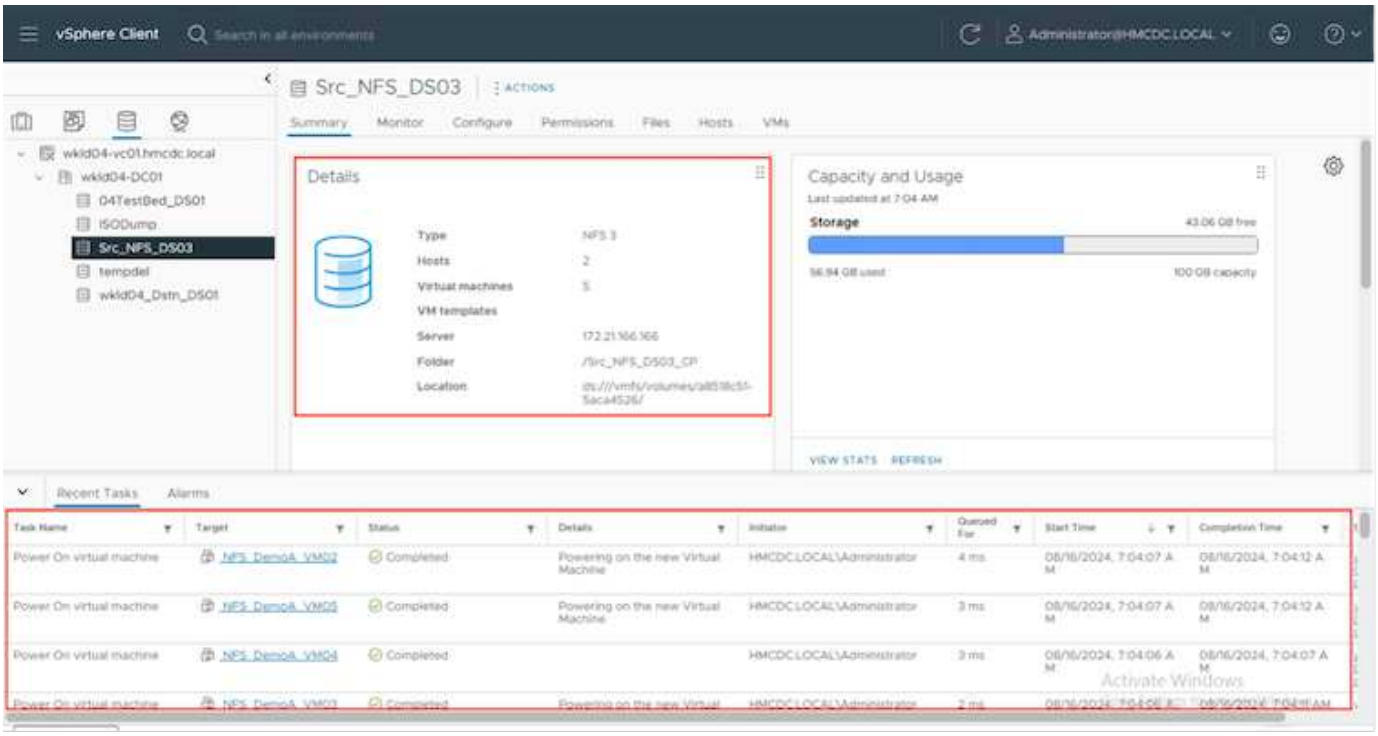
Migración planificada y conmutación por error

BlueXP DRaaS tiene dos métodos para realizar una conmutación por error real: migración planificada y conmutación por error. El primer método, la migración planificada, incorpora el apagado de la máquina virtual y la sincronización de la replicación del almacenamiento en el proceso para recuperar o mover eficazmente las máquinas virtuales al sitio de destino. La migración planificada requiere acceso al sitio de origen. El segundo método, conmutación por error, es una conmutación por error planificada/no planificada en la que las máquinas virtuales se recuperan en el sitio de destino desde el último intervalo de replicación de almacenamiento que pudo completarse. Dependiendo del RPO que se diseñó en la solución, se puede esperar cierta cantidad de pérdida de datos en el escenario de recuperación ante desastres.



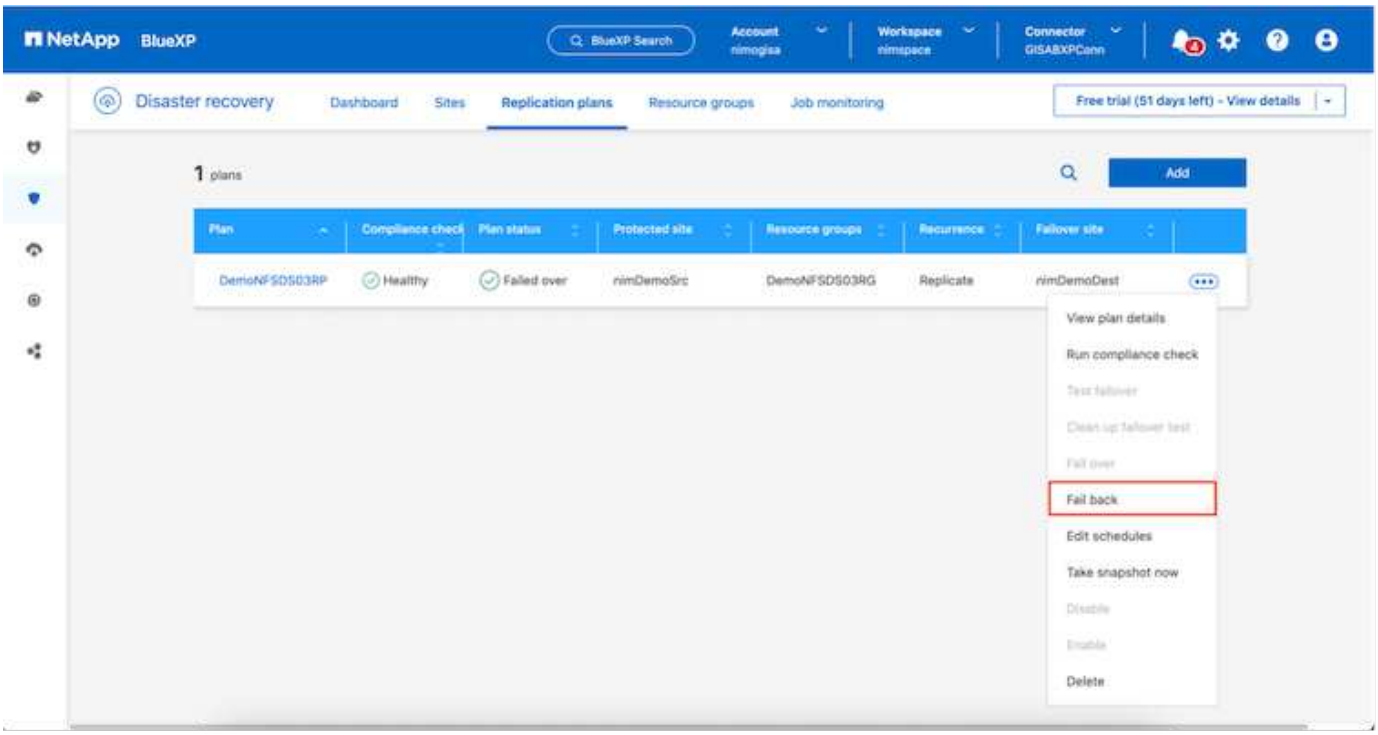
Cuando el administrador de VMware realiza una operación de conmutación por error, BlueXP DRaaS automatiza las siguientes tareas:

- Romper y conmutar por error las relaciones de NetApp SnapMirror .
- Conecte los almacenes de datos NFS replicados a los hosts ESXi en el sitio de recuperación ante desastres.
- Conecte los adaptadores de red de la máquina virtual a la red del sitio de destino apropiado.
- Reconfigure la configuración de red del sistema operativo invitado de la máquina virtual según lo definido para la red en el sitio de destino.
- Ejecute cualquier comando personalizado (si hay alguno) que se haya almacenado en el plan de replicación.
- Encienda las máquinas virtuales en el orden definido en el plan de replicación.



Recuperación por recuperación

Una conmutación por recuperación es un procedimiento opcional que restaura la configuración original de los sitios de origen y destino después de una recuperación.



Los administradores de VMware pueden configurar y ejecutar un procedimiento de conmutación por error cuando estén listos para restaurar los servicios en el sitio de origen original.

NOTA: BlueXP DRaaS replica (resincroniza) cualquier cambio en la máquina virtual de origen original antes de revertir la dirección de replicación. Este proceso comienza a partir de una relación que ha completado la

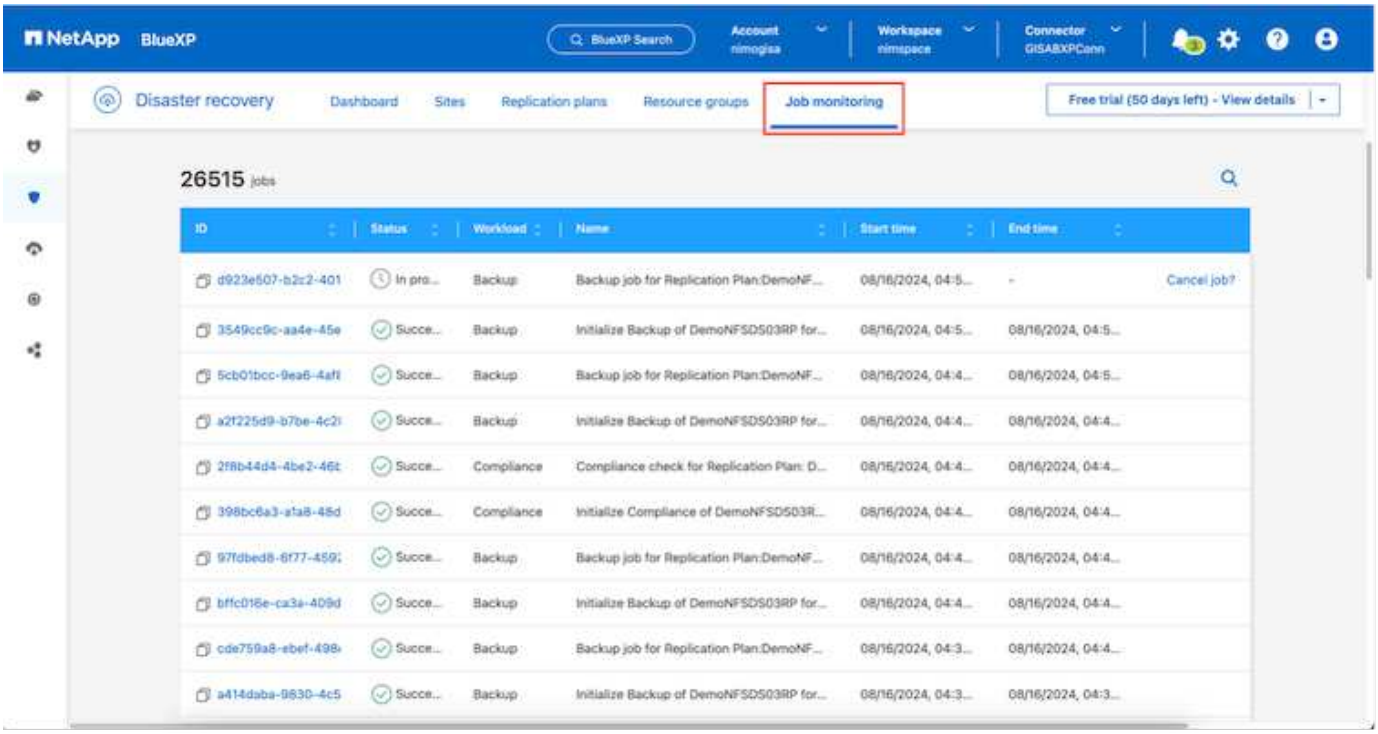
conmutación por error a un destino e implica los siguientes pasos:

- Apague y anule el registro de las máquinas virtuales y los volúmenes en el sitio de destino se desmontan.
- Romper la relación SnapMirror en la fuente original se rompe para hacerla de lectura/escritura.
- Vuelva a sincronizar la relación SnapMirror para revertir la replicación.
- Monte el volumen en la fuente, encienda y registre las máquinas virtuales de origen.

Para obtener más detalles sobre cómo acceder y configurar BlueXP DRaaS, consulte la"Obtenga más información sobre BlueXP Disaster Recovery para VMware" .

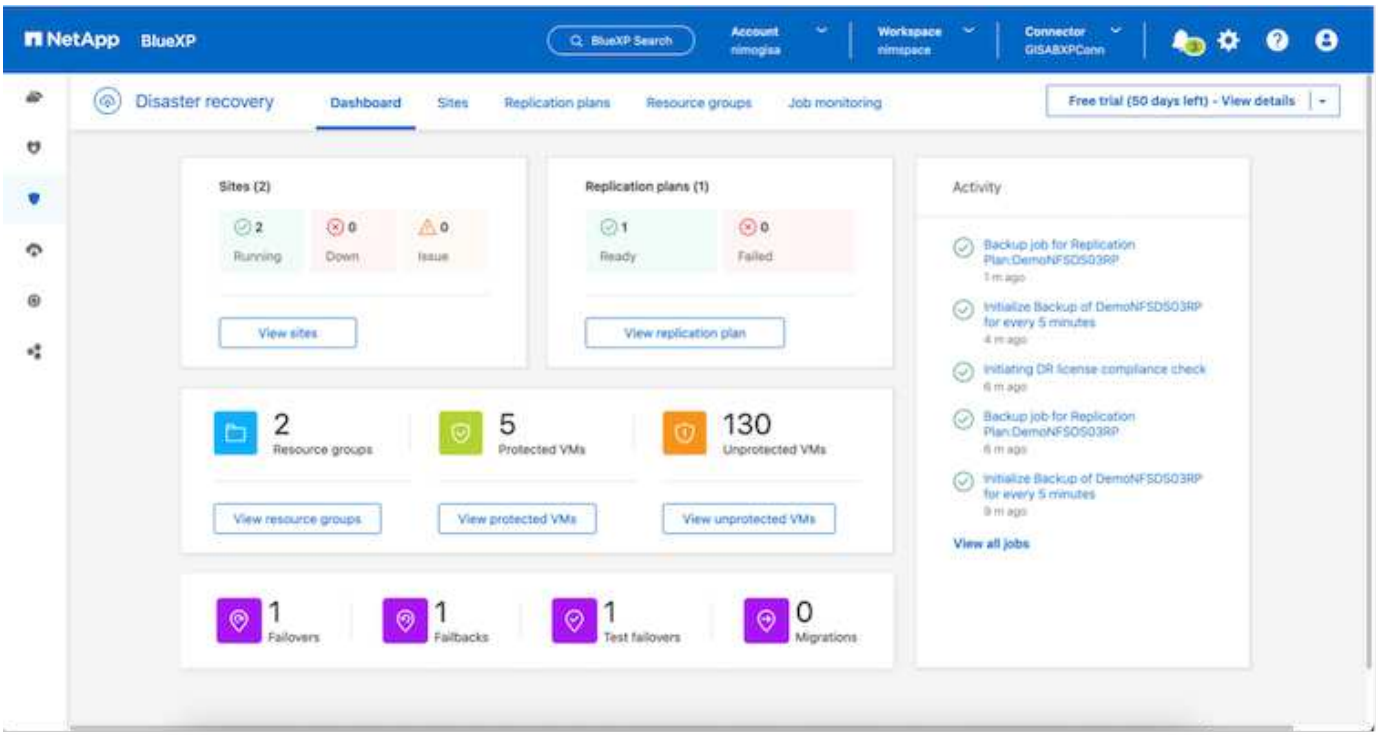
Monitoreo y tablero de control

Desde BlueXP o la CLI de ONTAP , puede supervisar el estado de salud de la replicación para los volúmenes de almacén de datos adecuados, y el estado de una conmutación por error o de una conmutación por error de prueba se puede rastrear a través de la Supervisión de trabajos.



Si un trabajo está actualmente en progreso o en cola y desea detenerlo, existe una opción para cancelarlo.

Con el panel de BlueXP disaster recovery , evalúe con confianza el estado de los sitios de recuperación ante desastres y los planes de replicación. Esto permite a los administradores identificar rápidamente sitios y planes saludables, desconectados o degradados.



Esto proporciona una solución poderosa para gestionar un plan de recuperación ante desastres personalizado y adaptado. La conmutación por error se puede realizar de forma planificada o con solo hacer clic en un botón cuando ocurre un desastre y se toma la decisión de activar el sitio de recuperación ante desastres.

Para obtener más información sobre este proceso, no dude en seguir el video tutorial detallado o utilizar el"simulador de soluciones" .

Proteja las cargas de trabajo con vSphere Metro Storage Cluster

Obtenga información sobre la integración de la alta disponibilidad de ONTAP con VMware vSphere Metro Storage Cluster (vMSC)

Obtenga información sobre las soluciones de NetApp que puede utilizar para integrar la alta disponibilidad de NetApp ONTAP con VMware vSphere Metro Storage Cluster (vMSC). Esto proporciona soluciones sólidas para la gestión de VMware Cloud Foundation (VCF) y los dominios de carga de trabajo de VI.

Esta combinación garantiza la disponibilidad continua de datos, conmutación por error sin inconvenientes y recuperación ante desastres en sitios dispersos geográficamente, lo que mejora la resiliencia y la continuidad operativa para cargas de trabajo críticas. La sincronización activa de SnapMirror permite que los servicios comerciales sigan funcionando incluso en caso de una falla total del sitio y permite que las aplicaciones conmuten por error de forma transparente mediante una copia secundaria. Con la sincronización activa de SnapMirror , no se requiere intervención manual ni scripts personalizados para activar una conmutación por error.

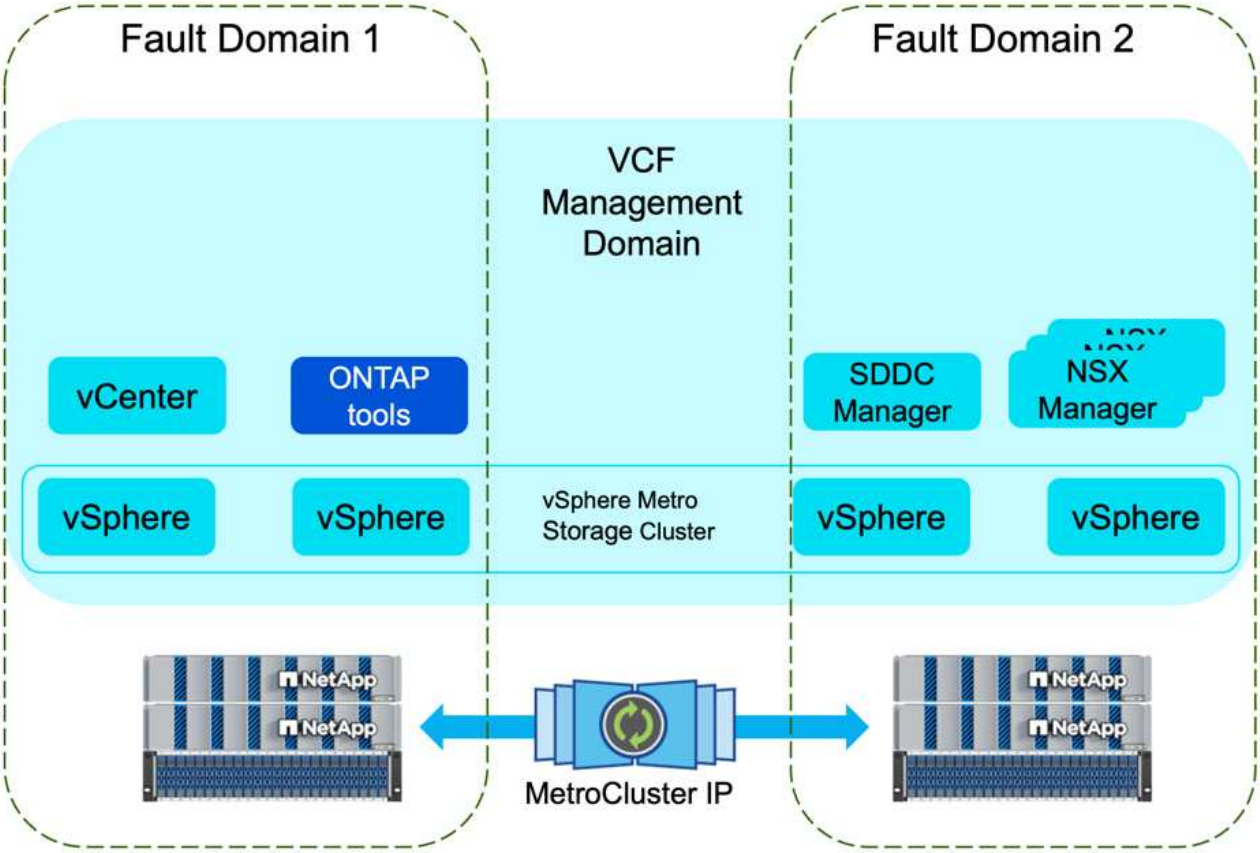
Consulte las siguientes soluciones para obtener más detalles.

- "Clúster extendido para el dominio de administración mediante la sincronización activa de SnapMirror"

- "Clúster extensible para el dominio de administración mediante MetroCluster"
- "Clúster extendido para el dominio de carga de trabajo VI mediante la sincronización activa de SnapMirror"
- "Clúster extensible para el dominio de carga de trabajo VI mediante MetroCluster"

Configurar un clúster extendido para un dominio de administración de VCF mediante MetroCluster

En este caso de uso, describimos el procedimiento para configurar un clúster extendido para el dominio de administración de VMware Cloud Foundation (VCF) utilizando ONTAP MetroCluster con NFS como almacén de datos principal. Este procedimiento incluye la implementación de hosts vSphere y vCenter Server, el aprovisionamiento de almacenes de datos NFS, la validación del clúster con la herramienta de importación de VCF, la configuración de los ajustes de NSX y la conversión del entorno en un dominio de administración de VCF.



Introducción

En esta solución demostraremos cómo implementar un dominio de administración de VCF extendido con NFS como almacén de datos principal usando ONTAP MetroCluster.

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

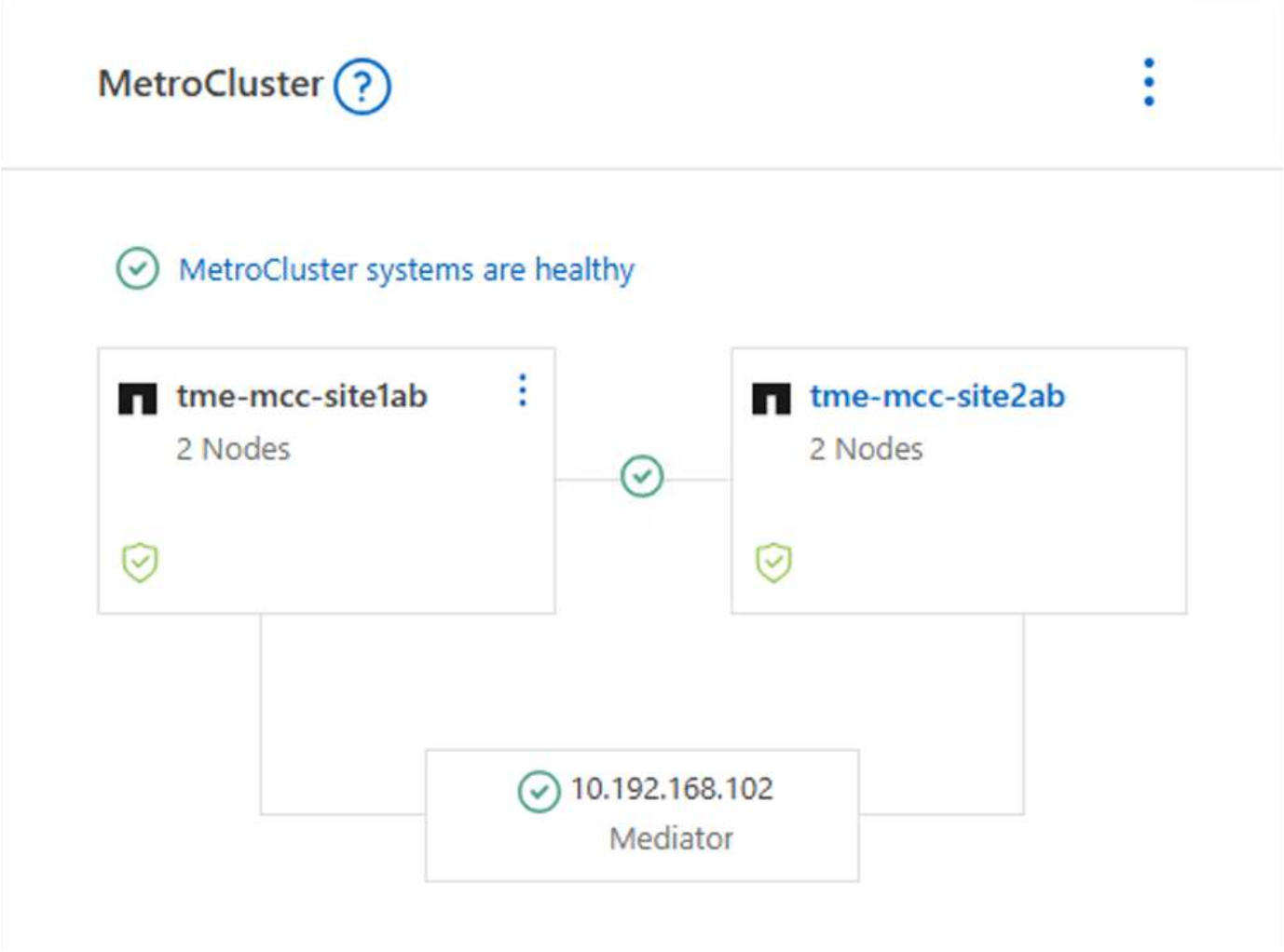
- Implementar hosts vSphere y servidores vCenter.
- Aprovisionar un almacén de datos NFS para los hosts de vSphere.
- Implemente SDDC Manager en el clúster de vSphere.
- Utilice la herramienta de importación VCF para validar el clúster vSphere.
- Configure un archivo JSON para crear un NSX durante la conversión VCF.
- Utilice la herramienta de importación de VCF para convertir el entorno de vSphere 8 en un dominio de administración de VCF.

Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Configuración de ONTAP MetroCluster compatible
- Máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico NFS.
- Se ha creado una interfaz lógica (LIF) en la red IP que transportará el tráfico NFS y está asociada con la SVM.
- Un clúster vSphere 8 con 4 hosts ESXi conectados a un conmutador de red.
- Descargue el software necesario para la conversión VCF.

Aquí se muestra una captura de pantalla de muestra del Administrador del sistema que muestra la configuración de MetroCluster
.



y aquí están las interfaces de red SVM de ambos dominios de falla.

Network interfaces | Subnets

+ Add

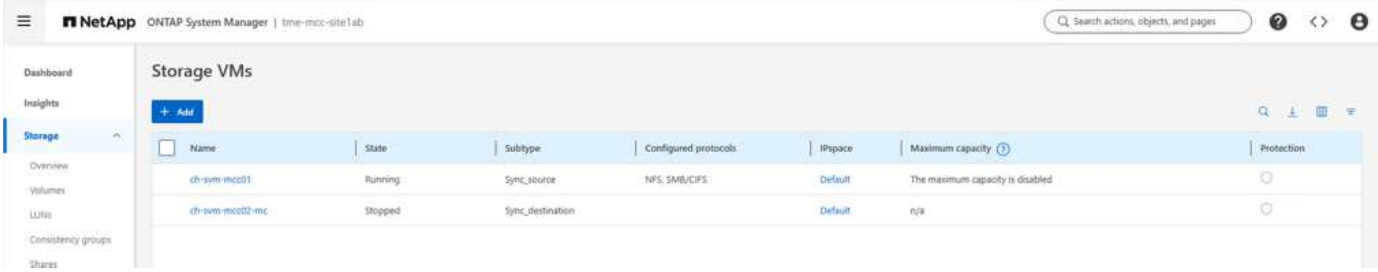
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

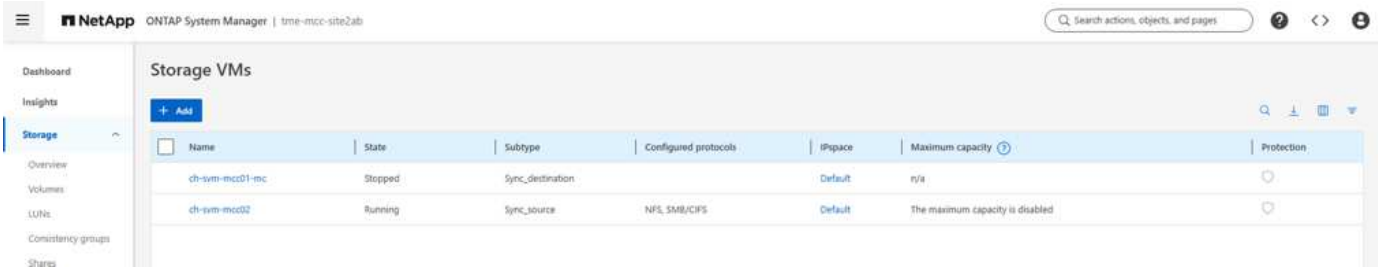
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTA] SVM estará activo en uno de los dominios de falla en MetroCluster.





Referirse "vMSC con MetroCluster" .

Para conocer el almacenamiento compatible y otras consideraciones para convertir o importar vSphere a VCF 5.2, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

Antes de crear un clúster de vSphere que se convertirá en un dominio de administración de VCF, consulte "Consideración de NSX en vSphere Cluster"

Para el software necesario, consulte "Descargar software para convertir o importar entornos vSphere existentes" .

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Pasos de implementación

Para implementar un dominio de administración extendido VCF con NFS como almacén de datos principal,

Complete los siguientes pasos:

- Implementar hosts vSphere y vCenter.
- Crear clúster de vSphere.
- Aprovisionar almacén de datos NFS.
- Copie la herramienta de importación VCF al dispositivo vCenter.
- Ejecute una comprobación previa en el dispositivo vCenter mediante la herramienta de importación VCF.
- Implemente la máquina virtual del administrador de SDDC en el clúster de vCenter.
- Cree un archivo JSON para un clúster NSX que se implementará durante el proceso de conversión.
- Cargue el software requerido en el administrador SDDC.
- Convierta el clúster vSphere en un dominio de administración de VCF.

Para obtener una descripción general del proceso de conversión, consulte "Convertir un entorno de vSphere en un dominio de administración o importar un entorno de vSphere como un dominio de carga de trabajo de VI en VMware Cloud Foundation" .

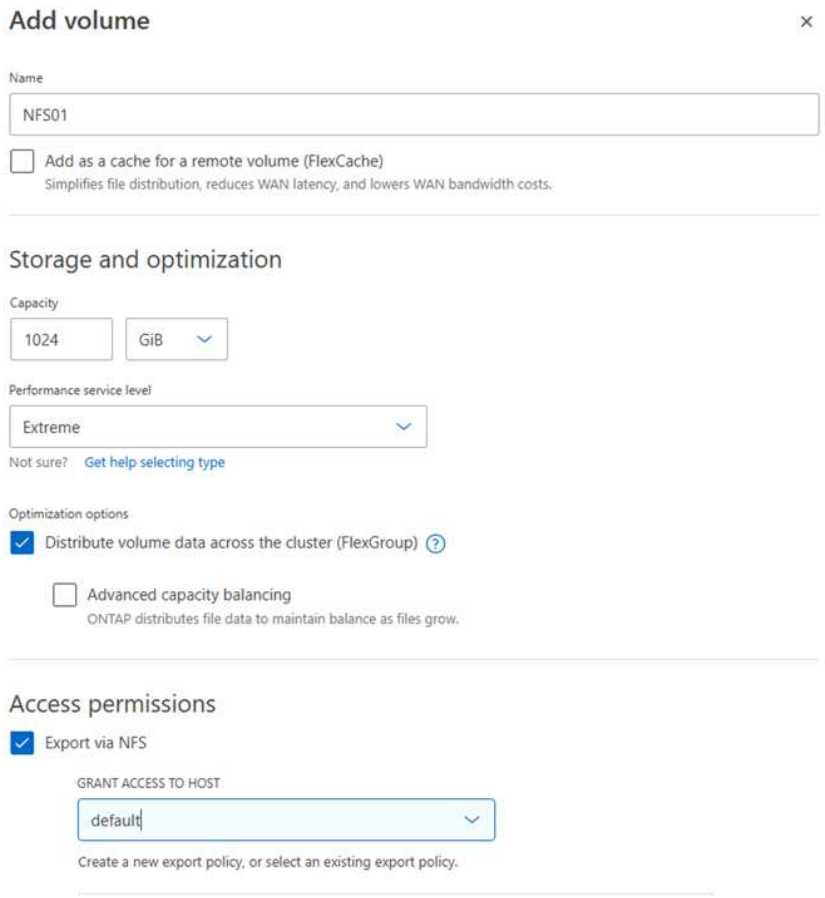
Implementar hosts vSphere y vCenter

Implemente vSphere en los hosts usando ISO descargado del portal de soporte de Broadcom o use la opción de implementación existente para el host vSphere.

Montar un almacén de datos NFS para alojar máquinas virtuales

En este paso, creamos el volumen NFS y lo montamos como almacén de datos para alojar las máquinas virtuales.

1. Mediante el Administrador del sistema, cree un volumen y adjúntelo a una política de exportación que incluya la subred IP del host vSphere.



2. Conecte mediante SSH al host vSphere y monte el almacén de datos NFS.

```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Not Supported
[root@SiteA-vs01:~]
```

3. Repita los pasos anteriores si necesita un almacén de datos adicional y asegúrese de que la aceleración de hardware sea compatible.

```
[root@MCCA01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS02        10.192.164.230  /NFS02  None          true     true            4      false  false  Supported
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Supported
[root@MCCA01:~]
```

Implementar vCenter en un almacén de datos NFS. Asegúrese de que SSH y Bash shell estén habilitados en el dispositivo vCenter.

Crear un clúster de vSphere

1. Inicie sesión en el cliente web de vSphere, cree el centro de datos y el clúster de vSphere agregando uno de los host donde está implementado NFS VAAI. Optamos por administrar todos los hosts del clúster con la opción de imagen única. [SUGERENCIA] No seleccione Administrar configuración a nivel de clúster. Para obtener más detalles, consulte "Consideración de NSX en vSphere Cluster" . Para conocer las mejores prácticas de vMSC con ONTAP MetroCluster, consulte "Directrices de diseño e implementación de vMSC"
2. Agregar otros hosts vSphere al clúster.
3. Cree un conmutador distribuido y agregue los grupos de puertos.
4. "Migrar la red de un vSwitch estándar a un conmutador distribuido."

Convertir el entorno de vSphere en un dominio de administración de VCF

La siguiente sección cubre los pasos para implementar el administrador SDDC y convertir el clúster vSphere 8 en un dominio de administración VCF 5.2. Cuando corresponda, se consultará la documentación de VMware para obtener detalles adicionales.

La herramienta de importación VCF de VMware by Broadcom es una utilidad que se utiliza tanto en el dispositivo vCenter como en el administrador SDDC para validar configuraciones y proporcionar servicios de conversión e importación para entornos vSphere y VCF.

Para más información, consulte "Opciones y parámetros de la herramienta de importación VCF" .

Copiar y extraer herramienta de importación VCF

La herramienta de importación de VCF se utiliza en el dispositivo vCenter para validar que el clúster de vSphere se encuentra en un estado correcto para el proceso de importación o conversión de VCF.

Complete los siguientes pasos:

1. Siga los pasos a continuación "Copiar la herramienta de importación de VCF al dispositivo vCenter de destino" en VMware Docs para copiar la herramienta de importación VCF a la ubicación correcta.
2. Extraiga el paquete utilizando el siguiente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar el dispositivo vCenter

Utilice la herramienta de importación VCF para validar el dispositivo vCenter antes de la conversión.

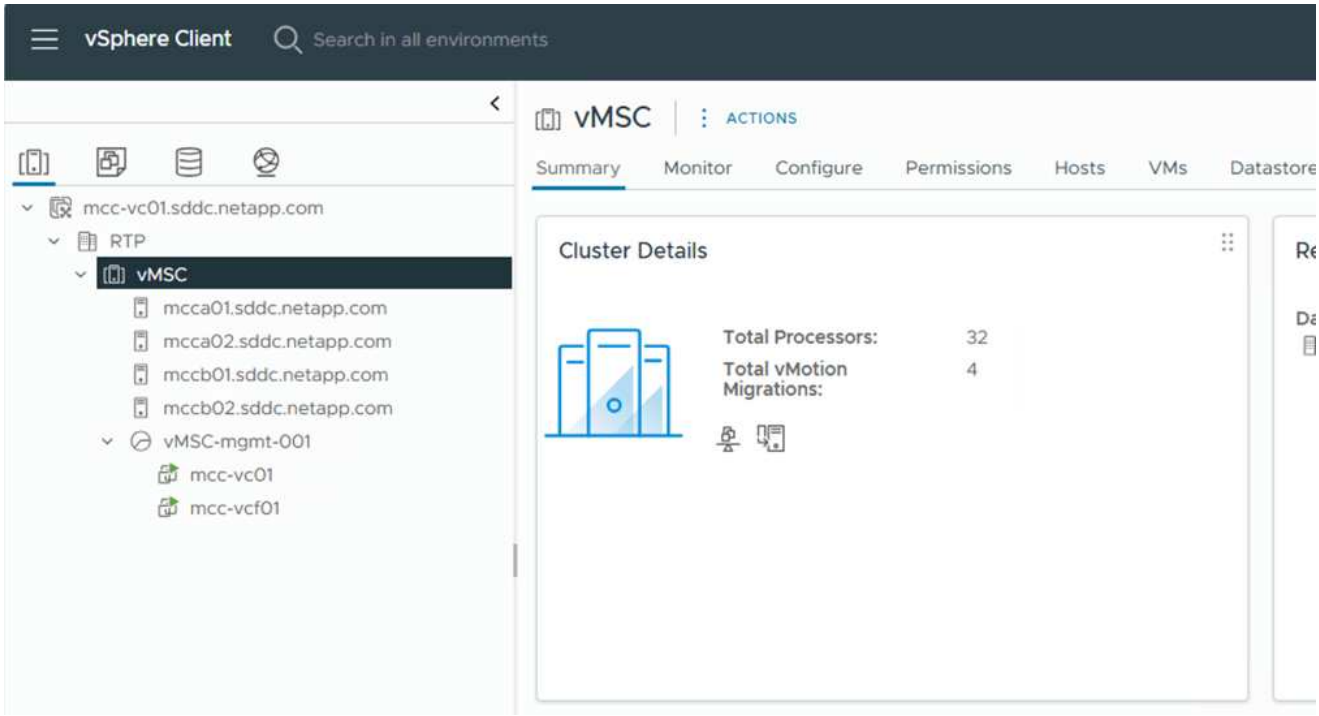
1. Siga los pasos a continuación "Ejecutar una comprobación previa en el vCenter de destino antes de la conversión" para ejecutar la validación.
2. La siguiente salida muestra que el dispositivo vCenter ha pasado la verificación previa.

```
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Enter vCenter SSO password:
[2025-03-20 23:02:05,971] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2025-03-20 23:02:06,089] [INFO] vc_precheck: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,092] [INFO] vc_precheck: Running pre-checks for vCenter mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,092] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2025-03-20 23:02:08,820] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2025-03-20 23:02:10,246] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2025-03-20 23:02:10,879] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2025-03-20 23:02:10,880] [INFO] vc_precheck: All pre-checks passed!
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]#
```

Implementar el SDDC Manager

El administrador de SDDC debe estar ubicado en el clúster de vSphere que se convertirá en un dominio de administración de VCF.

Siga las instrucciones de implementación en VMware Docs para completar la implementación.



Referirse a "Implementar el dispositivo SDDC Manager en el vCenter de destino" .

Crear un archivo JSON para la implementación de NSX

Para implementar NSX Manager al importar o convertir un entorno de vSphere a VMware Cloud Foundation, cree una especificación de implementación de NSX. La implementación de NSX requiere un mínimo de 3 hosts.

> Al implementar un clúster de NSX Manager en una operación de conversión o importación, se utiliza un segmento respaldado por VLAN de NSX. Para obtener detalles sobre las limitaciones del segmento respaldado por NSX-VLAN, consulte la sección "Consideraciones antes de convertir o importar entornos vSphere existentes en VMware Cloud Foundation". Para obtener información sobre las limitaciones de la red NSX-VLAN, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

El siguiente es un ejemplo de un archivo JSON para la implementación de NSX:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "******************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.114",
  "cluster_fqdn": "mcc-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-nsxa.sddc.netapp.com",
    "name": "mcc-nsxa",
    "ip_address": "10.61.185.111",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxb.sddc.netapp.com",
    "name": "mcc-nsxb",
    "ip_address": "10.61.185.112",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxc.sddc.netapp.com",
    "name": "mcc-nsxc",
    "ip_address": "10.61.185.113",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie el archivo JSON a la carpeta de inicio del usuario vcf en el Administrador de SDDC.

Subir software a SDDC Manager

Copie la herramienta de importación de VCF a la carpeta de inicio del usuario vcf y el paquete de implementación de NSX a la carpeta /nfs/vmware/vcf/nfs-mount/bundle/ en el Administrador de SDDC.

Ver "Cargue el software necesario en el dispositivo SDDC Manager" para obtener instrucciones detalladas.

Comprobación detallada en vCenter antes de la conversión

Antes de realizar una operación de conversión de dominio de administración o una operación de importación de dominio de carga de trabajo de VI, debe realizar una verificación detallada para asegurarse de que la configuración del entorno vSphere existente sea compatible con la conversión o importación. . Acceda por SSH al dispositivo SDDC Manager como usuario vcf. . Navegue hasta el directorio donde copió la herramienta de importación VCF. . Ejecute el siguiente comando para comprobar que el entorno de vSphere se puede convertir

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```

Convertir un clúster de vSphere en un dominio de administración de VCF

La herramienta de importación VCF se utiliza para realizar el proceso de conversión.

Se ejecuta el siguiente comando para convertir el clúster vSphere en un dominio de administración de VCF e implementar el clúster NSX:

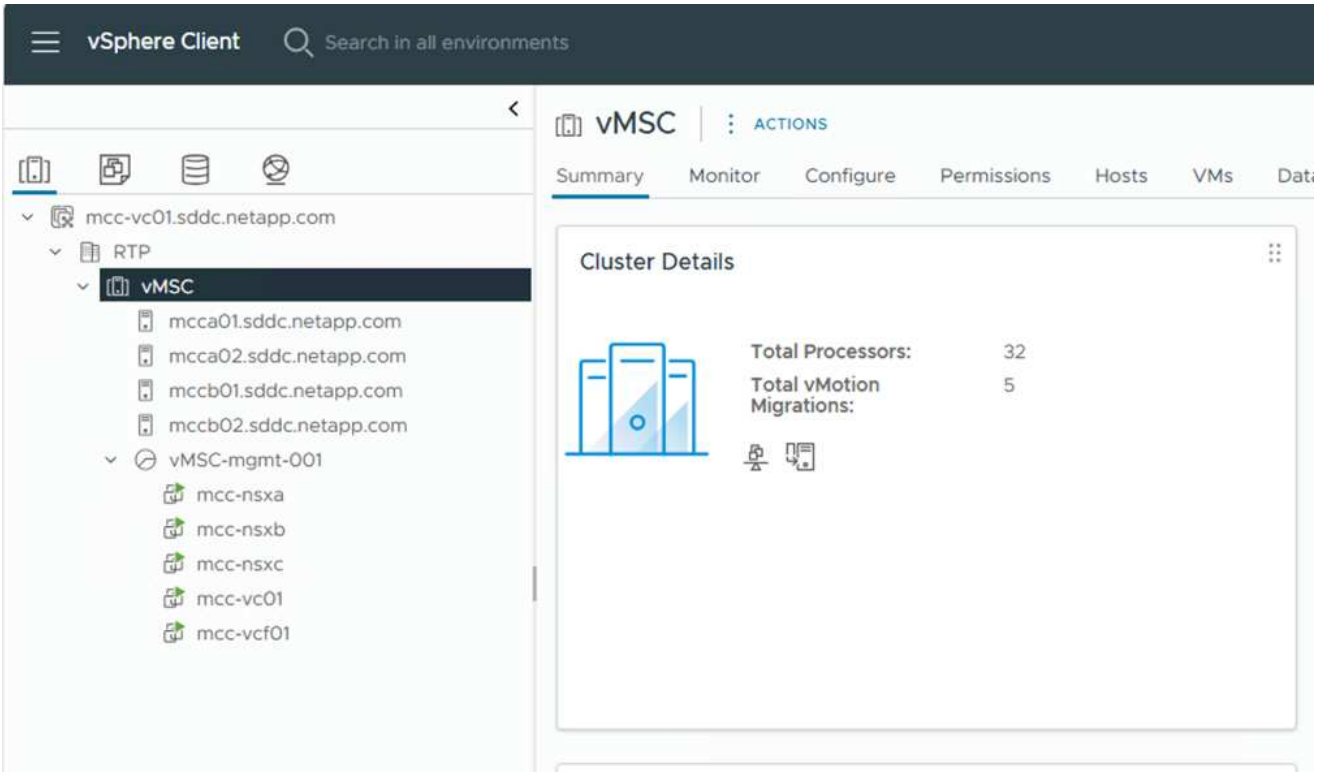
```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

Cuando hay varios almacenes de datos disponibles en el host vSphere, se indica qué almacén de datos debe considerarse como almacén de datos principal en el que se implementarán las máquinas virtuales NSX de manera
predeterminada.

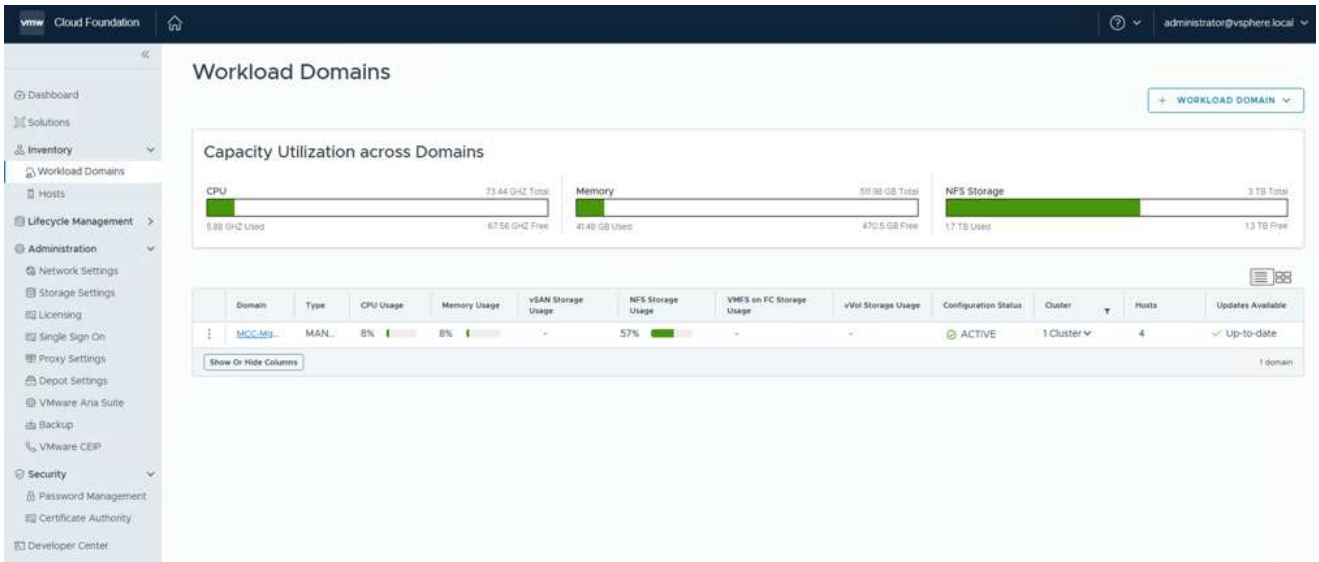
```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: ================================================================
[2025-03-24 19:29:00,583] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, as domain of type: MANAGEMENT
[2025-03-24 19:29:00,586] [INFO] discover_domain: [1/5] Starting discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,596] [INFO] discover_domain: [1/5] Completed discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com in 0.01s
[2025-03-24 19:29:00,596] [INFO] discover_domain: ================================================================
[2025-03-24 19:29:00,596] [INFO] discover_domain: [2/5] Starting discovery of clusters in vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,613] [INFO] discover_domain: >>>>>> [1/1] Starting discovery of cluster: vMSC
Please select a primary datastore for cluster vMSC:
1) NFS01
2) NFS02
Choose a number: 1
[2025-03-24 19:29:25,192] [INFO] discover_domain: >>>>>> [1/1] Discovered cluster: vMSC in 24.58s
[2025-03-24 19:29:25,193] [INFO] discover_domain: [2/5] Completed discovery of 1 clusters in vCenter: mcc-vc01.sddc.netapp.com in 24.6s
```

Para obtener instrucciones completas, consulte "Procedimiento de conversión de VCF" .

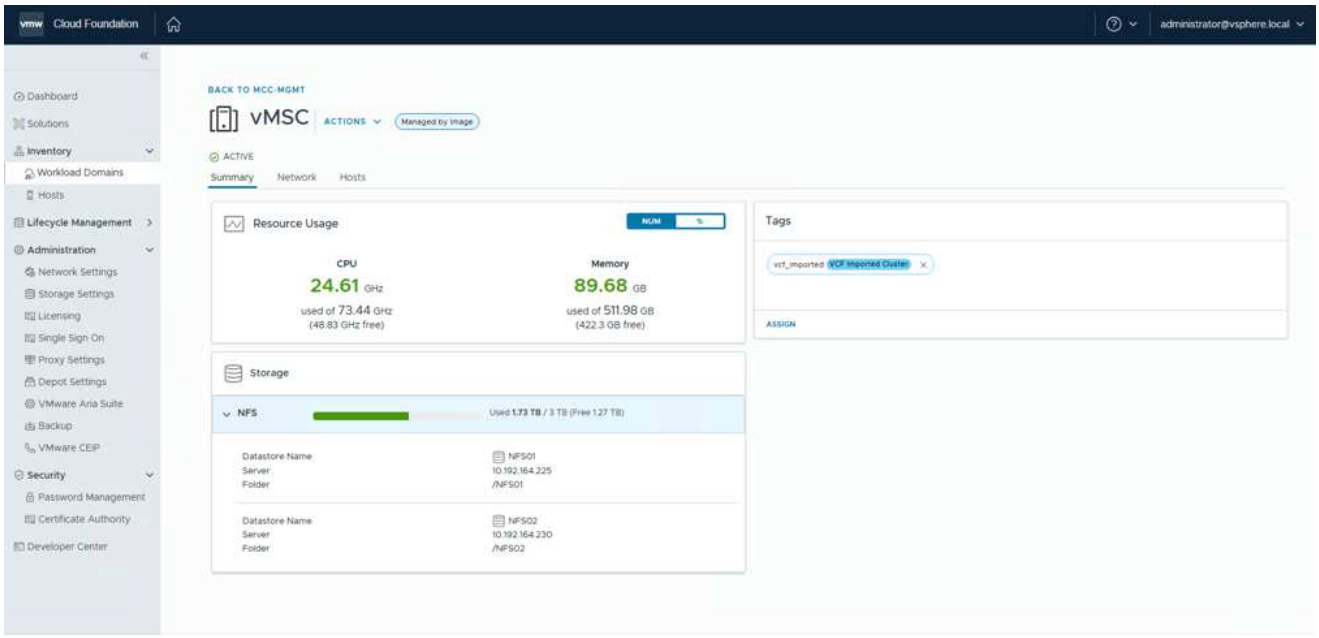
Las máquinas virtuales NSX se implementarán en
vCenter.



SDDC Manager muestra el dominio de administración creado con el nombre proporcionado y NFS como almacén de
datos.



Al inspeccionar el clúster, se proporciona la información del almacén de datos
NFS.



Añadir licencias a VCF

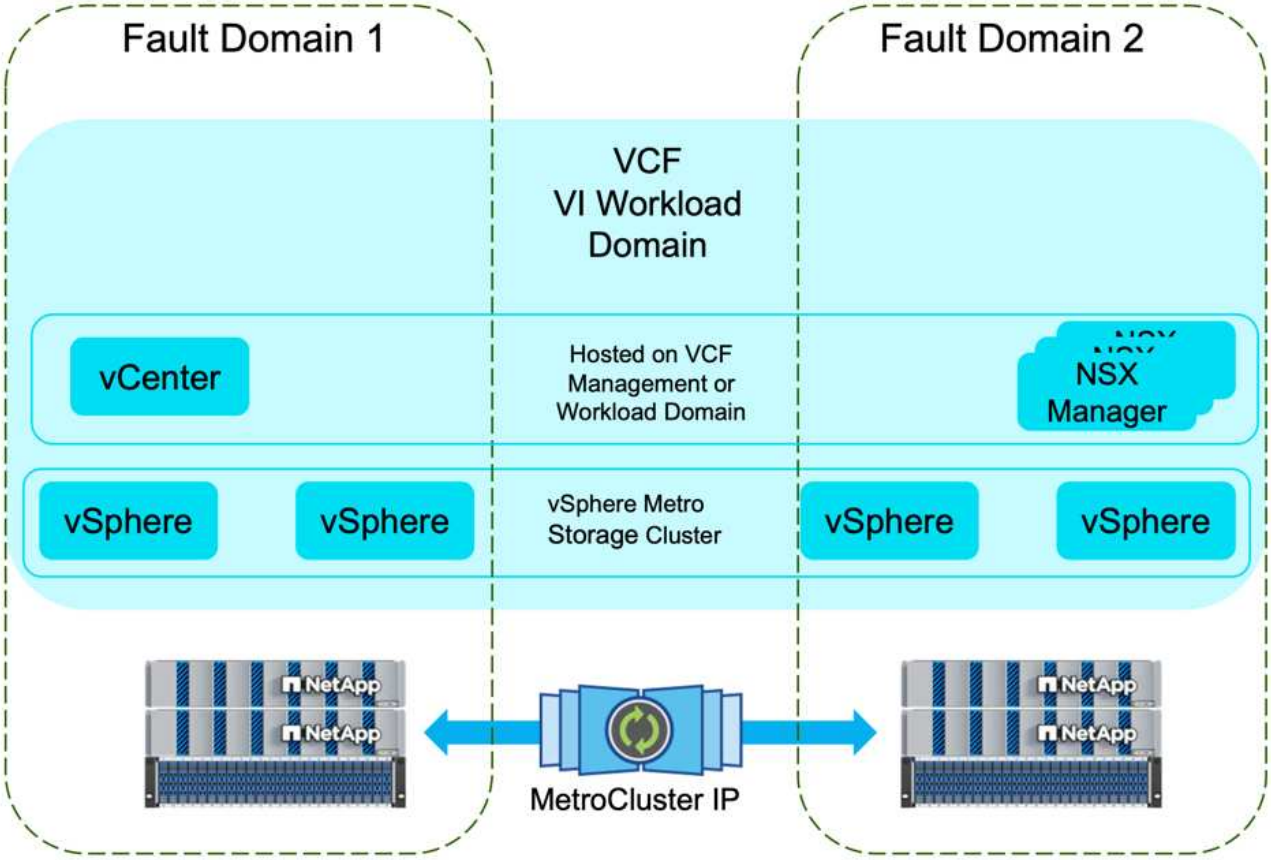
Después de completar la conversión, se debe agregar la licencia al entorno.

1. Inicie sesión en la interfaz de usuario del Administrador de SDDC.
2. Vaya a **Administración > Licencias** en el panel de navegación.
3. Haga clic en **+ Clave de licencia**.
4. Elija un producto del menú desplegable.
5. Introduzca la clave de licencia.
6. Proporcione una descripción de la licencia.
7. Haga clic en **Agregar**.
8. Repita estos pasos para cada licencia.

Configurar un clúster extendido para un dominio de carga de trabajo VI mediante MetroCluster

En este caso de uso, describimos el procedimiento para configurar un dominio de carga de trabajo VCF VI extendido con NFS como almacén de datos principal mediante ONTAP MetroCluster. Este procedimiento incluye la implementación de hosts vSphere y vCenter Server, el aprovisionamiento de almacenes de datos NFS, la validación del clúster vSphere, la configuración de NSX durante la conversión de VCF y la importación del entorno vSphere a un dominio de administración de VCF existente.

Las cargas de trabajo en VCF están protegidas por vSphere Metro Storage Cluster (vMSC). Generalmente, ONTAP MetroCluster con implementación FC o IP se utiliza para brindar tolerancia a fallas en almacenes de datos VMFS y NFS.



Introducción

En esta solución demostraremos cómo implementar el dominio de carga de trabajo VI VCF extendido con NFS como almacén de datos principal mediante ONTAP MetroCluster. El dominio de carga de trabajo de VI se puede implementar mediante SDDC Manager o importar un entorno vSphere existente como dominio de carga de trabajo de VI.

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Implementar hosts vSphere y servidores vCenter.
- Aprovisionar un almacén de datos NFS para los hosts de vSphere.
- Utilice la herramienta de importación VCF para validar el clúster vSphere.
- Configure un archivo JSON para crear un NSX durante la conversión VCF.
- Utilice la herramienta de importación de VCF para importar el entorno de vSphere 8 como dominio de carga de trabajo de VCF VI a un dominio de administración de VCF existente.

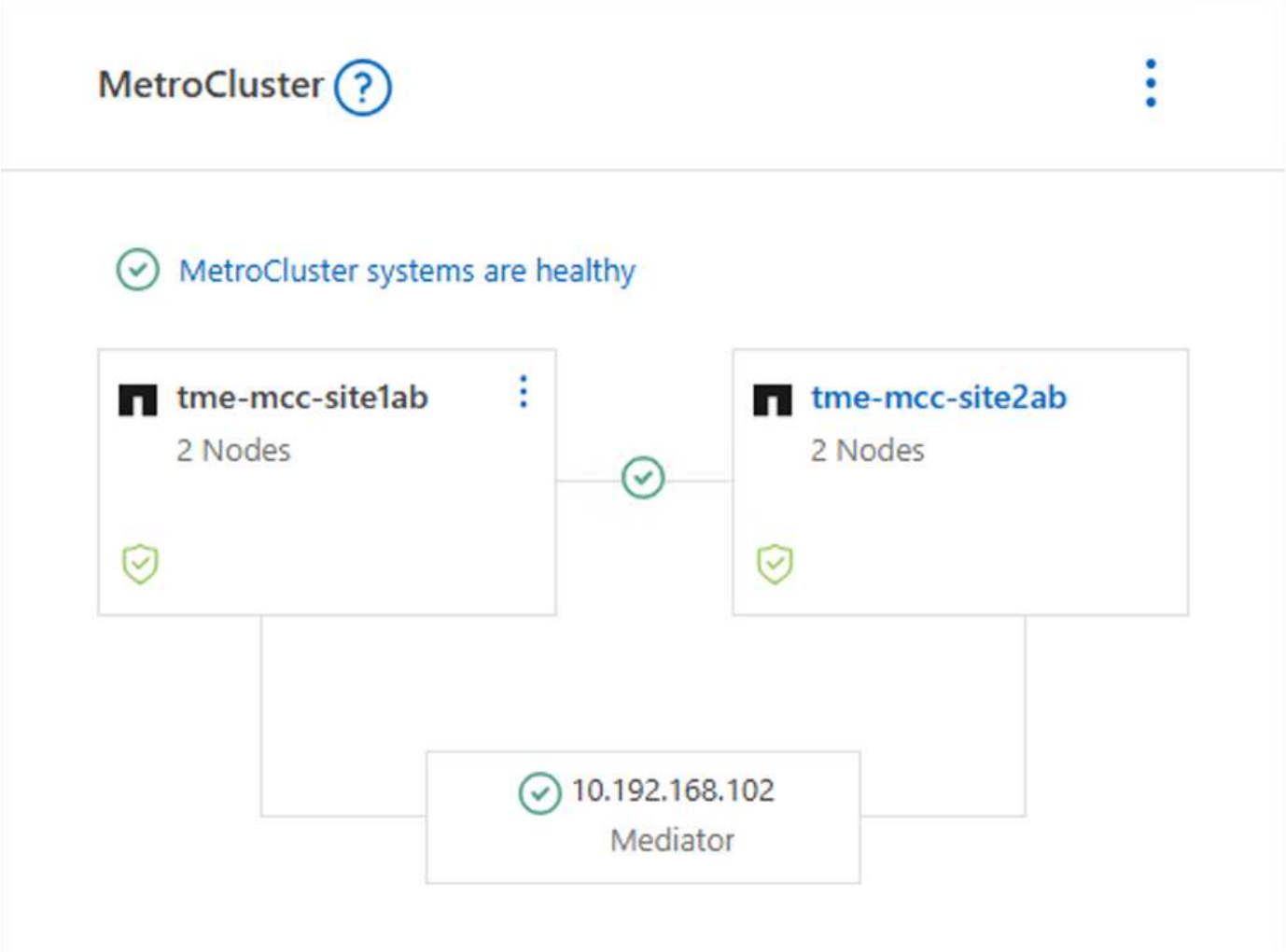
Prerrequisitos

Este escenario requiere los siguientes componentes y configuraciones:

- Configuración de ONTAP MetroCluster compatible

- Máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico NFS.
- Se ha creado una interfaz lógica (LIF) en la red IP que transportará el tráfico NFS y está asociada con la SVM.
- Un clúster vSphere 8 con 4 hosts ESXi conectados a un conmutador de red.
- Descargue el software necesario para la conversión VCF.

Aquí se muestra una captura de pantalla de muestra del Administrador del sistema que muestra la configuración de MetroCluster
.



y aquí están las interfaces de red SVM de ambos dominios de falla.

Network interfaces Subnets

+ Add

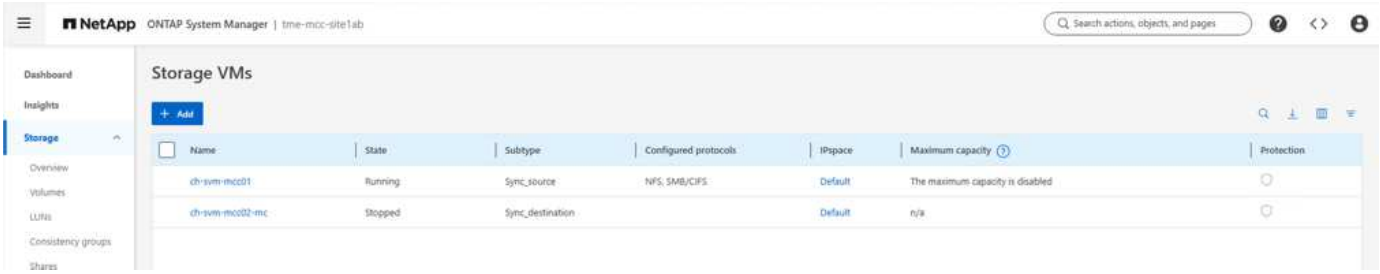
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

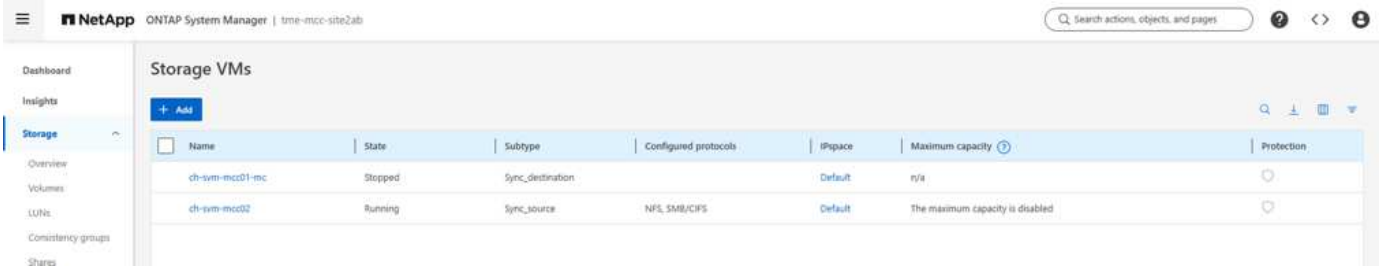
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTA] SVM estará activo en uno de los dominios de falla en MetroCluster.





Referirse "vMSC con MetroCluster" .

Para conocer el almacenamiento compatible y otras consideraciones para convertir o importar vSphere a VCF 5.2, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

Antes de crear un clúster de vSphere que se convertirá en un dominio de administración de VCF, consulte "Consideración de NSX en vSphere Cluster"

Para el software necesario, consulte "Descargar software para convertir o importar entornos vSphere existentes" .

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Pasos de implementación

Para implementar un dominio de administración extendido VCF con NFS como almacén de datos principal,

Complete los siguientes pasos:

- Implementar hosts vSphere y vCenter.
- Crear clúster de vSphere.
- Aprovisionar almacén de datos NFS.
- Copie la herramienta de importación VCF al dispositivo vCenter.
- Ejecute una comprobación previa en el dispositivo vCenter mediante la herramienta de importación VCF.
- Cree un archivo JSON para un clúster NSX que se implementará durante el proceso de importación.
- Cargue el software requerido en el administrador SDDC.
- Convierta el clúster vSphere en un dominio de carga de trabajo VCF VI.

Para obtener una descripción general del proceso de conversión, consulte "Convertir un entorno de vSphere en un dominio de administración o importar un entorno de vSphere como un dominio de carga de trabajo de VI en VMware Cloud Foundation" .

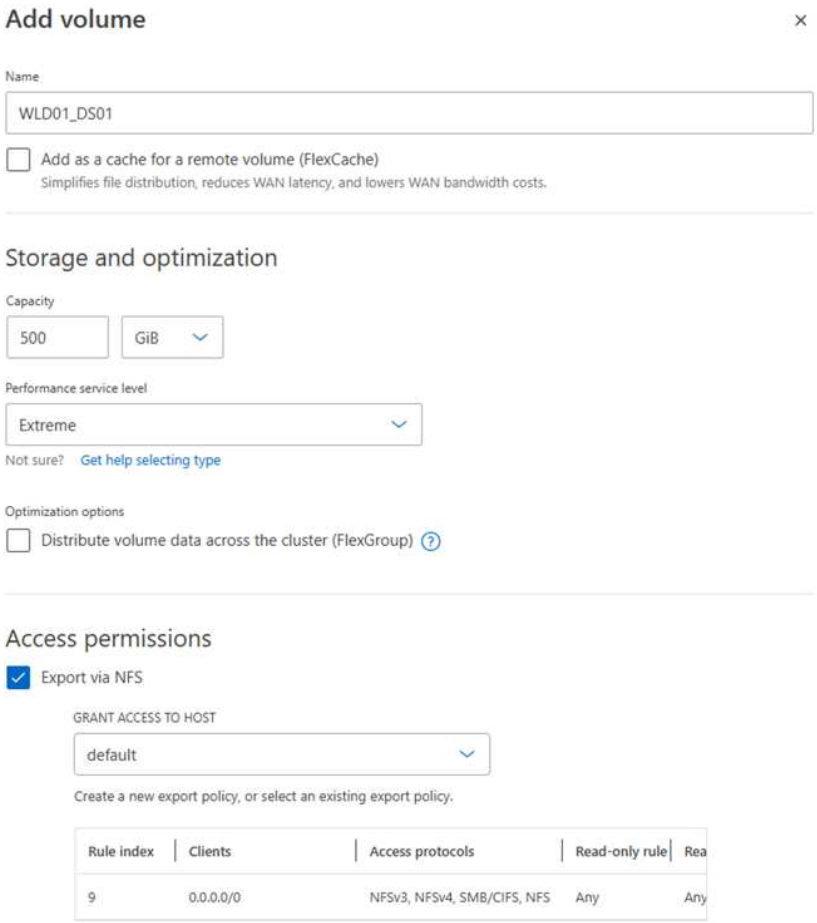
Implementar hosts vSphere y vCenter

Implemente vSphere en los hosts usando ISO descargado del portal de soporte de Broadcom o use la opción de implementación existente para el host vSphere.

Montar un almacén de datos NFS para alojar máquinas virtuales

En este paso, creamos el volumen NFS y lo montamos como almacén de datos para alojar las máquinas virtuales.

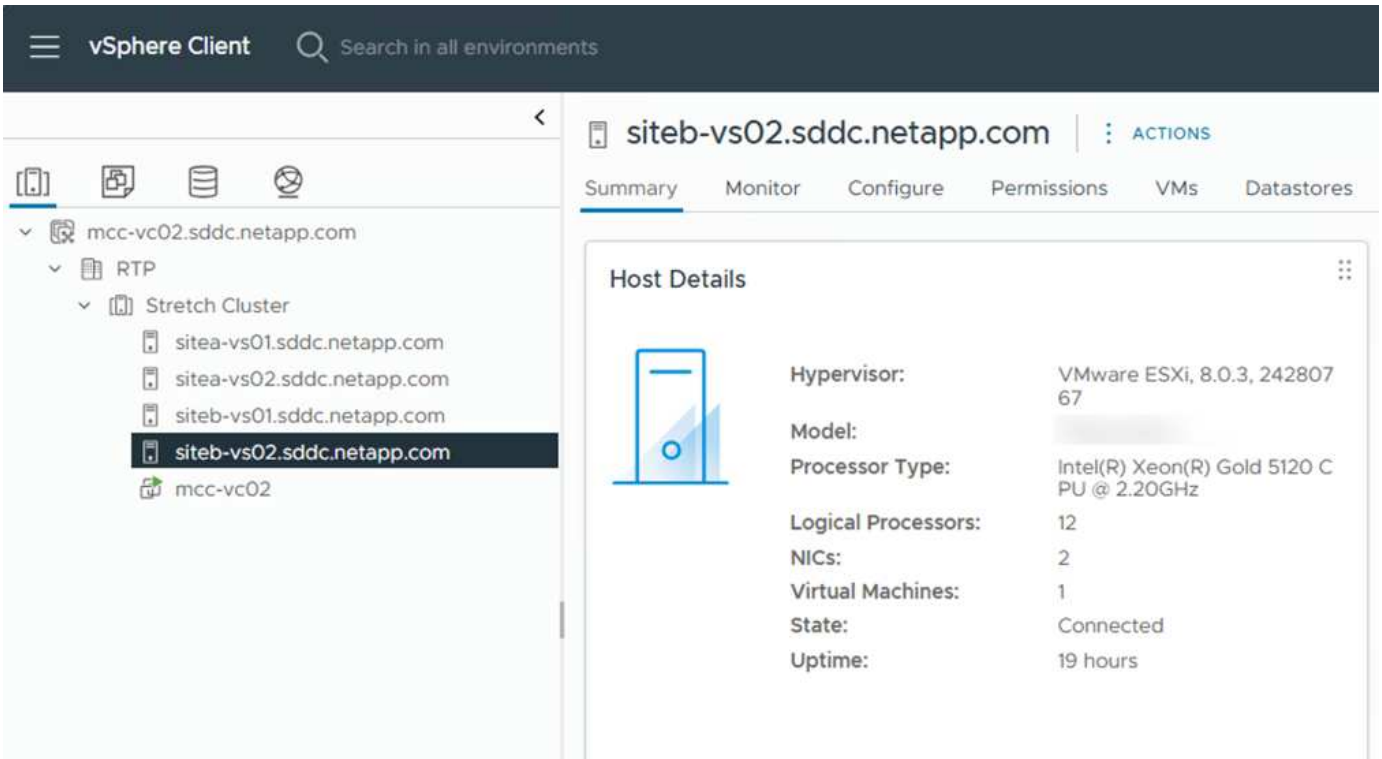
1. Mediante el Administrador del sistema, cree un volumen y adjúntelo a una política de exportación que incluya la subred IP del host
vSphere.



2. Conecte mediante SSH al host vSphere y monte el almacén de datos NFS.

```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02
esxcli storage nfs list
```

Implementar vCenter en un almacén de datos NFS. Asegúrese de que SSH y Bash shell estén habilitados en el dispositivo
vCenter.



Crear un clúster de vSphere

1. Inicie sesión en vSphere webclient, cree el centro de datos y el clúster de vSphere agregando uno de los host donde está implementado NFS VAAI. Optamos por administrar todos los hosts del clúster con la opción de imagen única. [SUGERENCIA] No seleccione Administrar configuración a nivel de clúster. Para obtener más detalles, consulte "Consideración de NSX en vSphere Cluster" . Para conocer las mejores prácticas de vMSC con ONTAP MetroCluster, consulte "Directrices de diseño e implementación de vMSC"
2. Agregar otros hosts vSphere al clúster.
3. Cree un conmutador distribuido y agregue los grupos de puertos.
4. "Migrar la red de un vSwitch estándar a un conmutador distribuido."

Convertir el entorno de vSphere a un dominio de carga de trabajo de VI VCF

La siguiente sección cubre los pasos para implementar el administrador SDDC y convertir el clúster vSphere 8 en un dominio de administración VCF 5.2. Cuando corresponda, se consultará la documentación de VMware para obtener detalles adicionales.

La herramienta de importación VCF de VMware by Broadcom es una utilidad que se utiliza tanto en el dispositivo vCenter como en el administrador SDDC para validar configuraciones y proporcionar servicios de conversión e importación para entornos vSphere y VCF.

Para más información, consulte "Opciones y parámetros de la herramienta de importación VCF" .

Copiar y extraer herramienta de importación VCF

La herramienta de importación de VCF se utiliza en el dispositivo vCenter para validar que el clúster de vSphere se encuentra en un estado correcto para el proceso de importación o conversión de VCF.

Complete los siguientes pasos:

1. Siga los pasos a continuación "Copiar la herramienta de importación de VCF al dispositivo vCenter de destino" en VMware Docs para copiar la herramienta de importación VCF a la ubicación correcta.
2. Extraiga el paquete utilizando el siguiente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar el dispositivo vCenter

Utilice la herramienta de importación de VCF para validar el dispositivo vCenter antes de la importación como dominio de carga de trabajo de VI.

1. Siga los pasos a continuación "Ejecutar una comprobación previa en el vCenter de destino antes de la conversión" para ejecutar la validación.

Crear un archivo JSON para la implementación de NSX

Para implementar NSX Manager al importar o convertir un entorno de vSphere a VMware Cloud Foundation, cree una especificación de implementación de NSX. La implementación de NSX requiere un mínimo de 3 hosts.

> Al implementar un clúster de NSX Manager en una operación de conversión o importación, se utiliza un segmento respaldado por VLAN de NSX. Para obtener detalles sobre las limitaciones del segmento respaldado por NSX-VLAN, consulte la sección "Consideraciones antes de convertir o importar entornos vSphere existentes en VMware Cloud Foundation". Para obtener información sobre las limitaciones de la red NSX-VLAN, consulte "Consideraciones antes de convertir o importar entornos vSphere existentes a VMware Cloud Foundation" .

El siguiente es un ejemplo de un archivo JSON para la implementación de NSX:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "****************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.105",
  "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",
    "name": "mcc-wld01-nsxa",
    "ip_address": "10.61.185.106",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",
    "name": "mcc-wld01-nsxb",
    "ip_address": "10.61.185.107",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",
    "name": "mcc-wld01-nsxc",
    "ip_address": "10.61.185.108",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie el archivo JSON a la carpeta de inicio del usuario vcf en el Administrador de SDDC.

Subir software a SDDC Manager

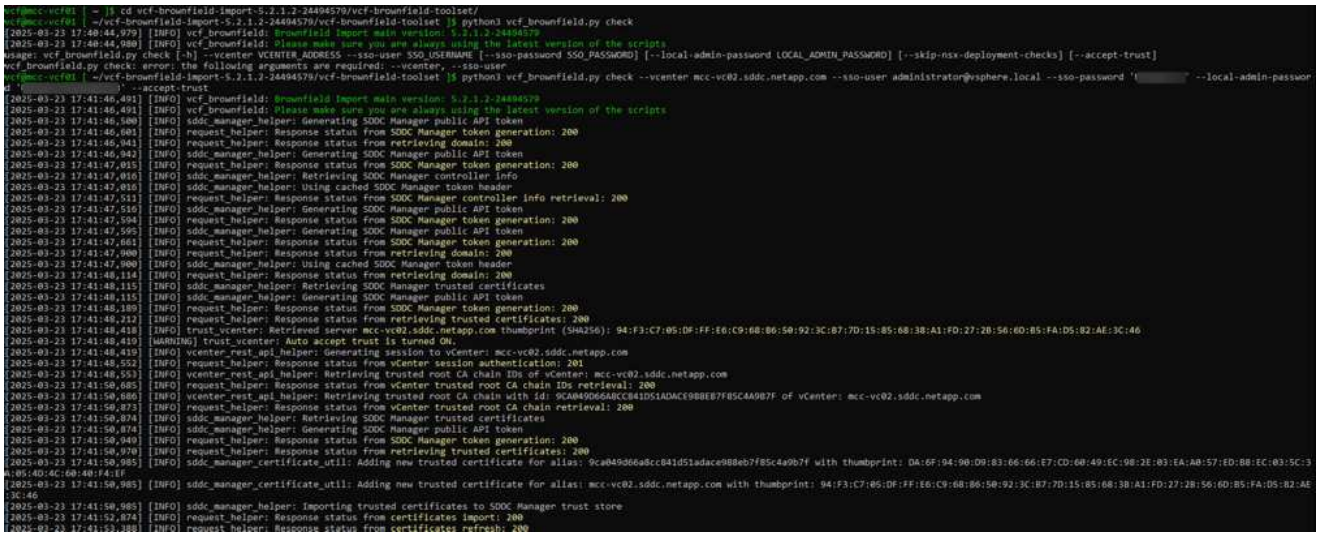
Copie la herramienta de importación de VCF a la carpeta de inicio del usuario vcf y el paquete de implementación de NSX a la carpeta /nfs/vmware/vcf/nfs-mount/bundle/ en el Administrador de SDDC.

Ver "Cargue el software necesario en el dispositivo SDDC Manager" para obtener instrucciones detalladas.

Comprobación detallada en vCenter antes de la conversión

Antes de realizar una operación de conversión de dominio de administración o una operación de importación de dominio de carga de trabajo de VI, debe realizar una verificación detallada para asegurarse de que la configuración del entorno vSphere existente sea compatible con la conversión o importación. . Acceda por SSH al dispositivo SDDC Manager como usuario vcf. . Navegue hasta el directorio donde copió la herramienta de importación VCF. . Ejecute el siguiente comando para comprobar que el entorno de vSphere se puede convertir

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```



Convertir un clúster de vSphere en un dominio de carga de trabajo de VCF VI

La herramienta de importación VCF se utiliza para realizar el proceso de conversión.

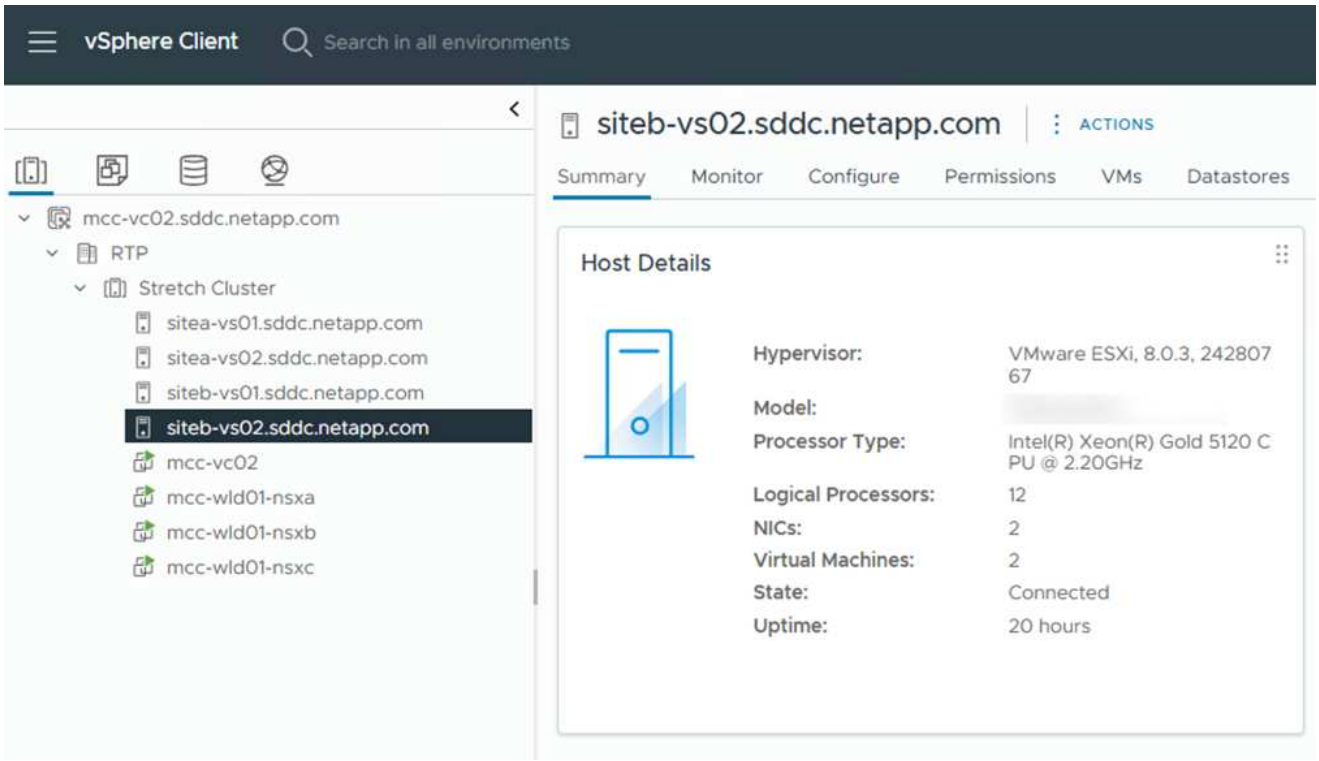
Se ejecuta el siguiente comando para convertir el clúster vSphere en un dominio de administración de VCF e implementar el clúster NSX:

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

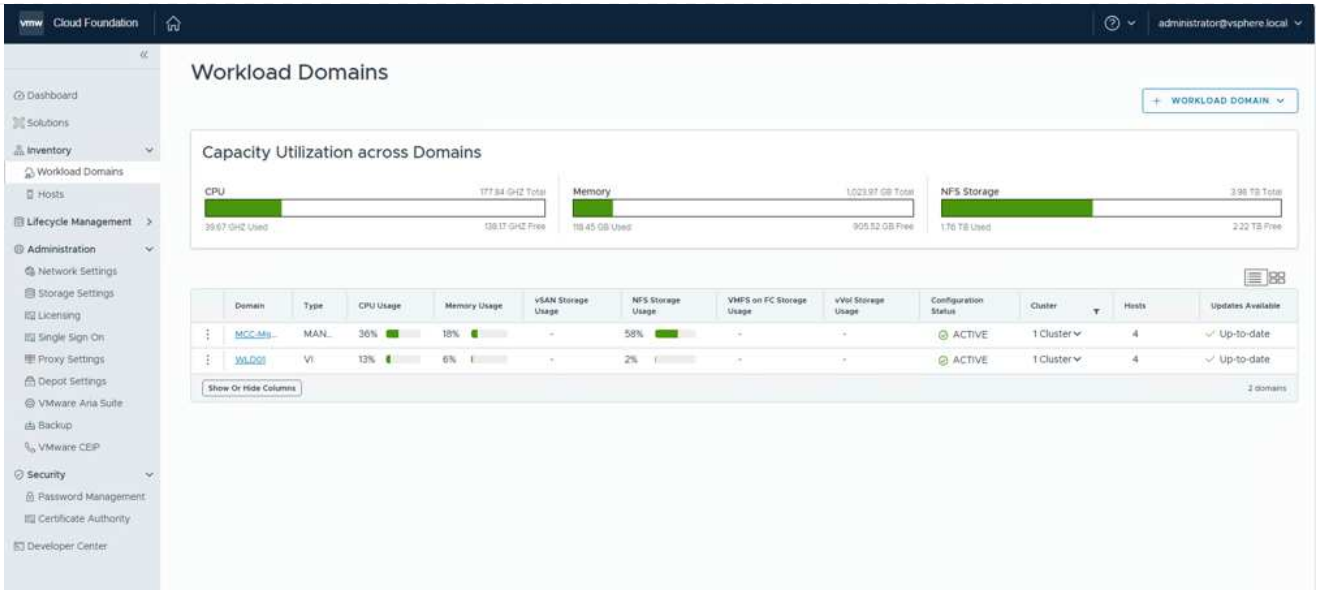
Incluso si hay varios almacenes de datos disponibles en el host vSphere, no es necesario indicar qué almacén de datos debe considerarse como almacén de datos principal.

Para obtener instrucciones completas, consulte "Procedimiento de conversión de VCF" .

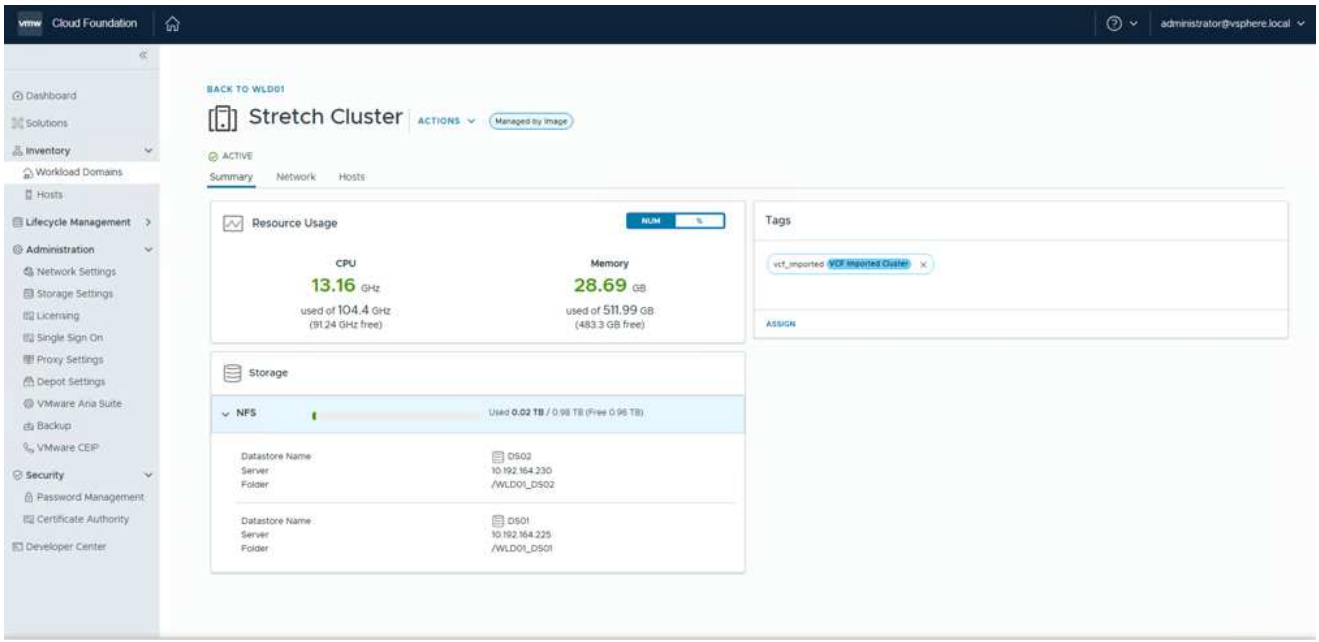
Las máquinas virtuales NSX se implementarán en vCenter.



SDDC Manager muestra el dominio de carga de trabajo VI creado con el nombre proporcionado y NFS como almacén de datos.



Al inspeccionar el clúster, se proporciona la información de los almacenes de datos NFS.



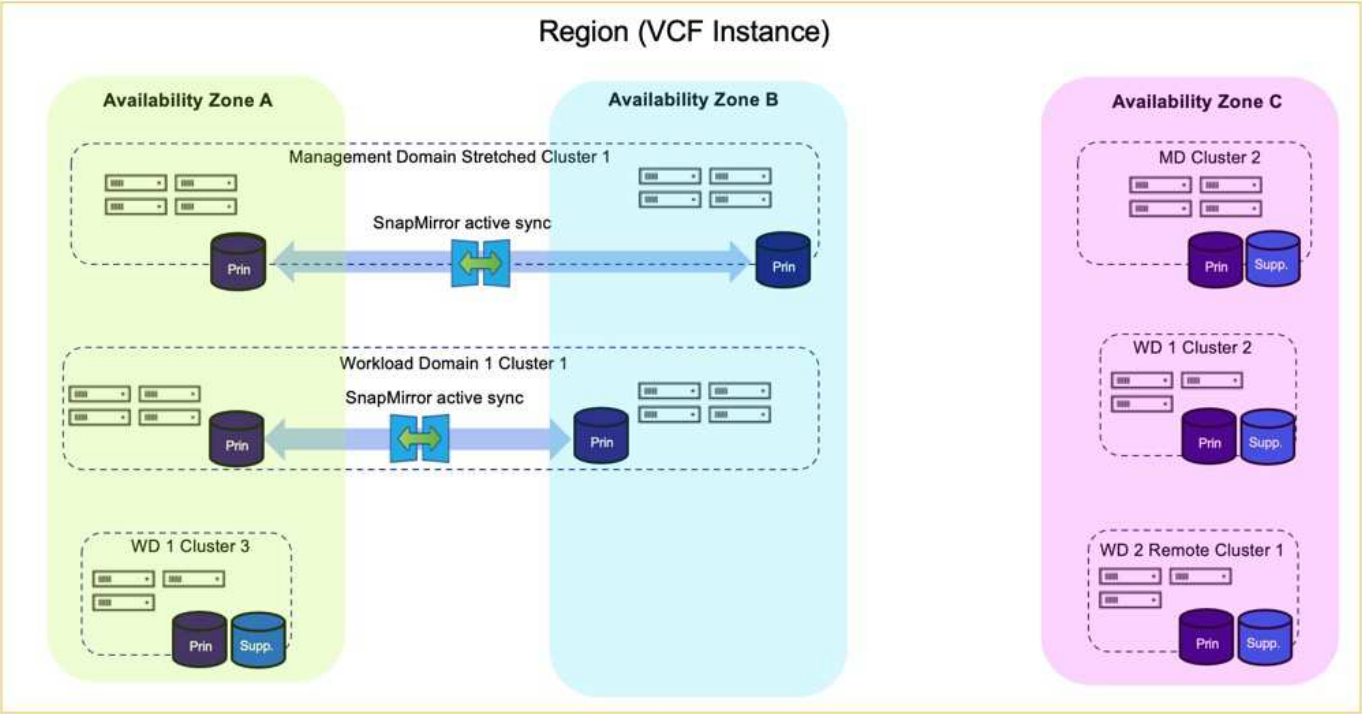
Añadir licencias a VCF

Después de completar la conversión, se debe agregar la licencia al entorno.

1. Inicie sesión en la interfaz de usuario del Administrador de SDDC.
2. Vaya a **Administración > Licencias** en el panel de navegación.
3. Haga clic en **+ Clave de licencia**.
4. Elija un producto del menú desplegable.
5. Introduzca la clave de licencia.
6. Proporcione una descripción de la licencia.
7. Haga clic en **Agregar**.
8. Repita estos pasos para cada licencia.

Configurar un clúster extendido para un dominio de administración de VCF mediante SnapMirror Active Sync

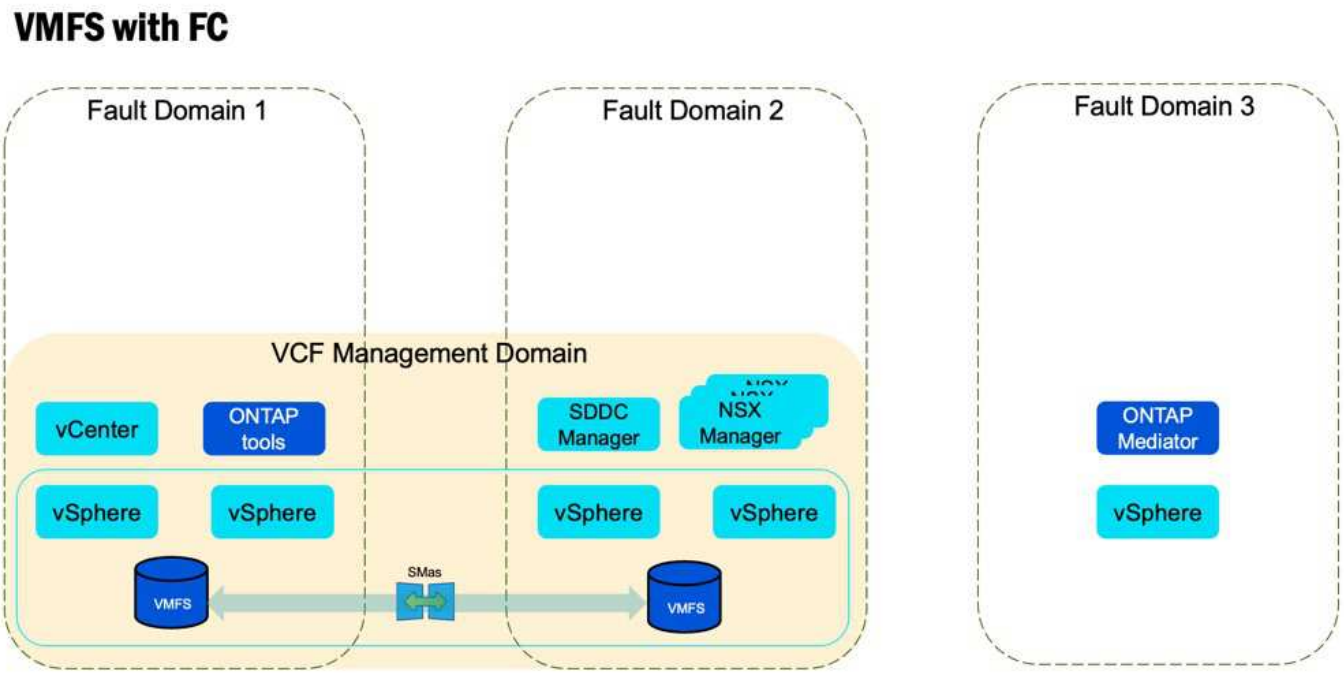
En este caso de uso, describimos el procedimiento para utilizar las ONTAP tools for VMware vSphere para configurar un clúster extendido para un dominio de administración de VCF. Este procedimiento incluye la implementación de hosts vSphere y vCenter Server, la instalación de herramientas ONTAP , la protección de almacenes de datos con SnapMirror Active Sync, la migración de máquinas virtuales a almacenes de datos protegidos y la configuración de almacenamiento complementario.



Descripción general del escenario

La solución de clúster extendido se puede implementar en un clúster predeterminado o en un clúster adicional

en los dominios de administración de VCF o de carga de trabajo. VMFS en FC es compatible tanto con el almacén de datos principal como con los almacenes de datos complementarios. VMFS en iSCSI solo es compatible con almacenes de datos complementarios. Consulte IMT para obtener soporte de VMFS en NVMe-oF con sincronización activa de SnapMirror .



Almacenamiento principal en el dominio de administración

A partir de VCF 5.2, el dominio de administración se puede implementar sin VSAN utilizando la herramienta de importación de VCF. La opción de conversión de la herramienta de importación VCF permite"una implementación de vCenter existente en un dominio de administración" . Todos los clústeres en vCenter pasarán a formar parte del dominio de administración.

1. Implementar hosts vSphere
2. Implementar el servidor vCenter en el almacén de datos local (vCenter debe coexistir en los hosts vSphere que se convertirán en un dominio de administración)
3. Implementar ONTAP tools for VMware vSphere
4. Implementar el complemento SnapCenter para VMware vSphere (opcional)
5. Crear un almacén de datos (la configuración de la zona FC debe estar establecida)
6. Proteger el clúster de vSphere
7. Migrar máquinas virtuales a un almacén de datos recién creado

> Cada vez que se expande o se reduce el clúster, es necesario actualizar la relación del clúster de host en las herramientas de ONTAP para el clúster a fin de indicar los cambios realizados en el origen o el destino.

Almacenamiento complementario en el dominio de administración

Una vez que el dominio de administración esté en funcionamiento, se pueden crear almacenes de datos adicionales utilizando herramientas ONTAP que activarán la expansión del grupo de consistencia.

> Si un clúster de vSphere está protegido, todos los almacenes de datos del clúster estarán protegidos.

Si el entorno VCF se implementa con la herramienta Cloud Builder, para crear el almacenamiento complementario con iSCSI, implemente las herramientas ONTAP para crear el almacén de datos iSCSI y proteger el clúster vSphere.

> Cada vez que se expande o se reduce el clúster, es necesario actualizar la relación del clúster de host en las herramientas de ONTAP para el clúster a fin de indicar los cambios realizados en el origen o el destino.

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

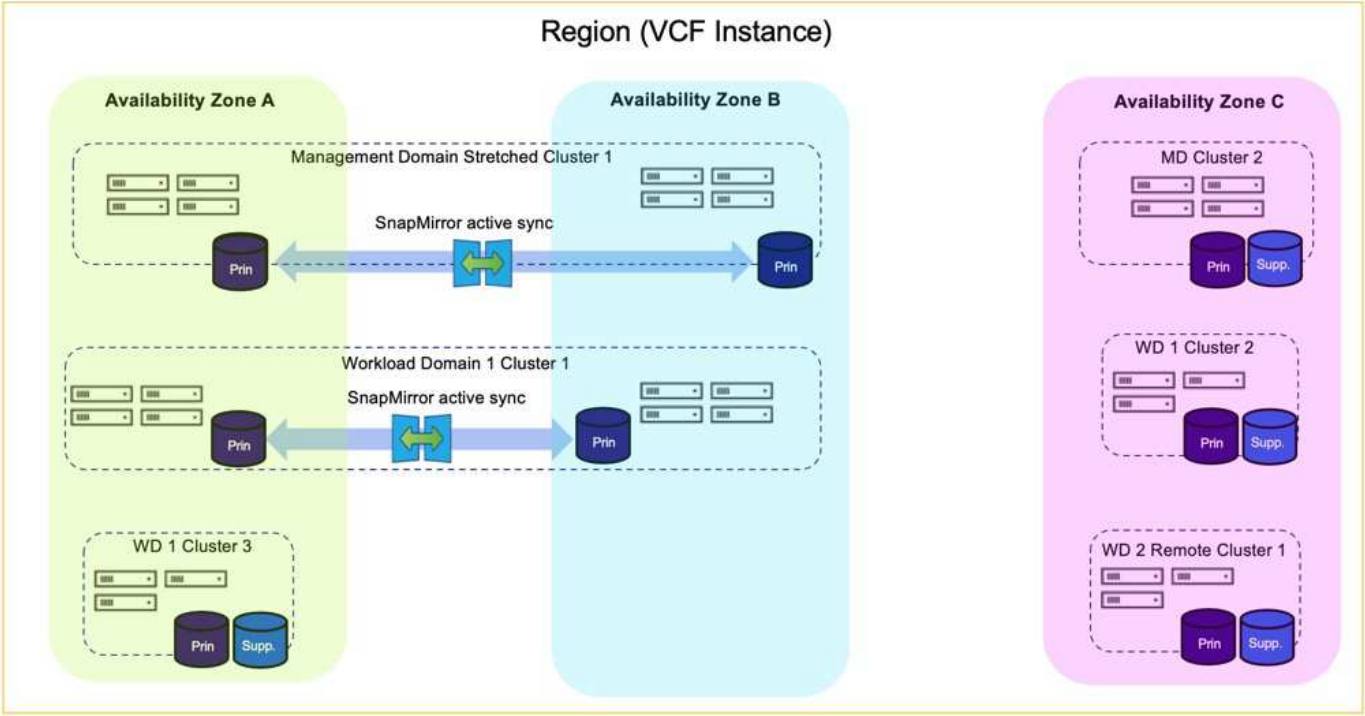
Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation 5.2" .

Demostración en vídeo de esta solución

Ampliar clúster para VCF con herramientas ONTAP

Configurar un clúster extendido para un dominio de carga de trabajo VI mediante SnapMirror Active Sync

En este caso de uso, describimos el procedimiento para configurar un clúster extendido para un dominio de carga de trabajo de infraestructura virtual (VI) mediante SnapMirror Active Sync con ONTAP tools for VMware vSphere. Este procedimiento incluye la creación de un dominio de carga de trabajo VCF con VMFS en Fibre Channel, el registro de vCenter con herramientas ONTAP , el registro de sistemas de almacenamiento y la protección del clúster vSphere.



Descripción general del escenario

Los almacenes de datos en el dominio de carga de trabajo VCF se pueden proteger con la sincronización activa de SnapMirror para proporcionar una solución de clúster extendido. La protección está habilitada en el nivel del clúster vSphere y todos los almacenes de datos de bloques ONTAP en el clúster estarán protegidos.

Almacenamiento principal en el dominio de carga de trabajo

El dominio de carga de trabajo se puede crear importándolo mediante la herramienta de importación VCF o implementándolo mediante el administrador SDDC. La implementación con el administrador SDDC proporcionará más opciones de red que importar un entorno existente.

1. Crear un dominio de carga de trabajo con VMFS en FC
2. "Registrar el dominio de carga de trabajo vCenter en el administrador de herramientas de ONTAP para implementar el complemento vCenter"
3. "Registrar sistemas de almacenamiento en las herramientas ONTAP"
4. "Proteger el clúster de vSphere"

> Cada vez que se expande o se reduce el clúster, es necesario actualizar la relación del clúster de host en las herramientas de ONTAP para el clúster a fin de indicar los cambios realizados en el origen o el destino.

Almacenamiento complementario en el dominio de carga de trabajo

Una vez que el dominio de carga de trabajo esté en funcionamiento, se pueden crear almacenes de datos adicionales utilizando herramientas ONTAP que activarán la expansión del grupo de consistencia.

Si un clúster de vSphere está protegido, todos los almacenes de datos del clúster estarán protegidos.

Información adicional

Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte"Documentación de ONTAP 9" centro.

Para obtener información sobre la configuración de VCF, consulte"Documentación de VMware Cloud Foundation" .

Demostración en vídeo de esta solución

Ampliar clúster para VCF con herramientas ONTAP

Migrar máquinas virtuales de VMware vSphere a almacenes de datos de ONTAP

Los entornos VMware vSphere pueden beneficiarse significativamente de la migración de máquinas virtuales a almacenes de datos respaldados por NetApp ONTAP. Ya sea que esté migrando de vSAN, sistemas de almacenamiento de terceros o actualizando su infraestructura existente, explore varios escenarios de vMotion y estrategias de migración para realizar una transición sin problemas de sus máquinas virtuales a almacenes de datos de ONTAP . Esto garantiza la continuidad del negocio al tiempo que aprovecha las funciones de almacenamiento de clase empresarial de ONTAP.

VMware vSphere de Broadcom admite almacenes de datos VMFS, NFS y vVol para alojar máquinas virtuales. Los clientes tienen la opción de crear esos almacenes de datos con infraestructuras hiperconvergentes o con sistemas de almacenamiento compartido centralizados.

Los clientes a menudo ven el valor del alojamiento en sistemas de almacenamiento basados en ONTAP para proporcionar instantáneas y clones de máquinas virtuales que ahorran espacio, flexibilidad para elegir varios modelos de implementación en los centros de datos y las nubes, eficiencia operativa con herramientas de monitoreo y alerta, seguridad, gobernanza y herramientas de cumplimiento opcionales para inspeccionar datos de máquinas virtuales, etc.

Las máquinas virtuales alojadas en almacenes de datos de ONTAP se pueden proteger mediante el complemento SnapCenter para VMware vSphere (SCV). SCV crea instantáneas basadas en almacenamiento y también las replica en el sistema de almacenamiento ONTAP remoto. Las restauraciones se pueden realizar desde sistemas de almacenamiento primario o secundario.

Los clientes tienen la flexibilidad de elegir Cloud Insights o Aria Operations o una combinación de ambos u otras herramientas de terceros que utilizan la API de ONTAP para solucionar problemas, monitorear el rendimiento, generar informes y funciones de notificación de alertas.

Los clientes pueden aprovisionar fácilmente almacenes de datos mediante el complemento vCenter de ONTAP Tools o su API, y las máquinas virtuales se pueden migrar a almacenes de datos de ONTAP incluso mientras están encendidos.

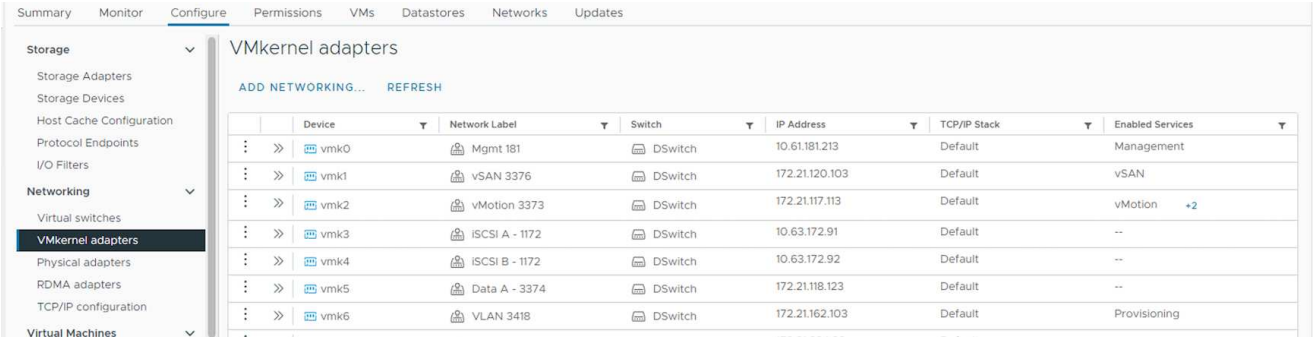
> Algunas máquinas virtuales que se implementan con herramientas de administración externa como Aria Automation, Tanzu (u otras versiones de Kubernetes) generalmente dependen de la política de almacenamiento de la máquina virtual. Si se migra entre almacenes de datos dentro de la misma política de almacenamiento de VM, debería tener menos impacto para las aplicaciones. Consulte con los propietarios de las aplicaciones para migrar correctamente esas máquinas virtuales al nuevo almacén de datos. Se presentó vSphere 8 "Notificaciones de vSphere vMotion para aplicaciones sensibles a la latencia" para preparar aplicaciones para vMotion.

Requisitos de red

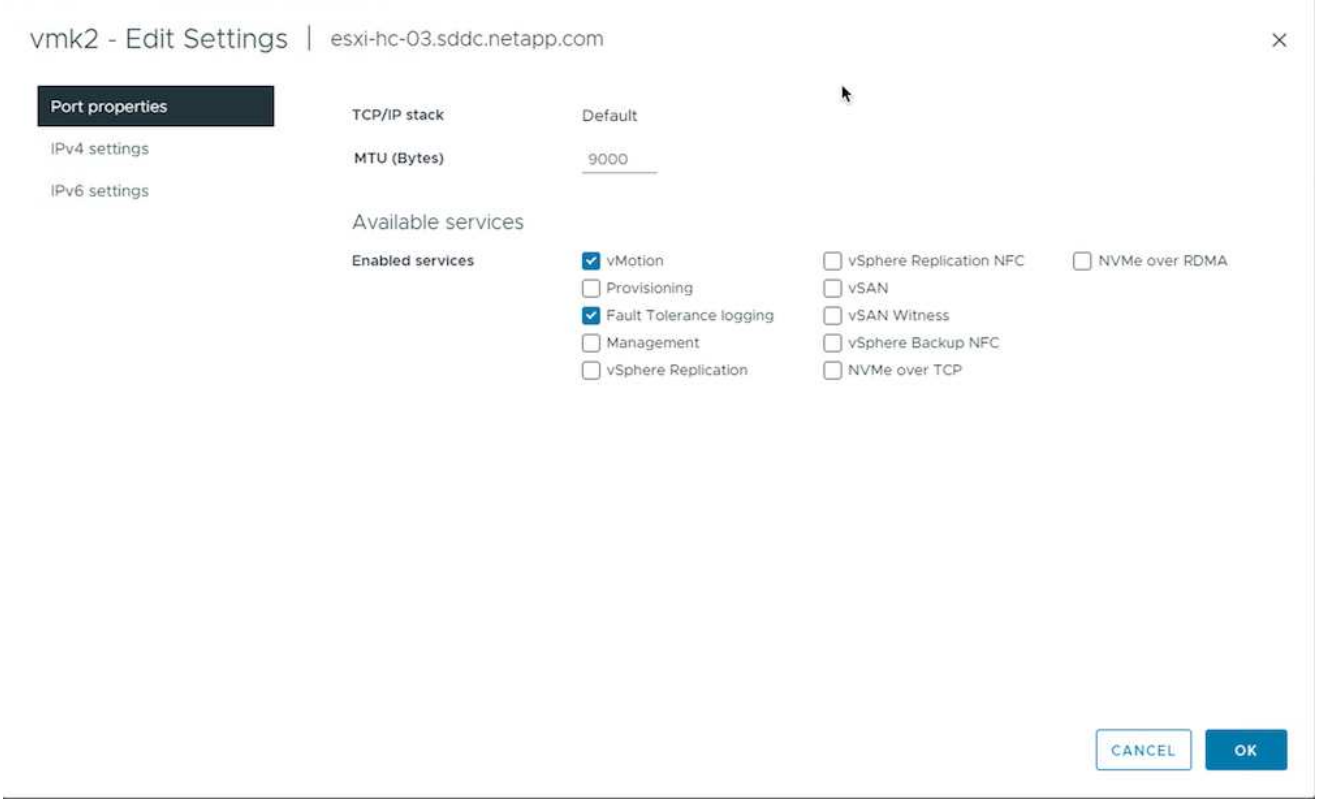
Migración de máquinas virtuales con vMotion

Se supone que ya existe una red de almacenamiento dual para el almacén de datos de ONTAP para proporcionar conectividad, tolerancia a fallas y mejora del rendimiento.

La migración de máquinas virtuales entre los hosts de vSphere también se gestiona mediante la interfaz VMKernel del host de vSphere. Para la migración en caliente (máquinas virtuales encendidas), se utiliza la interfaz VMKernel con el servicio vMotion habilitado, y para la migración en frío (máquinas virtuales apagadas), se utiliza la interfaz VMKernel con el servicio de aprovisionamiento habilitado para mover los datos. Si no se encuentra una interfaz válida, se utilizará la interfaz de administración para mover los datos, lo que puede no ser deseable para ciertos casos de uso.



Al editar la interfaz VMKernel, aquí está la opción para habilitar los servicios requeridos.



Asegúrese de que haya al menos dos NIC de enlace ascendente activas de alta velocidad disponibles para el grupo de puertos utilizado por las interfaces vMotion y Provisioning VMkernel.

Escenarios de migración de máquinas virtuales

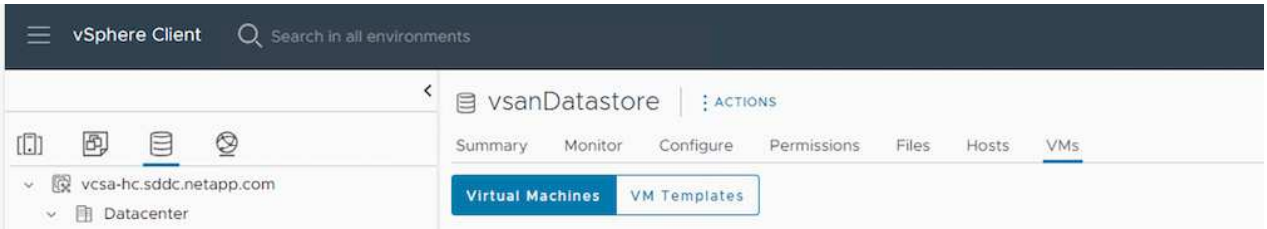
vMotion se utiliza a menudo para migrar las máquinas virtuales independientemente de su estado de energía. A continuación se encuentran disponibles consideraciones adicionales y procedimientos de migración para escenarios específicos.

> Entender "Condiciones de VM y limitaciones de vSphere vMotion" antes de continuar con cualquier opción de migración de VM.

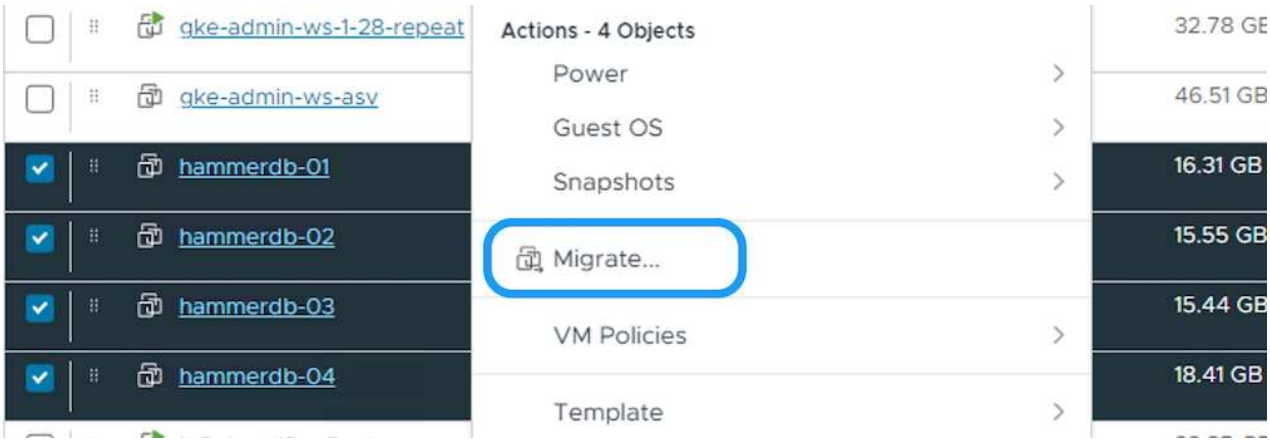
Migración de máquinas virtuales desde un almacén de datos de vSphere específico

Siga el procedimiento a continuación para migrar máquinas virtuales a un nuevo almacén de datos mediante la interfaz de usuario.

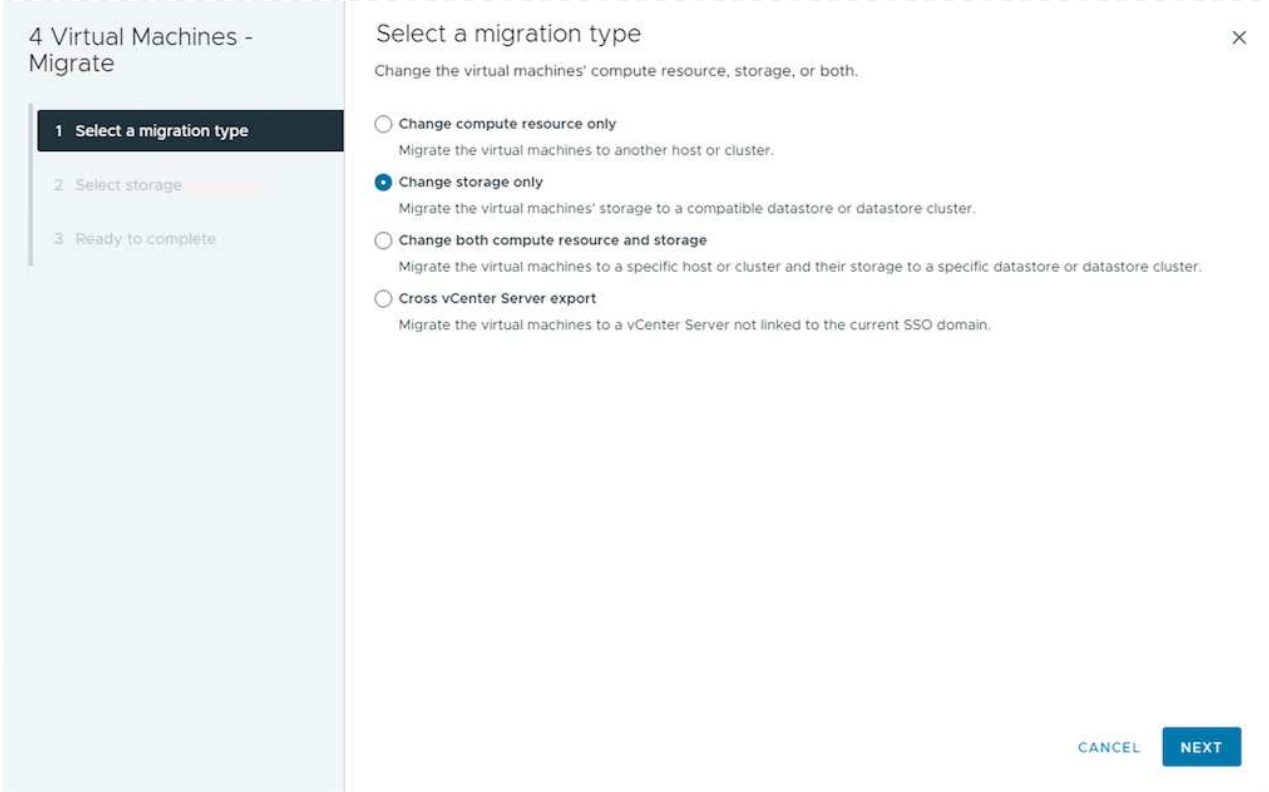
1. Con vSphere Web Client, seleccione el almacén de datos del inventario de almacenamiento y haga clic en la pestaña Máquinas virtuales.



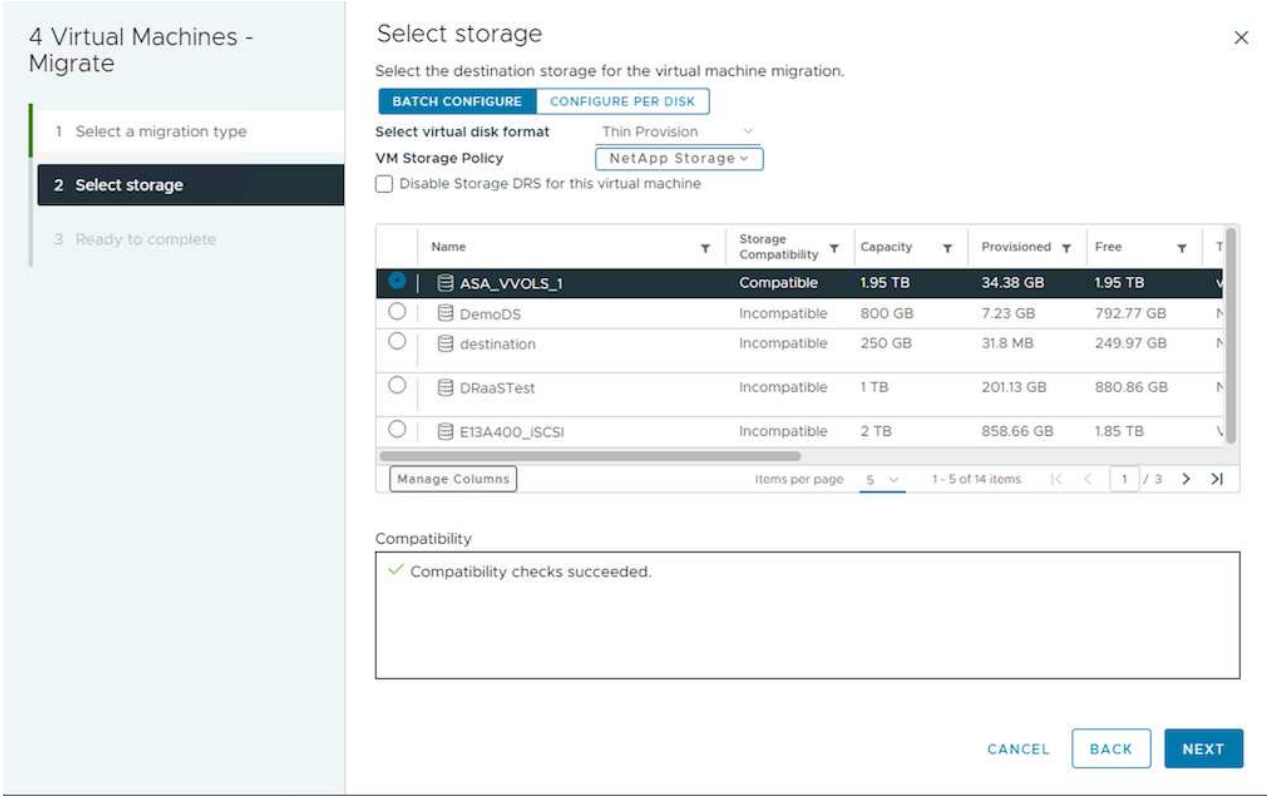
2. Seleccione las máquinas virtuales que necesitan migrarse y haga clic derecho para seleccionar la opción Migrar.



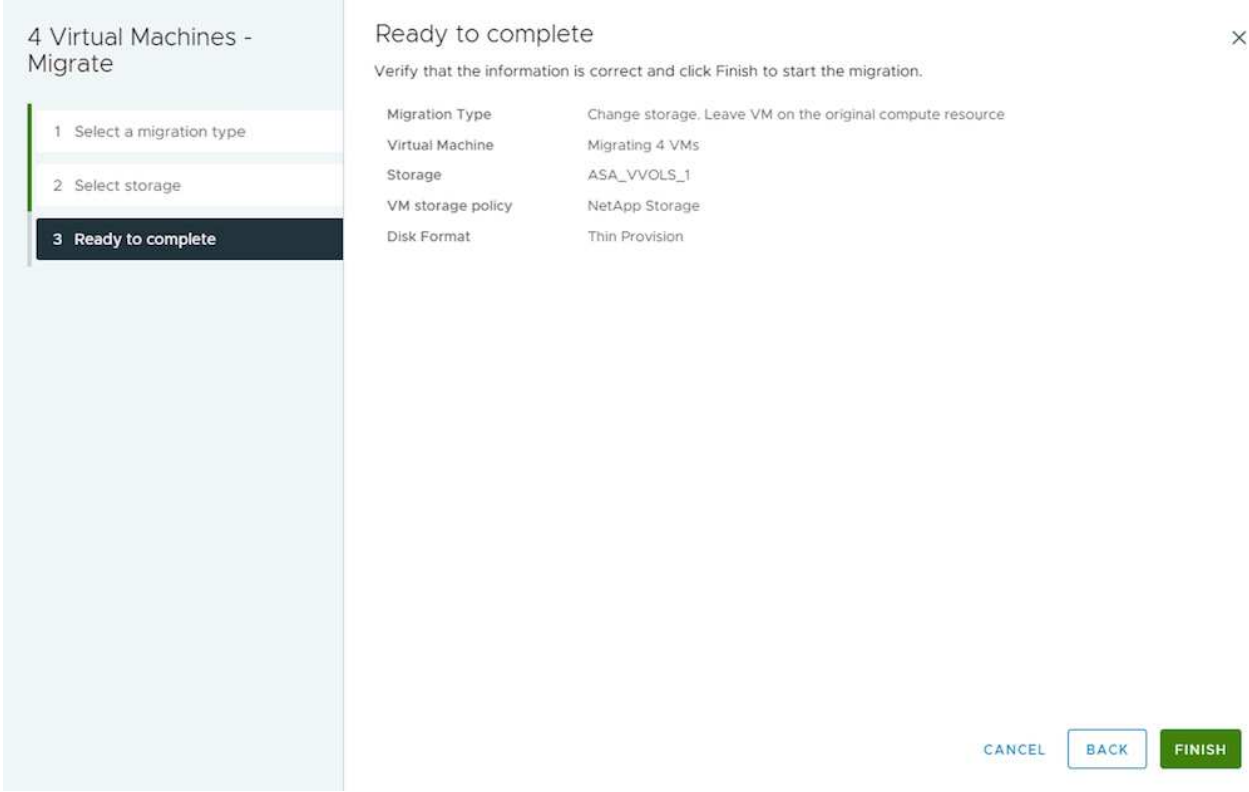
3. Elija la opción para cambiar solo el almacenamiento, haga clic en Siguiente



4. Seleccione la política de almacenamiento de VM deseada y elija el almacén de datos que sea compatible. Haga clic en Siguiente.



5. Revisar y hacer clic en Finalizar.



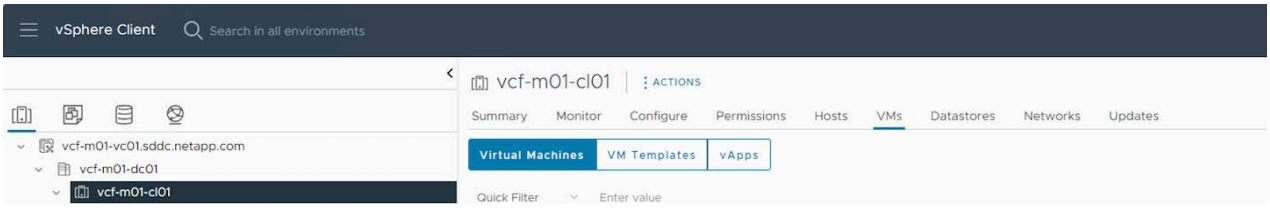
Para migrar máquinas virtuales mediante PowerCLI, aquí se muestra el script de muestra.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

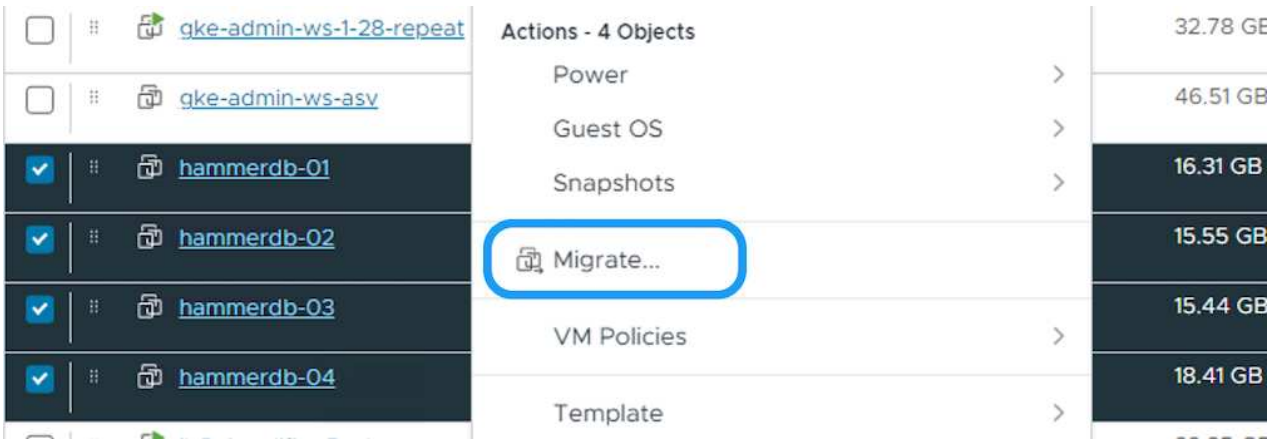
Migración de máquinas virtuales en el mismo clúster de vSphere

Siga el procedimiento a continuación para migrar máquinas virtuales a un nuevo almacén de datos mediante la interfaz de usuario.

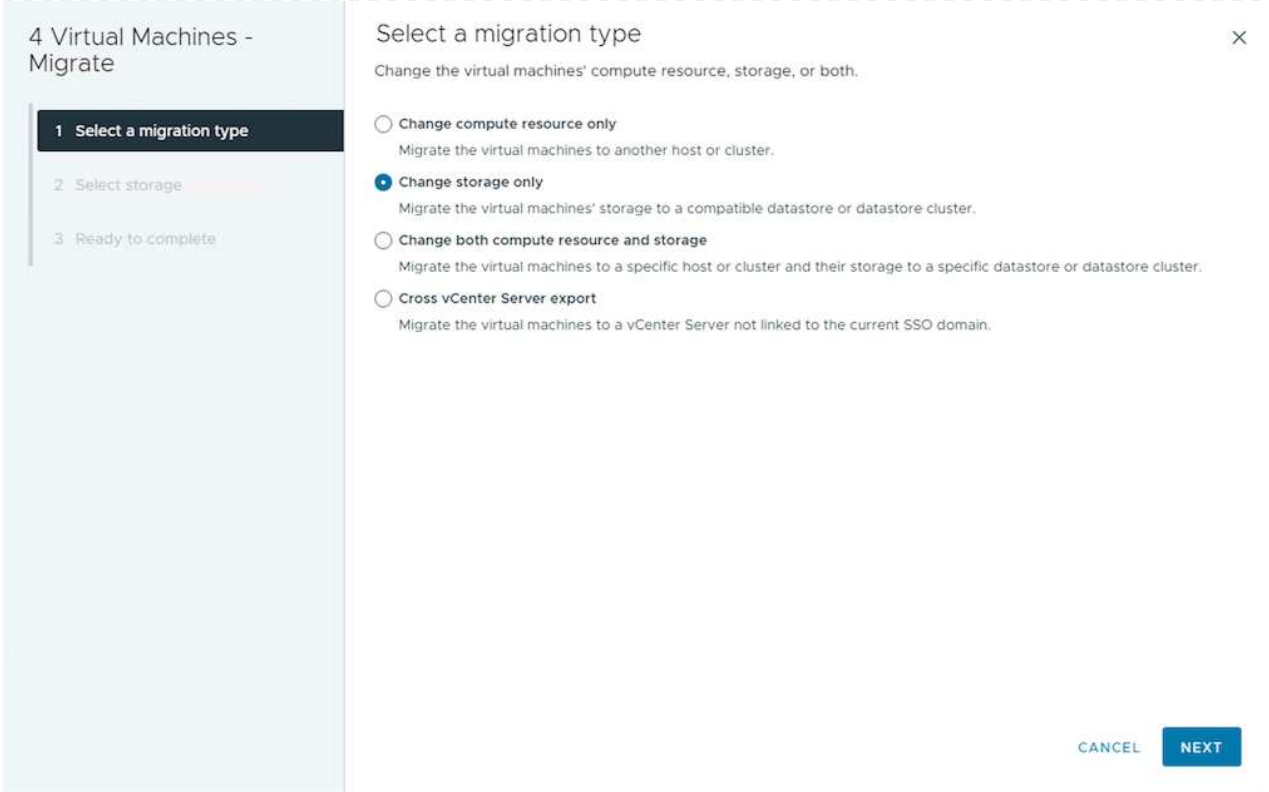
1. Con vSphere Web Client, seleccione el Clúster del inventario de Host y Clúster y haga clic en la pestaña Máquinas virtuales.



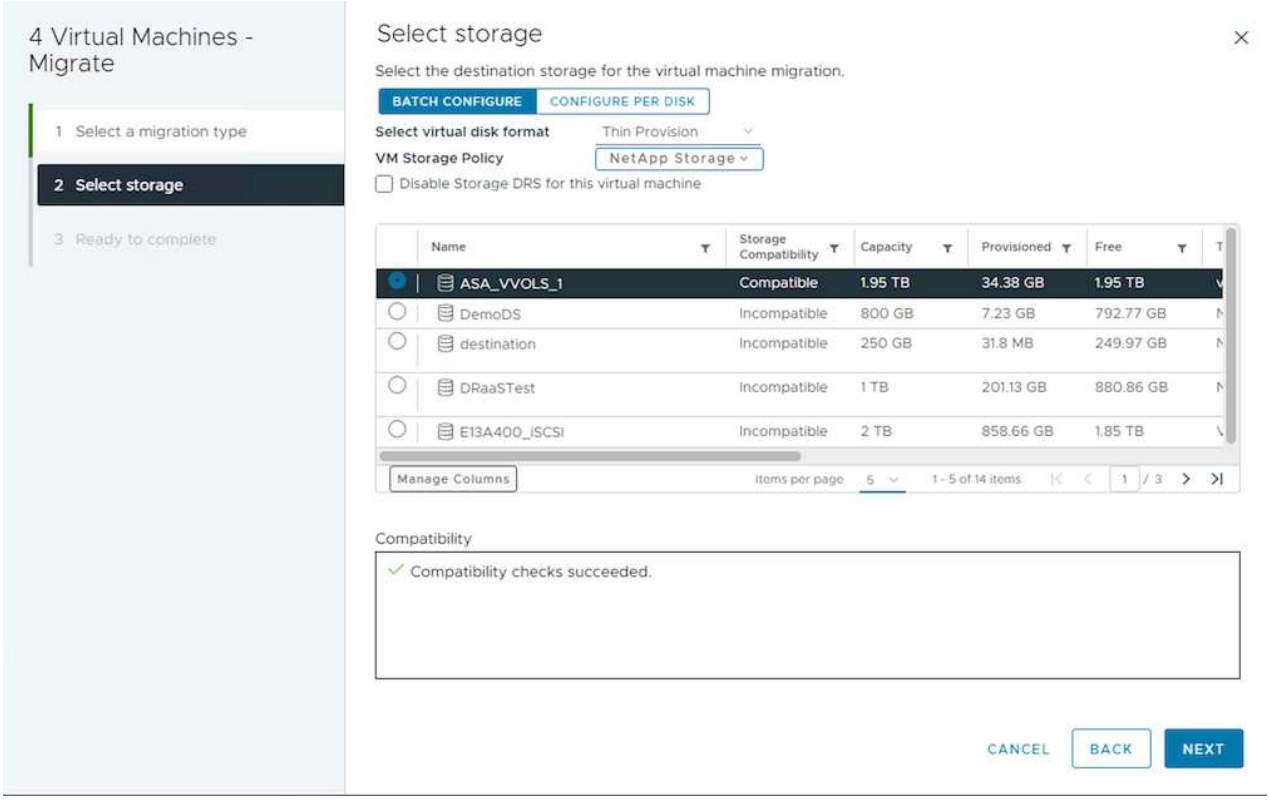
2. Seleccione las máquinas virtuales que necesitan migrarse y haga clic derecho para seleccionar la opción Migrar.



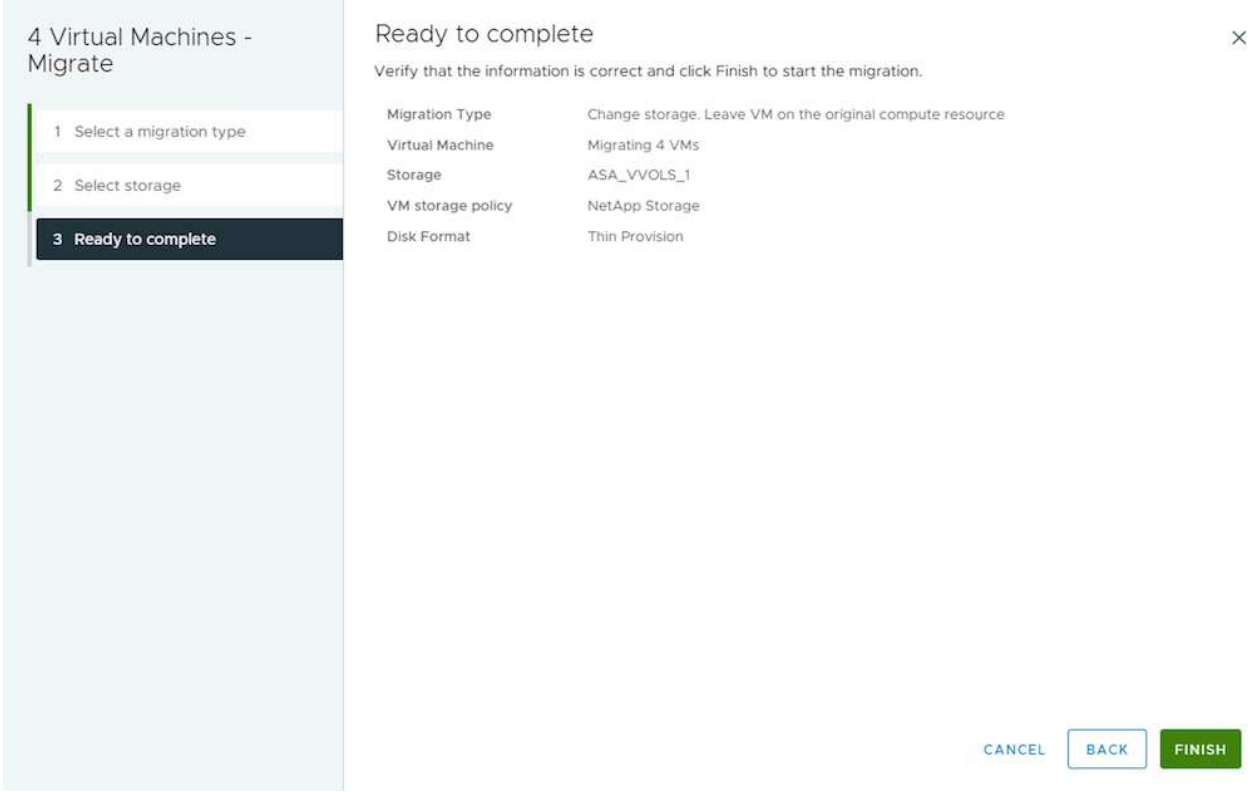
3. Elija la opción para cambiar solo el almacenamiento, haga clic en Siguiente



4. Seleccione la política de almacenamiento de VM deseada y elija el almacén de datos que sea compatible. Haga clic en Siguiente.



5. Revisar y hacer clic en Finalizar.



Para migrar máquinas virtuales mediante PowerCLI, aquí se muestra el script de muestra.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

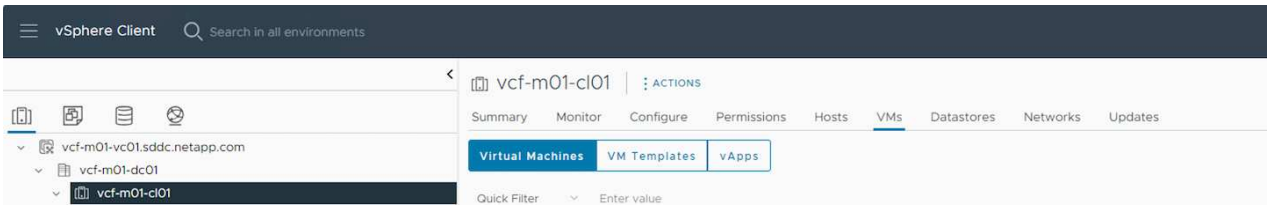
Cuando el clúster de almacén de datos se utiliza con DRS (programación dinámica de recursos) de almacenamiento totalmente automatizado y ambos almacenes de datos (de origen y de destino) son del mismo tipo (VMFS/NFS/vVol), mantenga ambos almacenes de datos en el mismo clúster de almacenamiento y migre las máquinas virtuales desde el almacén de datos de origen habilitando el modo de mantenimiento en el origen. La experiencia será similar a cómo se manejan los hosts de cómputo para mantenimiento.

Migración de máquinas virtuales entre varios clústeres de vSphere

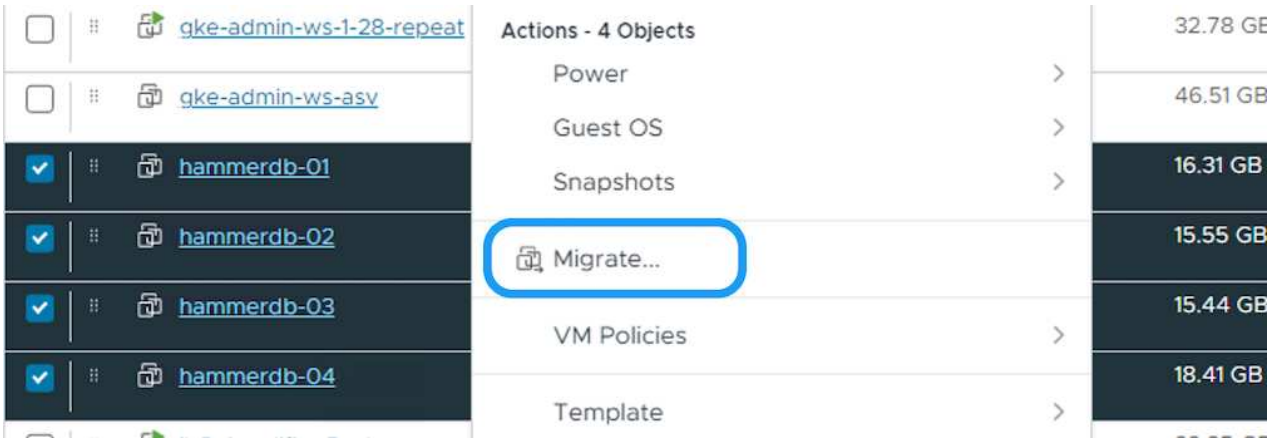
> Referirse "Compatibilidad de CPU y compatibilidad mejorada con vSphere vMotion" cuando los hosts de origen y destino son de diferentes familias o modelos de CPU.

Siga el procedimiento a continuación para migrar máquinas virtuales a un nuevo almacén de datos mediante la interfaz de usuario.

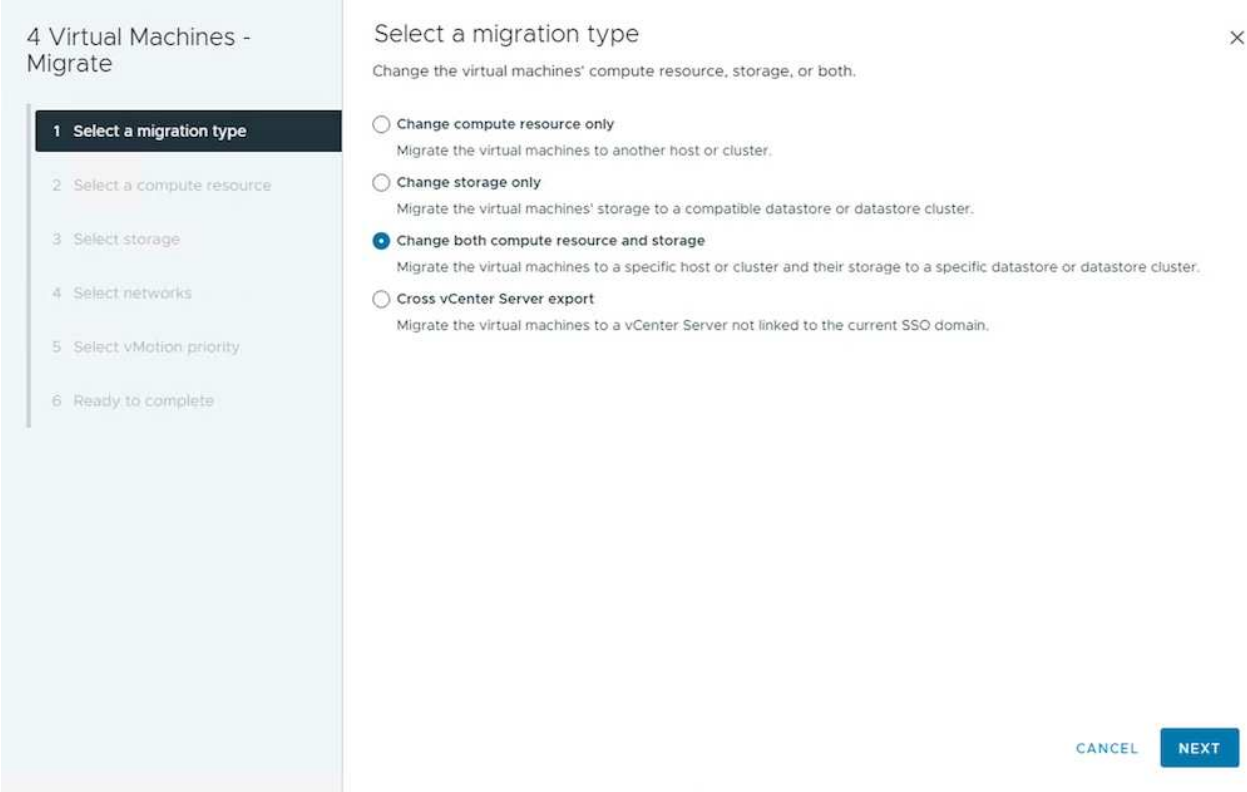
1. Con vSphere Web Client, seleccione el Clúster del inventario de Host y Clúster y haga clic en la pestaña Máquinas virtuales.



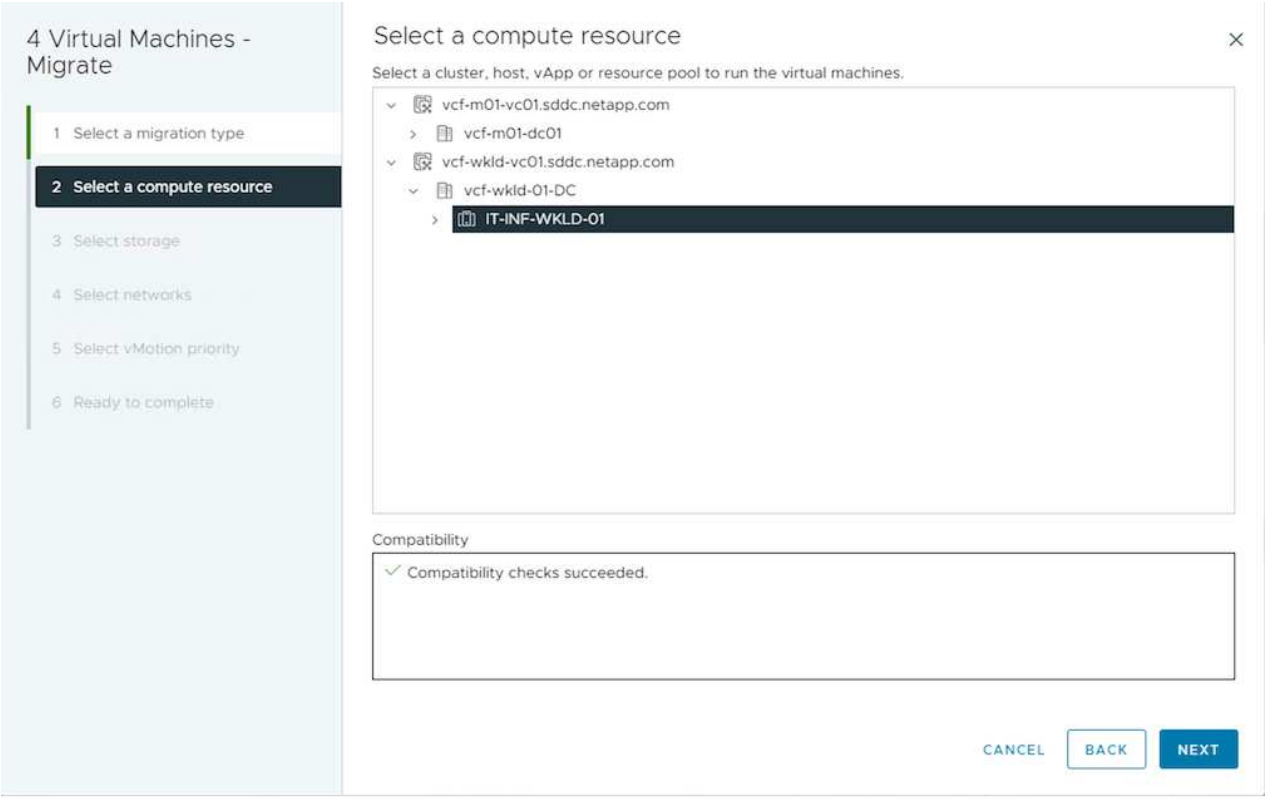
2. Seleccione las máquinas virtuales que necesitan migrarse y haga clic derecho para seleccionar la opción Migrar.



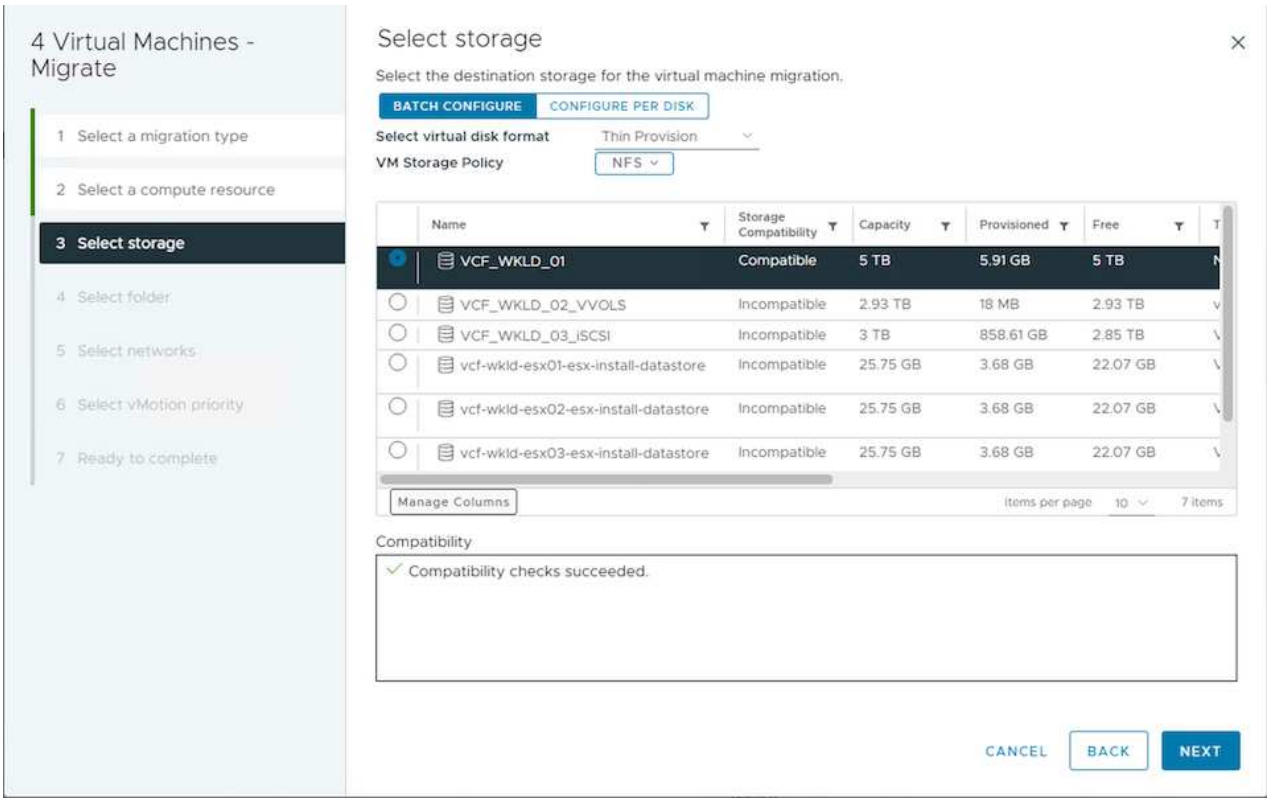
3. Elija la opción para cambiar el recurso computacional y el almacenamiento, haga clic en Siguiente



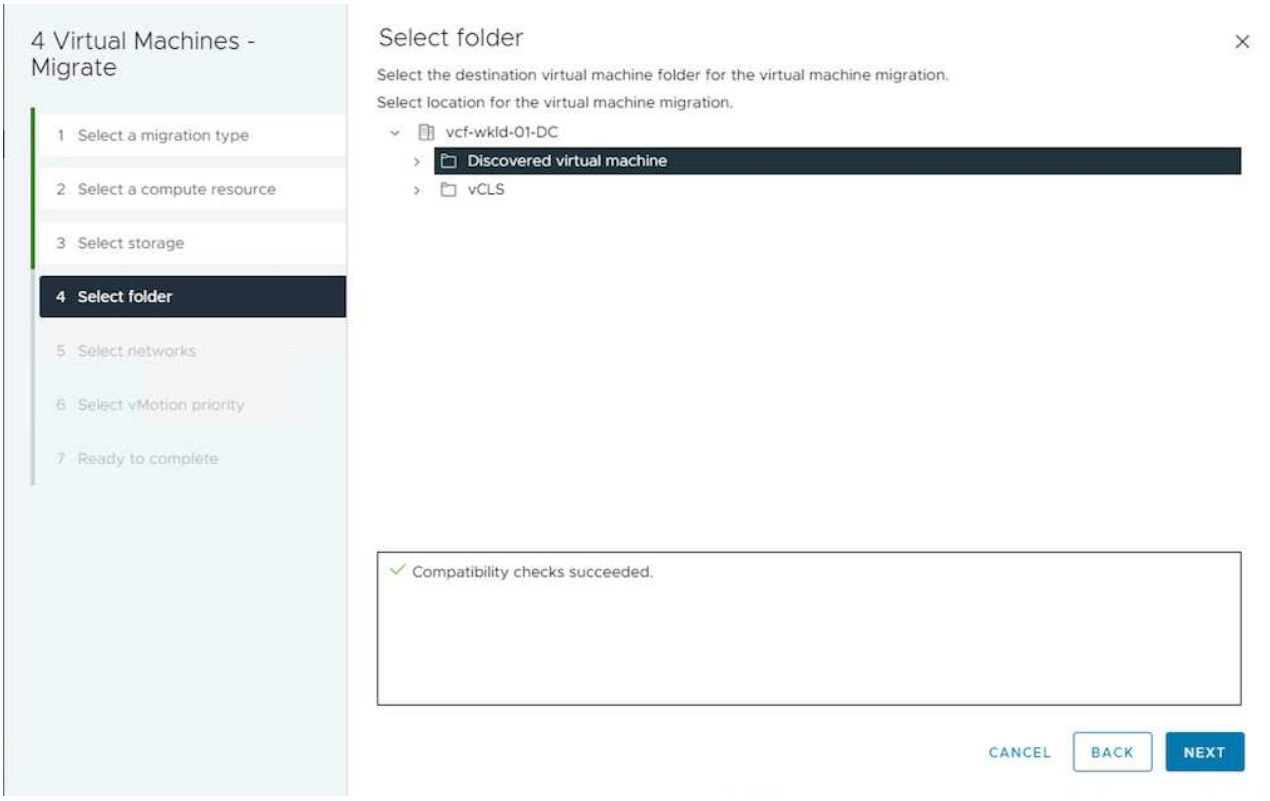
4. Navegue y seleccione el clúster correcto para migrar.



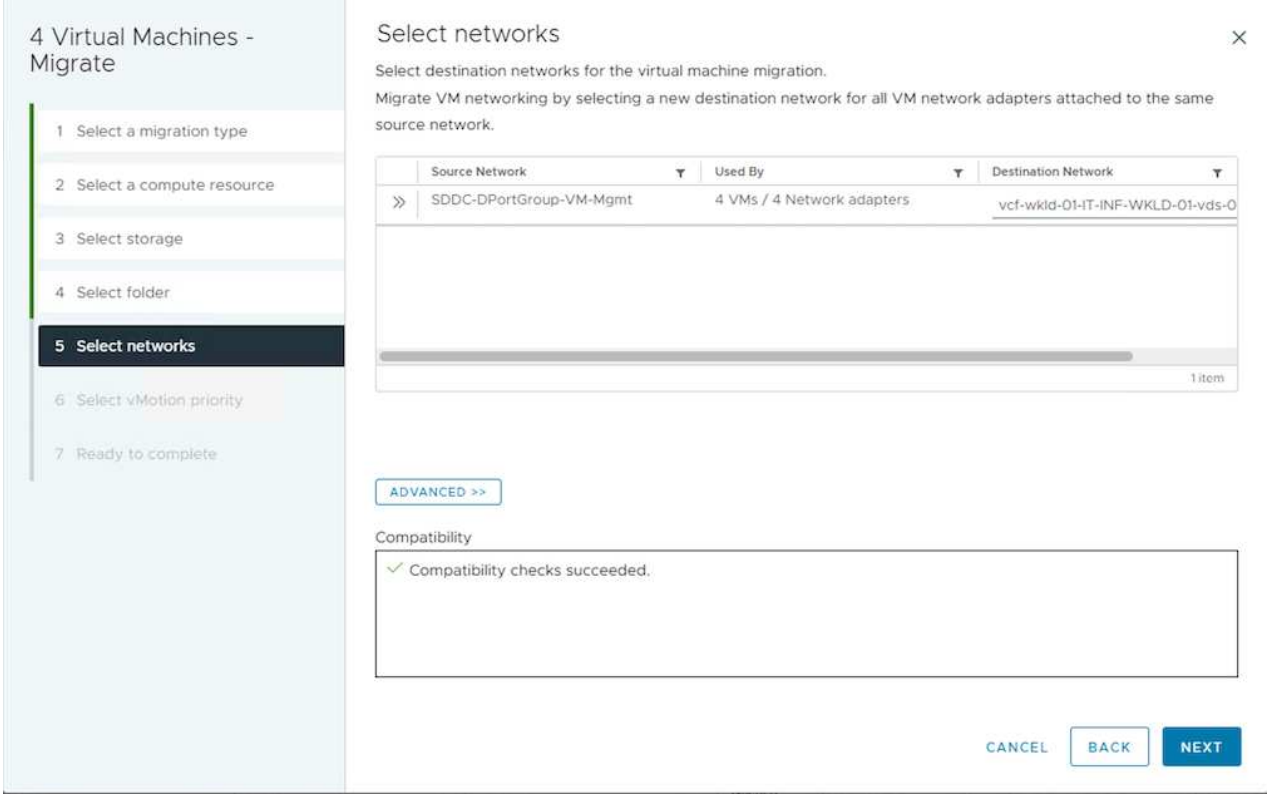
5. Seleccione la política de almacenamiento de VM deseada y elija el almacén de datos que sea compatible. Haga clic en Siguiente.



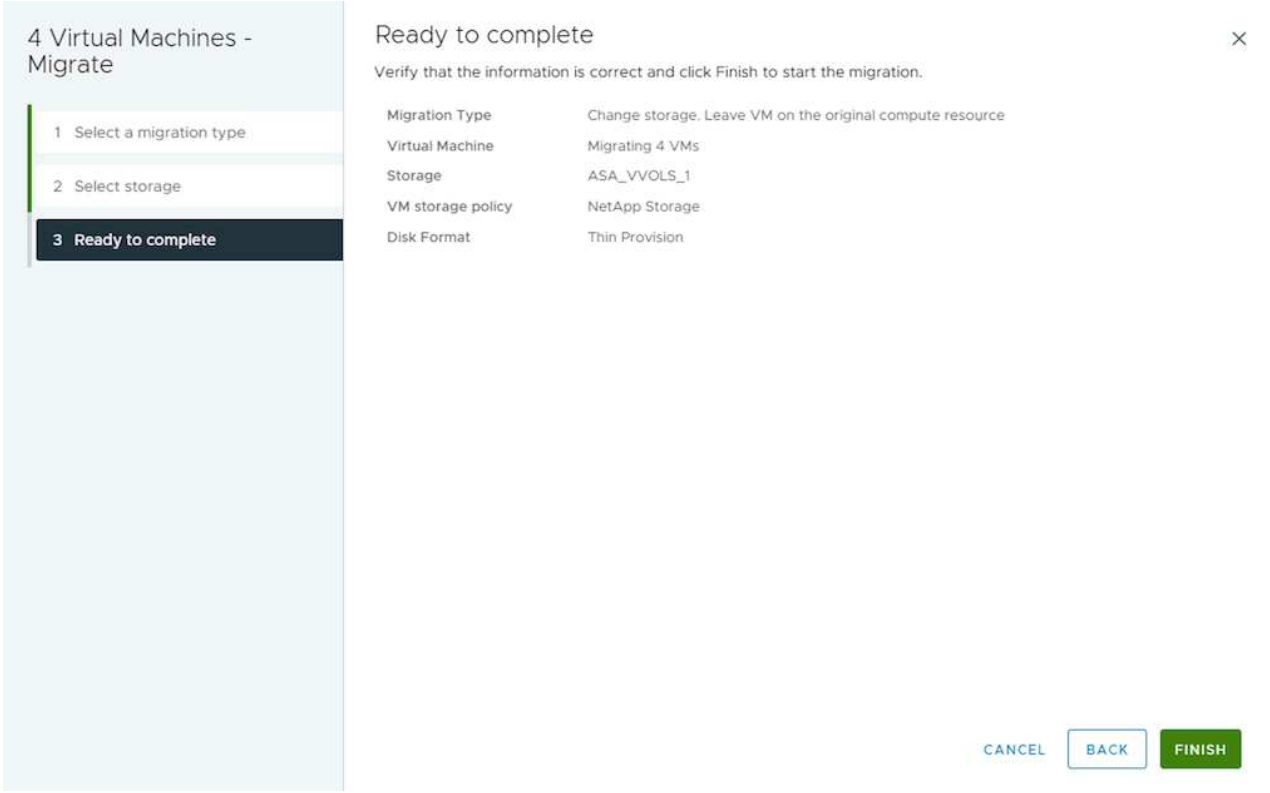
6. Seleccione la carpeta VM para colocar las VM de destino.



7. Seleccione el grupo de puertos de destino.



8. Revisar y hacer clic en Finalizar.



Para migrar máquinas virtuales mediante PowerCLI, aquí se muestra el script de muestra.

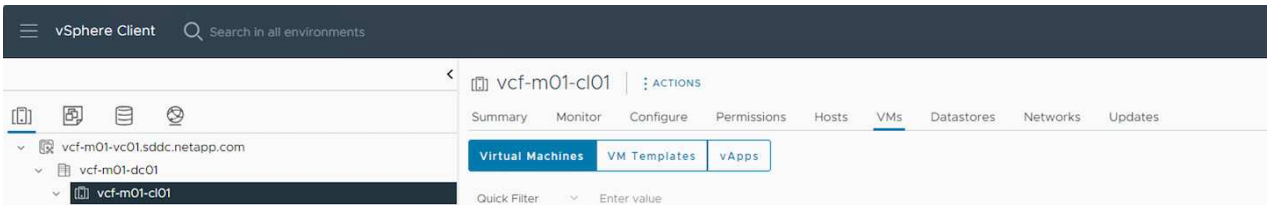
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

Migración de máquinas virtuales entre servidores vCenter en el mismo dominio SSO

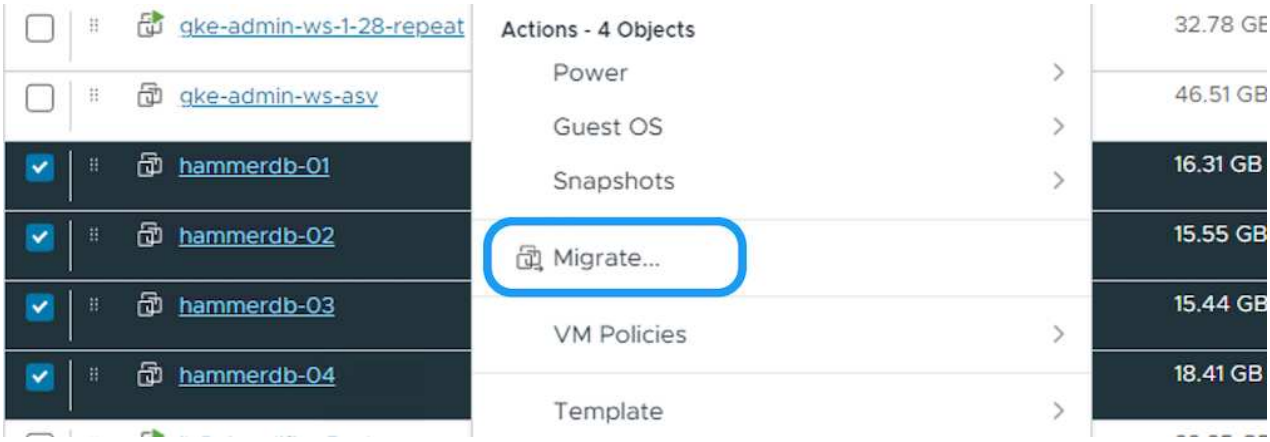
Siga el procedimiento a continuación para migrar máquinas virtuales al nuevo servidor vCenter que aparece en la misma interfaz de usuario de vSphere Client.

> Para conocer requisitos adicionales como versiones de vCenter de origen y destino, etc., consulte "Documentación de vSphere sobre los requisitos para vMotion entre instancias del servidor vCenter"

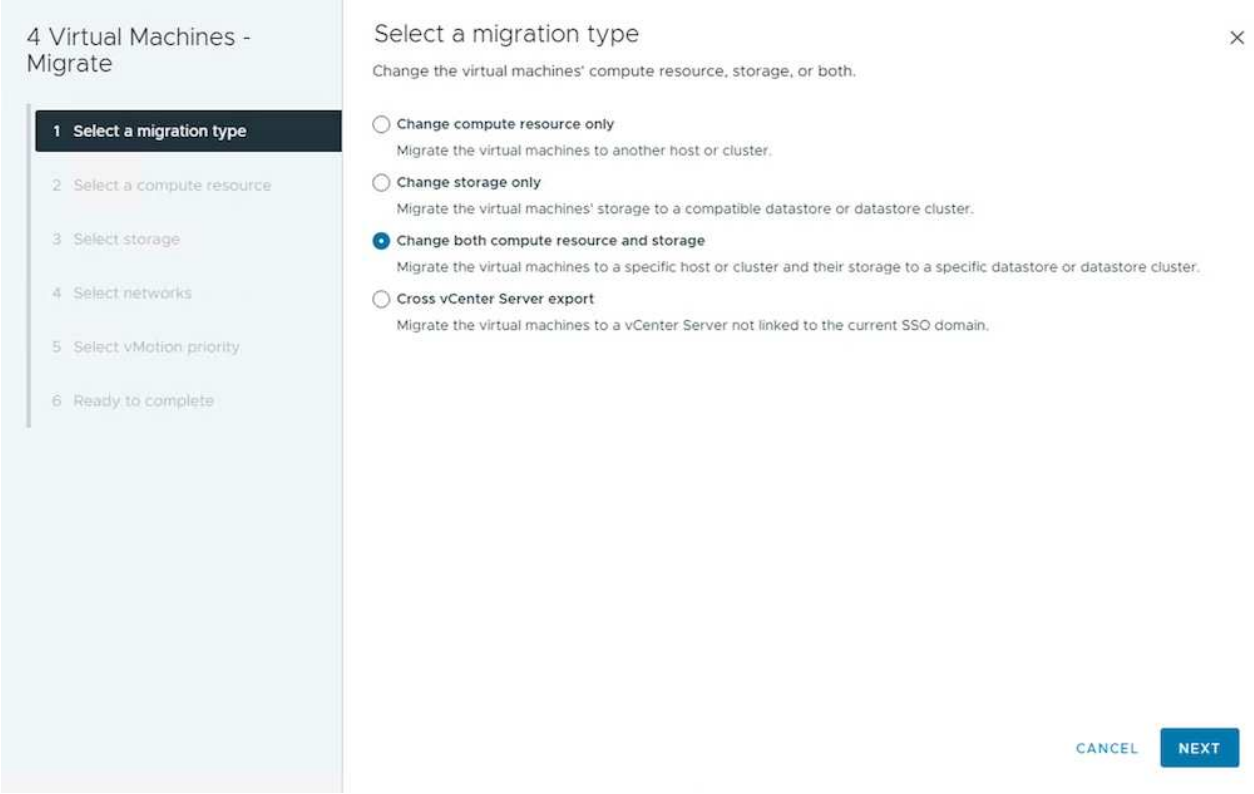
1. Con vSphere Web Client, seleccione el Clúster del inventario de Host y Clúster y haga clic en la pestaña Máquinas virtuales.



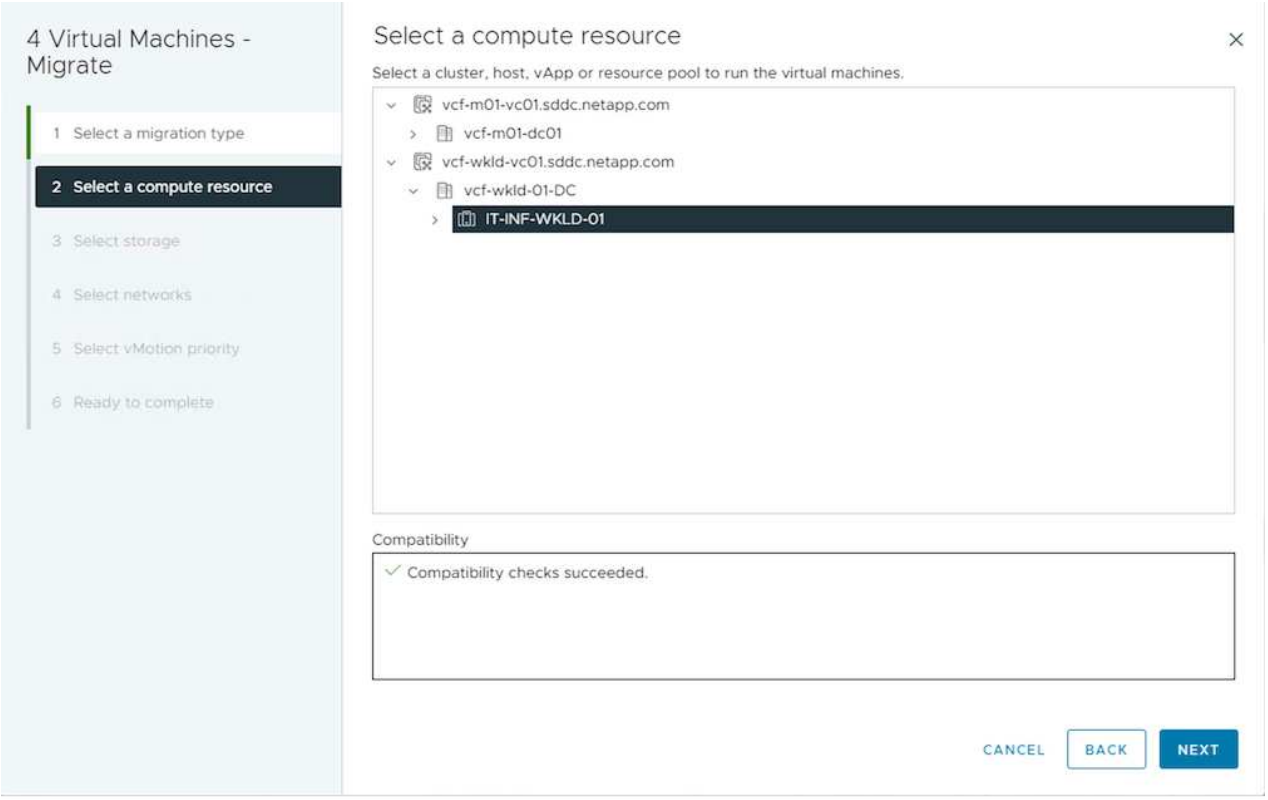
2. Seleccione las máquinas virtuales que necesitan migrarse y haga clic derecho para seleccionar la opción Migrar.



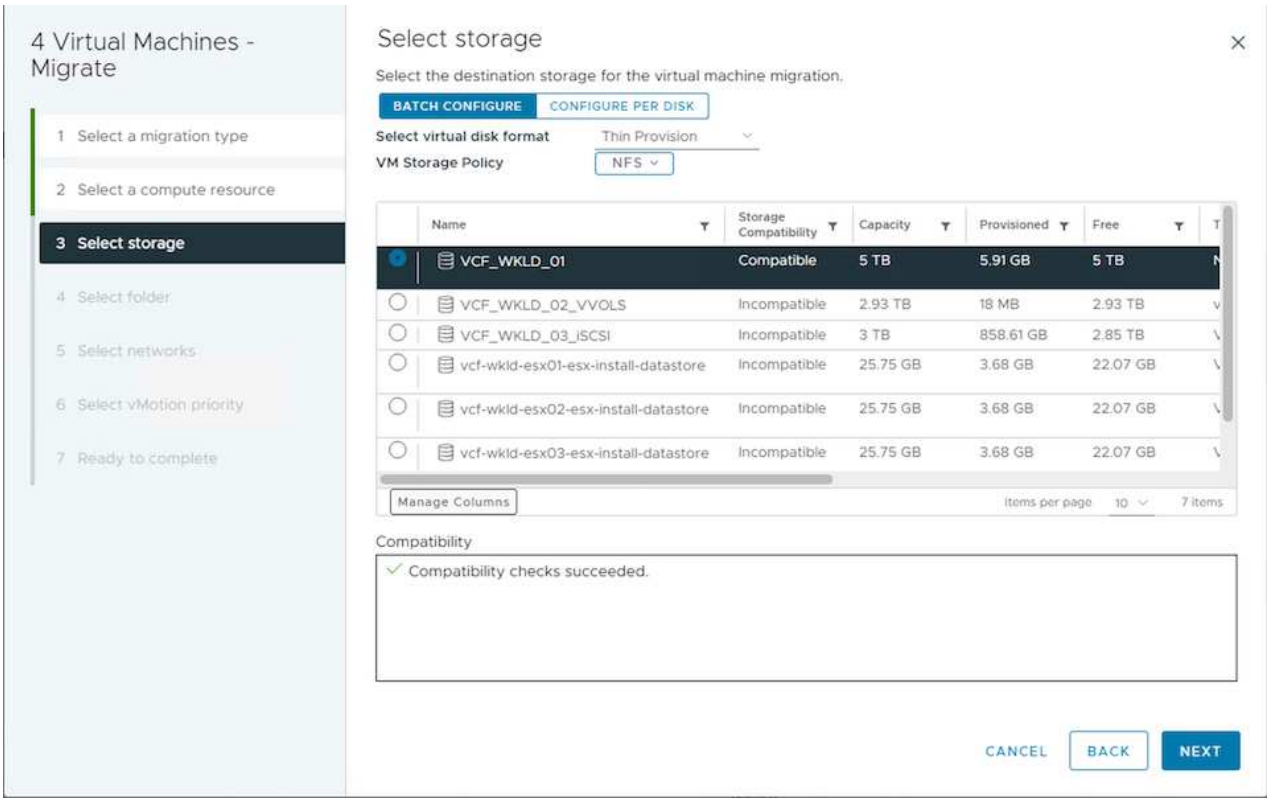
3. Elija la opción para cambiar el recurso computacional y el almacenamiento, haga clic en Siguiente



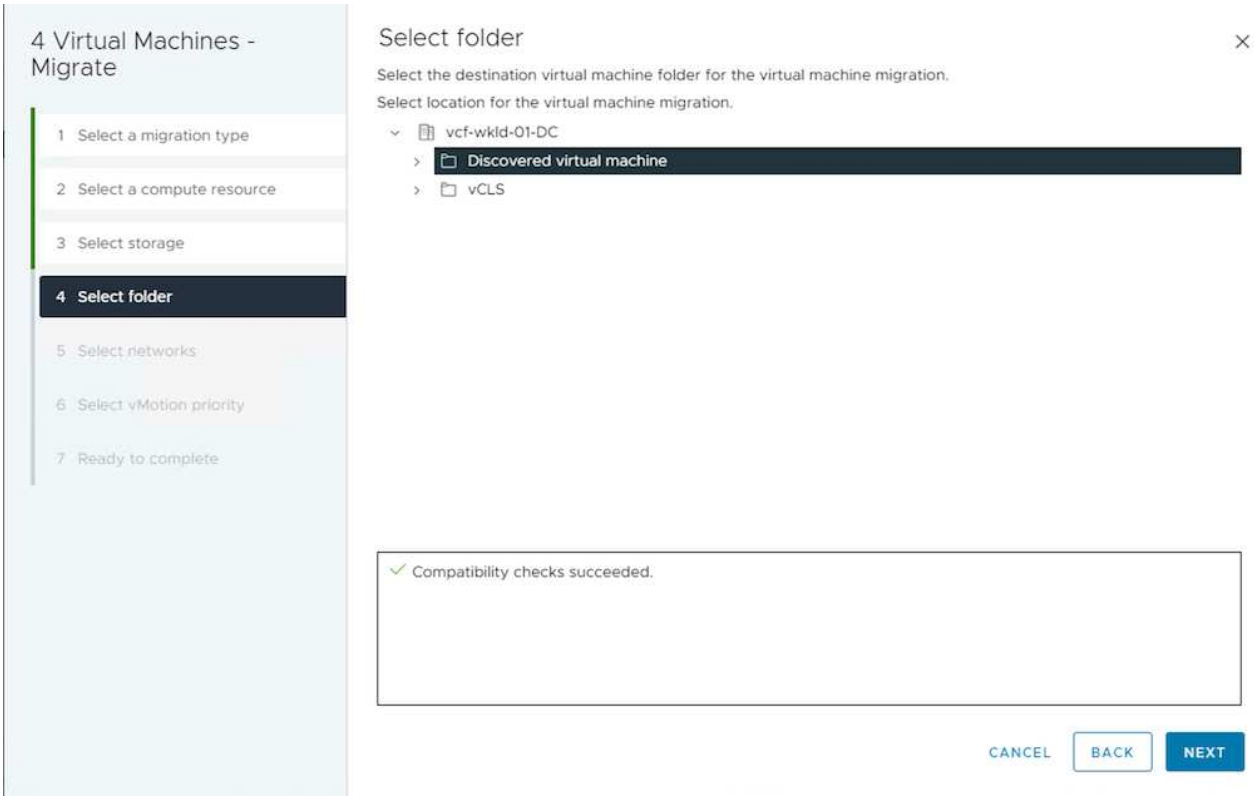
4. Seleccione el clúster de destino en el servidor vCenter de destino.



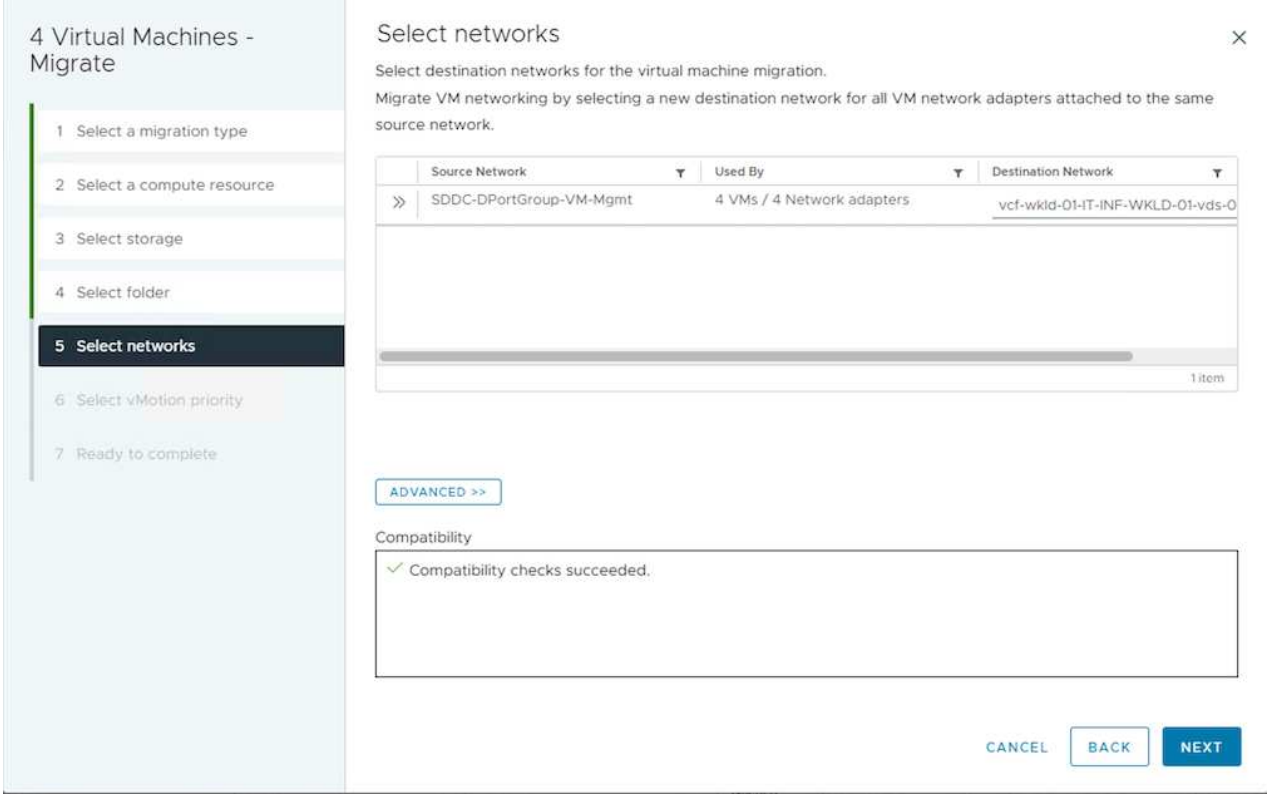
5. Seleccione la política de almacenamiento de VM deseada y elija el almacén de datos que sea compatible. Haga clic en Siguiente.



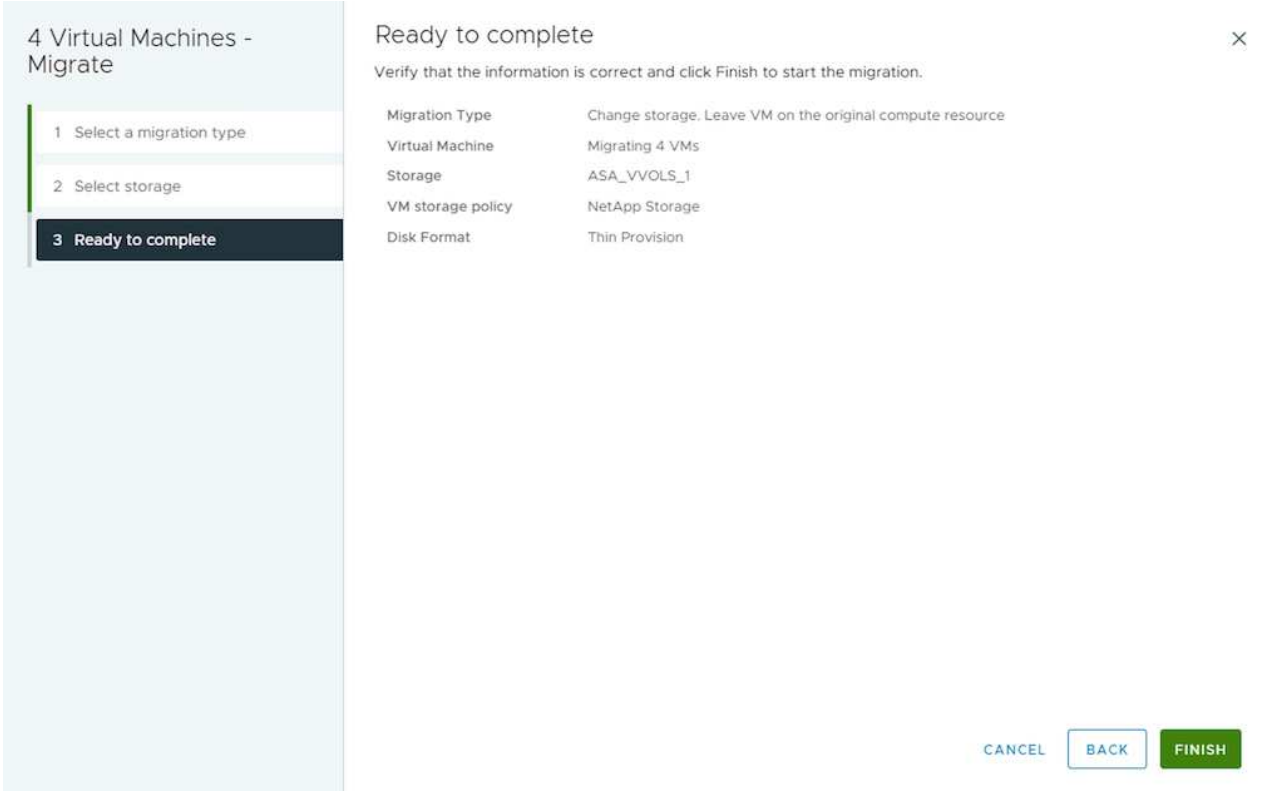
6. Seleccione la carpeta VM para colocar las VM de destino.



7. Seleccione el grupo de puertos de destino.



8. Revise las opciones de migración y haga clic en Finalizar.



Para migrar máquinas virtuales mediante PowerCLI, aquí se muestra el script de muestra.

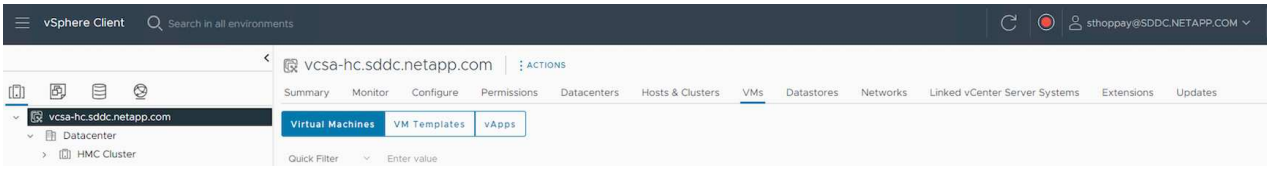
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migración de máquinas virtuales entre servidores vCenter en diferentes dominios SSO

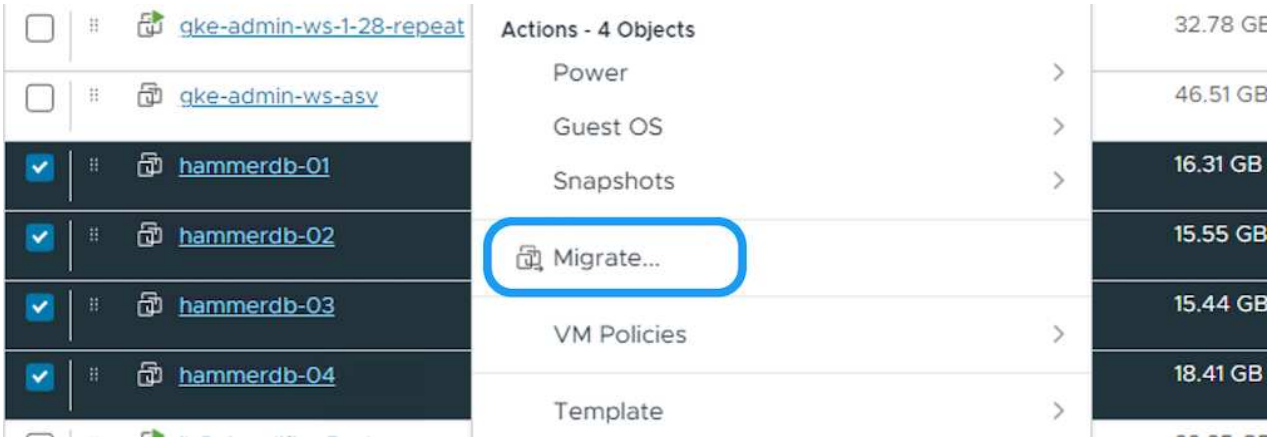
> Este escenario supone que existe comunicación entre los servidores vCenter. De lo contrario, consulte el escenario de ubicación del centro de datos que se detalla a continuación. Para conocer los prerrequisitos, consulte "Documentación de vSphere sobre Advanced Cross vCenter vMotion"

Siga el procedimiento a continuación para migrar máquinas virtuales a diferentes servidores vCenter mediante la interfaz de usuario.

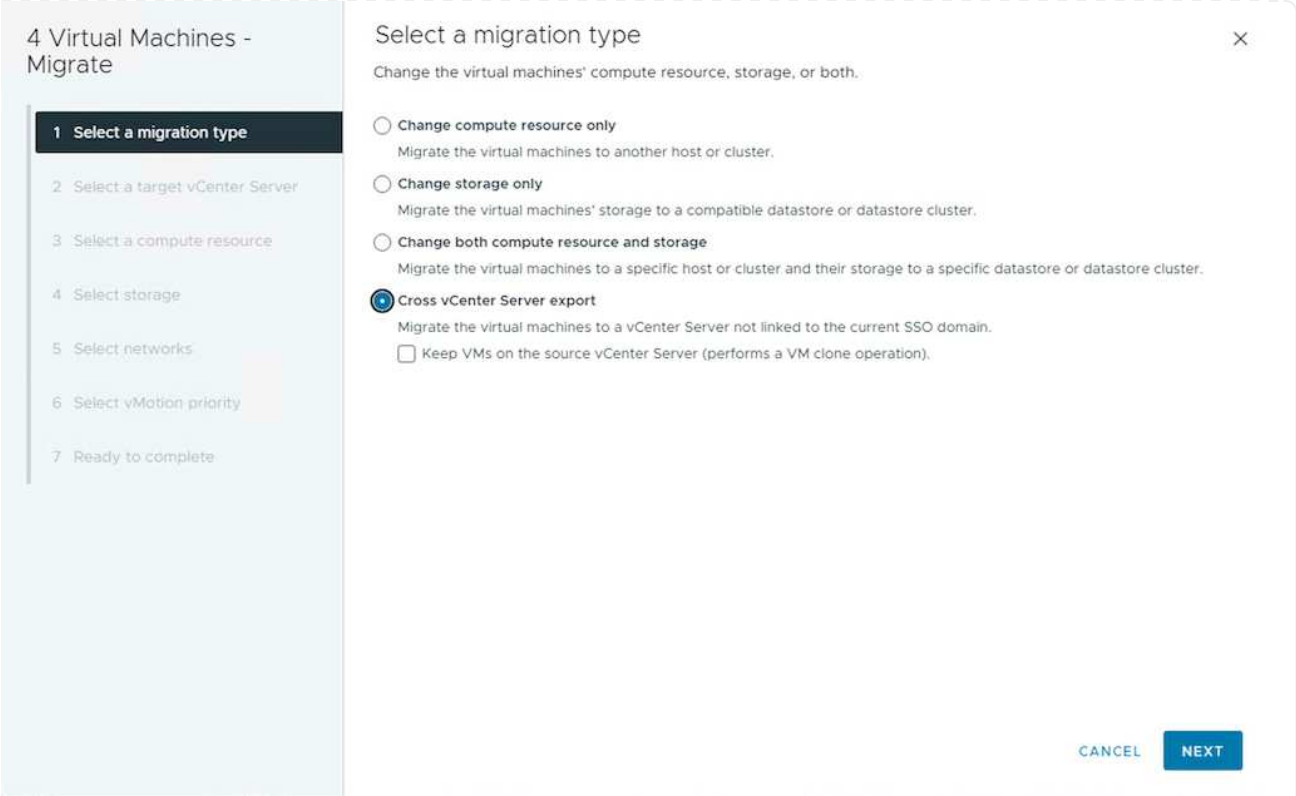
1. Con vSphere Web Client, seleccione el servidor vCenter de origen y haga clic en la pestaña Máquinas virtuales.



2. Seleccione las máquinas virtuales que necesitan migrarse y haga clic derecho para seleccionar la opción Migrar.

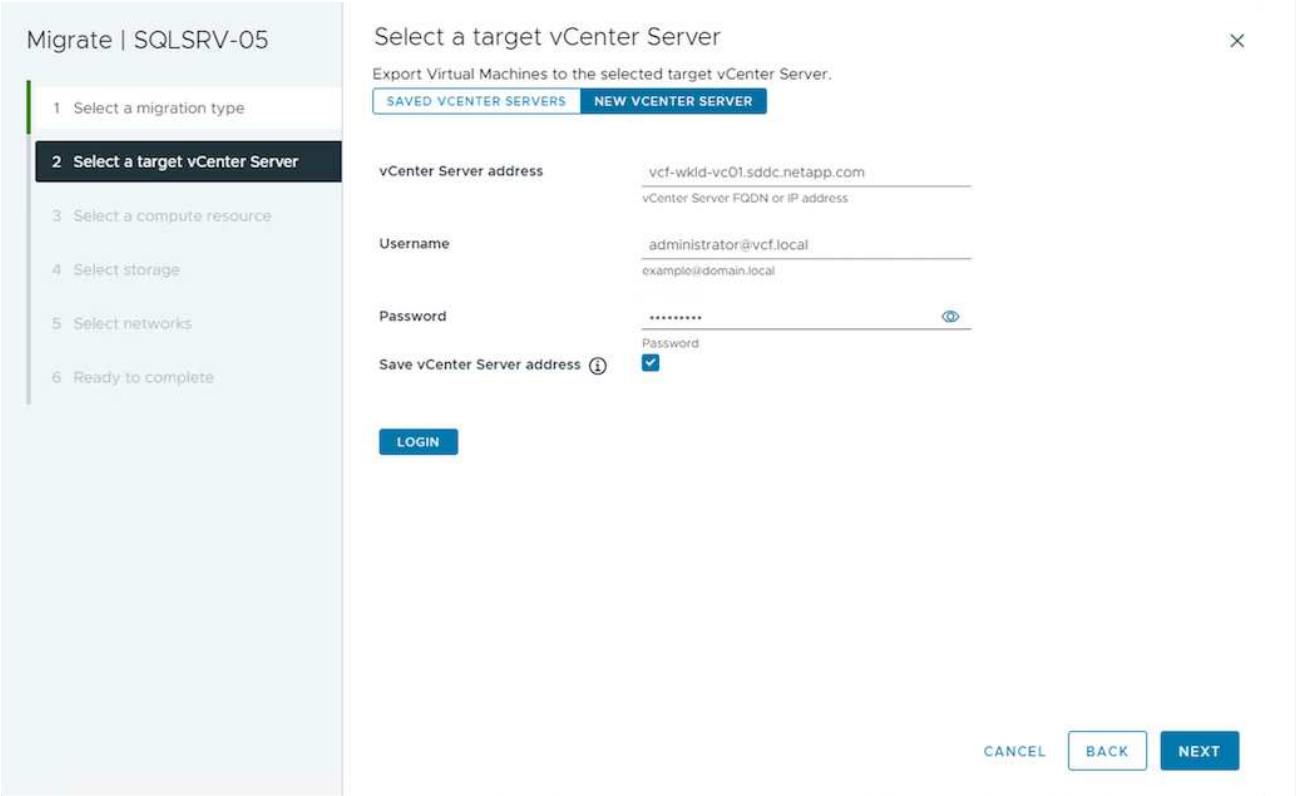


3. Seleccione la opción Exportación entre vCenter Server y haga clic en Siguiente

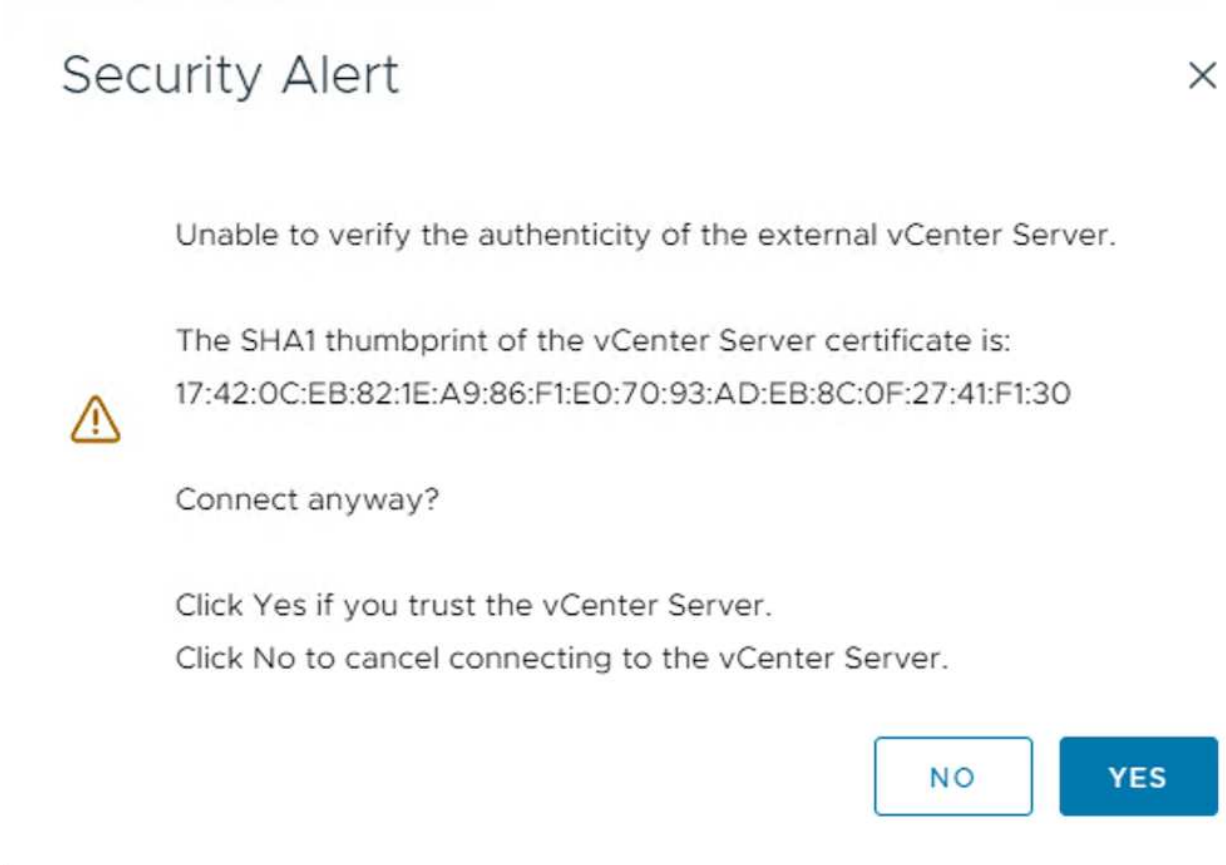


La máquina virtual también se puede importar desde el servidor vCenter de destino. Para ese procedimiento, consulte "Importar o clonar una máquina virtual con Advanced Cross vCenter vMotion"

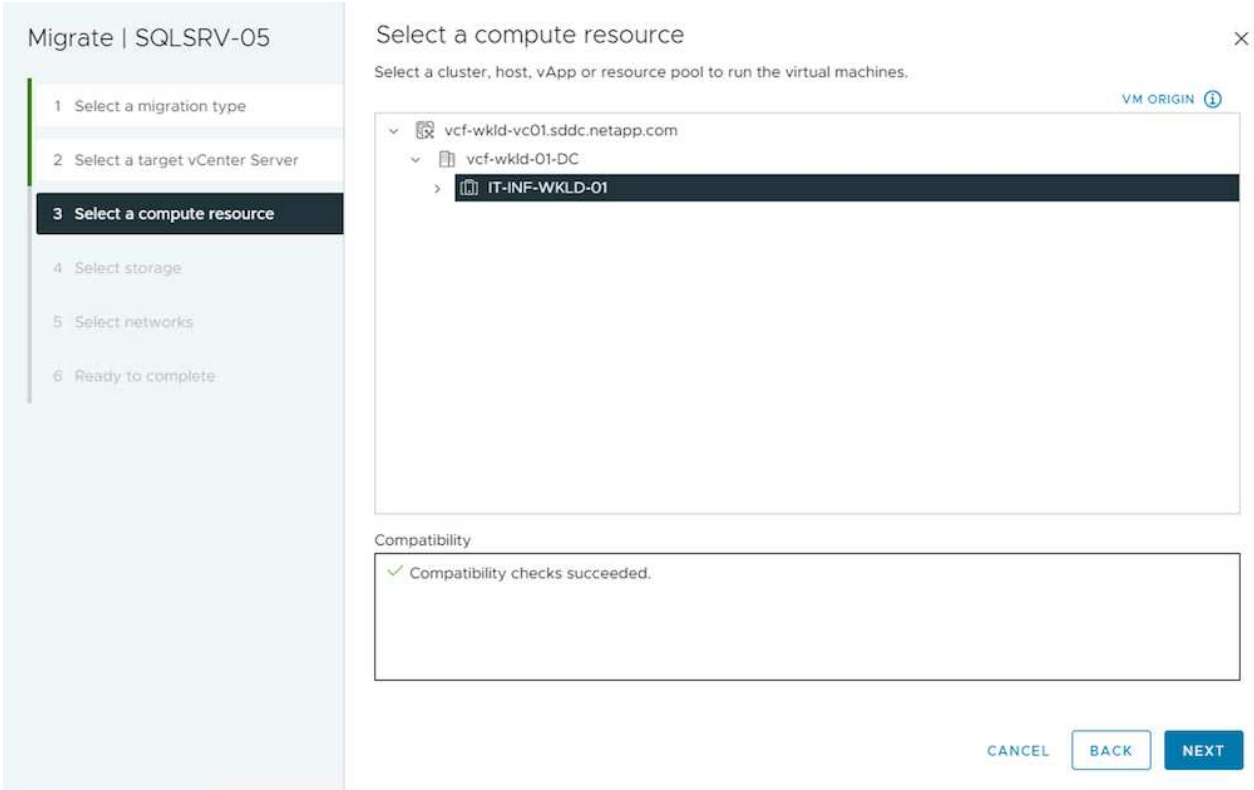
4. Proporcione los detalles de las credenciales de vCenter y haga clic en Iniciar sesión.



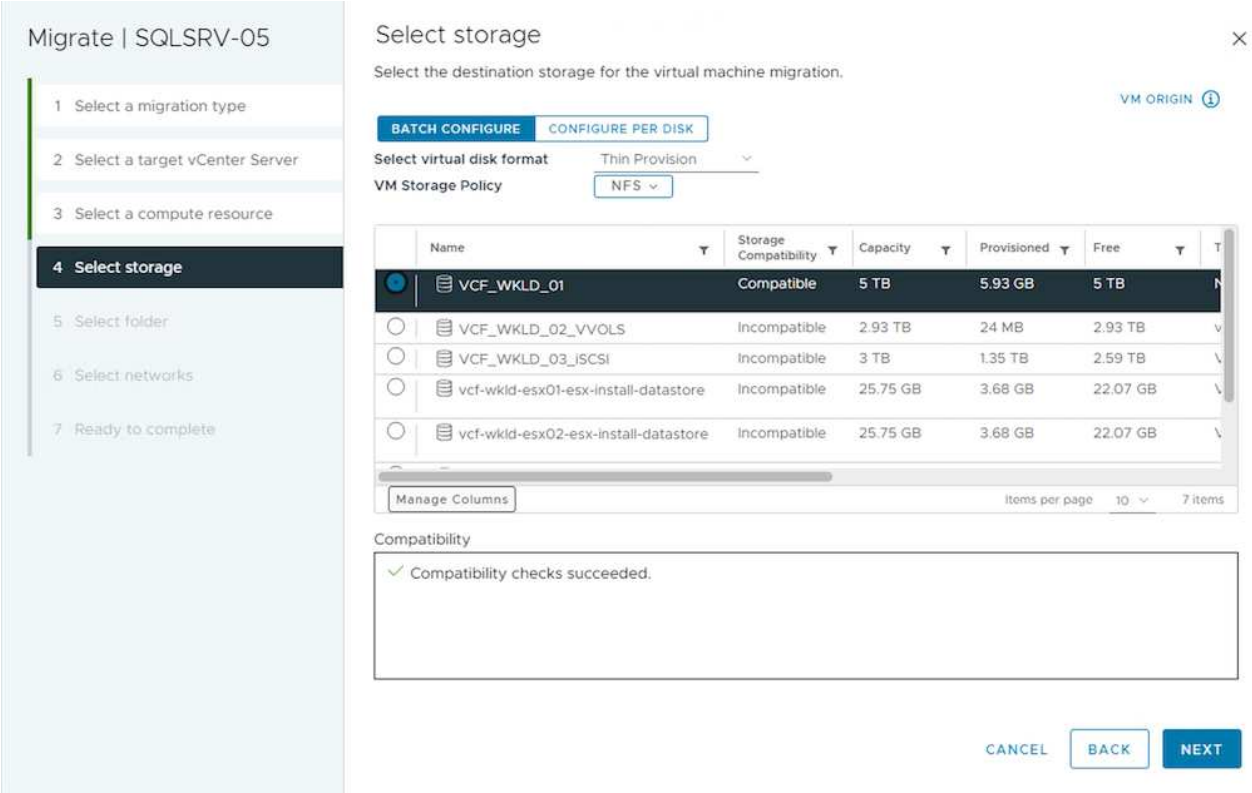
5. Confirmar y aceptar la huella digital del certificado SSL del servidor vCenter



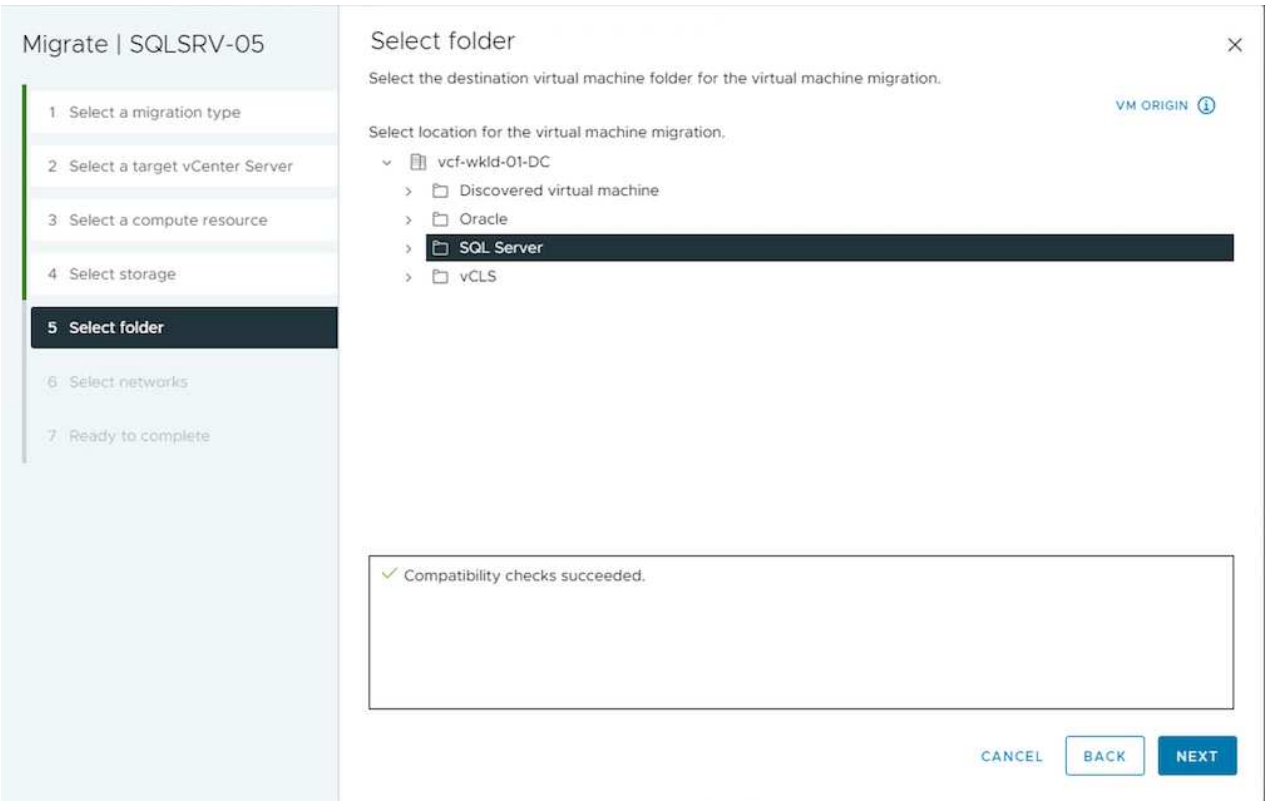
6. Expanda el vCenter de destino y seleccione el clúster de cómputo de destino.



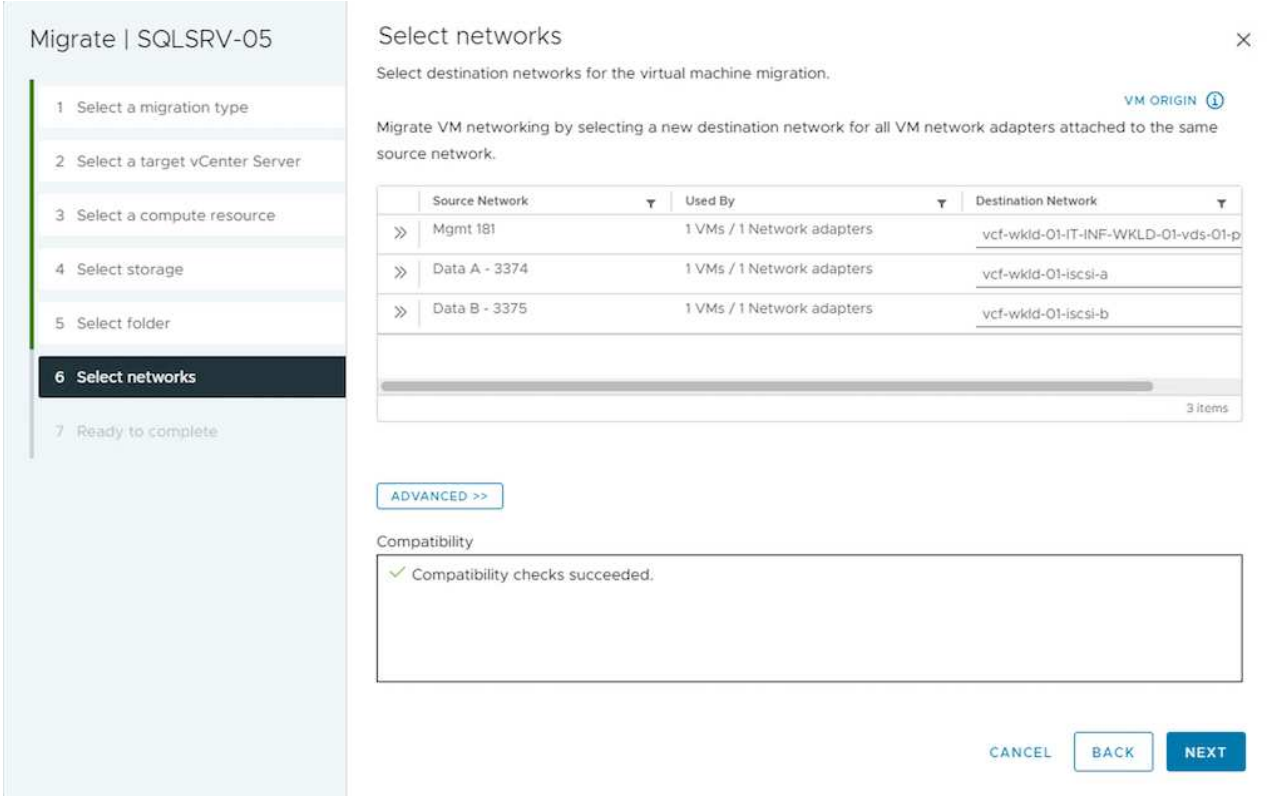
7. Seleccione el almacén de datos de destino según la política de almacenamiento de la máquina virtual.



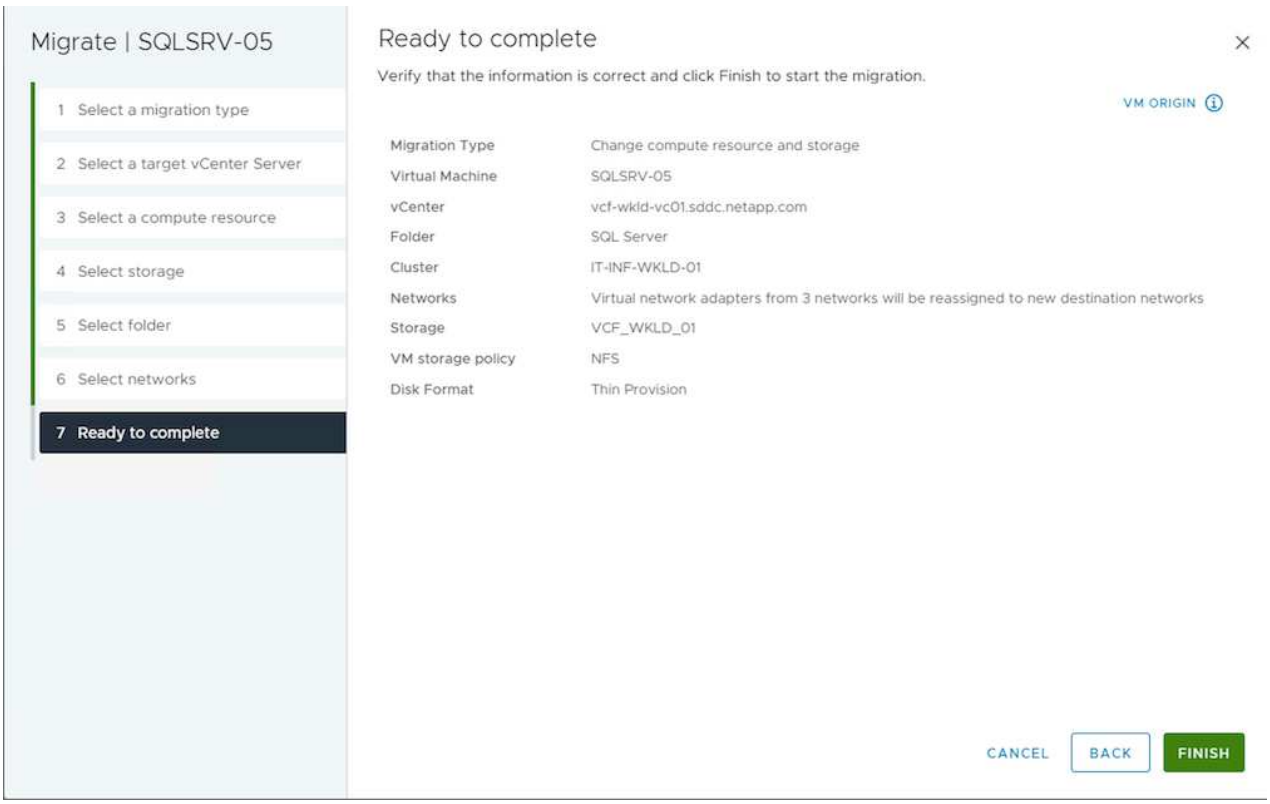
8. Seleccione la carpeta de la máquina virtual de destino.



9. Seleccione el grupo de puertos de VM para cada asignación de tarjeta de interfaz de red.



10. Revise y haga clic en Finalizar para iniciar vMotion en los servidores vCenter.



Para migrar máquinas virtuales mediante PowerCLI, aquí se muestra el script de muestra.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migración de máquinas virtuales entre ubicaciones de centros de datos

- Cuando el tráfico de capa 2 se extiende a través de centros de datos mediante NSX Federation u otras opciones, siga el procedimiento para migrar máquinas virtuales entre servidores vCenter.
- HCX ofrece varios "tipos de migración" Incluye vMotion asistido por replicación en todos los centros de datos para mover máquinas virtuales sin tiempo de inactividad.
- "Administrador de recuperación del sitio (SRM)"Generalmente está destinado a fines de recuperación ante desastres y también se utiliza a menudo para migraciones planificadas mediante replicación basada en matrices de almacenamiento.
- Uso de productos de Protección Continua de Datos (CDP) "API de vSphere para IO (VAIO)" para interceptar los datos y enviar una copia a una ubicación remota para una solución de RPO cercana a cero.
- También se pueden utilizar productos de copia de seguridad y recuperación. Pero a menudo da como resultado un RTO más largo.
- "Recuperación ante desastres como servicio (DRaaS) de BlueXP"Utiliza la replicación basada en matrices de almacenamiento y automatiza ciertas tareas para recuperar las máquinas virtuales en el sitio de destino.

Migración de máquinas virtuales en un entorno de nube híbrida

- "Configurar el modo vinculado híbrido"y seguir el procedimiento de"Migración de máquinas virtuales entre servidores vCenter en el mismo dominio SSO"
- HCX ofrece varios "tipos de migración" Incluye vMotion asistido por replicación en los centros de datos para mover la máquina virtual mientras está encendida.
  - "TR 4942: Migración de cargas de trabajo al almacén de datos de FSx ONTAP mediante VMware HCX"
  - "TR-4940: Migración de cargas de trabajo al almacén de datos de Azure NetApp Files mediante VMware HCX - Guía de inicio rápido"
  - "Migrar cargas de trabajo al almacén de datos de Google Cloud NetApp Volumes en Google Cloud VMware Engine mediante VMware HCX: guía de inicio rápido"
- "Recuperación ante desastres como servicio (DRaaS) de BlueXP"Utiliza la replicación basada en matrices de almacenamiento y automatiza ciertas tareas para recuperar las máquinas virtuales en el sitio de destino.
- Con productos de Protección Continua de Datos (CDP) compatibles que utilizan "API de vSphere para IO (VAIO)" para interceptar los datos y enviar una copia a una ubicación remota para una solución de RPO cercana a cero.

> Cuando la VM de origen reside en un almacén de datos de bloques vVol, se puede replicar con SnapMirror en Amazon FSx ONTAP o Cloud Volumes ONTAP (CVO) en otros proveedores de nube compatibles y consumir como volumen iSCSI con VM nativas de la nube.

Escenarios de migración de plantillas de VM

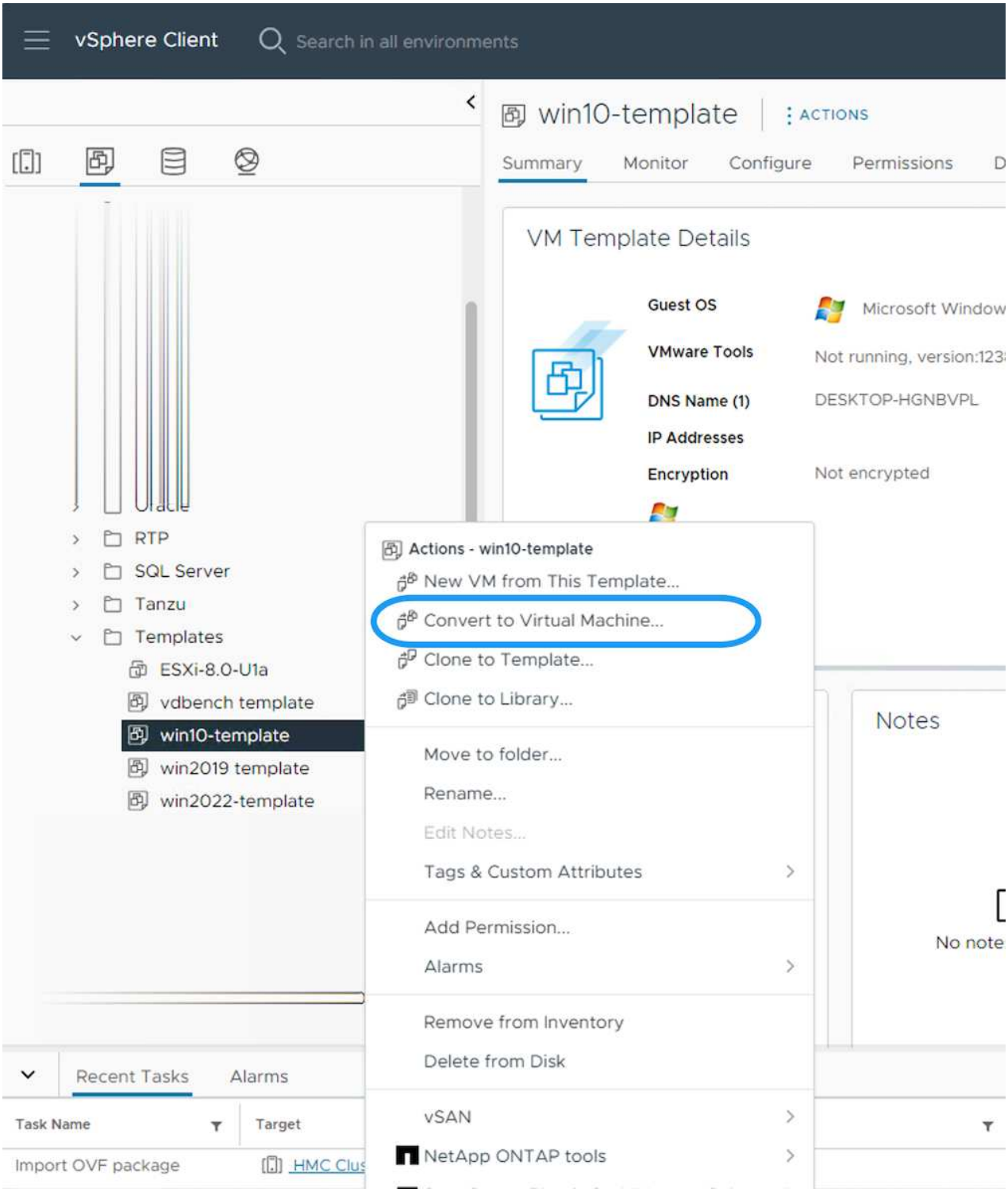
Las plantillas de VM pueden ser administradas por vCenter Server o por una biblioteca de contenido. La distribución de plantillas VM, plantillas OVF y OVA y otros tipos de archivos se manejan publicándolos en la

biblioteca de contenido local y las bibliotecas de contenido remotas pueden suscribirse a ellos.

- Las plantillas de VM almacenadas en el inventario de vCenter se pueden convertir a VM y utilizar las opciones de migración de VM.
- Las plantillas OVF y OVA y otros tipos de archivos almacenados en la biblioteca de contenido se pueden clonar en otras bibliotecas de contenido.
- Las plantillas de VM de la biblioteca de contenido se pueden alojar en cualquier almacén de datos y deben agregarse a una nueva biblioteca de contenido.

Migración de plantillas de máquinas virtuales alojadas en el almacén de datos

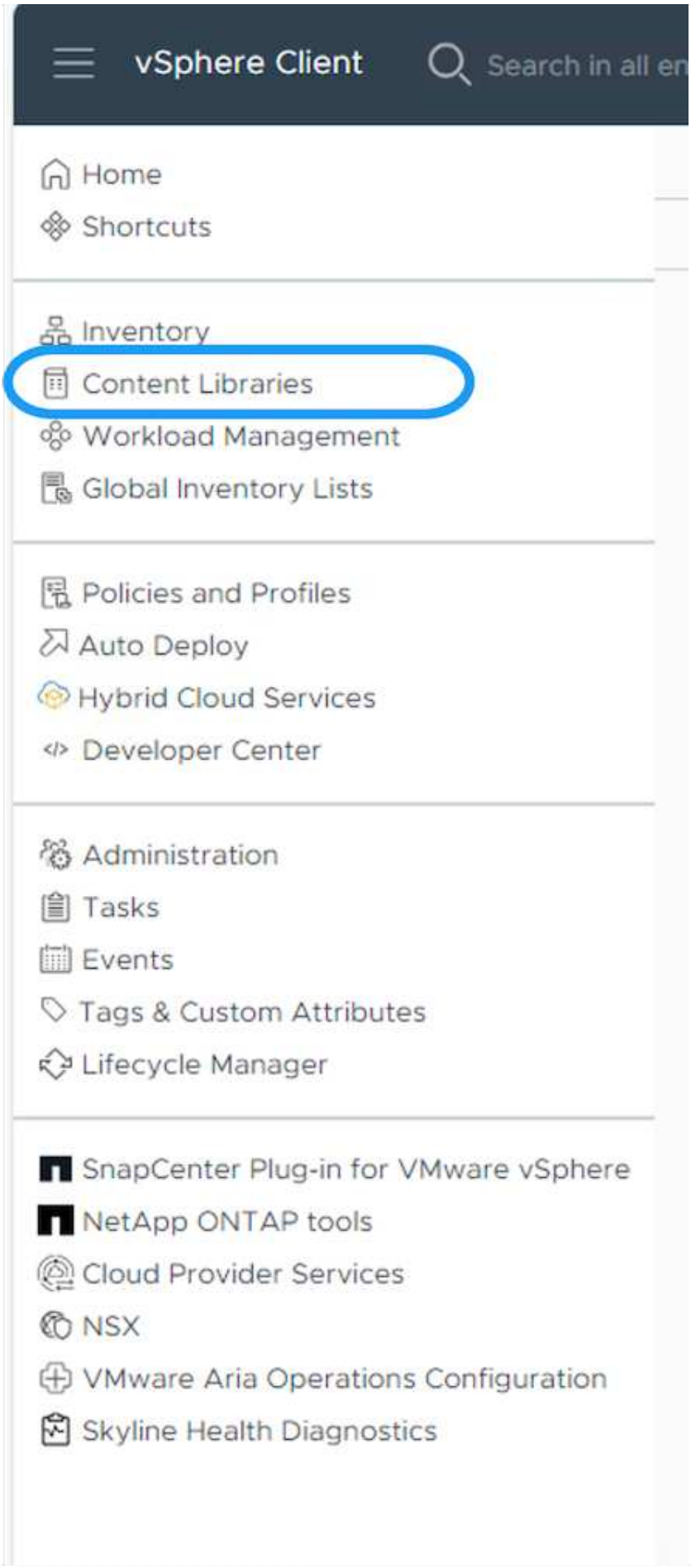
1. En vSphere Web Client, haga clic con el botón derecho en la plantilla de VM en la vista de la carpeta VM y Plantillas y seleccione la opción para convertir a VM.



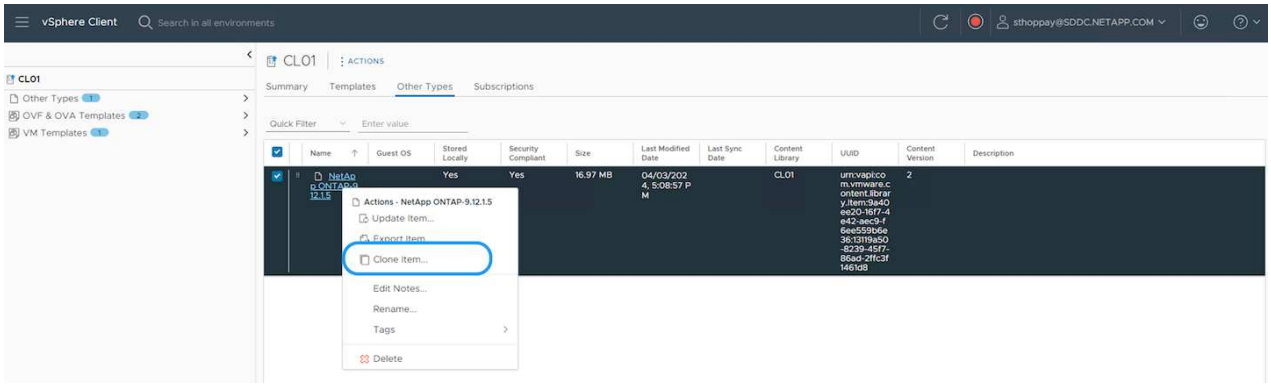
2. Una vez convertido como VM, siga las opciones de migración de VM.

Clon de elementos de la biblioteca de contenido

1. En vSphere Web Client, seleccione Bibliotecas de contenido

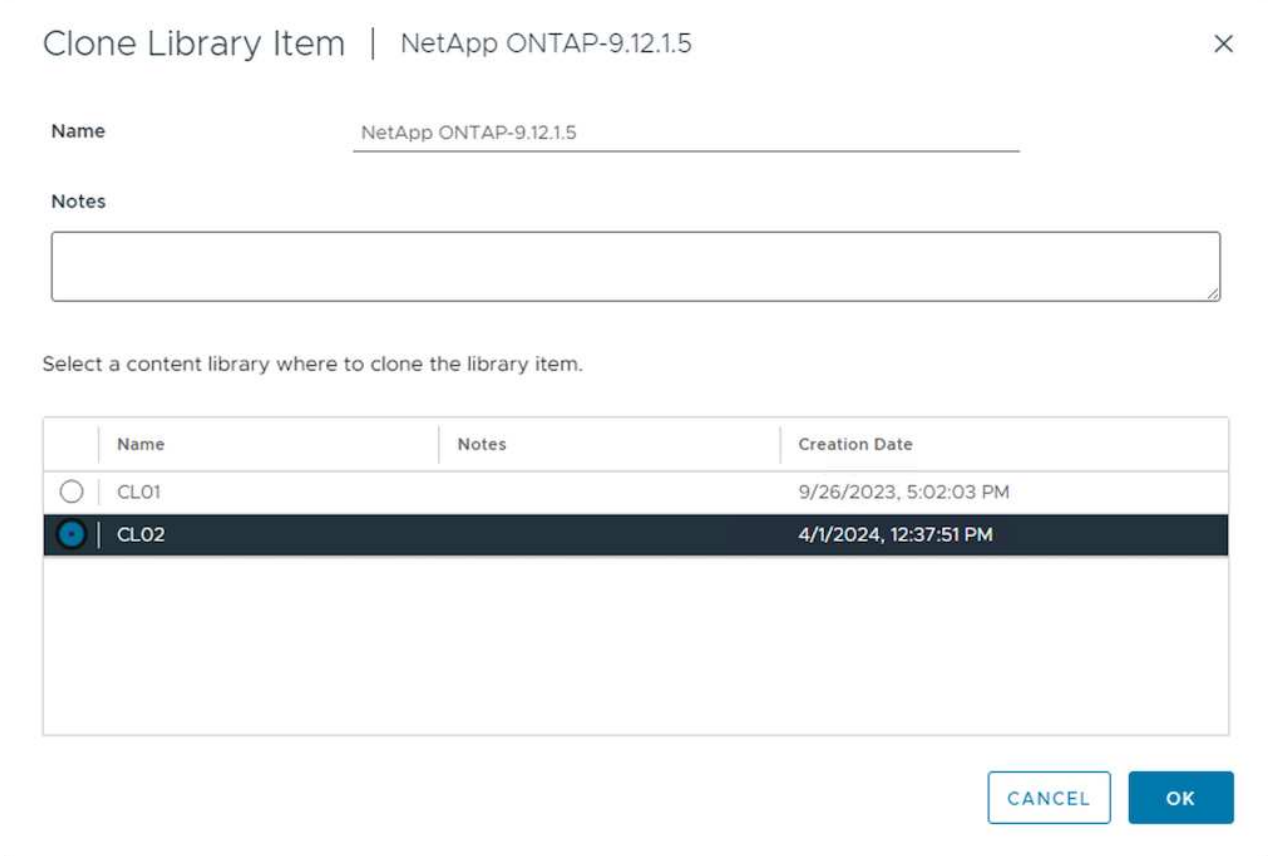

vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

2. Seleccione la biblioteca de contenido en la que se encuentra el elemento que desea clonar
3. Haga clic derecho en el elemento y haga clic en Clonar elemento.

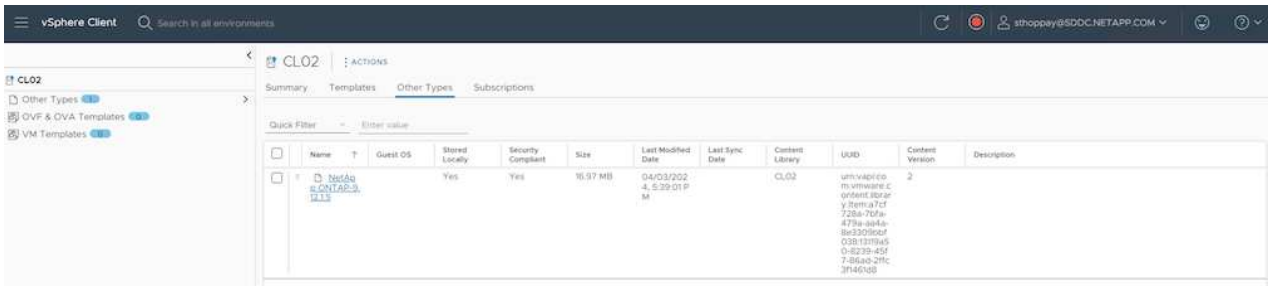


> Si utiliza el menú de acciones, asegúrese de que esté indicado el objeto de destino correcto para realizar la acción.

4. Seleccione la biblioteca de contenido de destino y haga clic en Aceptar.



5. Validar que el artículo esté disponible en la biblioteca de contenido de destino.

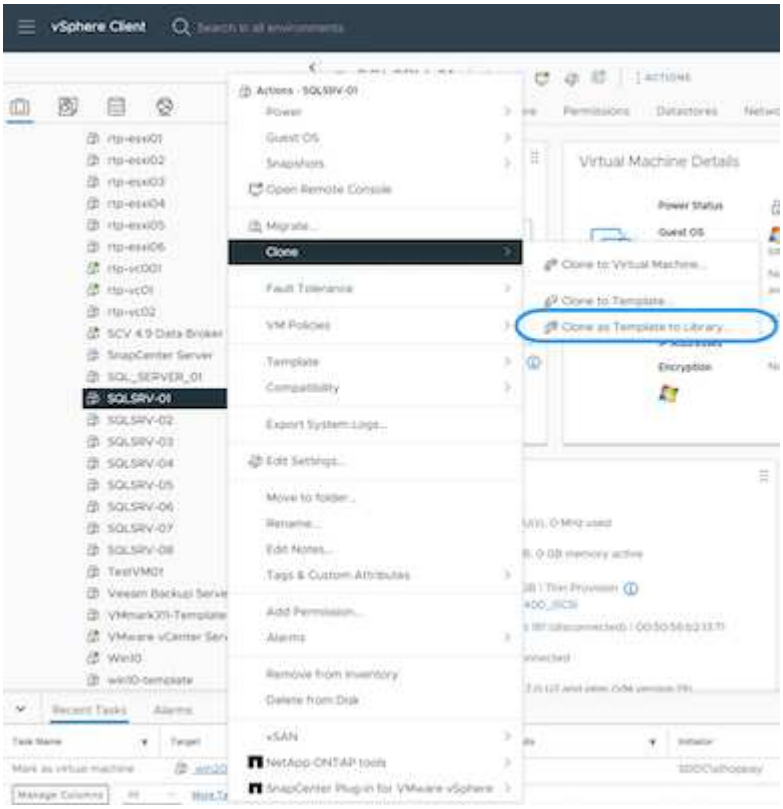


Aquí se muestra el script de PowerCLI de muestra para copiar los elementos de la biblioteca de contenido de la biblioteca de contenido CL01 a la CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibaryItem -ContentLibrary (Get-ContentLibary 'CL02' -Server
$targetvc)
```

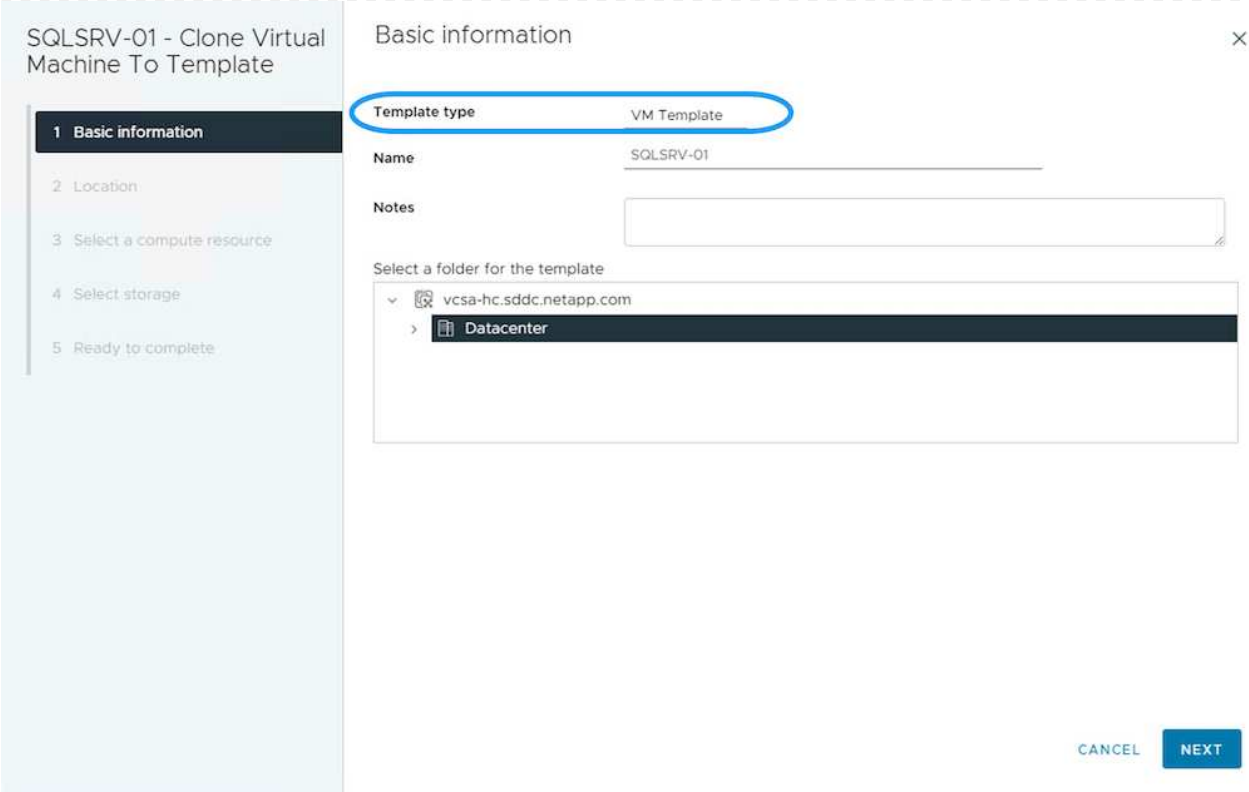
Agregar máquinas virtuales como plantillas en la biblioteca de contenido

1. En vSphere Web Client, seleccione la máquina virtual y haga clic con el botón derecho para elegir Clonar como plantilla en la biblioteca



> Cuando se selecciona una plantilla de VM para clonar en la biblioteca, solo se puede almacenar como plantilla OVF y OVA y no como plantilla de VM.

2. Confirme que el tipo de plantilla esté seleccionado como Plantilla de VM y siga las respuestas del asistente para completar la operación.



Para obtener detalles adicionales sobre las plantillas de VM en la biblioteca de contenido, consulte "Guía de administración de máquinas virtuales de vSphere"

Casos de uso

Migración de sistemas de almacenamiento de terceros (incluido vSAN) a almacenes de datos ONTAP .

- Según dónde esté aprovisionado el almacén de datos de ONTAP , seleccione las opciones de migración de VM anteriores.

Migración de la versión anterior a la última versión de vSphere.

- Si no es posible la actualización en el lugar, se puede instalar un nuevo entorno y utilizar las opciones de migración anteriores.

En la opción de migración entre vCenter, importe desde el destino si la opción de exportación no está disponible en el origen. Para ese procedimiento, consulte"Importar o clonar una máquina virtual con Advanced Cross vCenter vMotion"

Migración al dominio de carga de trabajo VCF.

- Migre máquinas virtuales de cada clúster de vSphere al dominio de carga de trabajo de destino.

> Para permitir la comunicación de red con máquinas virtuales existentes en otros clústeres en el vCenter de origen, extienda el segmento NSX agregando los hosts vSphere del vCenter de origen a la zona de transporte o utilice un puente L2 en el borde para permitir la comunicación L2 en VLAN. Consulte la documentación de NSX de "Configurar una máquina virtual perimetral para la conexión en puente"

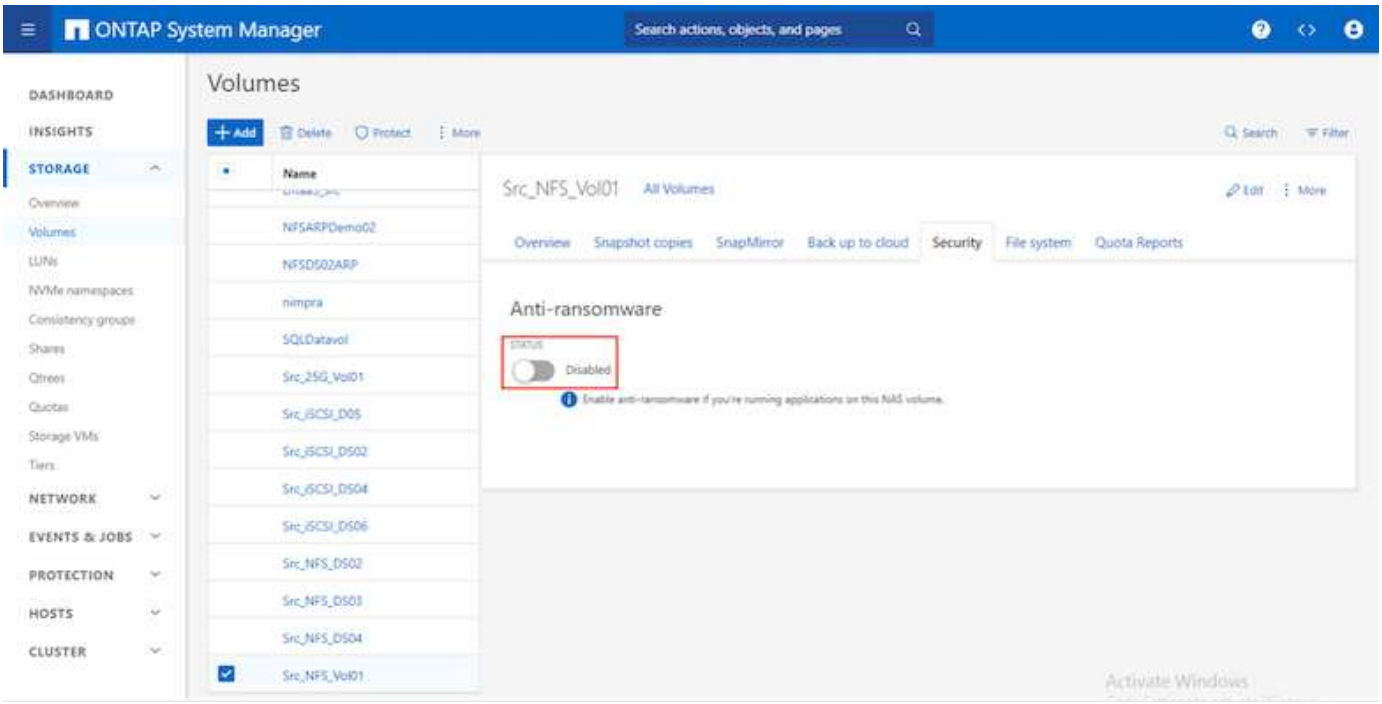
Recursos adicionales

- "Migración de máquinas virtuales de vSphere"
- "Migración de máquinas virtuales con vSphere vMotion"
- "Configuraciones de puerta de enlace de nivel 0 en NSX Federation"
- "Guía del usuario de HCX 4.8"
- "Documentación de VMware Live Recovery"
- "BlueXP disaster recovery para VMware"

Protección autónoma contra ransomware para almacenamiento NFS

Detectar ransomware lo antes posible es crucial para prevenir su propagación y evitar costosos tiempos de inactividad. Una estrategia eficaz de detección de ransomware debe incorporar múltiples capas de protección a nivel de host ESXi y de máquina virtual invitada. Si bien se implementan múltiples medidas de seguridad para crear una defensa integral contra ataques de ransomware, ONTAP permite agregar más capas de protección al enfoque de defensa general. Para nombrar algunas capacidades, comienza con instantáneas, protección autónoma contra ransomware, instantáneas a prueba de manipulaciones, etc.

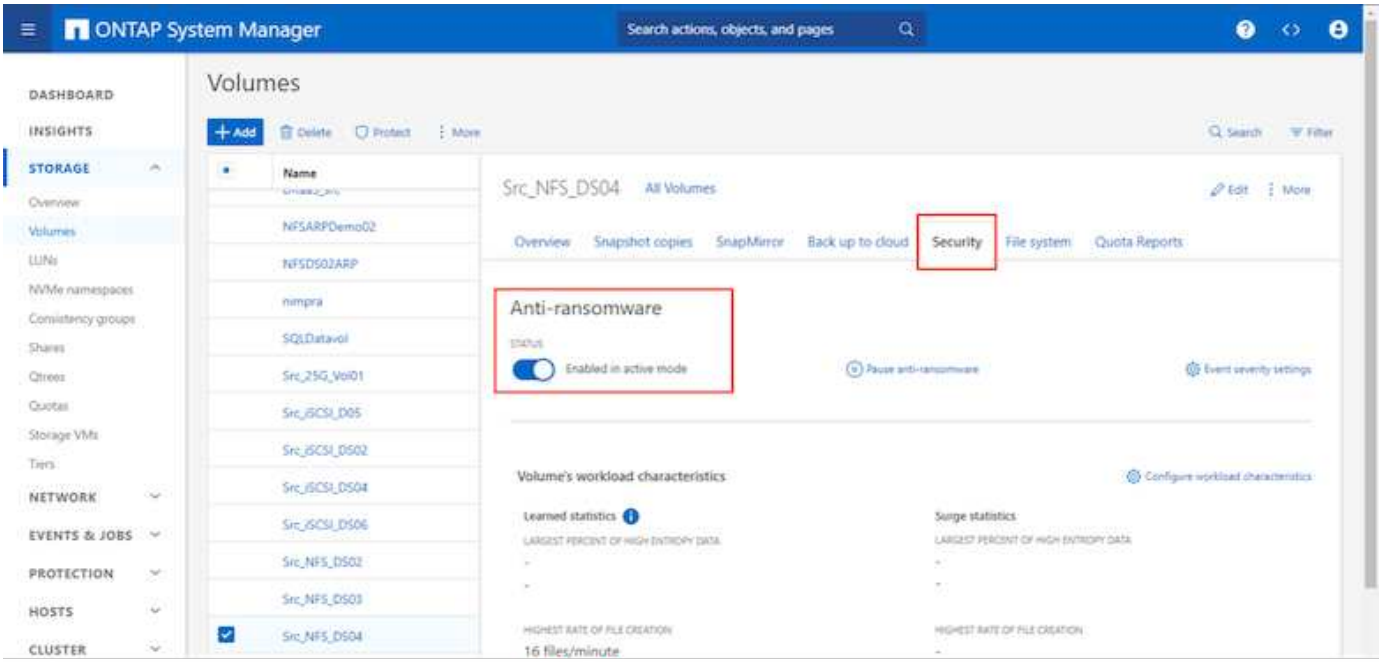
Veamos cómo las capacidades mencionadas anteriormente funcionan con VMware para proteger y recuperar los datos contra ransomware. Para proteger vSphere y las máquinas virtuales invitadas contra ataques, es esencial tomar varias medidas, incluida la segmentación, el uso de EDR/XDR/SIEM para puntos finales y la instalación de actualizaciones de seguridad y la adhesión a las pautas de refuerzo adecuadas. Cada máquina virtual que reside en un almacén de datos también aloja un sistema operativo estándar. Asegúrese de que los paquetes de productos antimalware para servidores empresariales estén instalados y actualizados periódicamente, lo cual constituye un componente esencial de una estrategia de protección contra ransomware de múltiples capas. Junto con esto, habilite la protección autónoma contra ransomware (ARP) en el volumen NFS que alimenta el almacén de datos. ARP aprovecha el ML integrado que analiza la actividad de la carga de trabajo del volumen más la entropía de los datos para detectar automáticamente el ransomware. ARP se puede configurar a través de la interfaz de administración incorporada de ONTAP o del Administrador del sistema y se habilita por volumen.



Con el nuevo ARP/AI de NetApp , que actualmente se encuentra en versión preliminar tecnológica, no es necesario un modo de aprendizaje. En lugar de ello, puede pasar directamente al modo activo con su capacidad de detección de ransomware impulsada por IA.

Con ONTAP One, todos estos conjuntos de funciones son completamente gratuitos. Acceda a la sólida suite de protección de datos, seguridad y todas las funciones que ofrece ONTAP de NetApp sin preocuparse por las barreras de licencia.

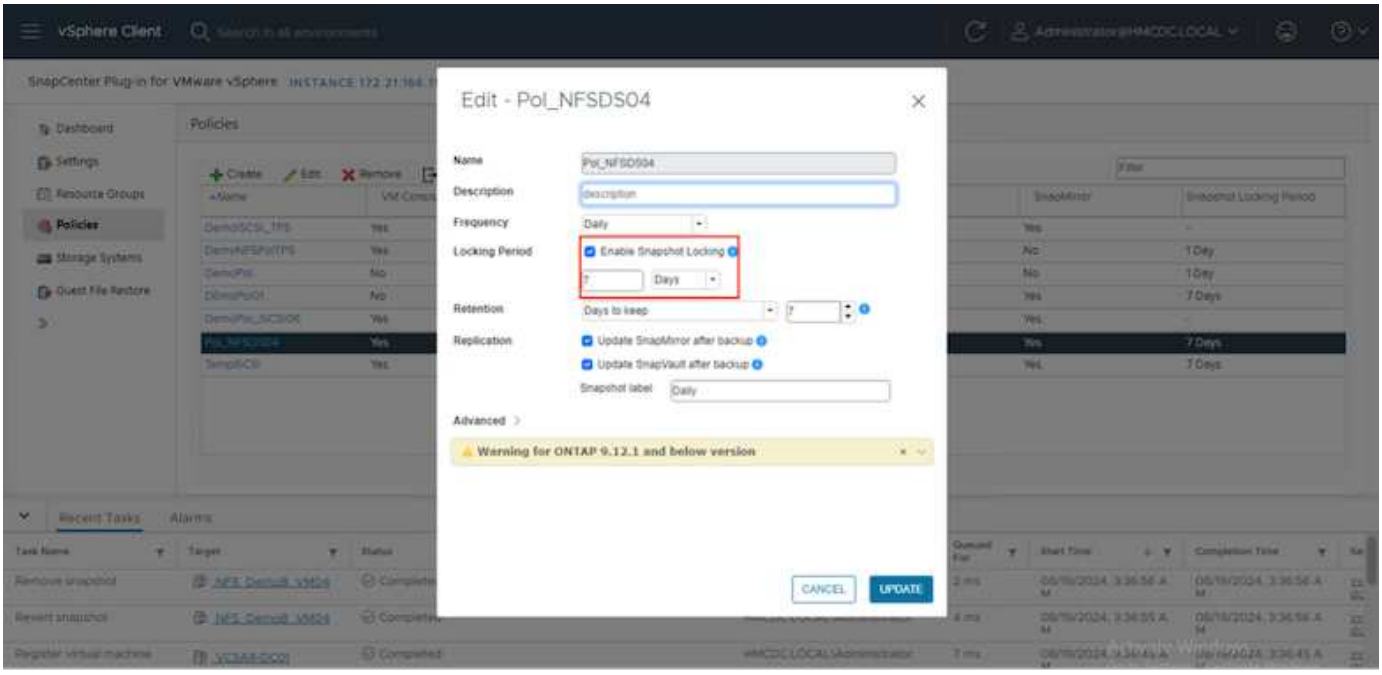
Una vez en modo activo, comienza a buscar actividad de volumen anormal que potencialmente podría ser ransomware. Si se detecta una actividad anormal, se toma inmediatamente una copia instantánea automática, que proporciona un punto de restauración lo más cercano posible a la infección del archivo. ARP puede detectar cambios en las extensiones de archivos específicas de la VM en un volumen NFS ubicado fuera de la VM cuando se agrega una nueva extensión al volumen cifrado o se modifica la extensión de un archivo.



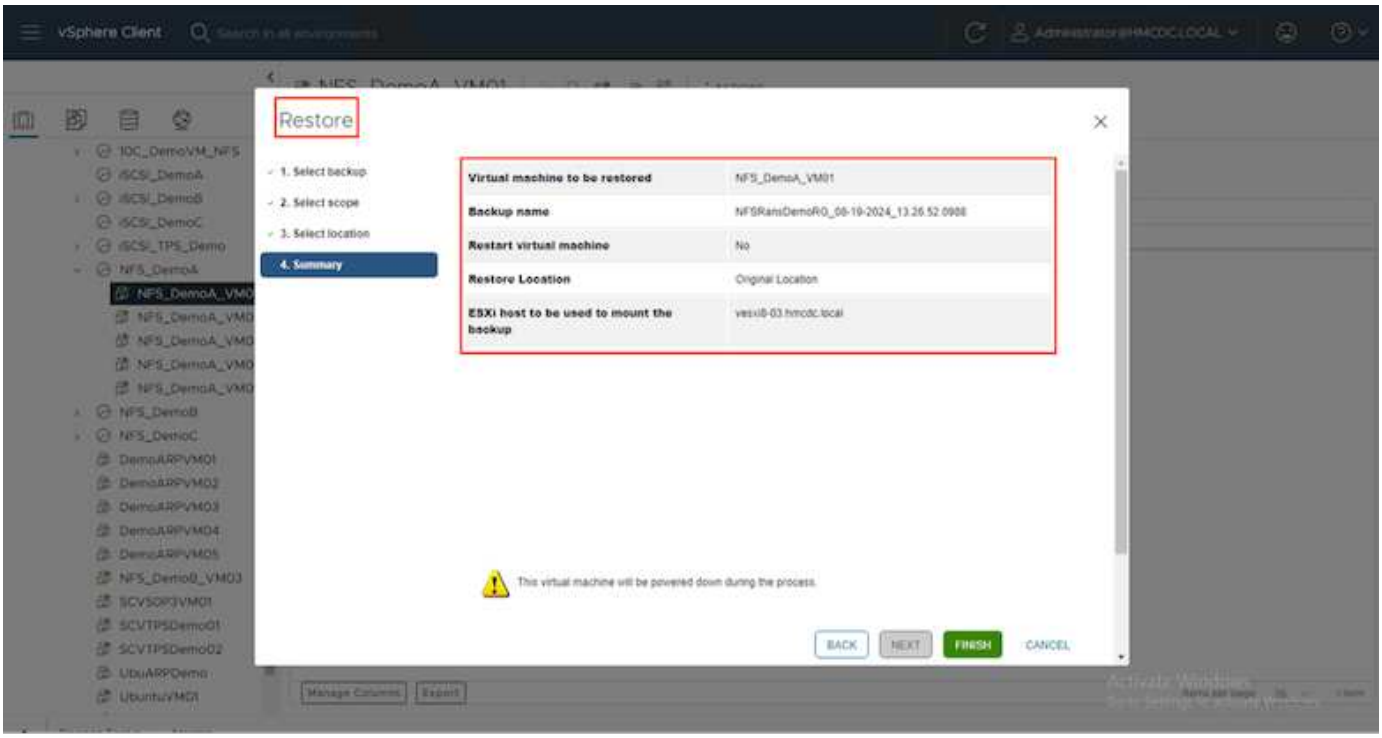
Si un ataque de ransomware tiene como objetivo la máquina virtual (VM) y altera los archivos dentro de la VM sin realizar cambios fuera de ella, la Protección avanzada contra ransomware (ARP) aún detectará la amenaza si la entropía predeterminada de la VM es baja, por ejemplo, para tipos de archivos como .txt, .docx o .mp4. Aunque ARP crea una instantánea protectora en este escenario, no genera una alerta de amenaza porque las extensiones de archivo fuera de la máquina virtual no han sido alteradas. En tales escenarios, las capas iniciales de defensa identificarían la anomalía, sin embargo ARP ayuda a crear una instantánea basada en la entropía.

Para obtener información detallada, consulte la sección "ARP y máquinas virtuales" en"Casos de uso y consideraciones de ARP" .

Al pasar de los archivos a los datos de respaldo, los ataques de ransomware apuntan cada vez más a las copias de seguridad y los puntos de recuperación de instantáneas al intentar eliminarlos antes de comenzar a cifrar los archivos. Sin embargo, con ONTAP, esto se puede evitar creando instantáneas a prueba de manipulaciones en sistemas primarios o secundarios con"Bloqueo de copia de instantáneas de NetApp" .



Los atacantes de ransomware o administradores maliciosos no pueden eliminar ni modificar estas copias instantáneas, por lo que están disponibles incluso después de un ataque. Si el almacén de datos o máquinas virtuales específicas se ven afectadas, SnapCenter puede recuperar los datos de las máquinas virtuales en segundos, minimizando el tiempo de inactividad de la organización.



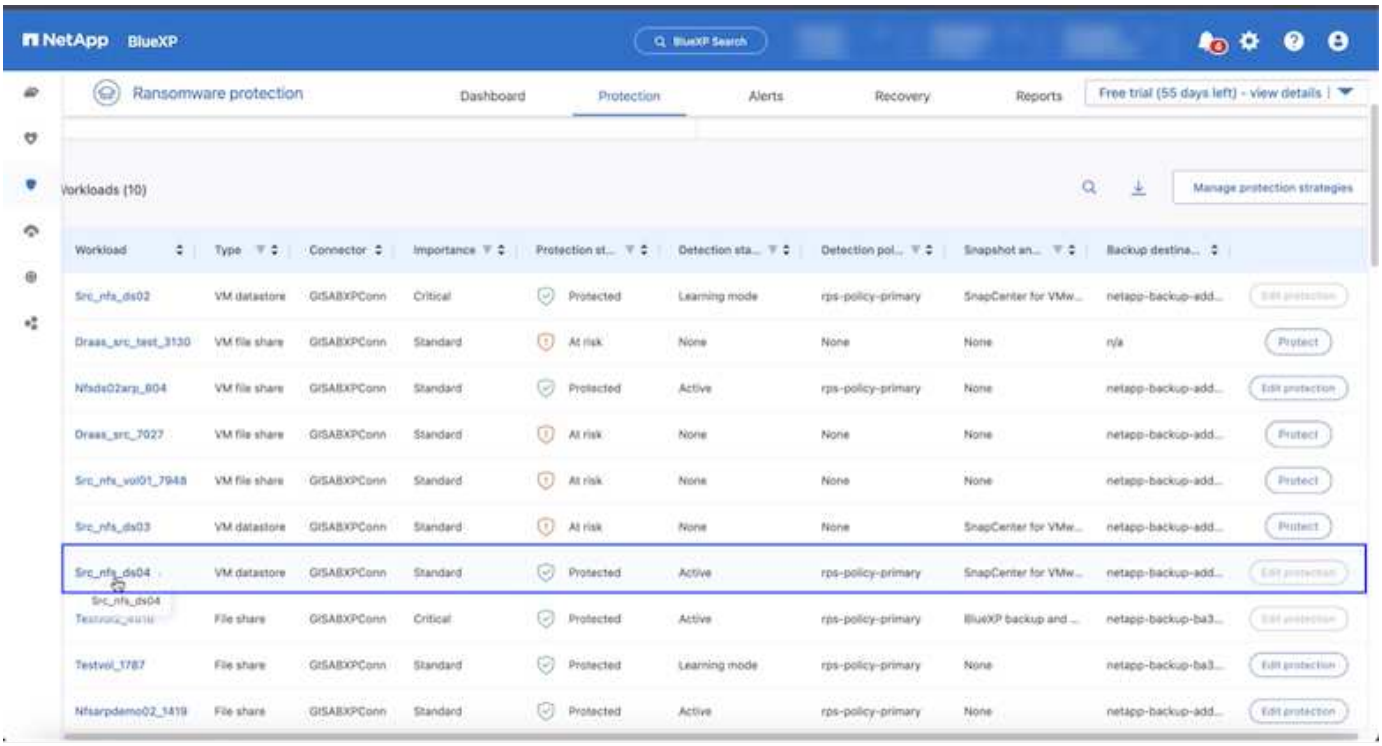
Lo anterior demuestra cómo el almacenamiento ONTAP agrega una capa adicional a las técnicas existentes, mejorando la protección del entorno para el futuro.

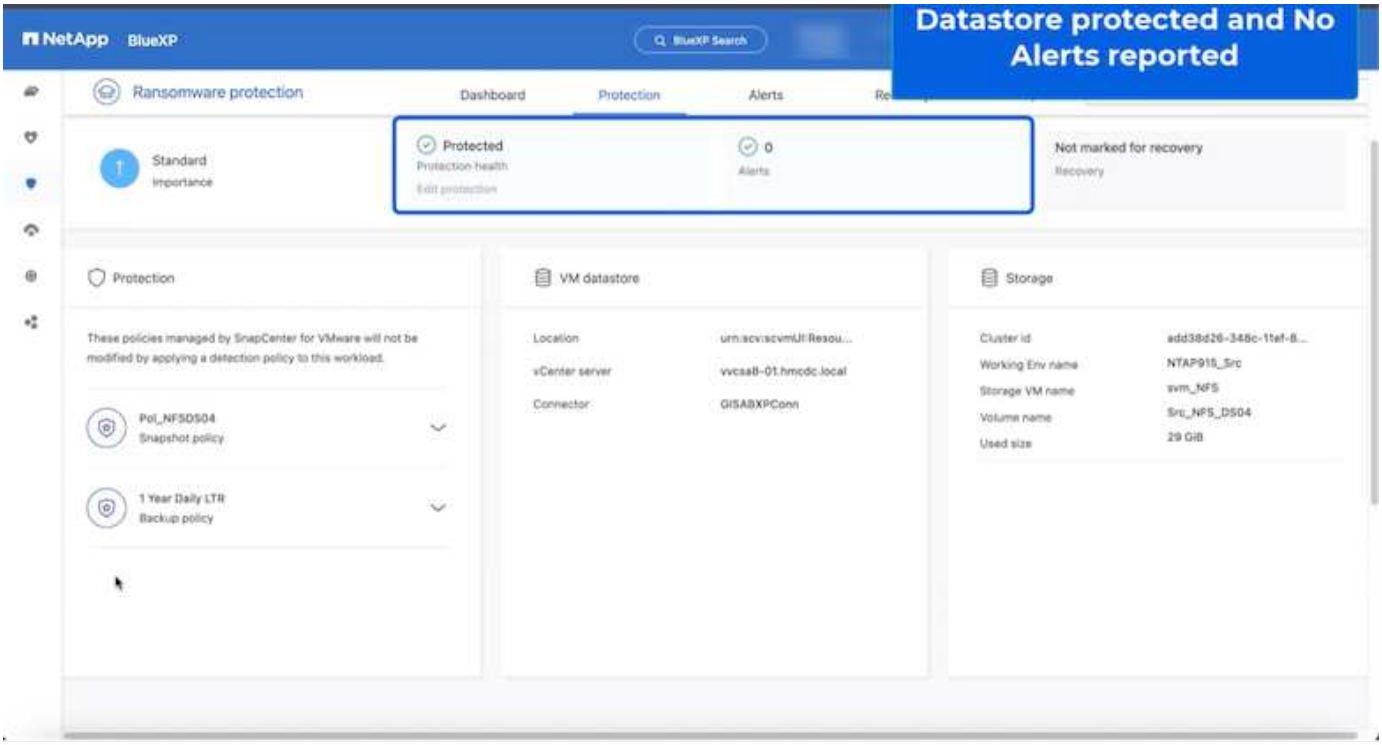
Para obtener información adicional, consulte la guía para"Soluciones de NetApp para ransomware" .

Ahora bien, si es necesario orquestar todo esto e integrarlo con herramientas SIEM, se puede utilizar un servicio de acceso directo como la BlueXP ransomware protection . Es un servicio diseñado para salvaguardar

los datos del ransomware. Este servicio ofrece protección para cargas de trabajo basadas en aplicaciones, como Oracle, MySQL, almacenes de datos de máquinas virtuales y recursos compartidos de archivos en almacenamiento NFS local.

En este ejemplo, el almacén de datos NFS "Src_NFS_DS04" está protegido mediante la BlueXP ransomware protection.

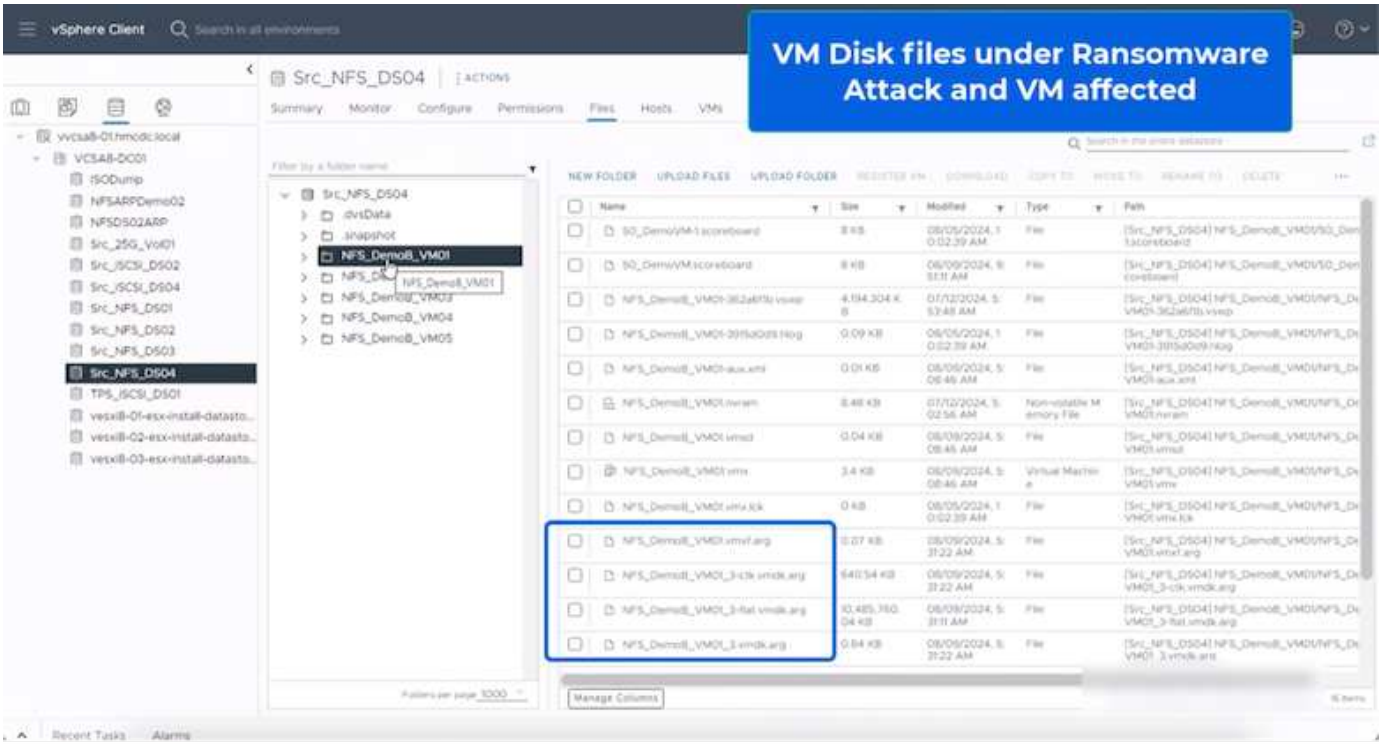




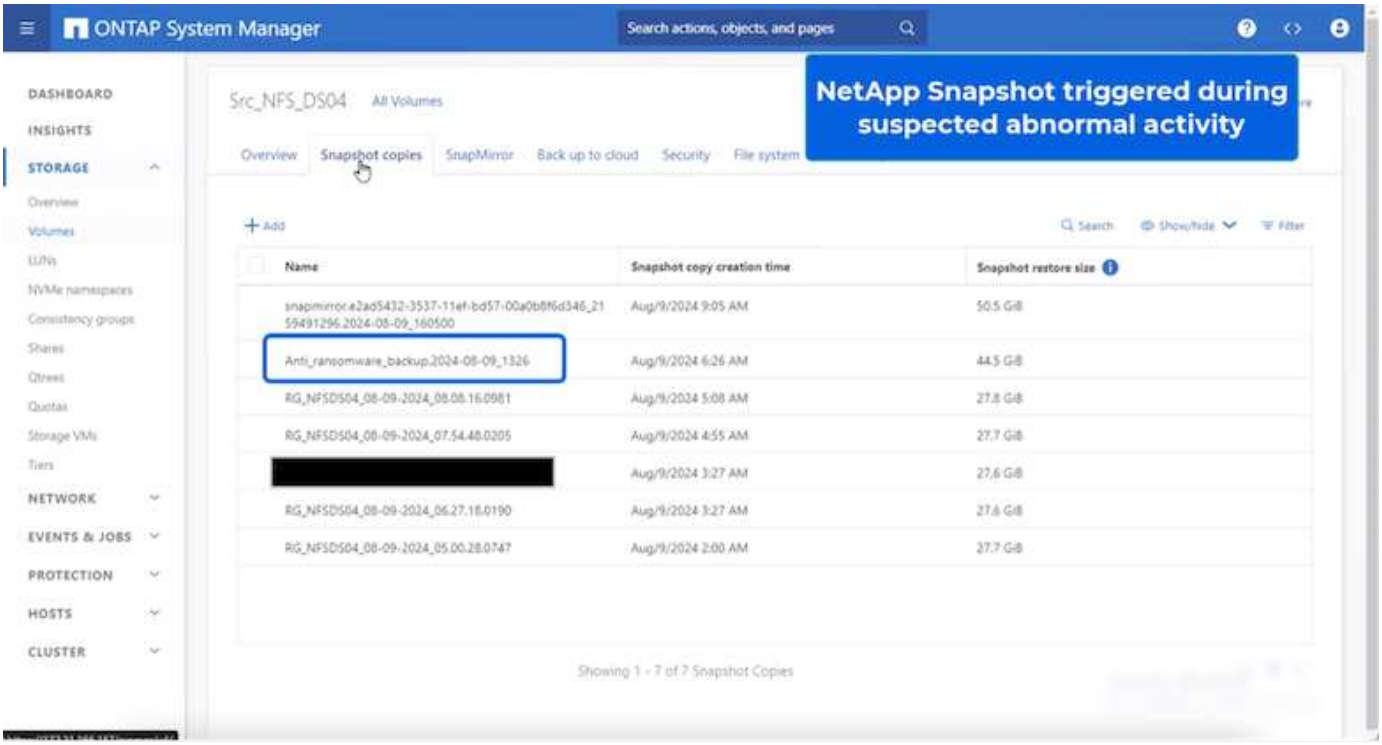
Para obtener información detallada sobre cómo configurar la BlueXP ransomware protection, consulte"Configurar la BlueXP ransomware protection" y"Configurar los ajustes de BlueXP ransomware

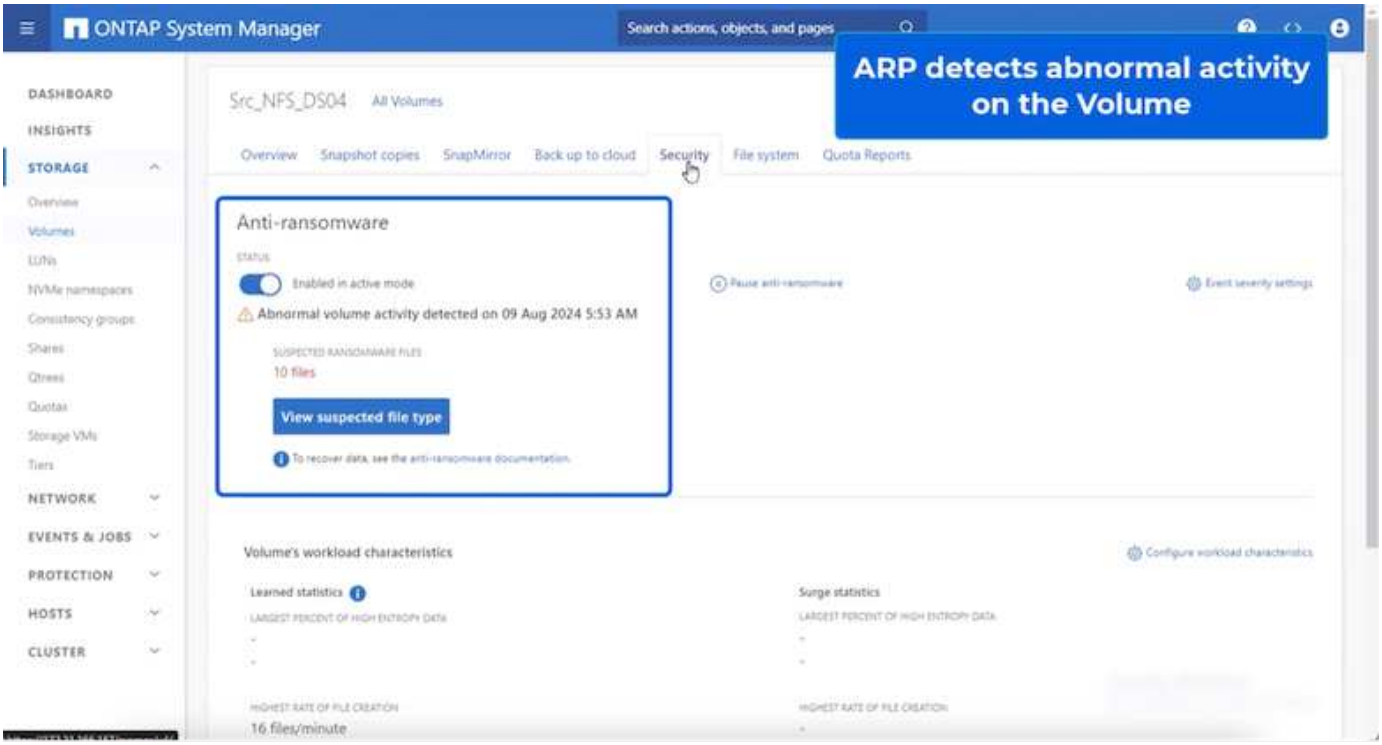
protection" .

Es hora de explicar esto con un ejemplo. En este tutorial, el almacén de datos "Src_NFS_DS04" se ve afectado.

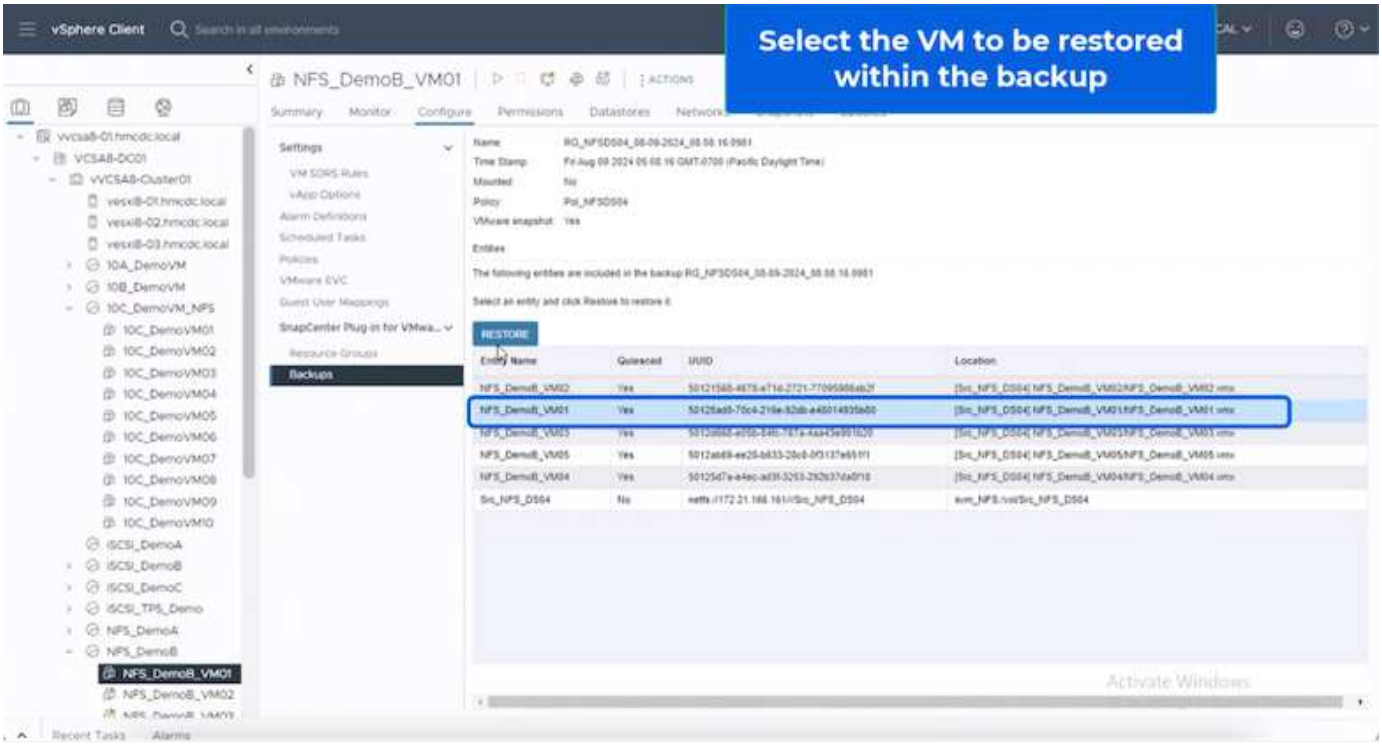


ARP activó inmediatamente una instantánea del volumen tras la detección.





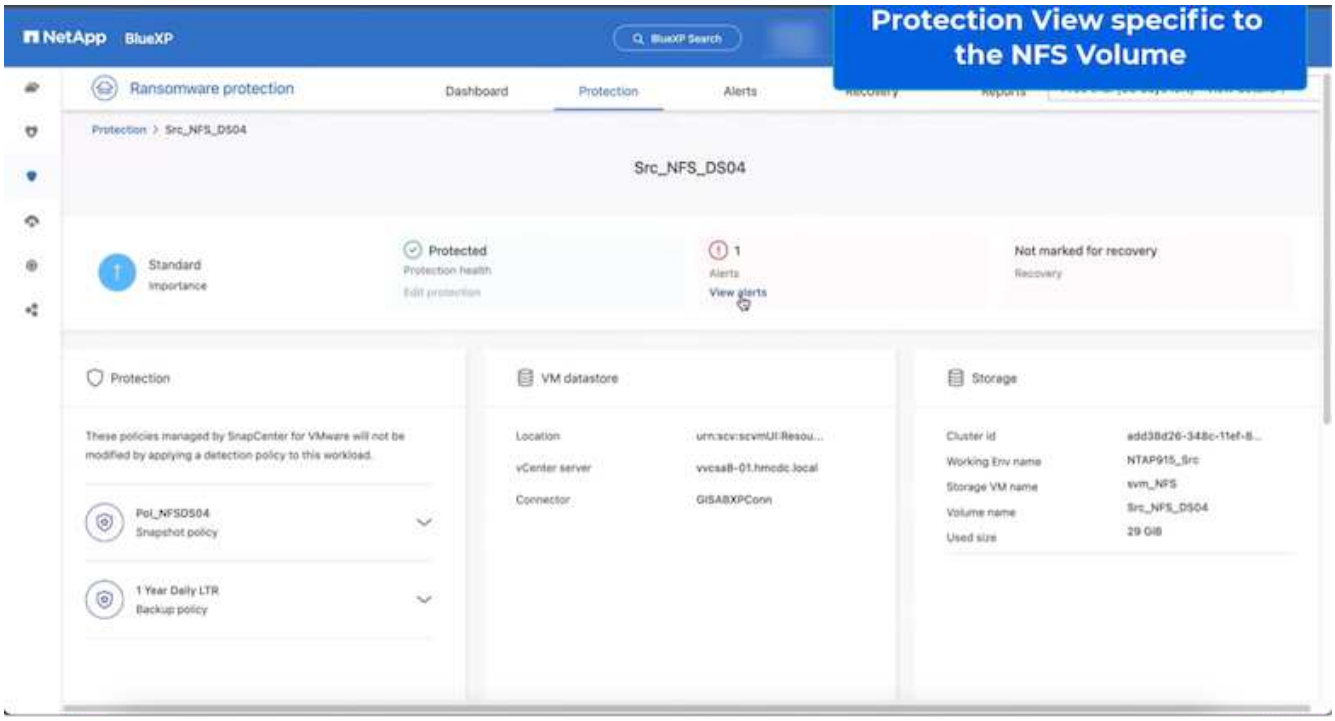
Una vez completado el análisis forense, las restauraciones se pueden realizar de manera rápida y sin problemas mediante la protección contra ransomware SnapCenter o BlueXP ransomware protection. Con SnapCenter, vaya a las máquinas virtuales afectadas y seleccione la instantánea adecuada para restaurar.



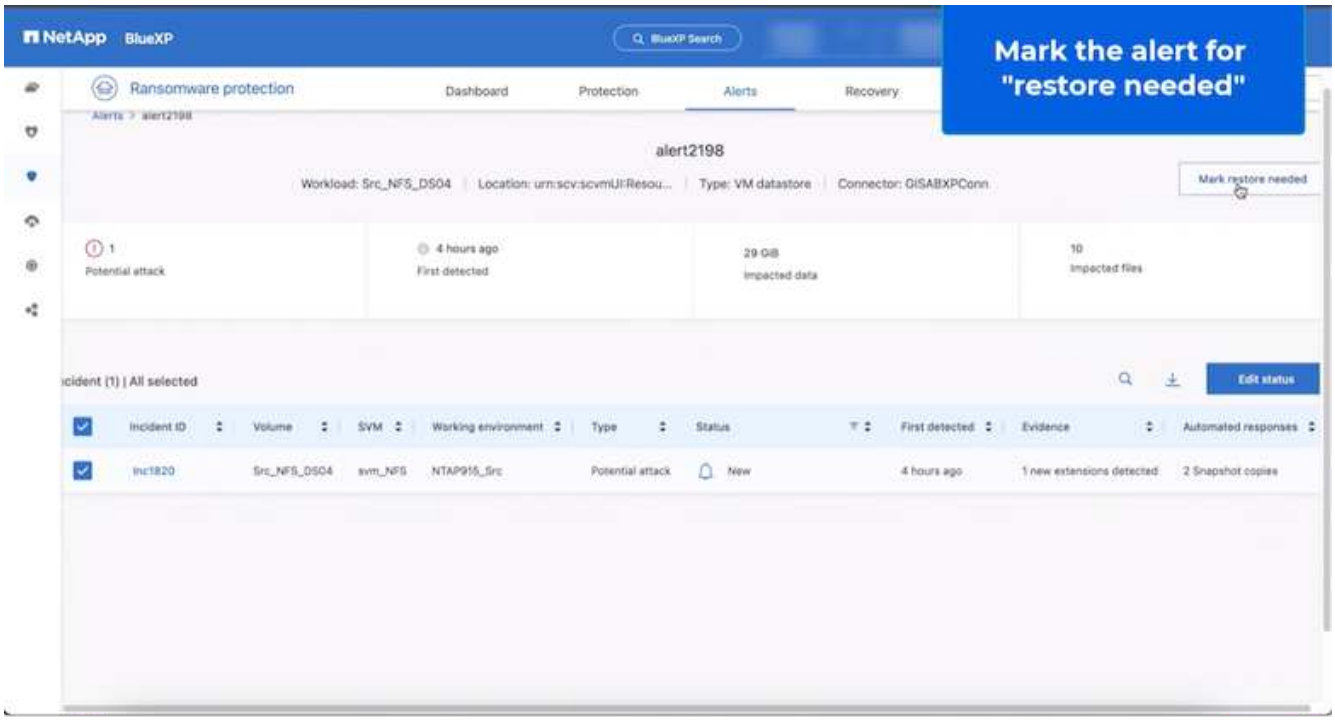
En esta sección se analiza cómo la BlueXP ransomware protection organiza la recuperación de un incidente de ransomware en el que los archivos de la máquina virtual están cifrados.

Si la máquina virtual está administrada por SnapCenter, la BlueXP ransomware protection restaura la máquina virtual a su estado anterior mediante el proceso consistente con la máquina virtual.

1. Acceda a la BlueXP ransomware protection y aparecerá una alerta en el Panel de BlueXP ransomware protection .
2. Haga clic en la alerta para revisar los incidentes en ese volumen específico para la alerta generada

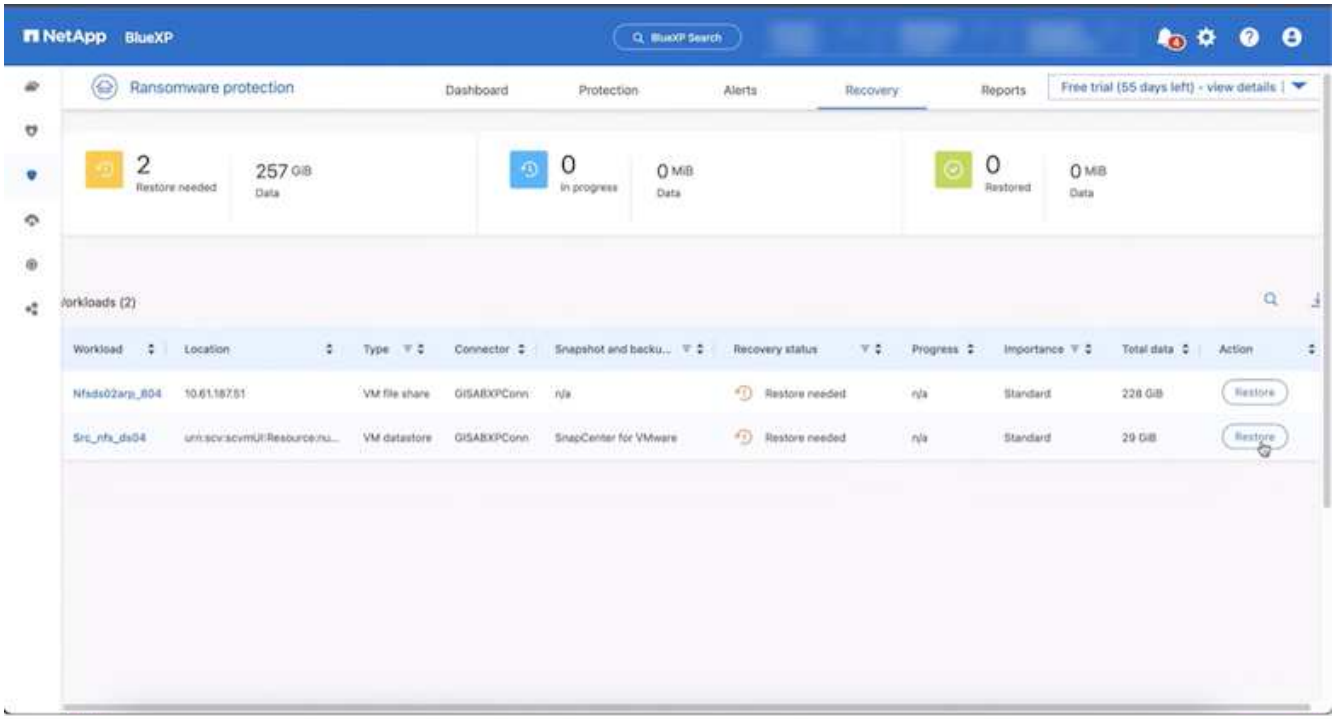


3. Marque el incidente de ransomware como listo para recuperación (después de que se neutralicen los incidentes) seleccionando "Marcar como necesaria la restauración".

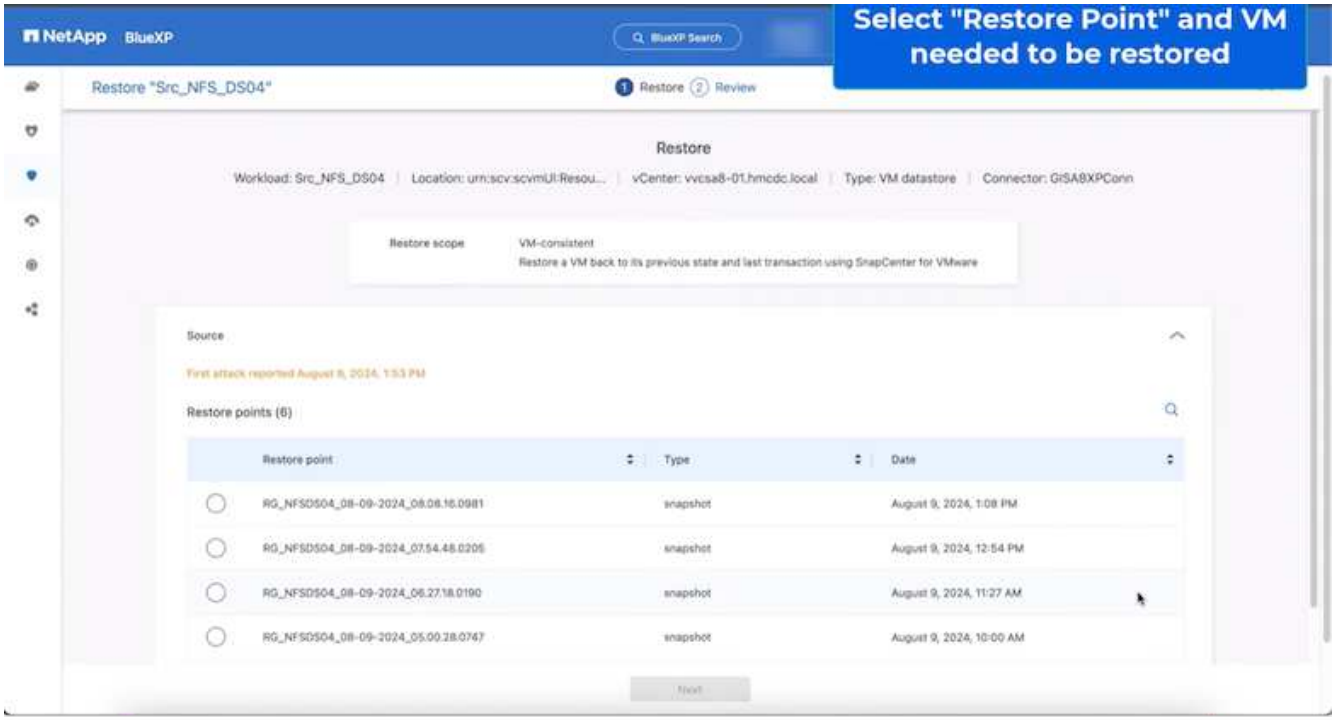


La alerta puede descartarse si el incidente resulta ser un falso positivo.

4. Vaya a la pestaña Recuperación y revise la información de la carga de trabajo en la página Recuperación y seleccione el volumen del almacén de datos que está en el estado "Se necesita restaurar" y seleccione Restaurar.

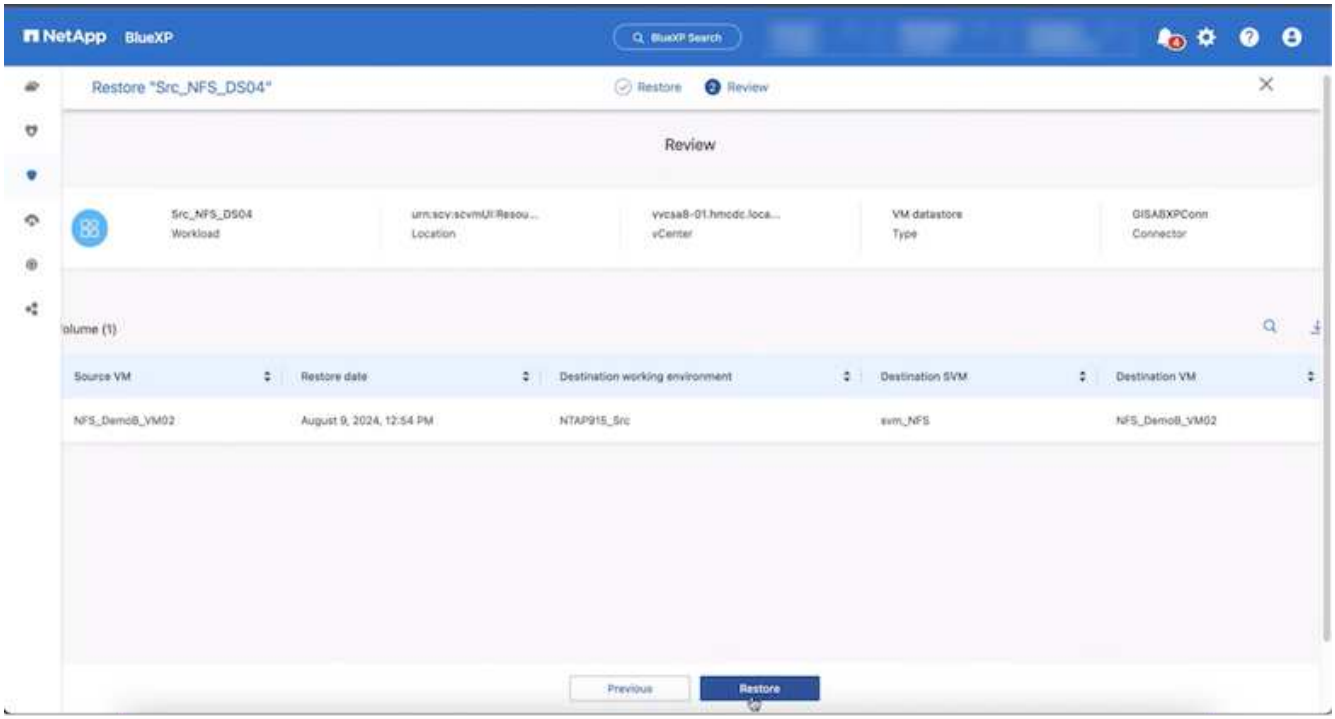


5. En este caso, el alcance de restauración es "Por VM" (para SnapCenter para VM, el alcance de restauración es "Por VM")

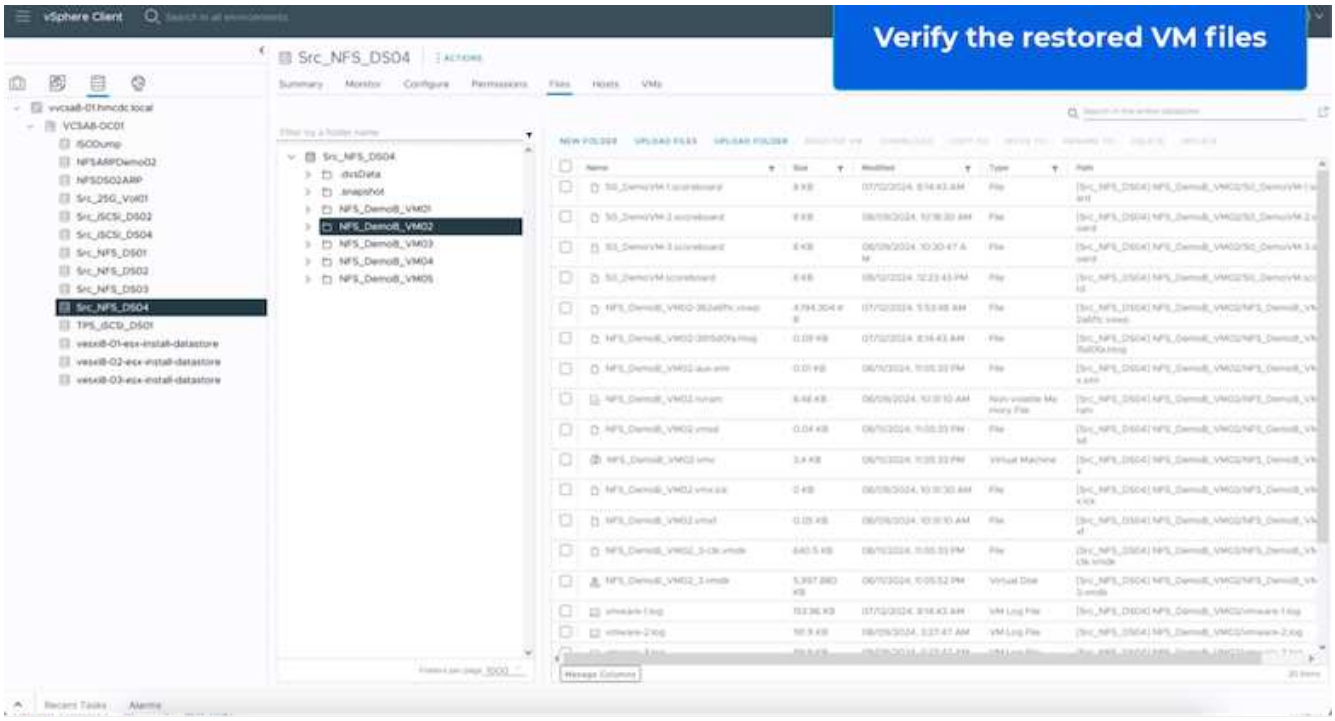


6. Seleccione el punto de restauración que desea utilizar para restaurar los datos y seleccione Destino y

haga clic en Restaurar.



7. Desde el menú superior, seleccione Recuperación para revisar la carga de trabajo en la página Recuperación, donde el estado de la operación se mueve a través de los estados. Una vez completada la restauración, los archivos de la máquina virtual se restauran como se muestra a continuación.



> La recuperación se puede realizar desde SnapCenter para VMware o el complemento de SnapCenter según la aplicación.

La solución de NetApp proporciona varias herramientas efectivas de visibilidad, detección y remediación,

ayudándole a detectar ransomware de forma temprana, evitar su propagación y recuperarse rápidamente, si es necesario, para evitar tiempos de inactividad costosos. Las soluciones tradicionales de defensa en capas siguen prevaleciendo, al igual que las soluciones de terceros y socios para visibilidad y detección. La remediación eficaz sigue siendo una parte crucial de la respuesta a cualquier amenaza.

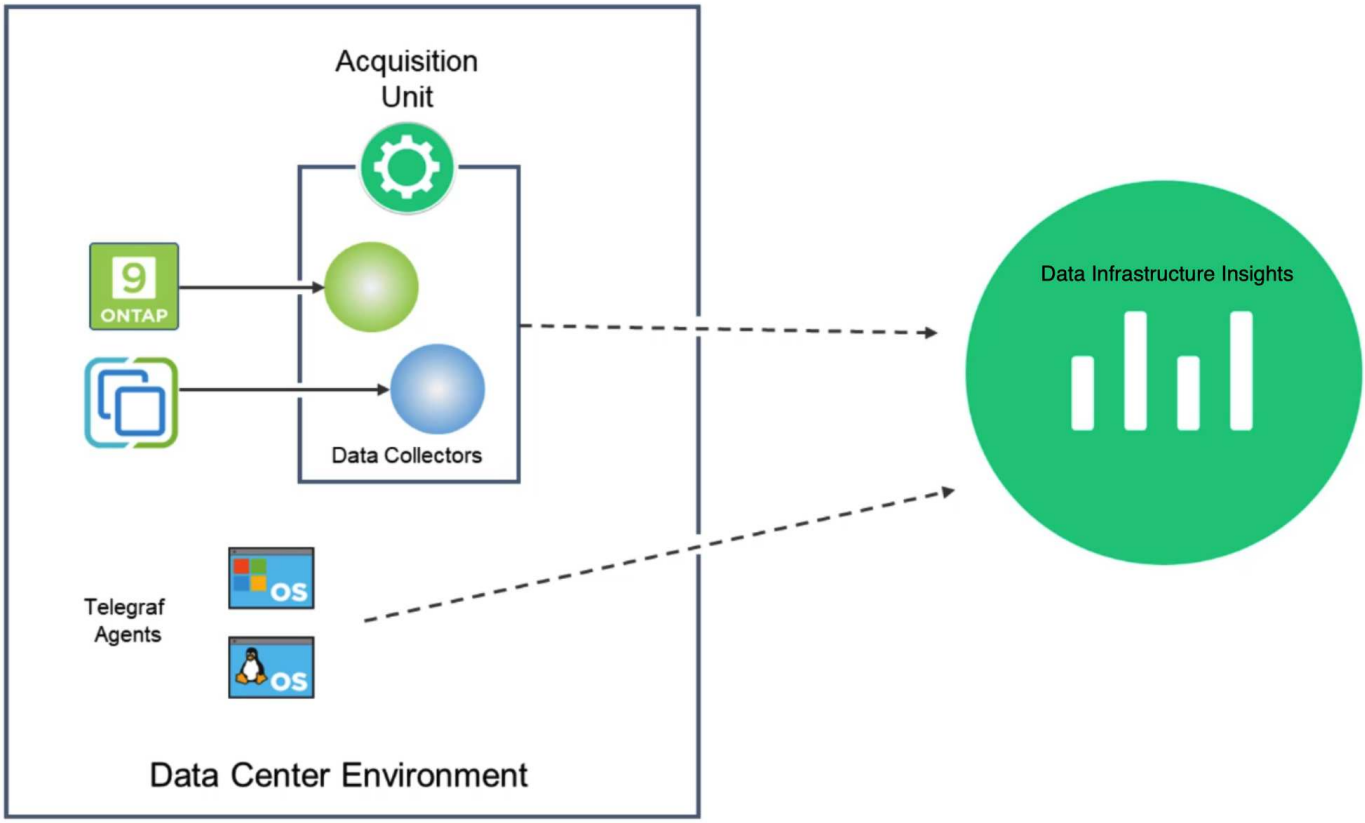
Supervise el almacenamiento local con Data Infrastructure Insights

NetApp Data Infrastructure Insights (anteriormente Cloud Insights) es una plataforma basada en la nube diseñada para monitorear y analizar el rendimiento, la salud y los costos de las infraestructuras de TI, tanto locales como en la nube. Aprenda a implementar recopiladores de datos, analizar métricas de rendimiento y utilizar paneles para identificar problemas y optimizar recursos.

Supervisión del almacenamiento local con Data Infrastructure Insights

Data Infrastructure Insights opera a través del software de la Unidad de Adquisición, que está configurado con recopiladores de datos para activos como los sistemas de almacenamiento VMware vSphere y NetApp ONTAP . Estos recopiladores recopilan datos y los transmiten a Data Infrastructure Insights. Luego, la plataforma utiliza una variedad de paneles, widgets y consultas métricas para organizar los datos en análisis reveladores que los usuarios pueden interpretar.

Diagrama de arquitectura de Data Infrastructure Insights :



Descripción general de la implementación de la solución

Esta solución proporciona una introducción al monitoreo de sistemas de almacenamiento locales de VMware vSphere y ONTAP mediante Data Infrastructure Insights.

Esta lista proporciona los pasos de alto nivel cubiertos en esta solución:

1. Configurar el recopilador de datos para un clúster de vSphere.
2. Configurar el recopilador de datos para un sistema de almacenamiento ONTAP .
3. Utilice reglas de anotación para etiquetar activos.
4. Explorar y correlacionar activos.
5. Utilice un panel de control de latencia de máquina virtual superior para aislar a los vecinos ruidosos.
6. Identificar oportunidades para dimensionar adecuadamente las máquinas virtuales.
7. Utilice consultas para aislar y ordenar métricas.

Prerrequisitos

Esta solución utiliza los siguientes componentes:

1. Matriz SAN All-Flash A400 de NetApp con ONTAP 9.13.
2. Clúster VMware vSphere 8.0.
3. Cuenta NetApp BlueXP .
4. Software de unidad de adquisición de Data Infrastructure Insights de NetApp instalado en una máquina virtual local con conectividad de red a activos para la recopilación de datos.

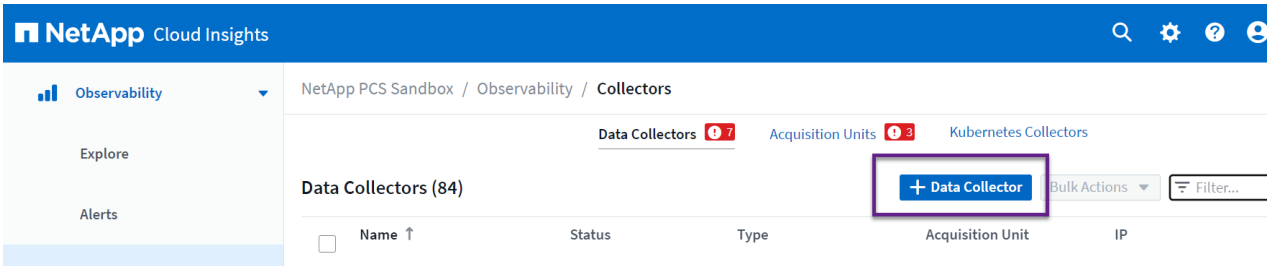
Implementación de la solución

Configurar recopiladores de datos

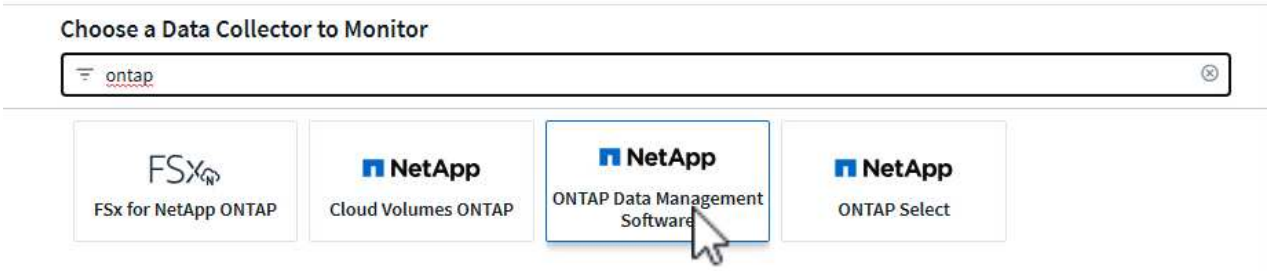
Para configurar recopiladores de datos para sistemas de almacenamiento VMware vSphere y ONTAP , complete los siguientes pasos:

Agregar un recopilador de datos para un sistema de almacenamiento ONTAP

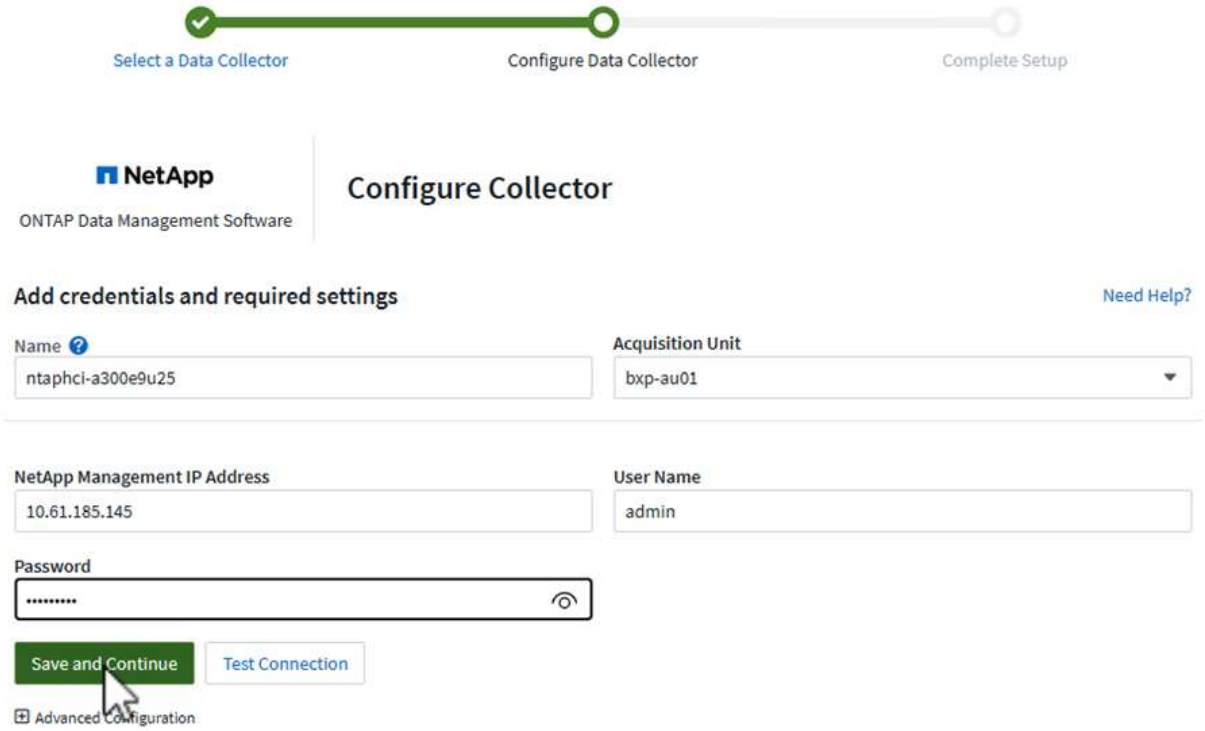
1. Una vez que haya iniciado sesión en Data Infrastructure Insights, navegue a **Observabilidad > Recopiladores > Recopiladores de datos** y presione el botón para instalar un nuevo recopilador de datos.



2. Desde aquí busque * ONTAP* y haga clic en * ONTAP Data Management Software*.

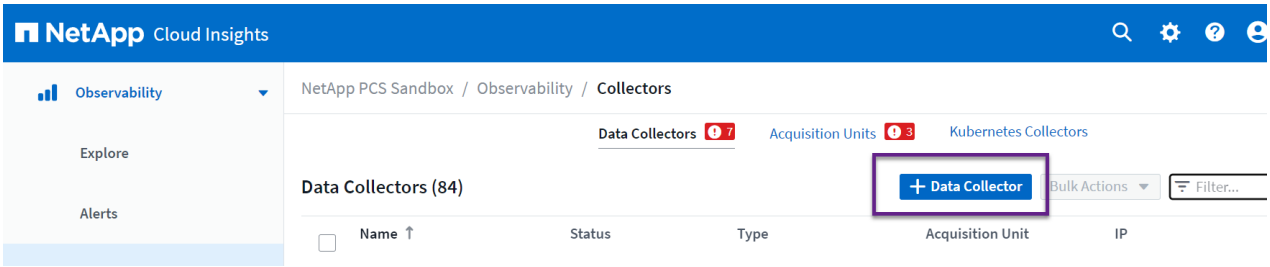


3. En la página **Configurar recopilador**, complete un nombre para el recopilador, especifique la **Unidad de adquisición** correcta y proporcione las credenciales para el sistema de almacenamiento ONTAP . Haga clic en **Guardar y continuar** y luego en **Completar configuración** en la parte inferior de la página para completar la configuración.

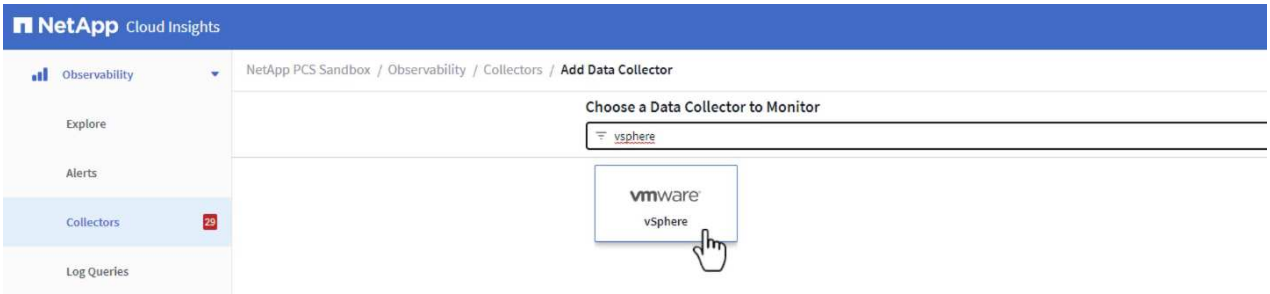


Agregar un recopilador de datos para un clúster de VMware vSphere

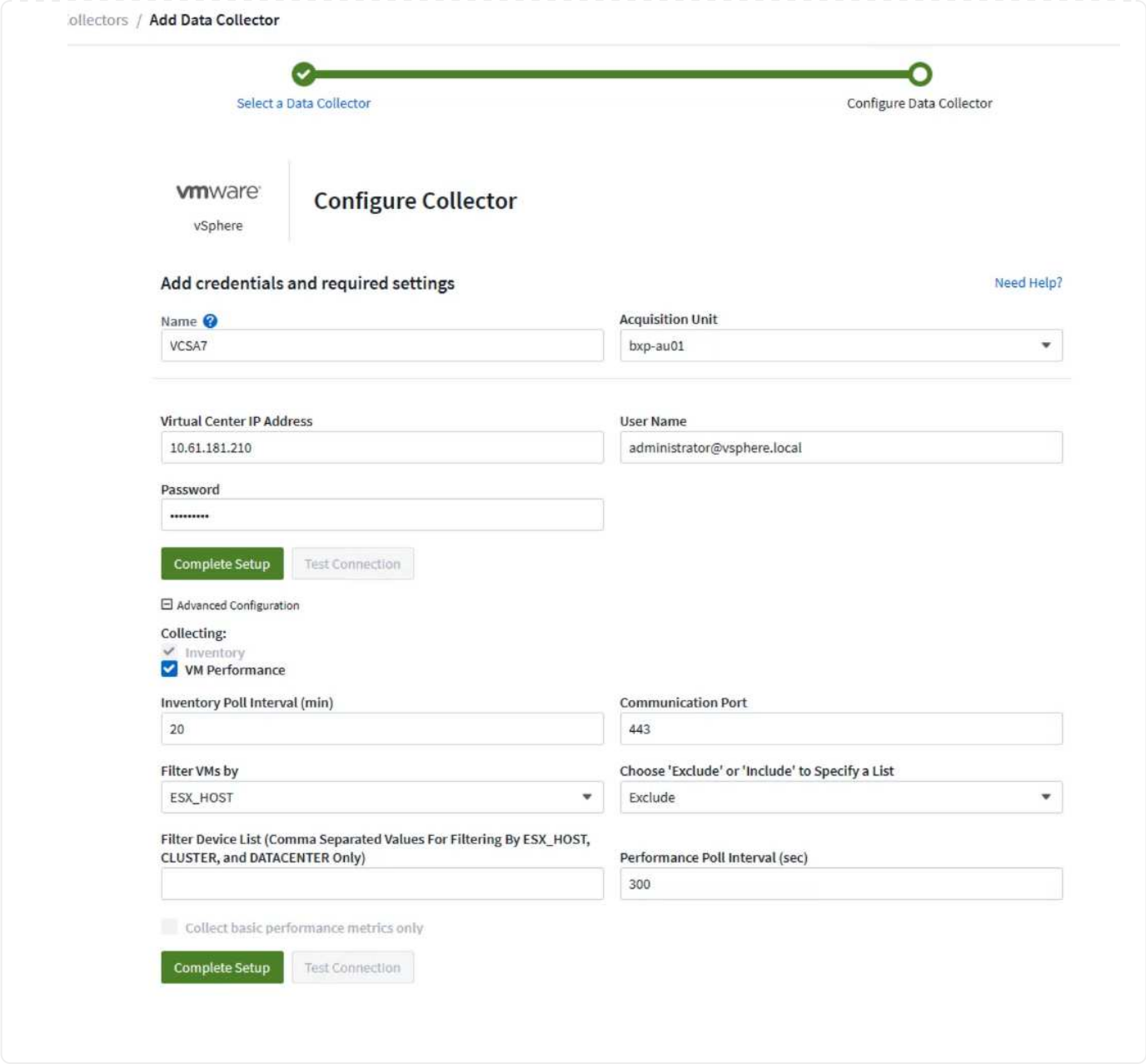
1. Una vez más, navegue a **Observabilidad > Recopiladores > Recopiladores de datos** y presione el botón para instalar un nuevo Recopilador de datos.



2. Desde aquí busque **vSphere** y haga clic en **VMware vSphere**.



3. En la página **Configurar recopilador**, complete un nombre para el recopilador, especifique la **Unidad de adquisición** correcta y proporcione las credenciales para el servidor vCenter. Haga clic en **Guardar y continuar** y luego en **Completar configuración** en la parte inferior de la página para completar la configuración.



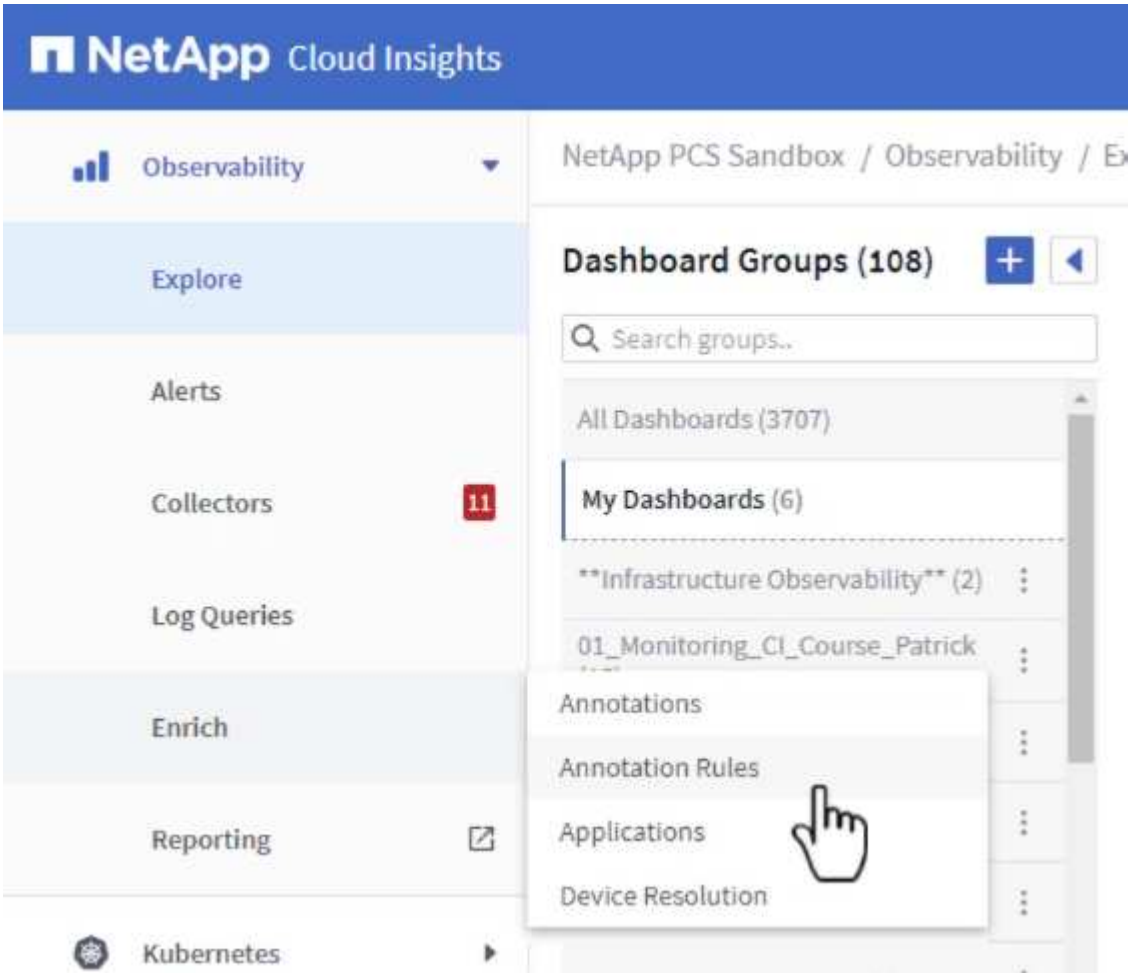
Agregar anotaciones a los activos

Las anotaciones son un método útil para etiquetar activos para que puedan filtrarse e identificarse de otro modo en las distintas vistas y consultas de métricas disponibles en Cloud Insights.

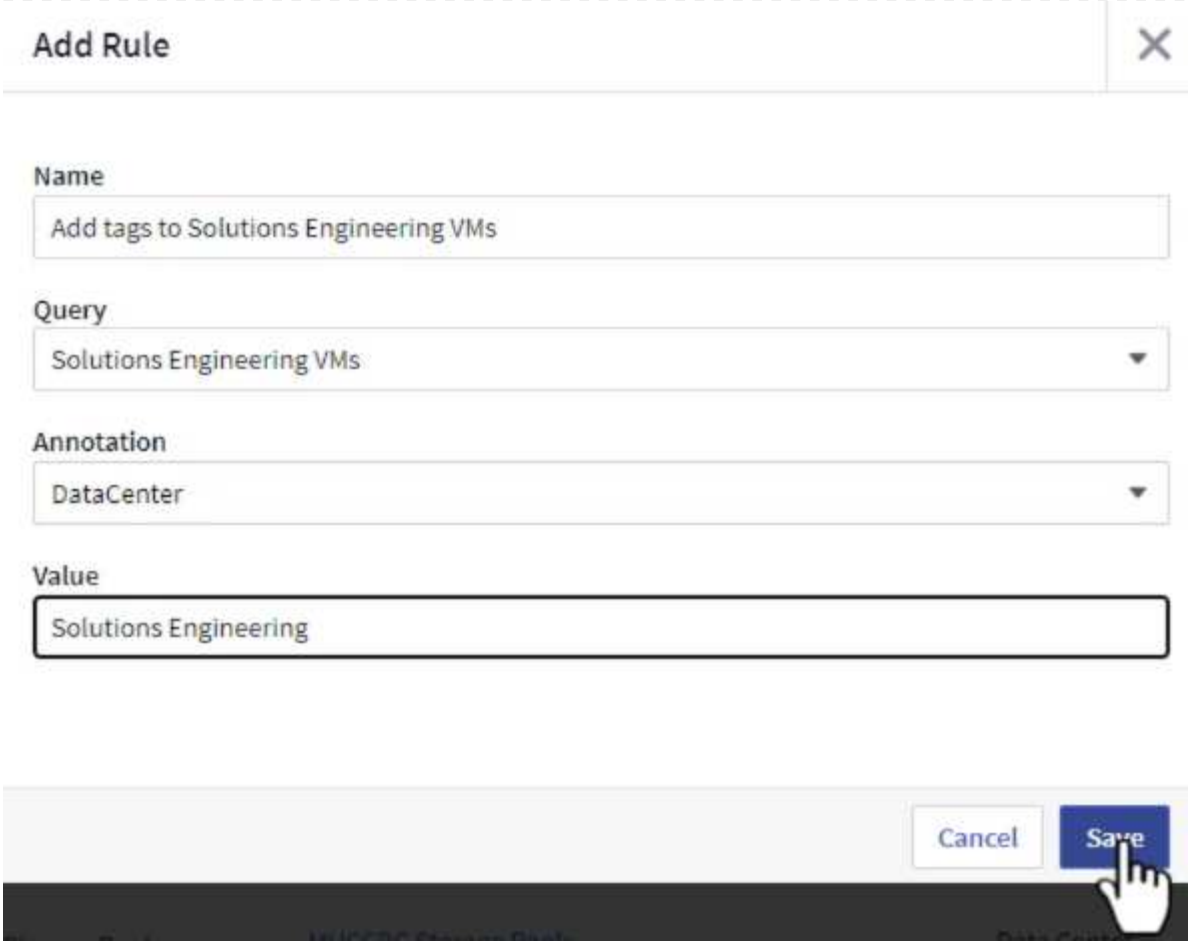
En esta sección, se agregarán anotaciones a los activos de las máquinas virtuales para filtrar por **Centro de datos**.

Utilice reglas de anotación para etiquetar activos

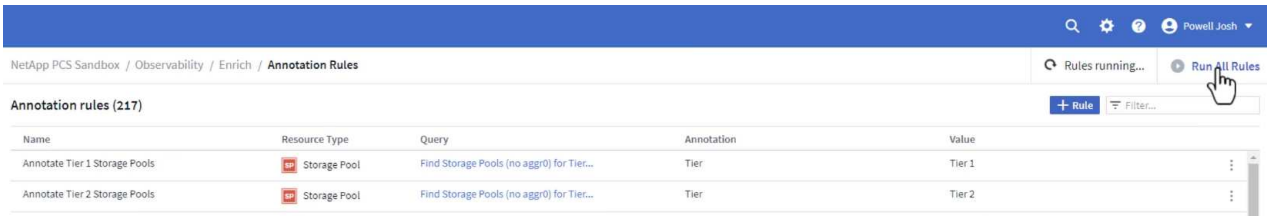
1. En el menú de la izquierda, navegue a **Observabilidad > Enriquecer > Reglas de anotación** y haga clic en el botón **+ Regla** en la esquina superior derecha para agregar una nueva regla.



2. En el cuadro de diálogo **Agregar regla**, ingrese un nombre para la regla, ubique una consulta a la que se aplicará la regla, el campo de anotación afectado y el valor que se completará.



3. Finalmente, en la esquina superior derecha de la página **Reglas de anotación**, haga clic en **Ejecutar todas las reglas** para ejecutar la regla y aplicar la anotación a los activos.



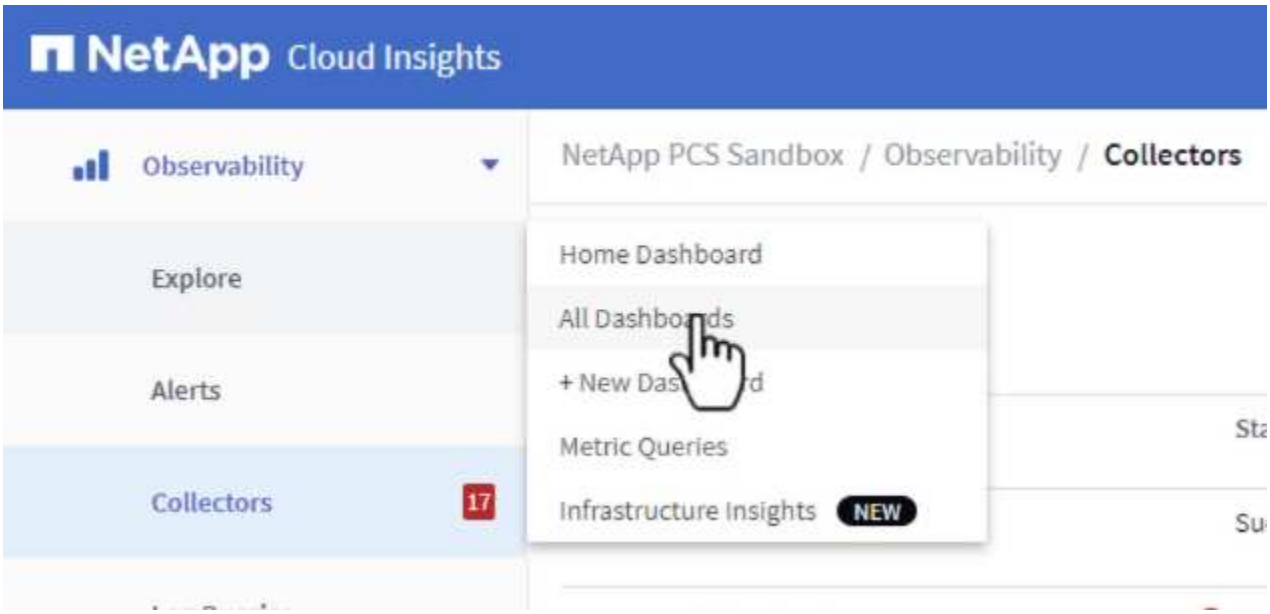
Explorar y correlacionar activos

Cloud Insights extrae conclusiones lógicas sobre los activos que se ejecutan juntos en sus sistemas de almacenamiento y clústeres de vSphere.

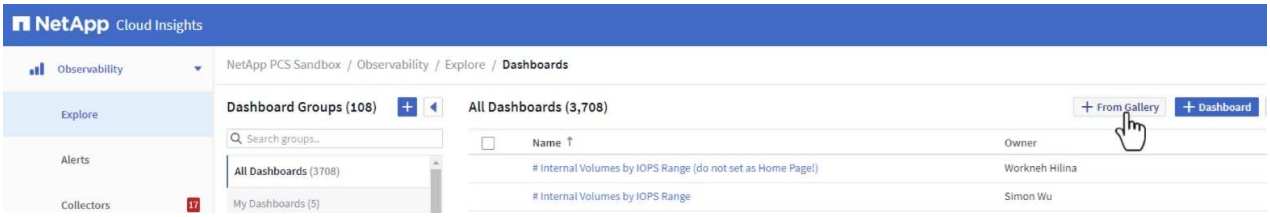
Esta sección ilustra cómo utilizar paneles para correlacionar activos.

Correlación de activos desde un panel de rendimiento de almacenamiento

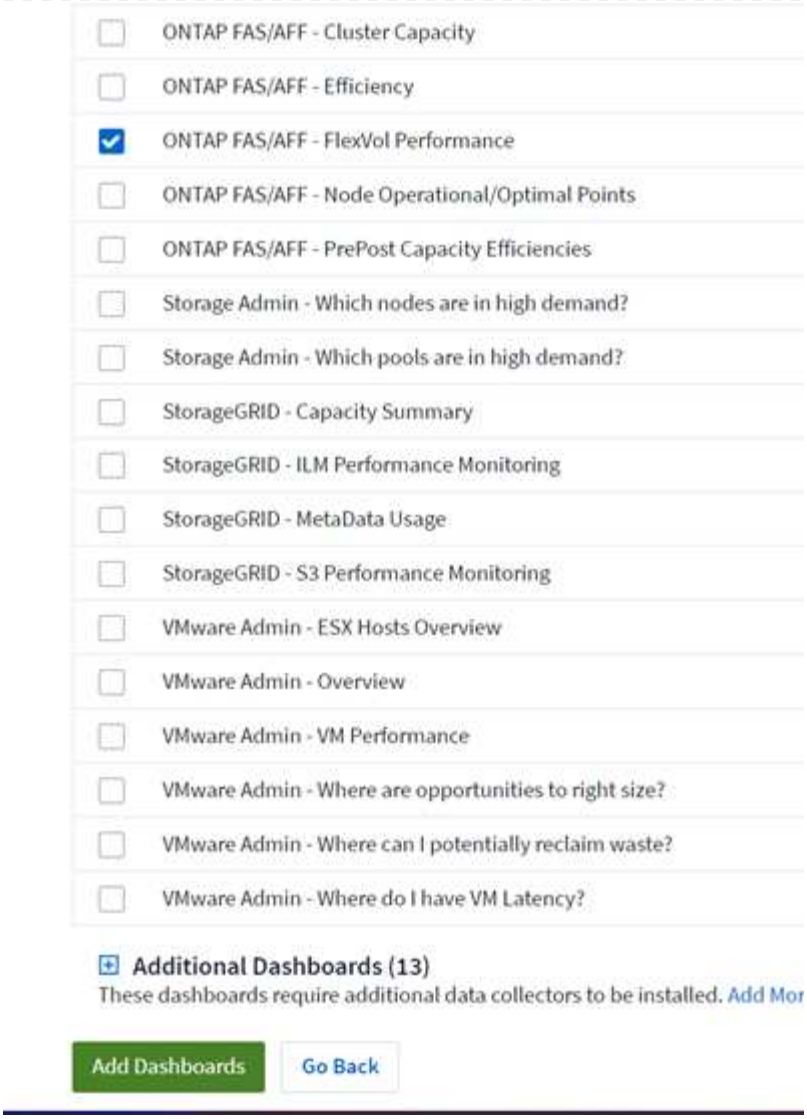
1. En el menú de la izquierda, navegue a **Observabilidad > Explorar > Todos los paneles**.



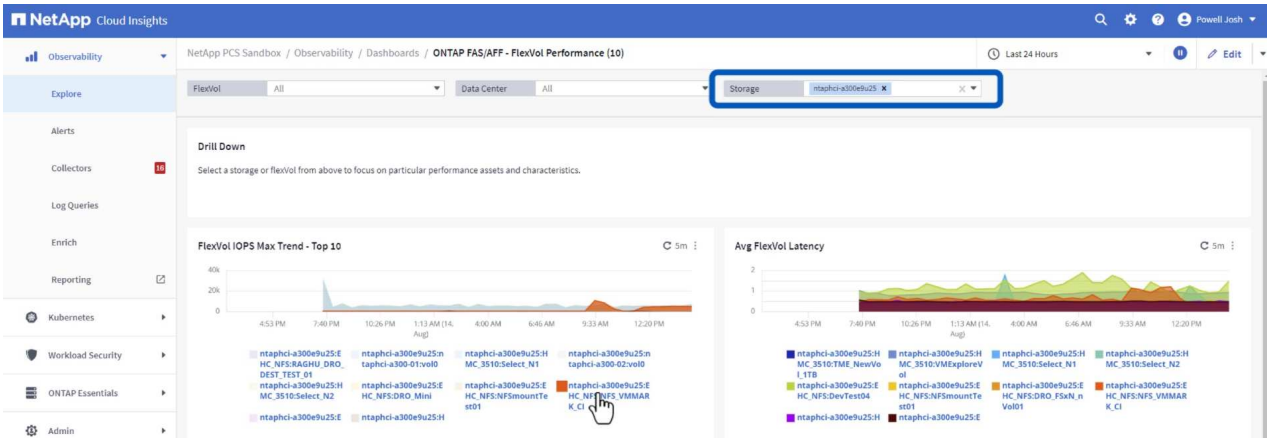
2. Haga clic en el botón **+ Desde la galería** para ver una lista de paneles listos para usar que se pueden importar.



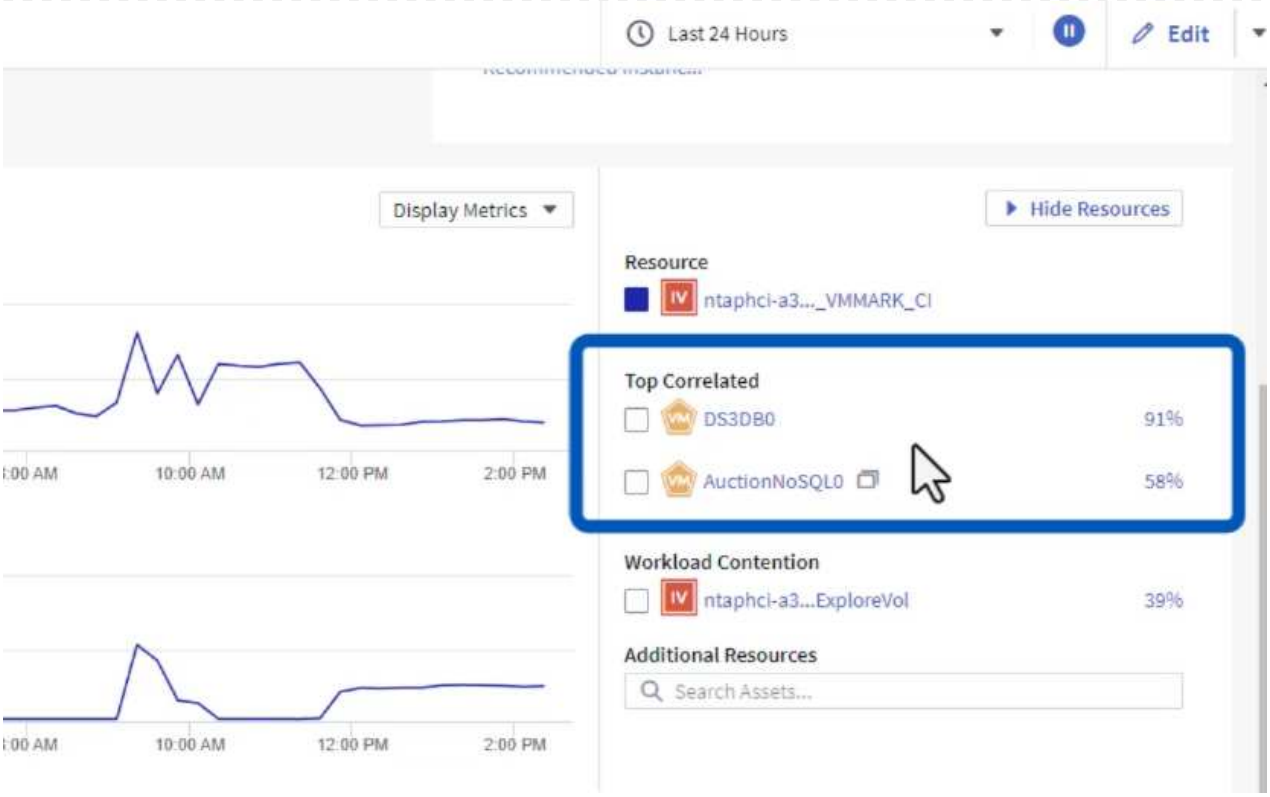
3. Seleccione un panel para el rendimiento de FlexVol de la lista y haga clic en el botón **Agregar paneles** en la parte inferior de la página.



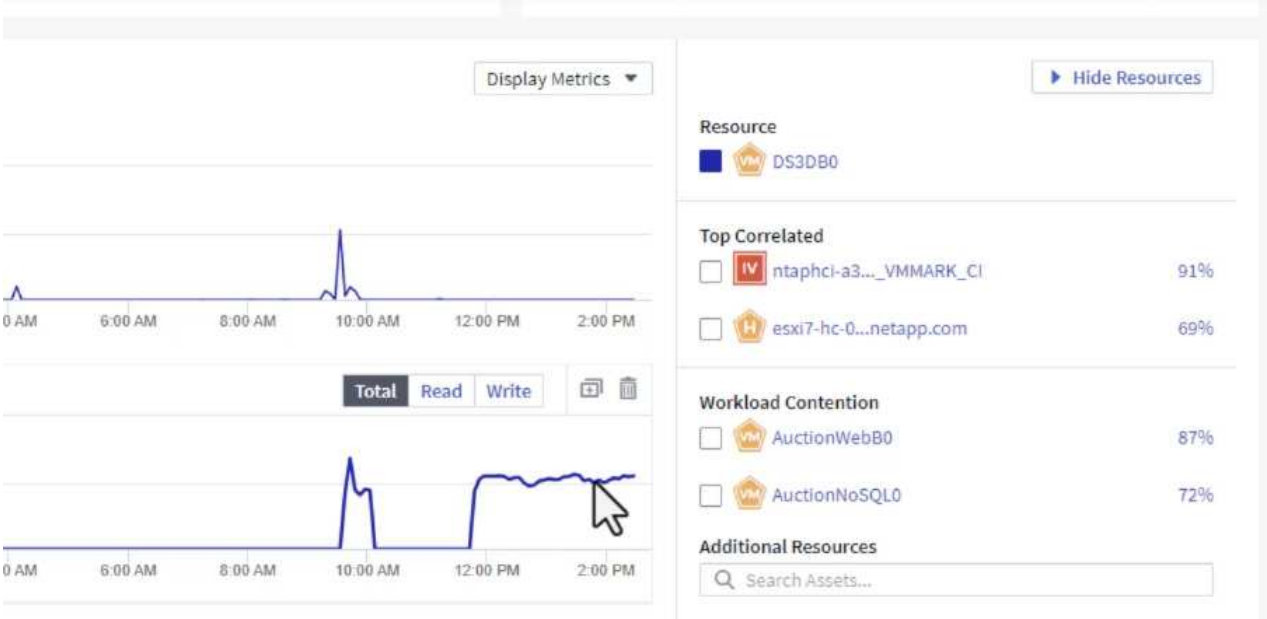
4. Una vez importado, abra el panel de control. Desde aquí puedes ver varios widgets con datos detallados de rendimiento. Agregue un filtro para ver un solo sistema de almacenamiento y seleccione un volumen de almacenamiento para explorar sus detalles.



5. Desde esta vista, puede ver varias métricas relacionadas con este volumen de almacenamiento y las máquinas virtuales más utilizadas y correlacionadas que se ejecutan en el volumen.



6. Al hacer clic en la VM con mayor utilización, se desglosan las métricas de esa VM para ver posibles problemas.



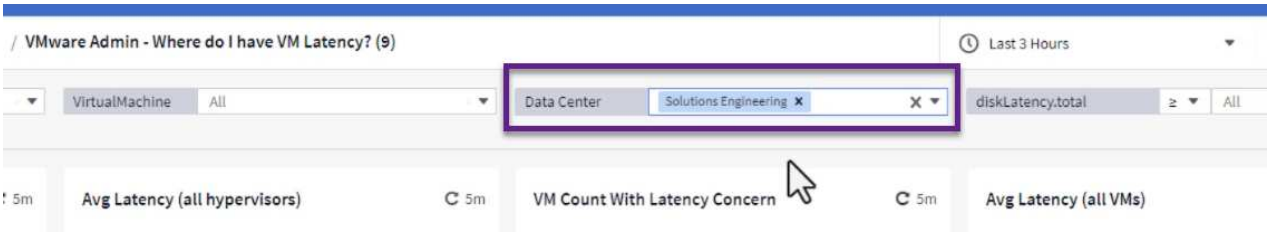
Utilice Cloud Insights para identificar vecinos ruidosos

Cloud Insights cuenta con paneles que pueden aislar fácilmente las máquinas virtuales pares que afectan negativamente a otras máquinas virtuales que se ejecutan en el mismo volumen de almacenamiento.

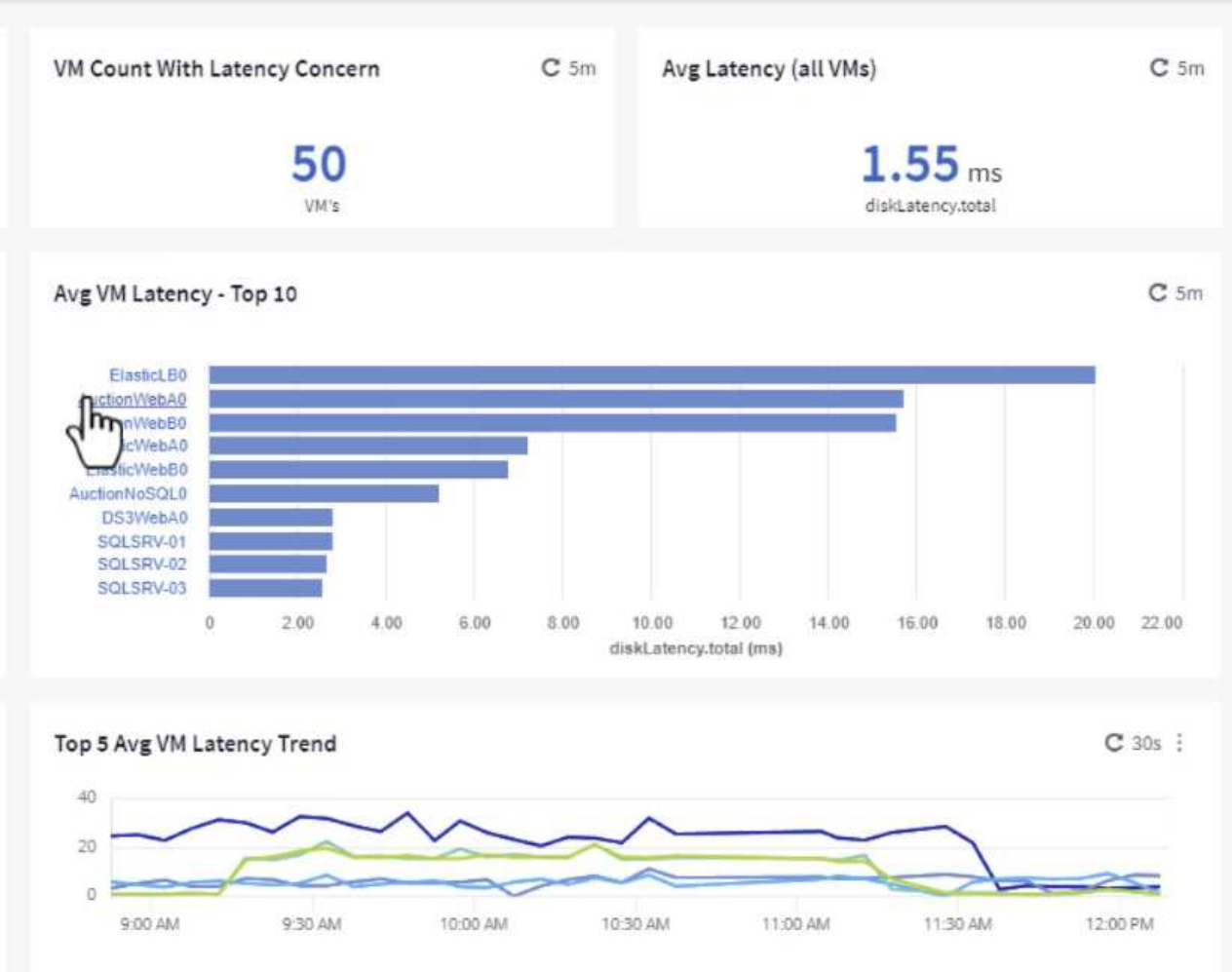
Utilice un panel de control de latencia de máquina virtual superior para aislar a los vecinos ruidosos

1. En este ejemplo, acceda a un panel disponible en la **Galería** llamado **VMware Admin - ¿Dónde tengo la latencia de VM?**

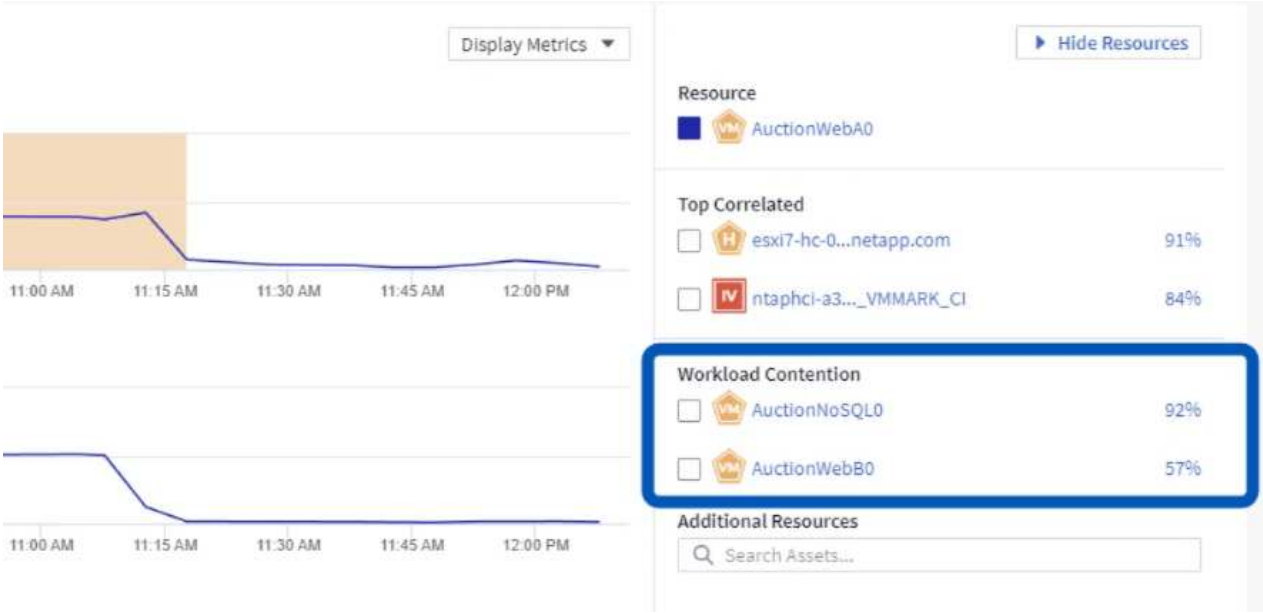
2. A continuación, filtre por la anotación **Centro de datos** creada en un paso anterior para ver un subconjunto de activos.



3. Este panel muestra una lista de las 10 principales máquinas virtuales por latencia promedio. Desde aquí, haga clic en la VM en cuestión para explorar sus detalles.



4. Las máquinas virtuales que potencialmente pueden causar contención de la carga de trabajo están enumeradas y disponibles. Analice en profundidad las métricas de rendimiento de estas máquinas virtuales para investigar cualquier problema potencial.

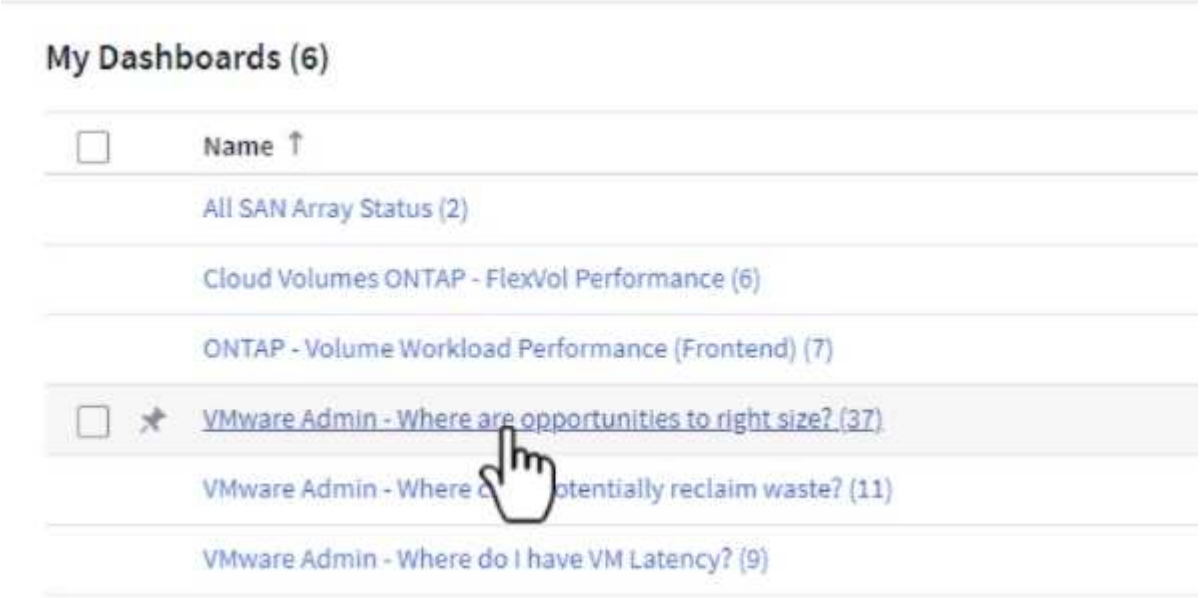


Visualizar los recursos sobreutilizados y subutilizados en Cloud Insights

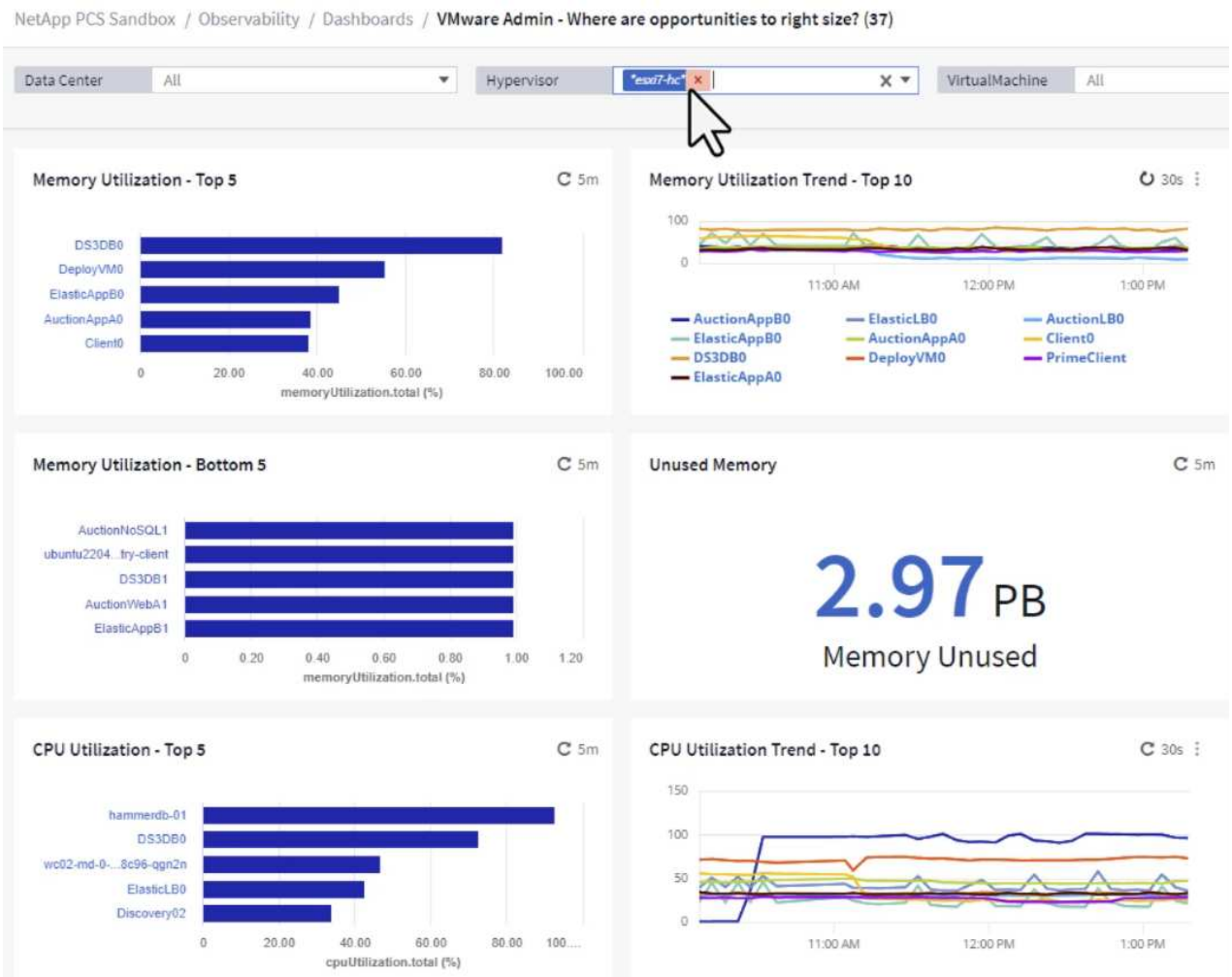
Al adaptar los recursos de la máquina virtual a los requisitos de carga de trabajo reales, se puede optimizar la utilización de los recursos, lo que genera ahorros de costos en infraestructura y servicios en la nube. Los datos en Cloud Insights se pueden personalizar para mostrar fácilmente las máquinas virtuales sobreutilizadas o subutilizadas.

Identificar oportunidades para dimensionar correctamente las máquinas virtuales

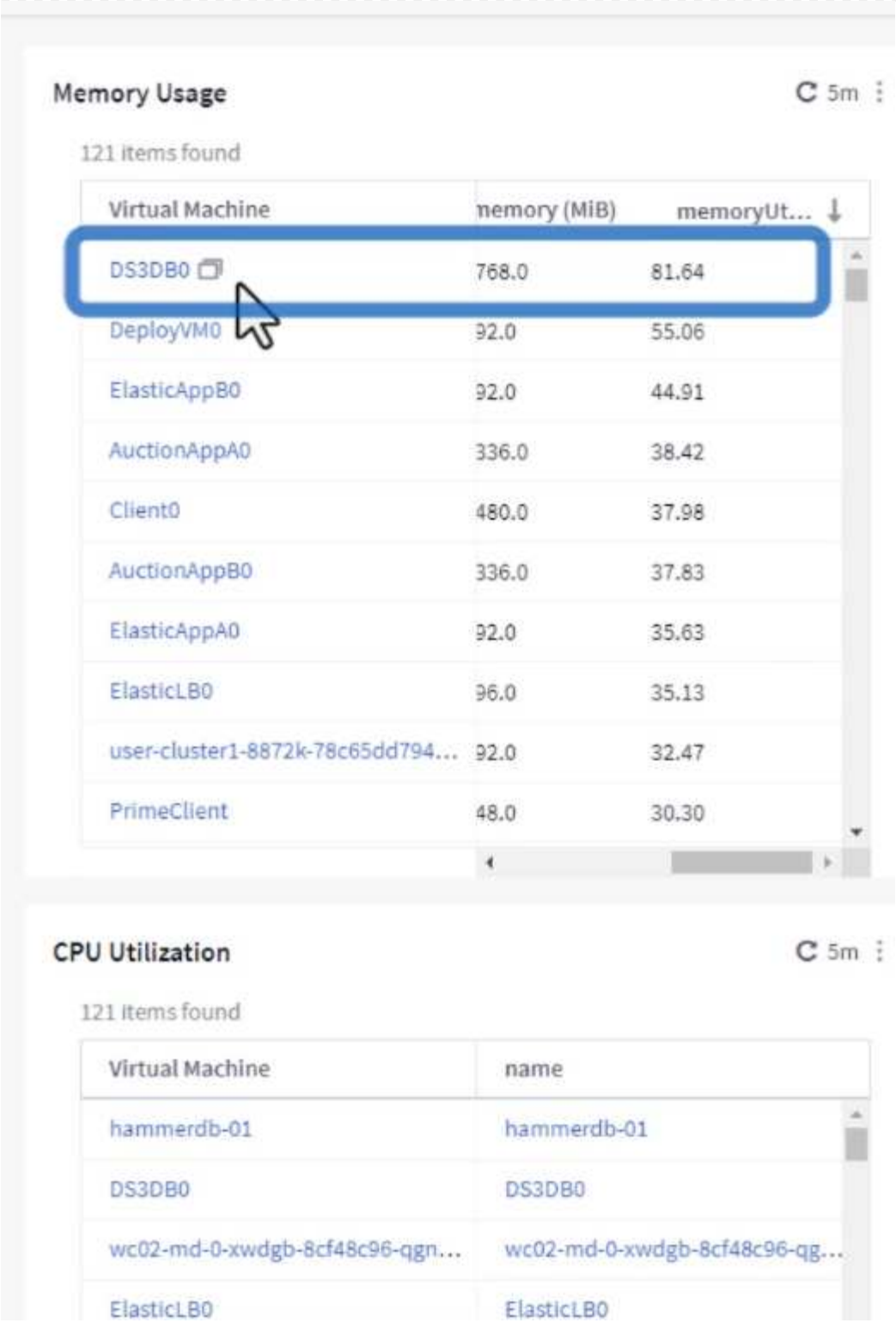
1. En este ejemplo, acceda a un panel de control disponible en la **Galería** llamado **VMware Admin: ¿Dónde están las oportunidades para dimensionar correctamente?**



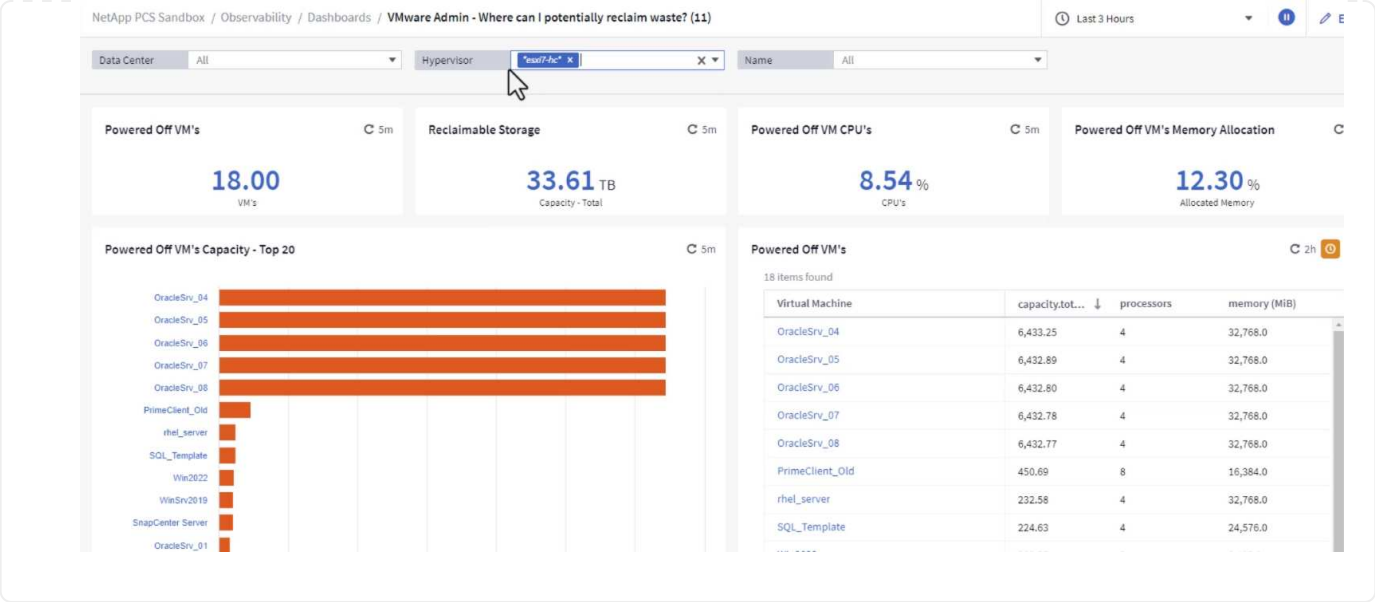
2. Primer filtro por todos los hosts ESXi en el clúster. Luego puede ver la clasificación de las máquinas virtuales superiores e inferiores por utilización de memoria y CPU.



3. Las tablas permiten ordenar y proporcionar más detalles según las columnas de datos elegidas.



4. Otro panel llamado **VMware Admin - ¿Dónde puedo recuperar potencialmente los desechos?** muestra las máquinas virtuales apagadas ordenadas por su uso de capacidad.

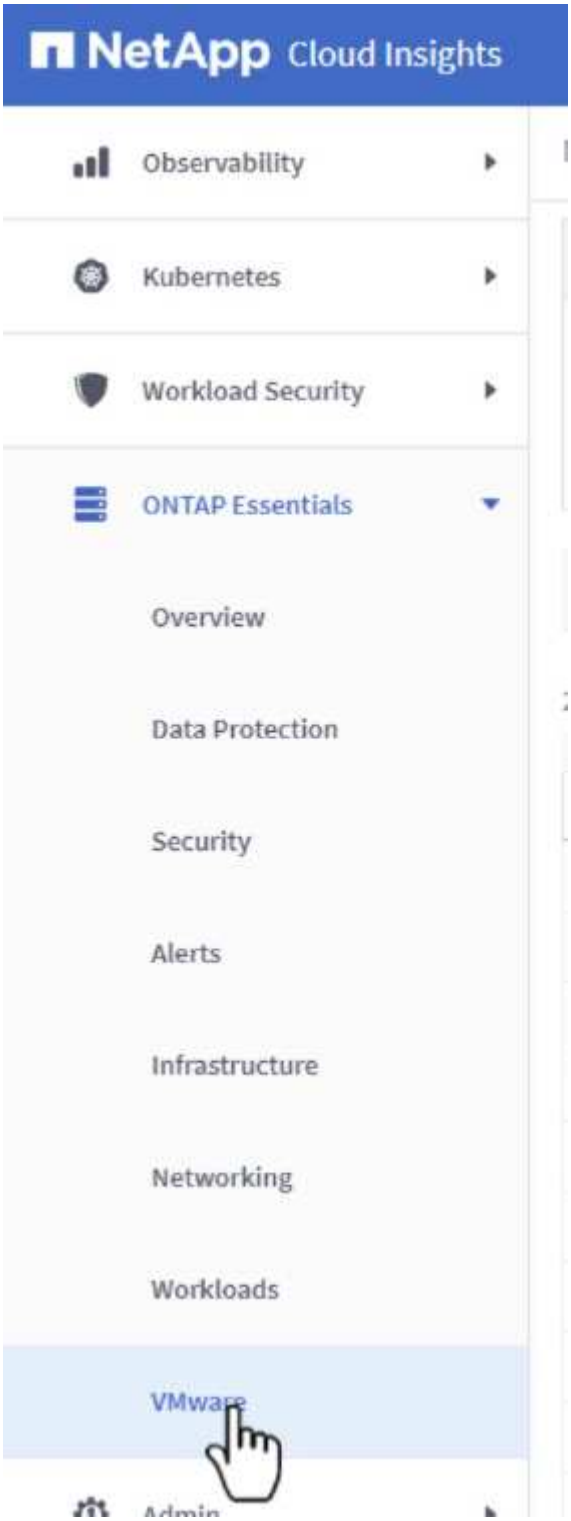


Utilice consultas para aislar y ordenar métricas

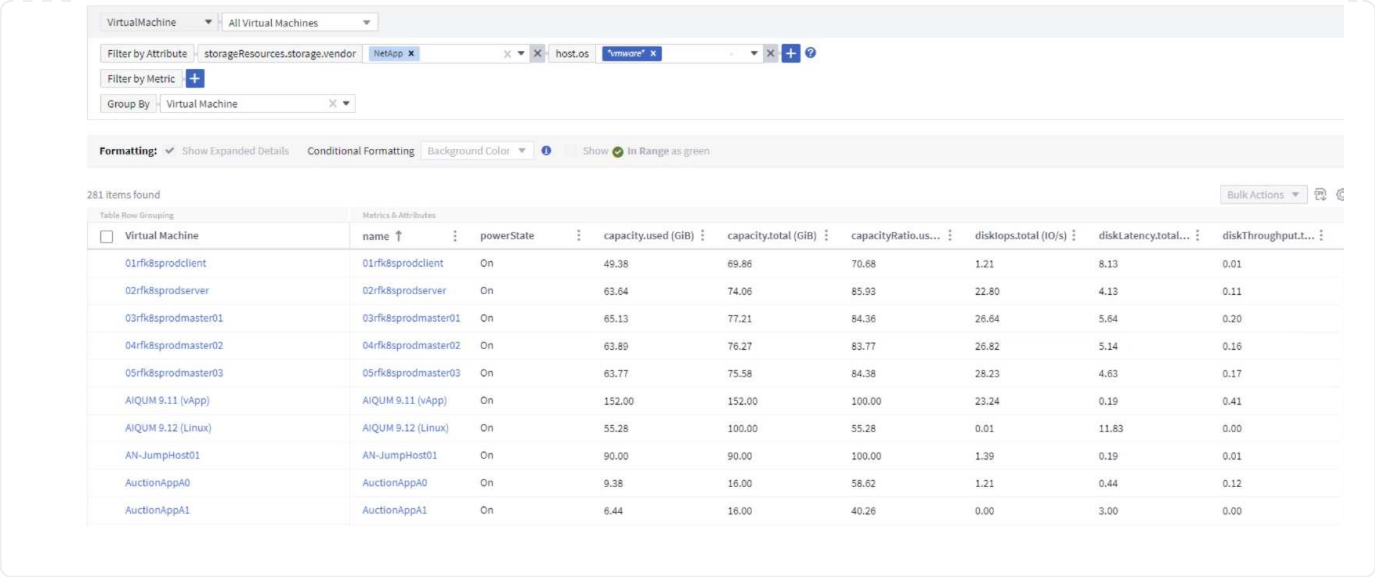
La cantidad de datos capturados por Cloud Insights es bastante amplia. Las consultas métricas proporcionan una forma poderosa de ordenar y organizar grandes cantidades de datos de maneras útiles.

Ver una consulta detallada de VMware en ONTAP Essentials

1. Vaya a * ONTAP Essentials > VMware * para acceder a una consulta de métricas de VMware completa.



2. En esta vista se le presentan múltiples opciones para filtrar y agrupar los datos en la parte superior. Todas las columnas de datos son personalizables y se pueden agregar columnas adicionales fácilmente.



Virtual Machine	name	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (IO/s)	diskLatency.total...	diskThroughput.t...
01rfk8sprodclient	01rfk8sprodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8sprodserver	02rfk8sprodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8sprodmaster01	03rfk8sprodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8sprodmaster02	04rfk8sprodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8sprodmaster03	05rfk8sprodmaster03	On	63.77	75.58	84.38	28.23	4.63	0.17
AIQUM 9.11 (vApp)	AIQUM 9.11 (vApp)	On	152.00	152.00	100.00	23.24	0.19	0.41
AIQUM 9.12 (Linux)	AIQUM 9.12 (Linux)	On	55.28	100.00	55.28	0.01	11.83	0.00
AN-JumpHost01	AN-JumpHost01	On	90.00	90.00	100.00	1.39	0.19	0.01
AuctionAppA0	AuctionAppA0	On	9.38	16.00	58.62	1.21	0.44	0.12
AuctionAppA1	AuctionAppA1	On	6.44	16.00	40.26	0.00	3.00	0.00

Conclusión

Esta solución fue diseñada como una introducción para aprender cómo comenzar a utilizar NetApp Cloud Insights y mostrar algunas de las poderosas capacidades que esta solución de observabilidad puede proporcionar. Hay cientos de paneles y consultas de métricas integrados en el producto, lo que hace que sea fácil comenzar a usarlo de inmediato. La versión completa de Cloud Insights está disponible como prueba de 30 días y la versión básica está disponible de forma gratuita para los clientes de NetApp .

Información adicional

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

- "Página de inicio de NetApp BlueXP y Data Infrastructure Insights"
- "Documentación de NetApp Data Infrastructure Insights"

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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