



Virtualización de VMware

NetApp Solutions

NetApp
December 19, 2024

Tabla de contenidos

- Soluciones de NetApp para la virtualización con VMware de Broadcom 1
 - VMware vSphere con ONTAP 1
 - VMware vSphere Foundation 1
 - Base de cloud de VMware 192
 - Migración de equipos virtuales 357
 - Multicloud híbrido de NetApp con soluciones de VMware 411
 - Casos de uso de multicloud híbrido de VMware 411
 - Automatización de VMware vSphere 412
 - Demostraciones y tutoriales 435

Soluciones de NetApp para la virtualización con VMware de Broadcom

VMware vSphere con ONTAP

ONTAP ha sido una solución de almacenamiento líder para entornos de VMware vSphere durante casi dos décadas y continúa añadiendo funcionalidades innovadoras para simplificar la gestión al tiempo que reduce los costes. Este documento presenta la solución ONTAP para vSphere, e incluye la información de producto más reciente y las prácticas recomendadas para simplificar la puesta en marcha, reducir el riesgo y simplificar la gestión.

Si desea más información, visite ["VMware vSphere con ONTAP"](#)

VMware vSphere Foundation

Guía de referencia de NFS para vSphere 8

Guía de referencia de NFS v3 para vSphere 8

VMware vSphere Foundation (VVF) es una plataforma de clase empresarial que puede ofrecer varias cargas de trabajo virtualizadas. El núcleo de vSphere es VMware vCenter, el hipervisor ESXi, los componentes de red y diversos servicios de recursos. Cuando se combinan con ONTAP, las infraestructuras virtualizadas que funcionan con VMware ofrecen una flexibilidad, escalabilidad y capacidad notables.

Usar NFS v3 con vSphere 8 y sistemas de almacenamiento de ONTAP

Este documento proporciona información sobre las opciones de almacenamiento disponibles para VMware Cloud vSphere Foundation mediante cabinas all-flash de NetApp. Las opciones de almacenamiento admitidas se cubren con instrucciones específicas para la implementación de almacenes de datos NFS. Además, se demuestra la recuperación ante desastres de almacenes de datos NFS de VMware Live Site Recovery. Finalmente, se revisa la protección autónoma frente a ransomware de NetApp para el almacenamiento NFS.

Casos de uso

Casos de uso cubiertos en esta documentación:

- Opciones de almacenamiento para los clientes que buscan entornos uniformes tanto en clouds públicos como privados.
- Puesta en marcha de infraestructura virtual para cargas de trabajo.
- Solución de almacenamiento escalable adaptada para satisfacer las necesidades en constante evolución, incluso cuando no se alinea directamente con los requisitos de recursos informáticos.
- Proteger máquinas virtuales y almacenes de datos con el plugin de SnapCenter para VMware vSphere.
- Uso de Live Site Recovery de VMware para la recuperación ante desastres de almacenes de datos NFS.
- Estrategia de detección de ransomware, incluidas varias capas de protección en host ESXi y máquina

virtual invitada.

Destinatarios

Esta solución está dirigida a las siguientes personas:

- Arquitectos de soluciones que buscan opciones de almacenamiento más flexibles para entornos VMware diseñadas para maximizar el TCO.
- Arquitectos de soluciones que buscan opciones de almacenamiento VVF que ofrezcan opciones de protección de datos y recuperación ante desastres con los principales proveedores de cloud.
- Administradores de almacenamiento que desean instrucciones específicas sobre cómo configurar VVF con el almacenamiento NFS.
- Administradores de almacenamiento que desean instrucciones específicas sobre cómo proteger máquinas virtuales y almacenes de datos que residen en el almacenamiento de ONTAP.

Visión general de la tecnología

La guía de referencia de NFS v3 VVF para vSphere 8 consta de los siguientes componentes principales:

VMware vSphere Foundation

VMware vCenter, un componente central de vSphere Foundation, es una plataforma de gestión centralizada para proporcionar configuración, control y administración de entornos vSphere. VCenter actúa como base para la gestión de infraestructuras virtualizadas y permite a los administradores poner en marcha, supervisar y gestionar máquinas virtuales, contenedores y hosts ESXi en el entorno virtual.

La solución VVF es compatible tanto con cargas de trabajo nativas de Kubernetes como con máquinas virtuales. Los componentes clave incluyen:

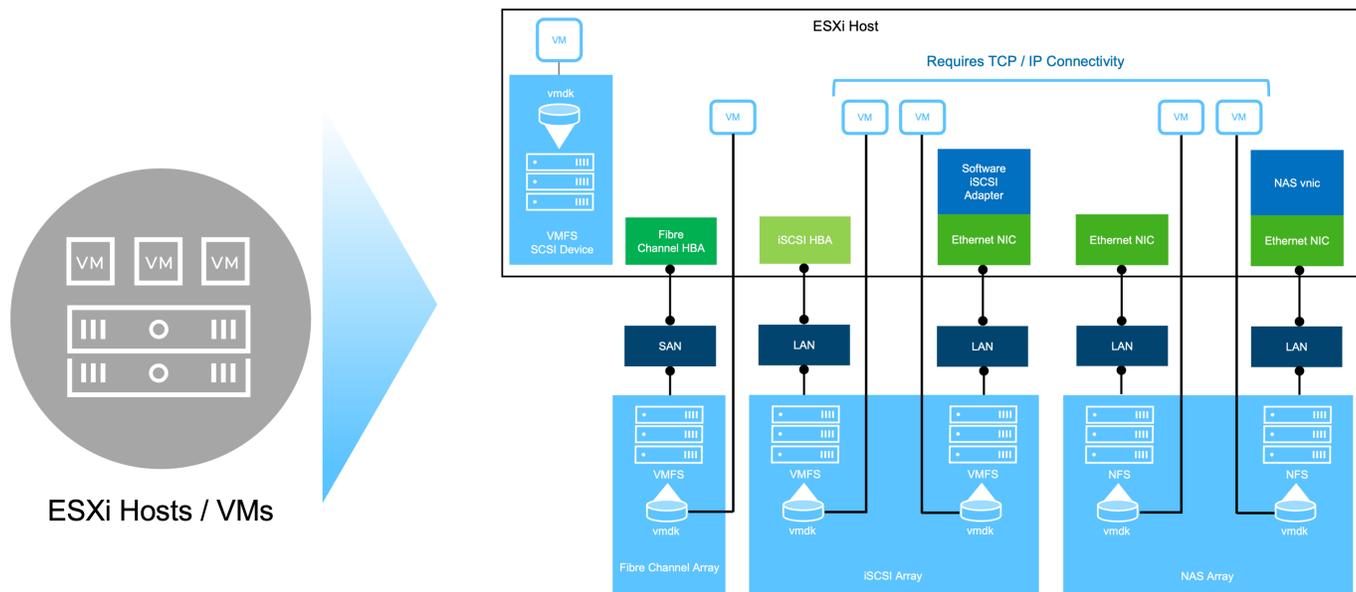
- vSphere de VMware
- vSAN de VMware
- Estándar ARIA
- Tanzu Kubernetes Grid Service para vSphere de VMware
- Switch distribuido de vSphere

Para obtener más información sobre los componentes incluidos en VVF, consulte Arquitectura y planificación, consulte "[Comparación directa de productos de VMware vSphere](#)".

Opciones de almacenamiento de VVF

El almacenamiento es esencial para un entorno virtual exitoso y potente. Ya sea mediante almacenes de datos de VMware o casos de uso conectados al invitado, libera las funcionalidades de tus cargas de trabajo a medida que puedes elegir el mejor precio por GB que proporcione el máximo valor a la vez que reduce el infrauso. ONTAP ha sido una solución de almacenamiento líder para entornos de VMware vSphere durante casi dos décadas y continúa añadiendo funcionalidades innovadoras para simplificar la gestión al tiempo que reduce los costes.

Las opciones de almacenamiento de VMware normalmente se organizan como ofertas de almacenamiento tradicional y de almacenamiento definidas por software. Los modelos tradicionales de almacenamiento incluyen almacenamiento local y en red, mientras que los modelos de almacenamiento definido por software incluyen vSAN y VMware Virtual Volumes (vVols).



Consulte "[Introducción a almacenamiento en entornos de vSphere](#)" para obtener más información sobre los tipos de almacenamiento compatibles para VMware vSphere Foundation.

ONTAP de NetApp

Existen numerosas razones de peso por las que decenas de miles de clientes han elegido ONTAP como su solución de almacenamiento principal para vSphere. Entre ellos se incluyen los siguientes:

1. **Sistema de almacenamiento unificado:** ONTAP ofrece un sistema de almacenamiento unificado que admite protocolos SAN y NAS. Esta versatilidad permite la integración perfecta de diversas tecnologías de almacenamiento en una única solución.
2. * Protección de datos robusta: * ONTAP proporciona capacidades sólidas de protección de datos a través de instantáneas eficientes en el espacio. Estos snapshots posibilitan procesos de backup y recuperación eficientes que garantizan la seguridad y la integridad de los datos de las aplicaciones.
3. * Herramientas de gestión integrales: * ONTAP ofrece una gran cantidad de herramientas diseñadas para ayudar a administrar los datos de las aplicaciones de manera efectiva. Estas herramientas optimizan las tareas de gestión del almacenamiento, mejoran la eficiencia operativa y simplifican la administración.
4. **Eficiencia de almacenamiento:** ONTAP incluye varias funciones de eficiencia de almacenamiento, habilitadas de forma predeterminada, diseñadas para optimizar la utilización del almacenamiento, reducir los costos y mejorar el rendimiento general del sistema.

El uso de ONTAP con VMware permite una gran flexibilidad cuando se trata de necesidades de aplicación determinadas. Se admiten los siguientes protocolos como almacén de datos VMware con ONTAP: * FCP * FCoE * NVMe/FC * NVMe/TCP * iSCSI * NFS v3 * NFS v4,1

El uso de un sistema de almacenamiento independiente del hipervisor permite descargar numerosas funciones y maximizar su inversión en sistemas de host vSphere. Este método no solo garantiza que los recursos del host se centren en las cargas de trabajo de las aplicaciones, sino que también evita efectos de rendimiento aleatorios en las aplicaciones de operaciones de almacenamiento.

El uso de ONTAP junto con vSphere es una excelente combinación que le permite reducir los gastos en hardware del host y software de VMware. También puede proteger sus datos con un coste menor y un alto rendimiento constante. Dado que las cargas de trabajo virtualizadas son móviles, puede explorar distintos

enfoques mediante Storage vMotion para mover equipos virtuales entre almacenes de datos de VMFS, NFS o vVols, todo ello en el mismo sistema de almacenamiento.

Cabinas all-flash NetApp

NetApp AFF (All Flash FAS) es una línea de productos de cabinas de almacenamiento all-flash. Se ha diseñado para ofrecer soluciones de almacenamiento de alto rendimiento y baja latencia para cargas de trabajo empresariales. La serie AFF combina las ventajas de la tecnología flash con las capacidades de gestión de datos de NetApp, por lo que proporciona a las organizaciones una plataforma de almacenamiento potente y eficiente.

La gama AFF está compuesta por los modelos A-Series y C-Series.

Las cabinas flash all-NVMe NetApp A-Series están diseñadas para cargas de trabajo de alto rendimiento, con una latencia ultrabaja y una alta resiliencia, lo que las convierte en adecuadas para aplicaciones de misión crítica.

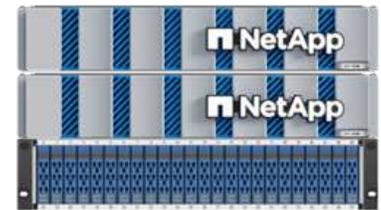
AFF A70



AFF A90



AFF A1K



Las cabinas flash QLC de C-Series se dirigen a casos de uso de mayor capacidad, y ofrecen la velocidad de la tecnología flash con la economía del flash híbrido.

AFF C250



AFF C400



AFF C800



Compatibilidad con protocolos de almacenamiento

Los AFF admiten todos los protocolos estándar utilizados para la virtualización, tanto almacenes de datos como almacenamiento conectado mediante invitado, como NFS, SMB, iSCSI, Fibre Channel (FC), Fibre Channel sobre Ethernet (FCoE), NVME over Fabrics y S3. Los clientes pueden elegir libremente qué funciona mejor para sus cargas de trabajo y aplicaciones.

NFS - NetApp AFF proporciona soporte para NFS, lo que permite el acceso basado en archivos de los almacenes de datos de VMware. Los almacenes de datos conectados a NFS de muchos hosts ESXi superan con creces los límites impuestos en los sistemas de archivos VMFS. El uso de NFS con vSphere proporciona algunas ventajas de facilidad de uso y visibilidad de la eficiencia del almacenamiento. ONTAP incluye funciones de acceso a archivos disponibles para el protocolo NFS. Puede habilitar un servidor NFS y exportar volúmenes o qtrees.

Para obtener una guía de diseño sobre configuraciones NFS, consulte ["Documentación sobre la gestión de almacenamiento de NAS"](#) la .

iSCSI - NetApp AFF proporciona una sólida compatibilidad con iSCSI, lo que permite el acceso a nivel de bloque a dispositivos de almacenamiento a través de redes IP. Ofrece una integración perfecta con iniciadores iSCSI, lo que permite aprovisionar y gestionar LUN iSCSI de manera eficaz. Funciones avanzadas de ONTAP, como rutas múltiples, autenticación CHAP y compatibilidad con ALUA.

Para obtener directrices de diseño sobre configuraciones de iSCSI, consulte la ["Documentación de referencia de configuración de SAN"](#).

Canal de fibra - NetApp AFF ofrece soporte integral para el canal de fibra (FC), una tecnología de red de alta velocidad comúnmente utilizada en redes de área de almacenamiento (SAN). ONTAP se integra sin problemas con la infraestructura de FC y proporciona un acceso por bloques fiable y eficiente a los dispositivos de almacenamiento. Ofrece funciones como la división en zonas, las rutas múltiples y el inicio de sesión estructural (FLOGI) para optimizar el rendimiento, mejorar la seguridad y garantizar una conectividad perfecta en entornos FC.

Para obtener una guía de diseño sobre configuraciones de Fibre Channel, consulte la ["Documentación de referencia de configuración de SAN"](#).

NVMe over Fabrics - NetApp ONTAP soporta NVMe over Fabrics. NVMe/FC permite utilizar dispositivos de almacenamiento NVMe sobre infraestructura Fibre Channel y NVMe/TCP sobre redes IP de almacenamiento.

Para obtener directrices de diseño en NVMe, consulte ["Configuración, compatibilidad y limitaciones de NVMe"](#).

Tecnología activo-activo

Las cabinas all-flash NetApp permiten rutas activo-activo que pasan por ambas controladoras, lo que elimina la necesidad de que el sistema operativo del host espere a que se produzca un error en una ruta activa antes de activar la ruta alternativa. Esto significa que el host puede utilizar todas las rutas disponibles en todas las controladoras, asegurando que las rutas activas siempre estén presentes sin importar si el sistema está en estado constante o si se debe someter a una operación de conmutación por error de la controladora.

Para obtener más información, consulte ["Protección de datos y recuperación ante desastres"](#) la documentación.

Garantías de almacenamiento

NetApp ofrece un conjunto único de garantías de almacenamiento con cabinas All-Flash NetApp. Sus ventajas únicas incluyen:

- **Garantía de eficiencia de almacenamiento:** * Consiga un alto rendimiento al tiempo que minimiza el costo de almacenamiento con la Garantía de Eficiencia de Almacenamiento. 4:1 para cargas de trabajo SAN.
Garantía de recuperación de ransomware: Recuperación de datos garantizada en caso de un ataque de ransomware.

Para obtener información detallada, consulte la ["Página de destino de NetApp AFF"](#).

Herramientas de ONTAP de NetApp para VMware vSphere

Un potente componente de vCenter es la capacidad de integrar complementos o extensiones que mejoran aún más su funcionalidad y proporcionan funciones y funcionalidades adicionales. Estos complementos amplían las funcionalidades de gestión de vCenter y permiten a los administradores integrar soluciones, herramientas y servicios de 3rd partes en su entorno vSphere.

Herramientas de NetApp ONTAP para VMware es una completa suite de herramientas diseñada para facilitar la gestión del ciclo de vida de las máquinas virtuales en entornos VMware a través de su arquitectura de complemento de vCenter. Estas herramientas se integran sin problemas con el ecosistema de VMware, lo que permite un aprovisionamiento eficiente de almacenes de datos y ofrece una protección esencial para las máquinas virtuales. Con las herramientas de ONTAP para VMware vSphere, los administradores pueden gestionar sin esfuerzo las tareas de gestión del ciclo de vida del almacenamiento.

Se pueden encontrar recursos exhaustivos de ONTAP Tools 10 ["Recursos de documentación de las herramientas de ONTAP para VMware vSphere"](#) .

Consulte la solución de implementación de las herramientas de ONTAP 10 en ["Utilice las herramientas de ONTAP 10 para configurar almacenes de datos NFS para vSphere 8"](#)

Plugin NFS de NetApp para VAAI de VMware

El complemento NFS de NetApp para VAAI (API de vStorage para integración de cabinas) mejora las operaciones de almacenamiento al descargar ciertas tareas en el sistema de almacenamiento de NetApp, lo que se traduce en una mejora del rendimiento y la eficiencia. Esto incluye operaciones como la copia completa, la puesta a cero de bloques y el bloqueo asistido por hardware. Además, el complemento VAAI optimiza el uso del almacenamiento reduciendo la cantidad de datos transferidos a través de la red durante las operaciones de aprovisionamiento y clonado de máquinas virtuales.

El plugin de NetApp NFS para VAAI puede descargarse del sitio de soporte de NetApp y se carga e instala en hosts ESXi mediante las herramientas ONTAP para VMware vSphere.

Consulte ["Plugin NFS de NetApp para documentación de VAAI de VMware"](#) si desea obtener más información.

Plugin de SnapCenter para VMware vSphere

El plugin de SnapCenter para VMware vSphere (SCV) es una solución de software de NetApp que ofrece una protección de datos completa para entornos VMware vSphere. Está diseñado para simplificar y agilizar el proceso de protección y gestión de máquinas virtuales y almacenes de datos. SCV utiliza almacenamiento Snapshot y replicación a cabinas secundarias para cumplir objetivos de tiempo de recuperación reducidos.

El plugin de SnapCenter para VMware vSphere ofrece las siguientes funcionalidades en una interfaz unificada, integrada con el cliente de vSphere:

Instantáneas basadas en políticas - SnapCenter le permite definir políticas para crear y administrar instantáneas consistentes con aplicaciones de máquinas virtuales (VM) en VMware vSphere.

- Automatización * - La creación y gestión automatizada de instantáneas basadas en políticas definidas ayudan a garantizar una protección de datos consistente y eficiente.

VM-Level Protection - La protección granular a nivel de VM permite una gestión y recuperación eficientes de máquinas virtuales individuales.

- Características de eficiencia del almacenamiento * - La integración con las tecnologías de almacenamiento de NetApp proporciona funciones de eficiencia del almacenamiento como deduplicación y compresión para instantáneas, minimizando los requisitos de almacenamiento.

El complemento de SnapCenter orquesta el modo inactivo de máquinas virtuales junto con los snapshots basados en hardware en las cabinas de almacenamiento de NetApp. La tecnología SnapMirror se utiliza para replicar copias de backups en sistemas de almacenamiento secundarios, incluso en el cloud.

Para obtener más información, consulte ["Documentación del plugin de SnapCenter para VMware vSphere"](#).

La integración de BlueXP habilita estrategias de backup de 3-2-1 que amplían las copias de datos en el almacenamiento de objetos en el cloud.

Para obtener más información sobre estrategias de backup 3-2-1 con BlueXP, visita ["3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales"](#).

Para obtener instrucciones de implementación paso a paso para el complemento SnapCenter, consulte la solución ["Utilice el complemento de SnapCenter para VMware vSphere para proteger las máquinas virtuales en los dominios de carga de trabajo de VCF"](#).

Consideraciones sobre el almacenamiento

El aprovechamiento de los almacenes de datos NFS de ONTAP con VMware vSphere se traduce en un entorno escalable, de alto rendimiento que proporciona un ratio de VM a almacén de datos inalcanzable con protocolos de almacenamiento basados en bloques. Esta arquitectura puede dar como resultado un aumento diez veces mayor de la densidad de los almacenes de datos, acompañado de la correspondiente reducción del número de almacenes de datos.

NConnect para NFS: Otra ventaja de usar NFS es la capacidad de aprovechar la función **nConnect**. nConnect permite múltiples conexiones TCP para volúmenes de almacenes de datos NFS v3, logrando así un mayor rendimiento. Esto ayuda a aumentar el paralelismo y para almacenes de datos NFS. Los clientes que implementen almacenes de datos con NFS versión 3 pueden aumentar el número de conexiones al servidor NFS, lo que maximiza el uso de tarjetas de interfaz de red de alta velocidad.

Para obtener información detallada sobre nConnect, consulte ["Función nConnect de NFS con VMware y NetApp"](#).

Troncalización de sesión para NFS: A partir de ONTAP 9.14.1, los clientes que usan NFSv4.1 pueden aprovechar el troncalización de sesión para establecer múltiples conexiones a varias LIF en el servidor NFS. Esto permite una transferencia de datos más rápida y mejora la resiliencia mediante el uso de múltiples rutas. La conexión de enlaces resulta especialmente ventajosa cuando se exportan volúmenes de FlexVol a clientes que admiten conexiones de enlaces, como clientes VMware y Linux, o cuando se utiliza NFS a través de protocolos RDMA, TCP o pNFS.

Consulte ["Descripción general de trunking NFS"](#) si desea obtener más información.

FlexVol Volumes: NetApp recomienda usar volúmenes **FlexVol** para la mayoría de los almacenes de datos NFS. Si bien los almacenes de datos de mayor tamaño pueden mejorar la eficiencia del almacenamiento y las ventajas operativas, es recomendable considerar la posibilidad de utilizar al menos cuatro almacenes de datos (volúmenes FlexVol) para almacenar equipos virtuales en una sola controladora ONTAP. Normalmente, los administradores ponen en marcha almacenes de datos respaldados por volúmenes FlexVol con capacidades que van de 4TB TB a 8TB TB. Este tamaño produce un buen equilibrio entre rendimiento, facilidad de gestión y protección de datos. Los administradores pueden empezar con poco y escalar el almacén de datos según sea necesario (hasta un máximo de 100TB PB). Los almacenes de datos más pequeños facilitan una recuperación de backups o desastres más rápida y se pueden mover rápidamente por el clúster. Este enfoque permite el máximo rendimiento utilizado de los recursos de hardware y habilita almacenes de datos con diferentes políticas de recuperación.

Volúmenes FlexGroup: Para los escenarios que requieren un almacén de datos grande, NetApp recomienda el uso de volúmenes **FlexGroup**. Los volúmenes FlexGroup no cuentan prácticamente con limitaciones de capacidad ni de recuento de archivos, lo que permite a los administradores aprovisionar fácilmente un único espacio de nombres masivo. El uso de volúmenes de FlexGroup no implica una sobrecarga adicional de gestión o mantenimiento. No es necesario disponer de varios almacenes de datos para el rendimiento con volúmenes de FlexGroup, ya que se escalan de forma inherente. Al utilizar ONTAP y FlexGroup Volumes con

VMware vSphere, puede establecer almacenes de datos sencillos y escalables que aprovechen toda la potencia de todo el clúster de ONTAP.

Protección contra ransomware

El software para la gestión de datos de NetApp ONTAP incluye una amplia suite de tecnologías integradas que te ayudan a proteger, detectar y recuperar tras ataques de ransomware. La función NetApp SnapLock Compliance integrada en ONTAP evita la eliminación de datos almacenados en un volumen habilitado mediante la tecnología WORM (escritura única, lectura múltiple) con retención avanzada de datos. Una vez establecido el período de retención y que la copia de Snapshot se bloquea, ni siquiera un administrador de almacenamiento con una Privileges completa del sistema o un miembro del equipo de soporte de NetApp puede eliminar la copia de Snapshot. Sin embargo, lo que es más importante, un hacker con credenciales comprometidas no puede eliminar los datos.

NetApp garantiza que podremos recuperar sus copias NetApp® Snapshot™ protegidas en matrices elegibles, y si no podemos, compensaremos a su organización.

Más información sobre la garantía de recuperación de ransomware, consulte: ["Garantía de recuperación de Ransomware"](#).

Consulte el ["Información general sobre la protección de ransomware autónoma"](#) para obtener más información en profundidad.

Consulte la solución completa en el centro de documentación de NetApps Solutions: ["Protección autónoma frente al ransomware para almacenamiento NFS"](#)

Consideraciones sobre la recuperación ante desastres

NetApp proporciona el almacenamiento más seguro del planeta. NetApp puede ayudar a proteger la infraestructura de aplicaciones y datos, mover datos entre el almacenamiento on-premises y el cloud, y ayudar a garantizar la disponibilidad de datos entre clouds. ONTAP incorpora potentes tecnologías de seguridad y protección de datos que ayudan a proteger a los clientes ante desastres detectando amenazas de forma proactiva y recuperando rápidamente datos y aplicaciones.

VMware Live Site Recovery, anteriormente conocido como VMware Site Recovery Manager, ofrece una automatización optimizada y basada en políticas para proteger las máquinas virtuales dentro del cliente web vSphere. Esta solución aprovecha las tecnologías avanzadas de gestión de datos de NetApp a través del adaptador de replicación de almacenamiento como parte de las herramientas de ONTAP para VMware. Al aprovechar las funcionalidades de NetApp SnapMirror para la replicación basada en cabinas, los entornos de VMware pueden beneficiarse de una de las tecnologías más fiables y maduras de ONTAP. SnapMirror garantiza transferencias de datos seguras y muy eficientes ya que copia solo los bloques del sistema de archivos modificados, en vez de máquinas virtuales o almacenes de datos completos. Además, estos bloques aprovechan técnicas de ahorro de espacio como la deduplicación, la compresión y la compactación. Con la introducción de SnapMirror independiente de las versiones en sistemas ONTAP modernos, obtiene flexibilidad a la hora de seleccionar los clústeres de origen y destino. SnapMirror se ha convertido realmente en una potente herramienta para la recuperación ante desastres y, en combinación con la recuperación del sitio activo, ofrece una mayor escalabilidad, rendimiento y ahorros en costes en comparación con las alternativas de almacenamiento local.

Para obtener más información, consulte el ["Descripción general de Site Recovery Manager de VMware"](#).

Consulte la solución completa en el centro de documentación de NetApps Solutions: ["Protección autónoma frente al ransomware para almacenamiento NFS"](#)

BlueXP DRaaS (Recuperación ante desastres como servicio) para NFS es una solución de recuperación ante

desastres rentable diseñada para cargas de trabajo de VMware que se ejecutan en sistemas ONTAP locales con almacenes de datos NFS. Aprovecha la replicación de NetApp SnapMirror para protegerte contra las interrupciones del sitio y los eventos de corrupción de datos, como los ataques de ransomware. Integrado con la consola de NetApp BlueXP, este servicio permite una identificación automatizada y de gestión sencilla del almacenamiento de ONTAP y los vCenter de VMware. Las organizaciones pueden crear y probar planes de recuperación de desastres y lograr un objetivo de punto de recuperación (RPO) de hasta 5 minutos mediante la replicación en el nivel de bloque. DRaaS de BlueXP utiliza la tecnología FlexClone de ONTAP para realizar pruebas con ahorro de espacio sin afectar a los recursos de producción. El servicio orquesta los procesos de conmutación al nodo de respaldo y conmutación de retorno tras recuperación, lo que permite que las máquinas virtuales protegidas se pongan en marcha en el sitio de recuperación ante desastres designado con un esfuerzo mínimo. Frente a otras alternativas conocidas, DRaaS de BlueXP ofrece estas funciones por una fracción del coste, lo que lo convierte en una solución eficiente para que las organizaciones configuren, prueben y ejecuten operaciones de recuperación ante desastres para sus entornos VMware mediante los sistemas de almacenamiento ONTAP.

Consulte la solución completa en el centro de documentación de NetApps Solutions: ["Recuperación ante desastres mediante DRaaS de BlueXP para almacenes de datos NFS"](#)

Descripción general de soluciones

Soluciones cubiertas en esta documentación:

- **Función nConnect NFS con NetApp y VMware.** Haga clic en ["aquí"](#) para ver los pasos de despliegue.
 - **Utilice las herramientas de ONTAP 10 para configurar almacenes de datos NFS para vSphere 8.** Haga clic en ["aquí"](#) para ver los pasos de despliegue.
 - * Implementar y utilizar el complemento SnapCenter para VMware vSphere para proteger y restaurar máquinas virtuales*. Haga clic en ["aquí"](#) para ver los pasos de despliegue.
 - **Recuperación ante desastres de almacenes de datos NFS con VMware Site Recovery Manager.** Haga clic en ["aquí"](#) para ver los pasos de despliegue.
 - **Protección autónoma contra ransomware para almacenamiento NFS.** Haga clic en ["aquí"](#) para ver los pasos de despliegue.

La función nConnect de NFS con NetApp y VMware

A partir de VMware vSphere 8,0 U1 (como vista previa técnica), la función nconnect permite múltiples conexiones TCP para los volúmenes de almacenes de datos de NFS v3 para lograr un mayor rendimiento. Los clientes que utilizan un almacén de datos NFS ahora pueden aumentar el número de conexiones al servidor NFS, lo que maximiza el uso de las tarjetas de interfaz de red de alta velocidad.



La función está disponible generalmente para NFS v3 con 8,0 U2, consulte la sección de almacenamiento en ["Notas de la versión de VMware vSphere 8,0 Update 2"](#). Se ha añadido compatibilidad con NFS v4,1 con vSphere 8,0 U3. Para obtener más información, compruebe ["Notas de la versión de vSphere 8,0 Update 3"](#)

Casos de uso

- Alojamiento de más equipos virtuales por almacén de datos NFS en el mismo host.
- Impulso del rendimiento de los almacenes de datos NFS.
- Proporcione una opción para ofrecer servicio en un nivel más alto para aplicaciones basadas en

contenedores y máquinas virtuales.

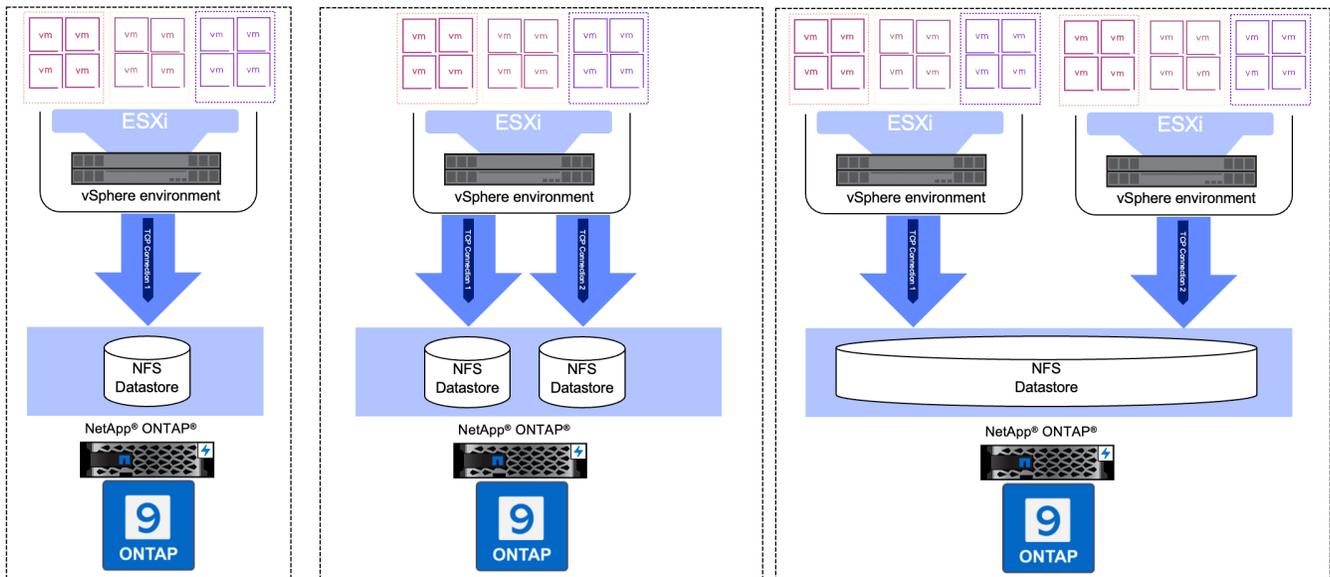
Detalles técnicos

El objetivo de nconnect es proporcionar varias conexiones TCP por almacén de datos NFS en un host de vSphere. Esto ayuda a aumentar el paralelismo y el rendimiento de almacenes de datos NFS. En ONTAP, cuando se establece un montaje NFS, se crea un ID de conexión (CID). Ese CID proporciona hasta 128 operaciones simultáneas en vuelo. Cuando el cliente supera ese número, ONTAP aplica un control de flujo hasta que libera algunos recursos disponibles a medida que se completan otras operaciones. Estas pausas suelen ser solo unos pocos microsegundos, pero al transcurso de millones de operaciones, estas pueden sumar y crear problemas de rendimiento. NConnect puede tomar el límite de 128 y multiplicarlo por el número de sesiones nconnect en el cliente, lo que proporciona más operaciones simultáneas por CID y puede potencialmente agregar beneficios de rendimiento. Para obtener más información, consulte ["Prácticas recomendadas y guía de implementación de NFS"](#)

Almacén de datos NFS predeterminado

Para solucionar las limitaciones de rendimiento de la conexión única de los almacenes de datos NFS, se montan almacenes de datos adicionales o se añaden hosts adicionales para aumentar la conexión.

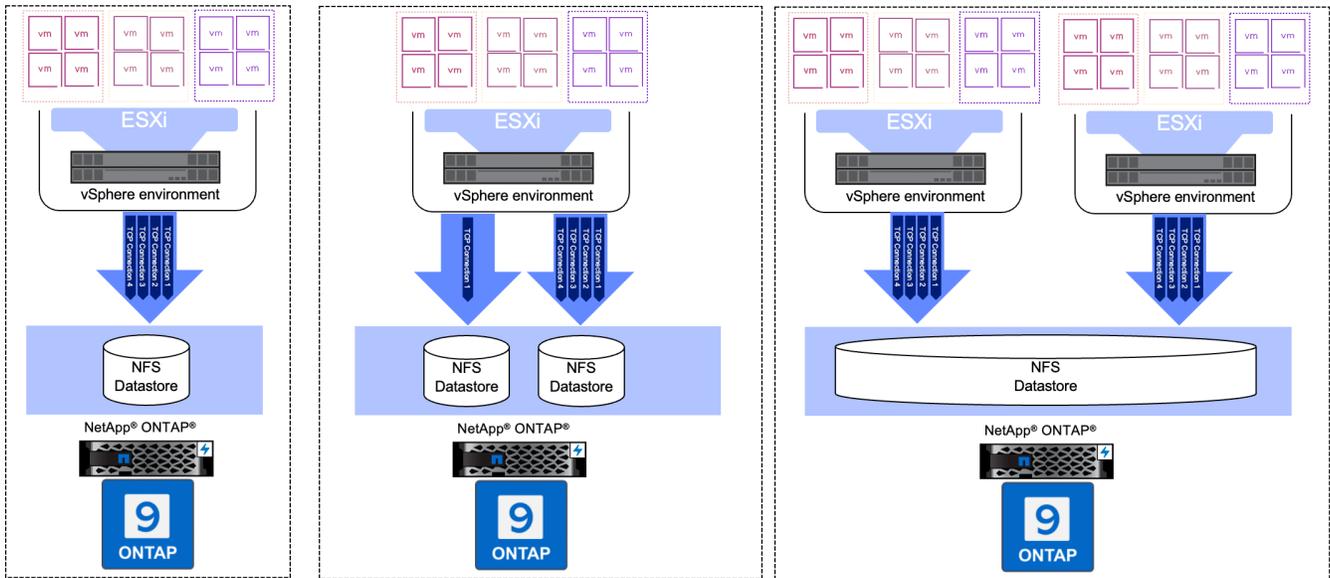
Without nConnect feature with NetApp and VMware



Con almacén de datos nConnect NFS

Una vez creado el almacén de datos NFS con las Herramientas de ONTAP o con otras opciones, el número de conexión por almacén de datos NFS se puede modificar usando la CLI de vSphere, PowerCLI, govc tool u otras opciones de API. Para evitar problemas de rendimiento junto con vMotion, conserve el número de conexiones del almacén de datos NFS en todos los hosts de vSphere que forman parte del clúster de vSphere.

With nConnect feature with NetApp and VMware



Requisito previo

Para utilizar la función nconnect, se deben cumplir las siguientes dependencias.

Versión de ONTAP	Versión de vSphere	Comentarios
9,8 o superior	8 Actualización 1	Vista previa técnica con opción para aumentar el número de conexiones.
9,8 o superior	8 Actualización 2	Generalmente disponible con la opción de aumentar y disminuir el número de conexiones.
9,8 o superior	8 Actualización 3	NFS 4,1 y soporte multivía.

Actualizar el número de conexión al almacén de datos NFS

Cuando se crea un almacén de datos NFS con herramientas de ONTAP o con vCenter, se usa una sola conexión TCP. Para aumentar el número de conexiones, se puede utilizar la CLI de vSphere. El comando de referencia se muestra a continuación.

```

# Increase the number of connections while creating the NFS v3 datastore.
esxcli storage nfs add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To specify the number of connections while mounting the NFS 4.1
datastore.
esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the number of connections for existing NFSv3
datastore.
esxcli storage nfs param set -v <datastore_name> -c
<number_of_connections>
# For NFSv4.1 datastore
esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# To set VMkernel adapter for an existing NFS 4.1 datastore
esxcli storage nfs41 param set -I <NFS_Server_FQDN_or_IP>:vmk2 -v
<datastore_name> -c <number_of_connections>

```

O utilice PowerCLI similar al que se muestra a continuación

```

$datastoreSys = Get-View (Get-VMHost host01.vsphere.local).ExtensionData
.ConfigManager.DatastoreSystem
$nfSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfSpec.RemoteHost = "nfs_server.ontap.local"
$nfSpec.RemotePath = "/DS01"
$nfSpec.LocalPath = "DS01"
$nfSpec.AccessMode = "readWrite"
$nfSpec.Type = "NFS"
$nfSpec.Connections = 4
$datastoreSys.CreateNasDatastore ($nfSpec)

```

Aquí está el ejemplo de aumentar el número de conexiones con la herramienta govc.

```

$env.GOVc_URL = 'vcenter.vsphere.local'
$env.GOVc_USERNAME = 'administrator@vsphere.local'
$env.GOVc_PASSWORD = 'XXXXXXXXXX'
$env.GOVc_Datastore = 'DS01'
# $env.GOVc_INSECURE = 1
$env.GOVc_HOST = 'host01.vsphere.local'
# Increase number of connections while creating the datastore.
govc host.esxcli storage nfs add -H nfs_server.ontap.local -v DS01 -s
/DS01 -c 2
# For NFS 4.1, replace nfs with nfs41
govc host.esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v
<datastore_name> -s <remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
govc host.esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the connections for existing datastore.
govc host.esxcli storage nfs param set -v DS01 -c 4
# For NFSv4.1 datastore
govc host.esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# View the connection info
govc host.esxcli storage nfs list

```

Consulte ["Artículo de la base de conocimientos de VMware 91497"](#) si quiere más información.

Consideraciones de diseño

El número máximo de conexiones admitidas en ONTAP depende del modelo de plataforma de almacenamiento. Busque `exec_ctx` en ["Prácticas recomendadas y guía de implementación de NFS"](#) si quiere más información.

A medida que se aumenta el número de conexiones por almacén de datos NFSv3, disminuye el número de almacenes de datos NFS que se pueden montar en ese host de vSphere. El número total de conexiones admitidas por host de vSphere es 256. Comprobar ["Artículo de la base de conocimientos de VMware 91481"](#) Para LIF de almacenes de datos por host de vSphere.



El almacén de datos de VVol no admite la función nConnect. Sin embargo, los extremos de protocolo cuentan para el límite de conexión. Se crea un extremo de protocolo para cada LIF de datos de las SVM cuando se crea un almacén de datos de VVol.

Utilice las herramientas de ONTAP 10 para configurar almacenes de datos NFS para vSphere 8

Las herramientas de ONTAP para VMware vSphere 10 cuentan con una arquitectura de última generación que permite una alta disponibilidad y escalabilidad nativas para el proveedor VASA (es compatible con vVols iSCSI y NFS). Esto simplifica la gestión de varios servidores de VMware vCenter y clústeres de ONTAP.

En esta situación, mostraremos cómo poner en marcha y utilizar herramientas de ONTAP para VMware vSphere 10 y cómo configurar un almacén de datos NFS para vSphere 8.

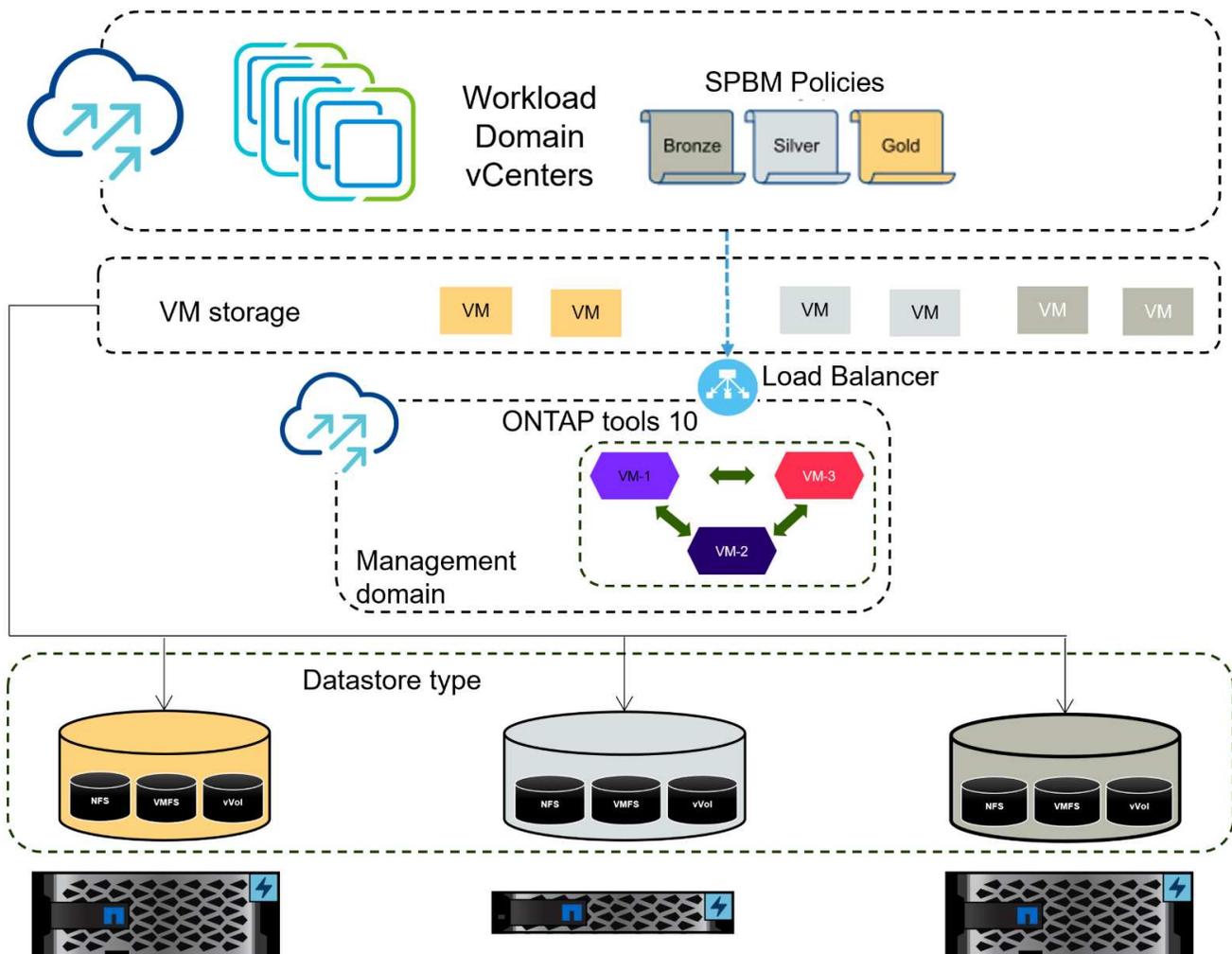
Descripción general de la solución

Este escenario cubre los siguientes pasos de alto nivel:

- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico de NFS.
- Cree un grupo de puertos distribuidos para la red NFS en el clúster de vSphere 8.
- Cree un adaptador vmkernel para NFS en los hosts ESXi del clúster de vSphere 8.
- Ponga en marcha las herramientas de ONTAP 10 y regístrese con el clúster de vSphere 8.
- Cree un nuevo almacén de datos NFS en el clúster de vSphere 8.

Arquitectura

El siguiente diagrama muestra los componentes de la arquitectura de una herramienta de ONTAP para la implementación de VMware vSphere 10.



Requisitos previos

Esta solución requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP AFF con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.
- La puesta en marcha del clúster de vSphere 8 se completó y se puede acceder al cliente de vSphere.
- Se ha descargado la plantilla OVA de las herramientas de ONTAP para VMware vSphere 10 del sitio de soporte de NetApp.

NetApp recomienda diseños de red redundantes para NFS, lo que proporciona tolerancia a fallos para sistemas de almacenamiento, switches, adaptadores de red y sistemas host. Es común poner en marcha NFS con una única subred o varias subredes, en función de los requisitos de la arquitectura.

Consulte "[Prácticas recomendadas para ejecutar NFS con VMware vSphere](#)" Para obtener información detallada específica de VMware vSphere.

Para obtener orientación de red sobre el uso de ONTAP con VMware vSphere, consulte la "[Configuración de red: NFS](#)" De la documentación de aplicaciones empresariales de NetApp.

Se pueden encontrar recursos exhaustivos de ONTAP Tools 10 "[Recursos de documentación de las herramientas de ONTAP para VMware vSphere](#)".

Pasos de despliegue

Para implementar las herramientas de ONTAP 10 y utilizarlo para crear un almacén de datos NFS en el dominio de gestión de VCF, lleve a cabo los siguientes pasos:

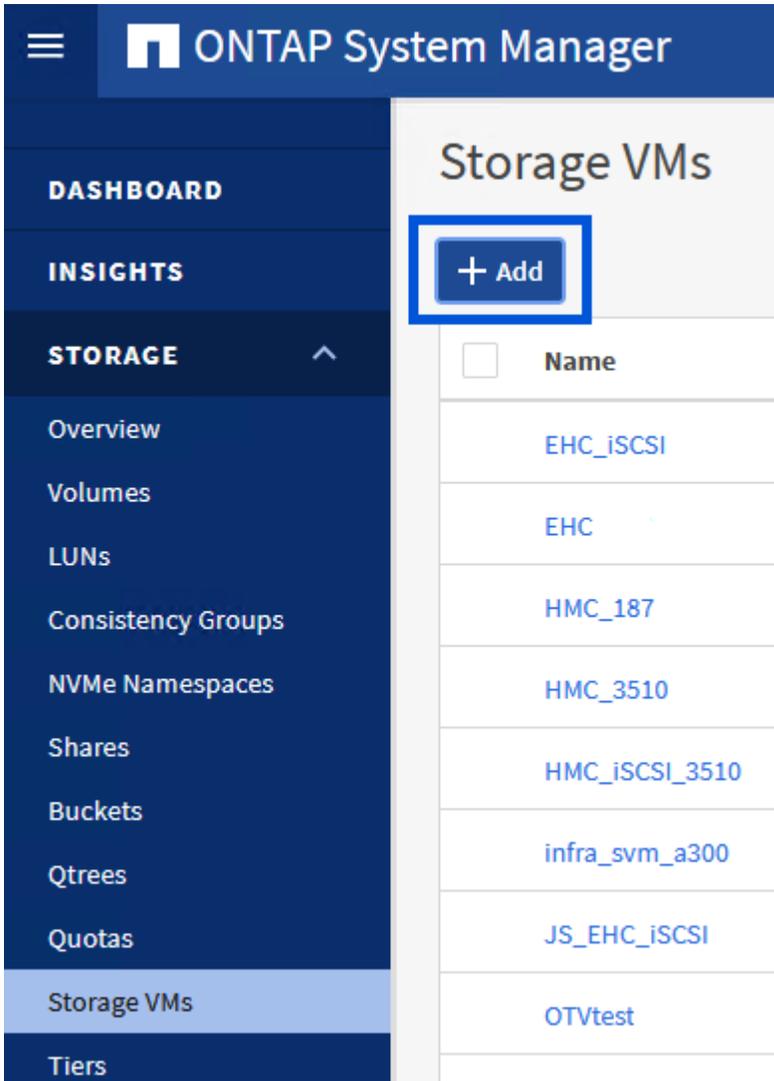
Crear SVM y LIF en el sistema de almacenamiento ONTAP

El siguiente paso se lleva a cabo en ONTAP System Manager.

Crear la máquina virtual de almacenamiento y las LIF

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

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



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

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



No es necesario marcar el botón **Permitir acceso al cliente NFS** aquí, ya que se utilizarán las herramientas de ONTAP para VMware vSphere para automatizar el proceso de implementación del almacén de datos. Esto incluye proporcionar acceso de cliente para los hosts ESXi. Y n.o 160;

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes o utilizar una configuración independiente.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

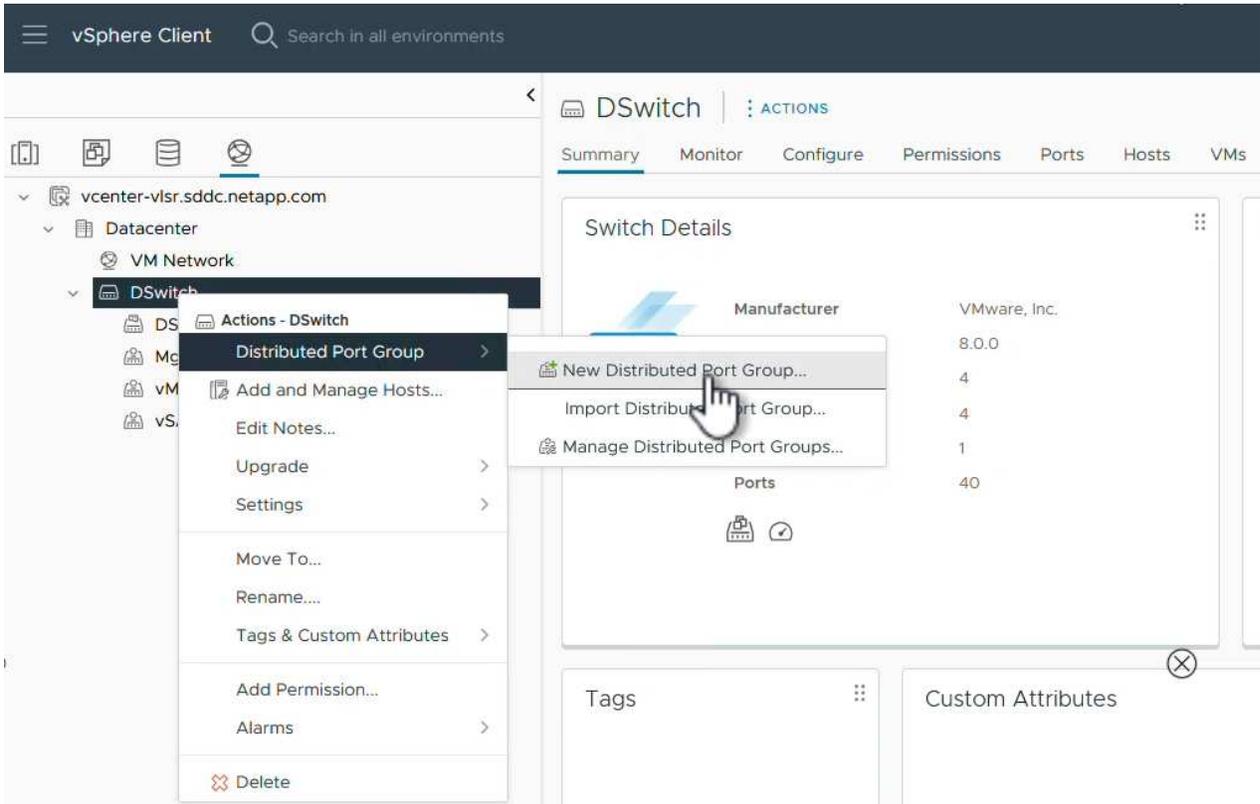
Configure las redes para NFS en los hosts ESXi

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

Cree 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 el tráfico NFS:

1. En el cliente vSphere , desplácese hasta **Inventory > Networking** para el dominio de la carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos....**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

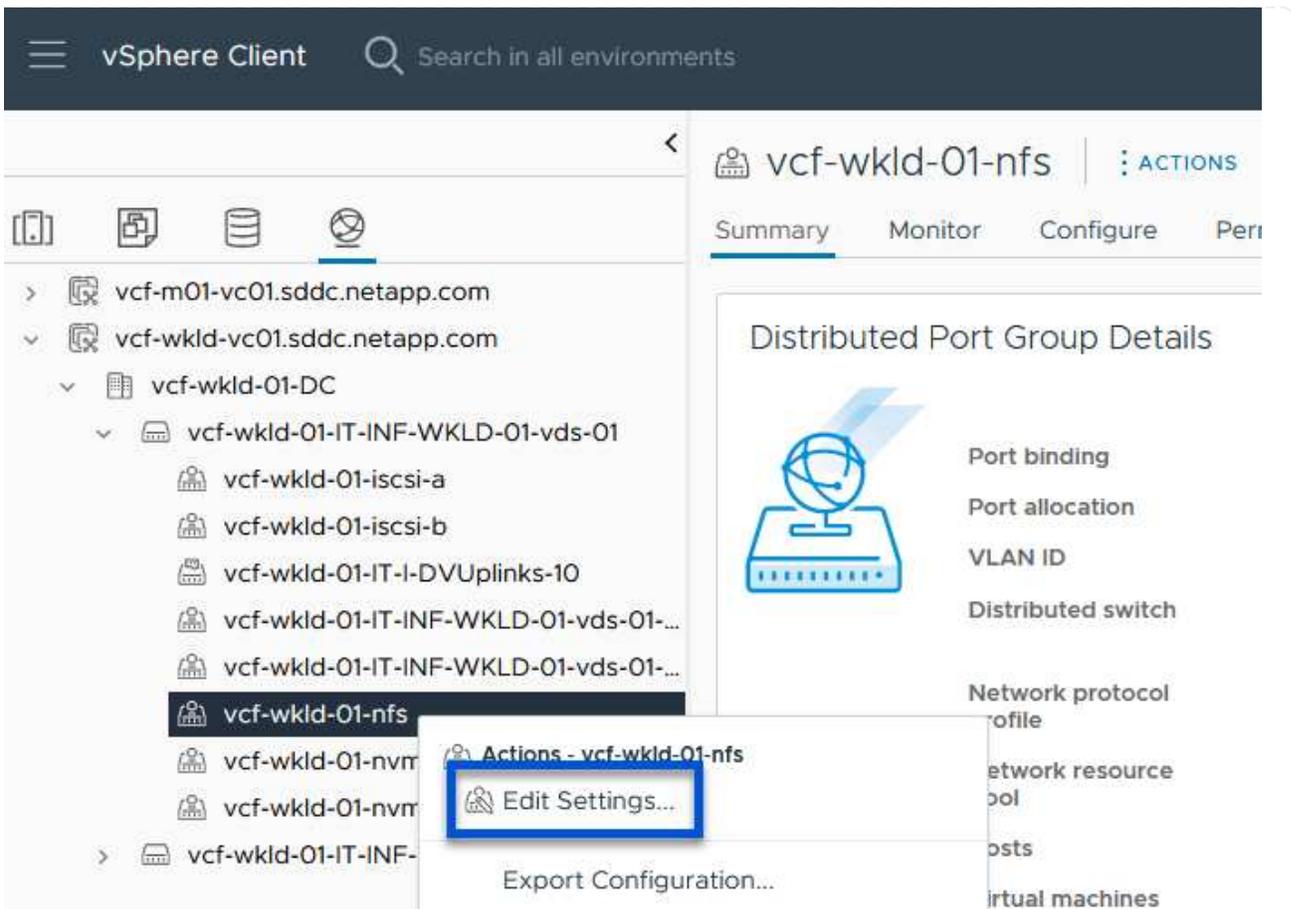
Port binding	Static binding
Port allocation	Elastic ?
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

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 en **Editar configuración....**



6. En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda. Habilite el trabajo en equipo 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 hacia abajo a **Uplinks no utilizados**.

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

Uplink 1

Uplink 2

Standby uplinks

Unused uplinks

CANCEL

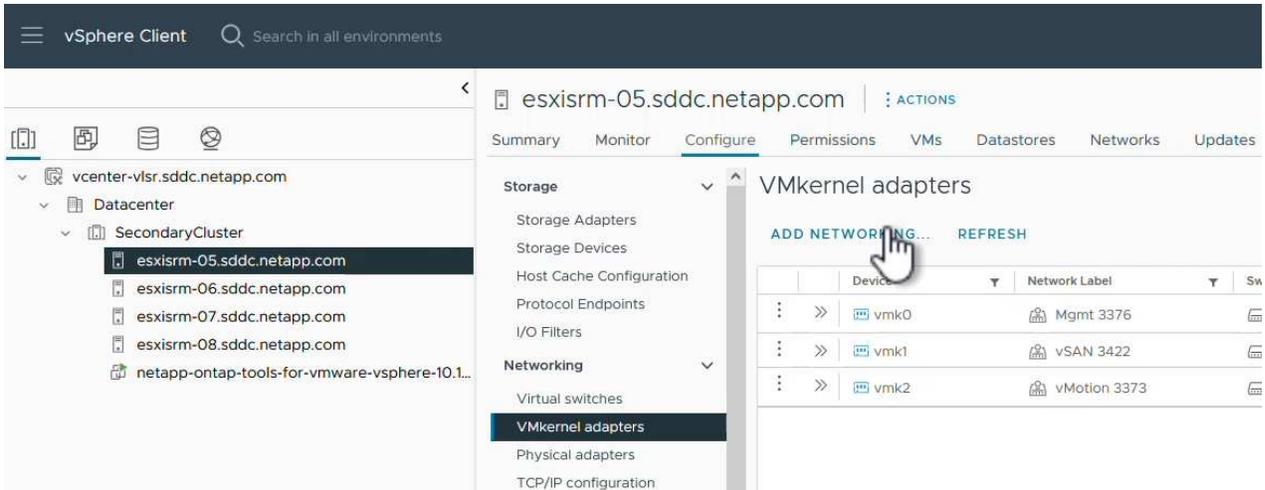
OK

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

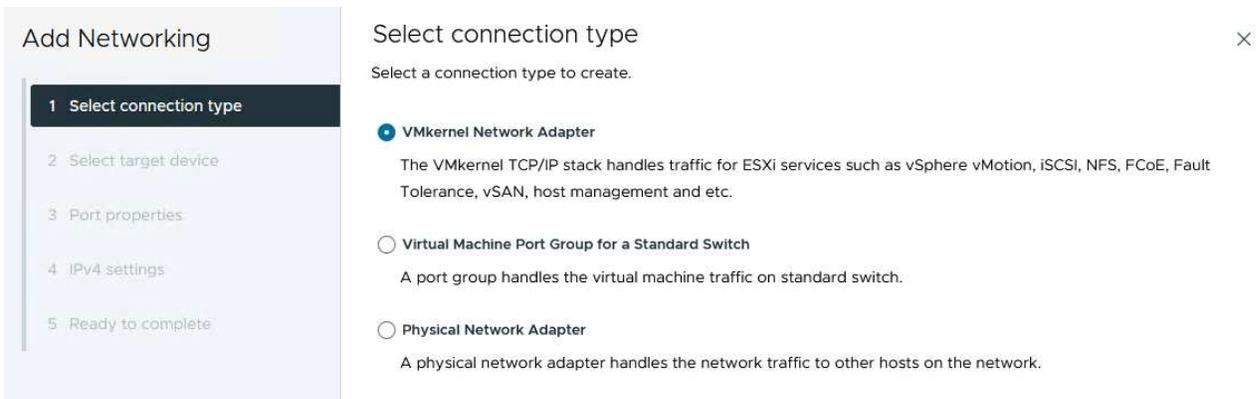
Crear un adaptador de VMkernel en cada host ESXi

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

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de la carga de trabajo. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** 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.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	Mgmt 3376	--	DSwitch
<input checked="" type="radio"/>	NFS 3374	--	DSwitch
<input type="radio"/>	vMotion 3373	--	DSwitch
<input type="radio"/>	vSAN 3422	--	DSwitch

Manage Columns 4 items

CANCEL

BACK

NEXT

4. En la página **Propiedades del puerto**, mantenga los valores predeterminados (no hay servicios habilitados) y haga clic en **Siguiente** para continuar.
5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings**
- 5 Ready to complete

IPv4 settings



Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
- Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

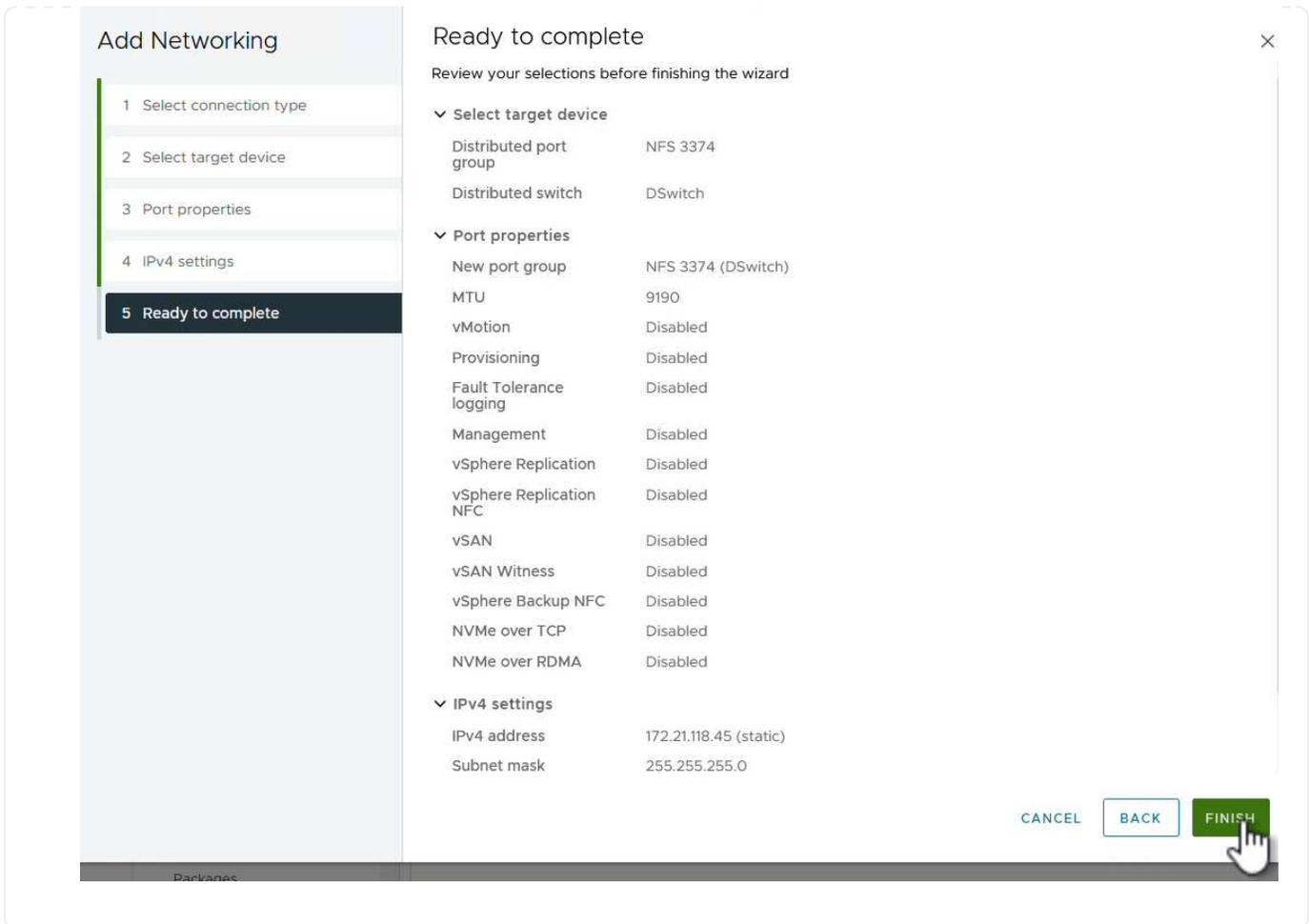
DNS server addresses

CANCEL

BACK

NEXT

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



Implemente y utilice las herramientas de ONTAP 10 para configurar el almacenamiento

Los siguientes pasos se realizan en un clúster de vSphere 8 mediante el cliente de vSphere e implican la puesta en marcha de OTV, la configuración de ONTAP tools Manager y la creación de un almacén de datos vVols NFS.

Para obtener la documentación completa sobre la puesta en marcha y el uso de las herramientas de ONTAP para VMware vSphere 10, consulte "[Ponga en marcha herramientas de ONTAP para VMware vSphere](#)".

Ponga en marcha herramientas de ONTAP para VMware vSphere 10

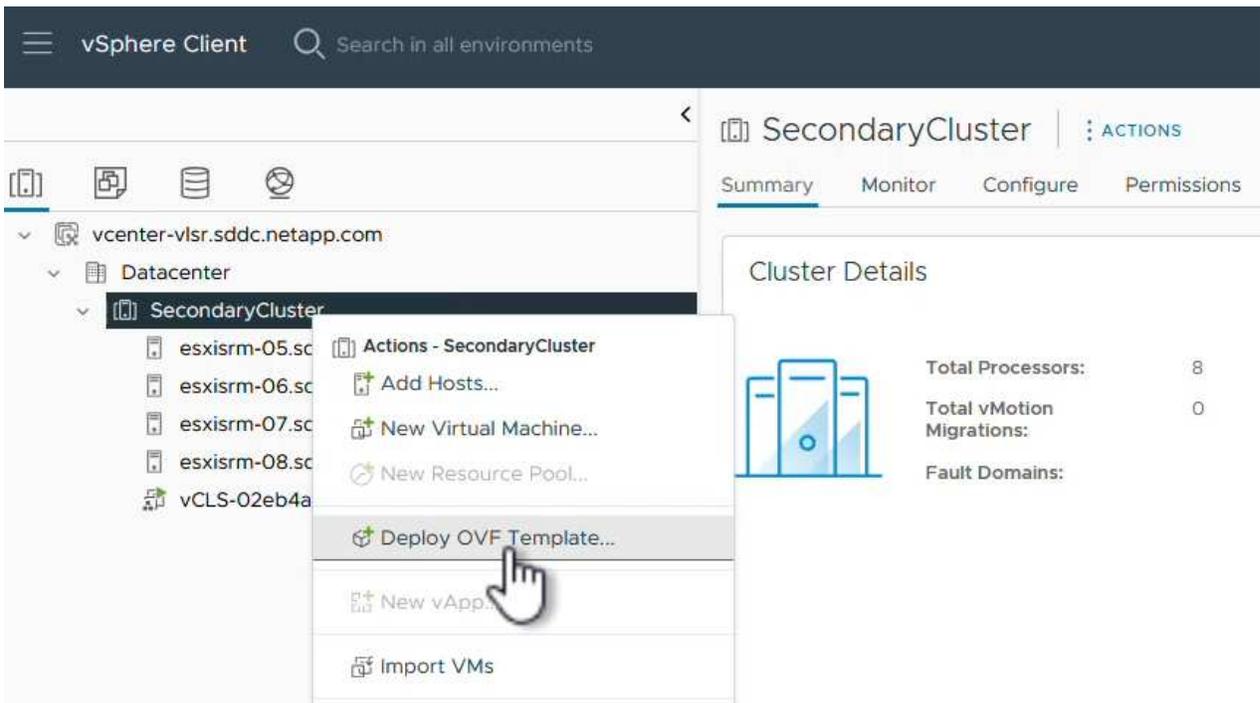
Las herramientas de ONTAP para VMware vSphere 10 se ponen en marcha como dispositivo de máquina virtual y proporcionan una interfaz de usuario integrada de vCenter para gestionar el almacenamiento de ONTAP. Las herramientas de ONTAP 10 cuenta con un nuevo portal de gestión global para gestionar conexiones a varios servidores vCenter y back-ends de almacenamiento de ONTAP.



En un caso de puesta en marcha sin alta disponibilidad, se necesitan tres direcciones IP disponibles. Se asigna una dirección IP para el balanceador de carga, otra para el plano de control de Kubernetes y la restante para el nodo. En una puesta en marcha de alta disponibilidad, son necesarias dos direcciones IP adicionales para el segundo y el tercer nodo, además de los tres iniciales. Antes de la asignación, los nombres de host deben asociarse a las direcciones IP en DNS. Es importante que las cinco direcciones IP estén en la misma VLAN, que se eligió para la implementación.

Complete lo siguiente para poner en marcha herramientas de ONTAP para VMware vSphere:

1. Obtenga la imagen OVA de las herramientas de ONTAP de "[Sitio de soporte de NetApp](#)" y descárguela en una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el clúster de vSphere 8.
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 de **Desplegar plantilla OVF** haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de herramientas ONTAP descargado en el paso anterior.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

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

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 Configuration
- 7 Select storage**
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

VM Storage Policy

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	T
vsanDatastore	--	799.97 GB	26.05 GB	783.98 GB	

Items per page 10 1 Item

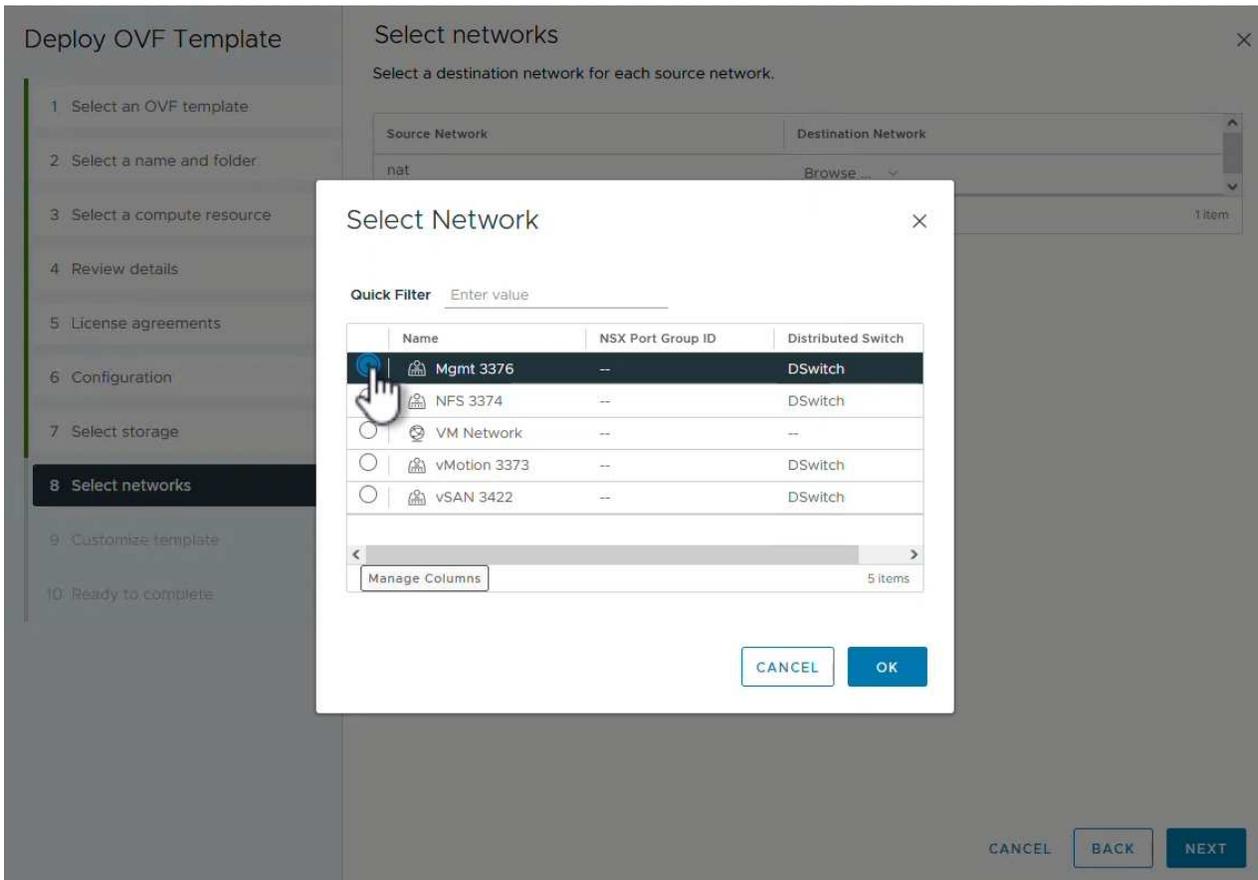
Compatibility

CANCEL

BACK

NEXT

7. En la página Seleccionar red, seleccione la red que se utiliza para el tráfico de gestión.



8. En la página Configuración, seleccione la configuración de despliegue que se va a utilizar. En este escenario se utiliza el método de implementación fácil.



Herramientas de ONTAP 10 tiene múltiples configuraciones de puesta en marcha, incluidas puestas en marcha de alta disponibilidad con múltiples nodos. Para obtener documentación sobre todas las configuraciones de implementación y los requisitos previos, consulte ["Requisitos previos para implementar herramientas de ONTAP para VMware vSphere"](#) .

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 Configuration**
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Configuration

Select a deployment configuration

<input checked="" type="radio"/> Easy deployment (S)	Description Deploy local provisioner Non-HA Small single node instance of ONTAP tools	
<input type="radio"/> Easy deployment (M)		
<input type="radio"/> Advanced deployment (S)		
<input type="radio"/> Advanced deployment (M)		
<input type="radio"/> High-Availability deployment (S)		
<input type="radio"/> High-Availability deployment (M)		
<input type="radio"/> High-Availability deployment (L)		
<input type="radio"/> Recovery		
8 Items		

CANCEL

BACK

NEXT

9. En la página Personalizar plantilla, rellene toda la información necesaria:

- Nombre de usuario de la aplicación que se utilizará para registrar el proveedor VASA y el SRA en vCenter Server.
- Habilite ASUP para obtener soporte automatizado.
- URL de proxy ASUP si es necesario.
- Nombre de usuario y contraseña del administrador.
- Servidores NTP.
- Contraseña de usuario de mantenimiento para acceder a funciones de gestión desde la consola.
- IP de Equilibrador de Carga.
- IP virtual para el plano de control K8s.
- Máquina virtual principal para seleccionar la máquina virtual actual como primaria (para configuraciones de alta disponibilidad).
- Nombre de host de la máquina virtual
- Proporcione los campos de propiedades de red necesarios.

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 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Customize the deployment properties of this software solution.

! 10 properties have invalid values X

System Configuration		8 settings
Application username(*)	Username to assign to the Application	<input type="text" value="vsphere-services"/>
Application password(*)	Password to assign to the Application	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
Enable ASUP	Select this checkbox to enable ASUP	<input checked="" type="checkbox"/>
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.	<input type="text"/>
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '.', ':', '-' special characters are supported	<input type="text"/>
Administrator password(*)	Password to assign to the Administrator	<input type="password"/>

CANCEL BACK NEXT

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 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Maintenance user password(*)	Password to assign to maint user account	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
Deployment Configuration		3 settings
Load balancer IP(*)	Load balancer IP (*)	<input type="text" value="172.21.120.57"/>
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane	<input type="text" value="172.21.120.58"/>
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools.	<input checked="" type="checkbox"/>
Node Configuration		10 settings
HostName(*)	Specify the hostname for the VM	<input type="text"/>
IP Address(*)	Specify the IP address for the appliance	<input type="text"/>
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack.	<input type="text"/>

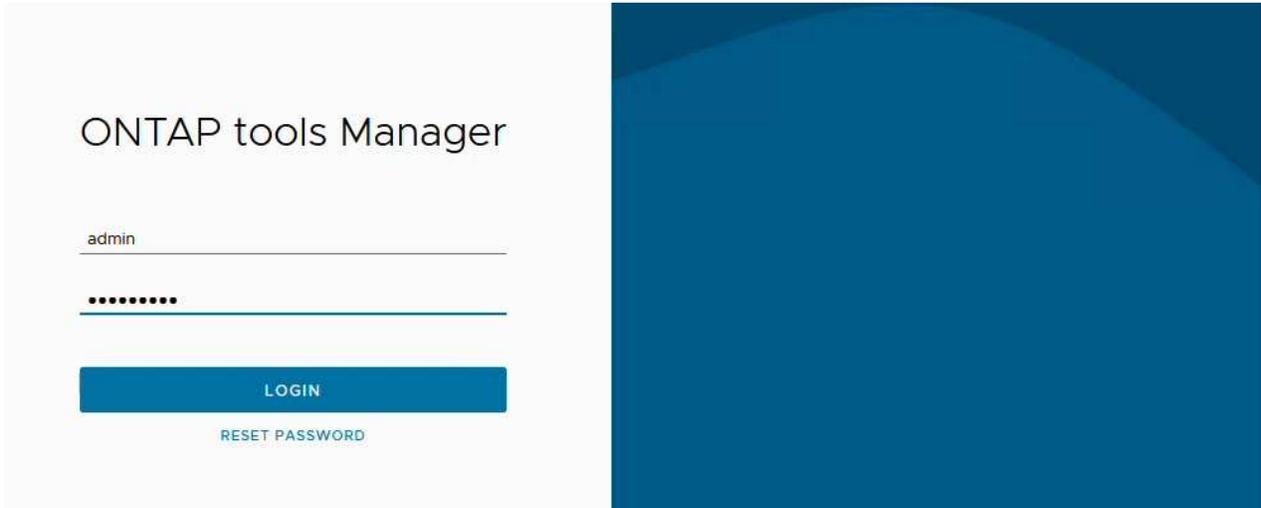
CANCEL BACK NEXT

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

Conecte el backend de almacenamiento y vCenter Server a las herramientas de ONTAP 10.

El gestor de herramientas de ONTAP se utiliza para configurar los ajustes globales de las herramientas de ONTAP 10.

1. Para acceder al administrador de herramientas de ONTAP, vaya a <https://<loadBalanceIP>:8443/virtualization/ui/> en un explorador web e inicie sesión con las credenciales de administración proporcionadas durante la implementación.



2. En la página **Empezar**, haga clic en **Ir a Backends de Almacenamiento**.

Getting Started



ONTAP tools Manager allows you to manage ONTAP Storage Backends and associate them with vCenters. You can also download support log bundles.



Storage Backends

Add, modify, and remove storage backends.

[Go to Storage Backends](#)



vCenters

Add, modify, and remove vCenters and associate storage backends with them.

[Go to vCenters](#)



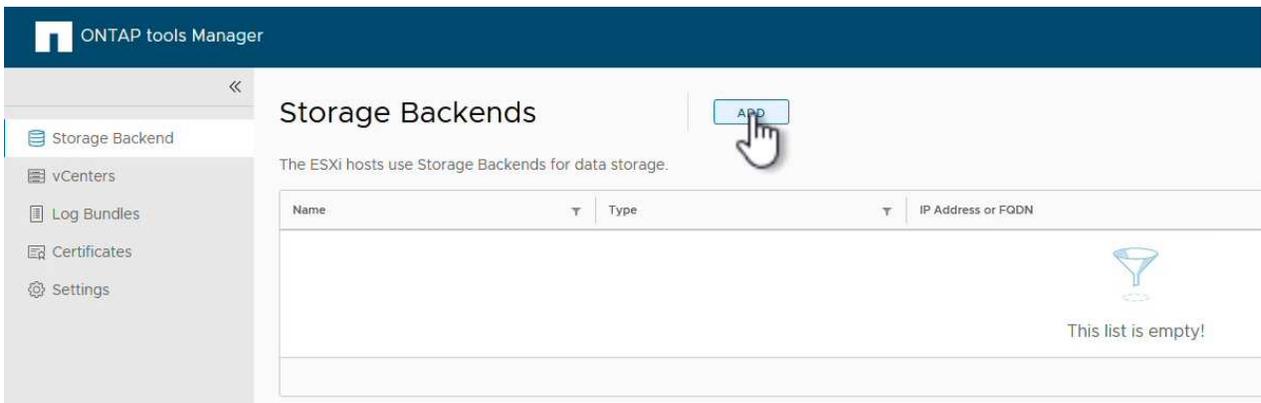
Log Bundles

Generate and download log bundles for support purposes.

[Go to Log Bundles](#)

Don't show again

3. En la página **Backends de almacenamiento**, haga clic en **ADD** para completar las credenciales de un sistema de almacenamiento ONTAP que se registrará con las herramientas de ONTAP 10.



4. En la casilla **Agregar backend de almacenamiento**, rellene las credenciales del sistema de almacenamiento ONTAP.

Add Storage Backend

Hostname: * 172.16.9.25

Username: * admin

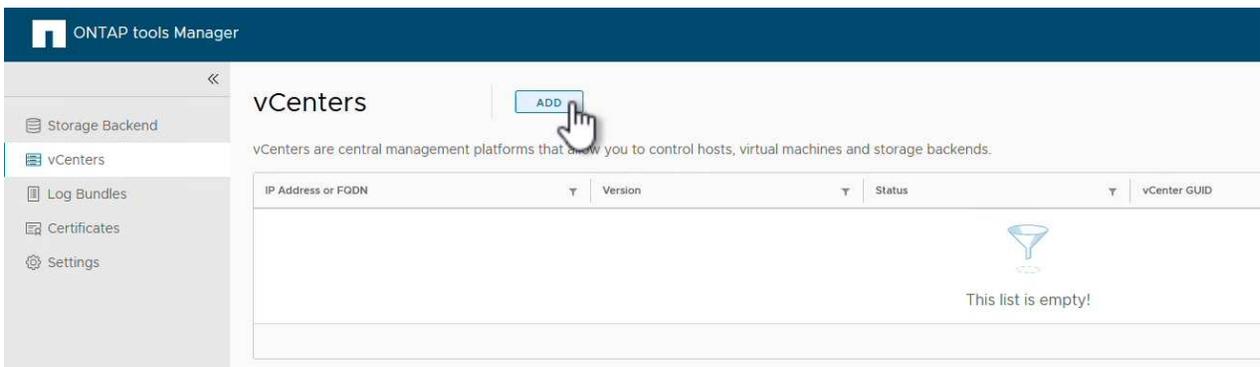
Password: * ●●●●●●●● 

Port: * 443

CANCEL

ADD 

5. En el menú de la izquierda, haga clic en **vCenters**, y luego en **ADD** para completar las credenciales de un servidor de vCenter que se registrará con las herramientas de ONTAP 10.



The screenshot shows the ONTAP tools Manager interface. The top navigation bar is dark blue with the ONTAP logo and the text "ONTAP tools Manager". On the left, there is a sidebar menu with options: Storage Backend, vCenters (highlighted), Log Bundles, Certificates, and Settings. The main content area is titled "vCenters" and contains a description: "vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends." Below the description is a table with columns: IP Address or FQDN, Version, Status, and vCenter GUID. The table is currently empty, with a message "This list is empty!" and a funnel icon in the center. An "ADD" button is visible above the table, with a mouse cursor pointing to it.

6. En la casilla **Agregar vCenter**, rellene las credenciales del sistema de almacenamiento ONTAP.

Add vCenter

Server IP Address or FQDN: *

Username: *

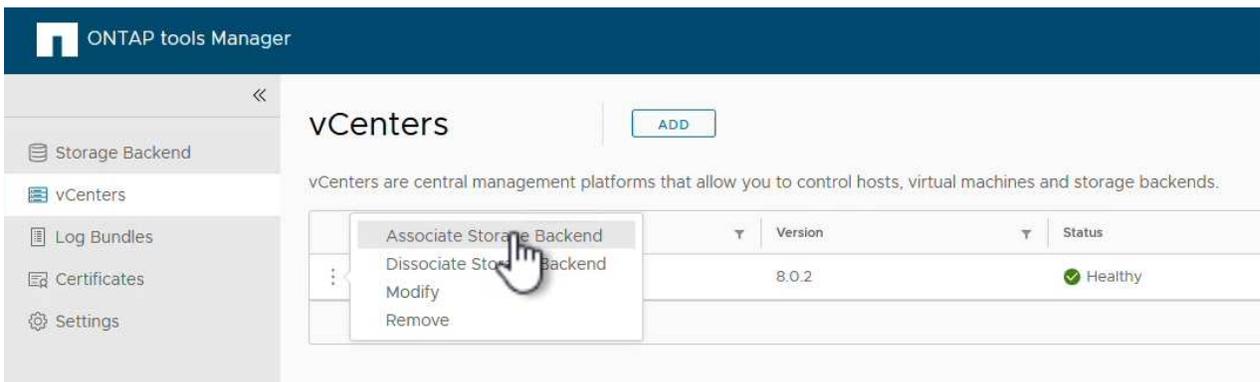
Password: * 

Port: *

CANCEL

ADD 

7. En el menú vertical de tres puntos para el servidor vCenter recién detectado, seleccione **Associate Storage Backend**.



The screenshot shows the ONTAP tools Manager interface. The left sidebar contains a menu with options: Storage Backend, vCenters, Log Bundles, Certificates, and Settings. The main area is titled 'vCenters' and includes an 'ADD' button. Below the title, there is a table with columns for 'Version' and 'Status'. A context menu is open over the first row of the table, showing options: Associate Storage Backend, Dissociate Storage Backend, Modify, and Remove. A hand cursor is pointing at the 'Associate Storage Backend' option.

	Version	Status
	8.0.2	Healthy

8. En el cuadro **Asociar backend de almacenamiento**, seleccione el sistema de almacenamiento ONTAP que se asociará con el servidor vCenter y haga clic en **Asociar** para completar la acción.

Associate Storage Backend

vcenter-vlsr.sddc.netapp.com



Storage Backend

ntaphci-a300e9u25

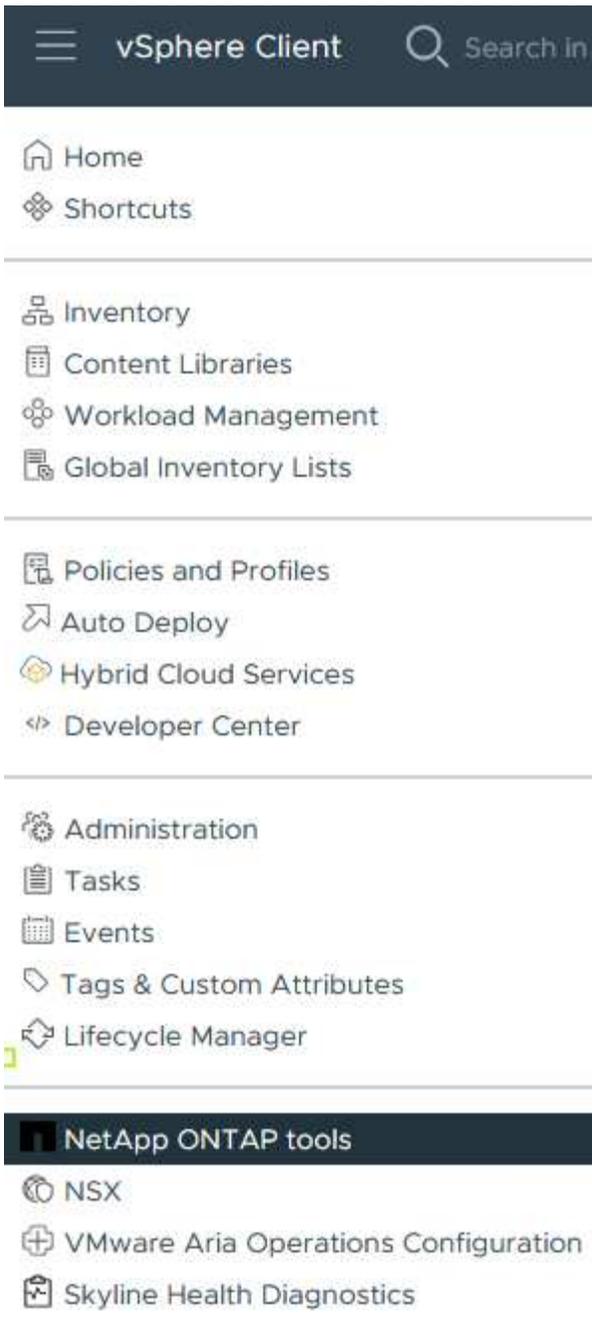


CANCEL

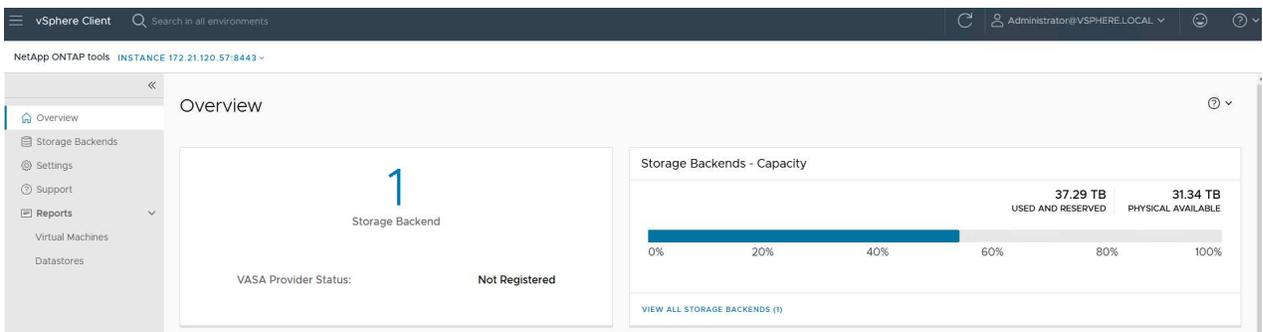
ASSOCIATE



9. Para verificar la instalación, inicie sesión en el cliente vSphere y seleccione **NetApp ONTAP tools** en el menú de la izquierda.



10. En la consola de herramientas de ONTAP, deberá observar que un back-end de almacenamiento está asociado con vCenter Server.

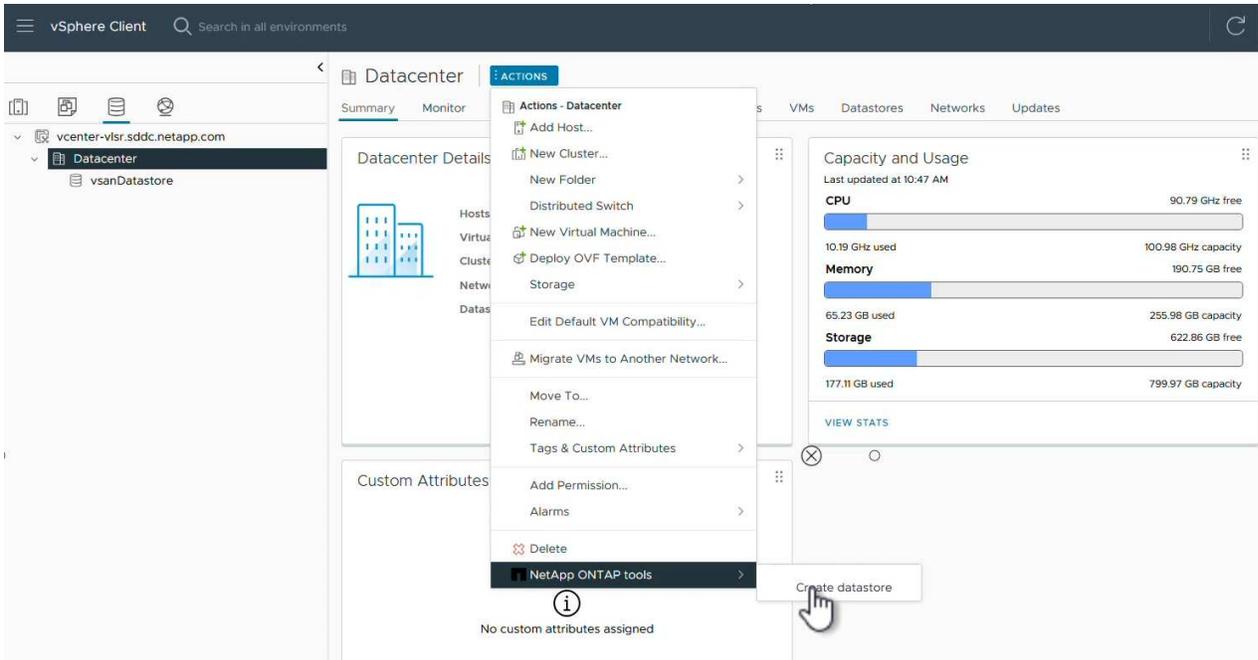




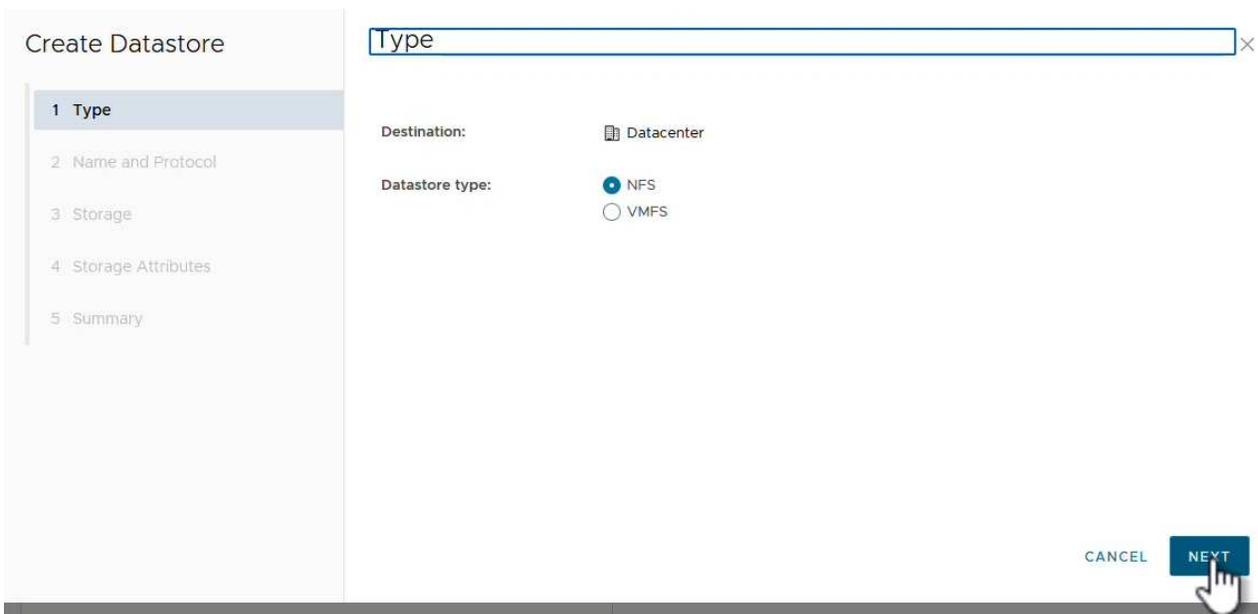
Cree un almacén de datos NFS con las herramientas de ONTAP 10

Complete los siguientes pasos para implementar un almacén de datos de ONTAP, que se ejecute en NFS, con las herramientas de ONTAP 10.

1. En el cliente de vSphere, desplácese hasta el inventario de almacenamiento. En el menú **ACCIONES**, seleccione **Herramientas de NetApp ONTAP > Crear almacén de datos**.



2. En la página **Type** del asistente Create Datastore, haga clic en el botón de opción NFS y luego en **Next** para continuar.



3. En la página **Name and Protocol**, rellene el nombre, el tamaño y el protocolo del almacén de datos. Haga clic en **Siguiente** para continuar.

The screenshot shows the 'Name and Protocol' step of the 'Create Datastore' wizard. On the left, a sidebar lists five steps: 1 Type, 2 Name and Protocol (highlighted), 3 Storage, 4 Storage Attributes, and 5 Summary. The main area contains the following fields:

- Datastore name:** NFS_DS1
- Size:** 2 TB (with a note: 'Minimum supported size is 1 GB.')
- Protocol:** NFS 3
- Advanced Options:** expanded, showing **Datastore Cluster:** (empty dropdown).

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is clicking the NEXT button.

4. En la página **Almacenamiento** seleccione una Plataforma (filtra el sistema de almacenamiento por tipo) y una VM de almacenamiento para el volumen. Opcionalmente, seleccione una política de exportación personalizada. Haga clic en **Siguiente** para continuar.

The screenshot shows the 'Storage' step of the 'Create Datastore' wizard. On the left, a sidebar lists five steps: 1 Type, 2 Name and Protocol, 3 Storage (highlighted), 4 Storage Attributes, and 5 Summary. The main area contains the following fields:

- Platform: *** Performance (A)
- Storage VM: *** VCF_NFS (with ID: ntaphci-a300e9u25 (172.16.9.25))
- Advanced Options:** expanded, showing **Custom Export Policy:** Search or specify policy name (with a note: 'Choose an existing policy or give a new name to the default policy.')

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is clicking the NEXT button.

5. En la página **Atributos de almacenamiento**, seleccione el agregado de almacenamiento que desea utilizar y, opcionalmente, las opciones avanzadas como la reserva de espacio y la calidad del servicio. Haga clic en **Siguiente** para continuar.

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 Summary

Storage Attributes

Specify the storage details for provisioning the datastore.

Aggregate: * EHCaggr02 (16.61 TB Free) ▾

Volume: A new volume will be created automatically.

^ Advanced Options

Space Reserve: * Thin ▾

Enable QoS

CANCEL

BACK

NEXT

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

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 Summary

Summary

A new datastore will be created with these settings.

Type

Destination: Datacenter

Datastore type: NFS

Name and Protocol

Datastore name: NFS_DS1

Size: 2 TB

Protocol: NFS 3

Storage

Platform: Performance (A)

Storage VM: VCF_NFS

CANCEL

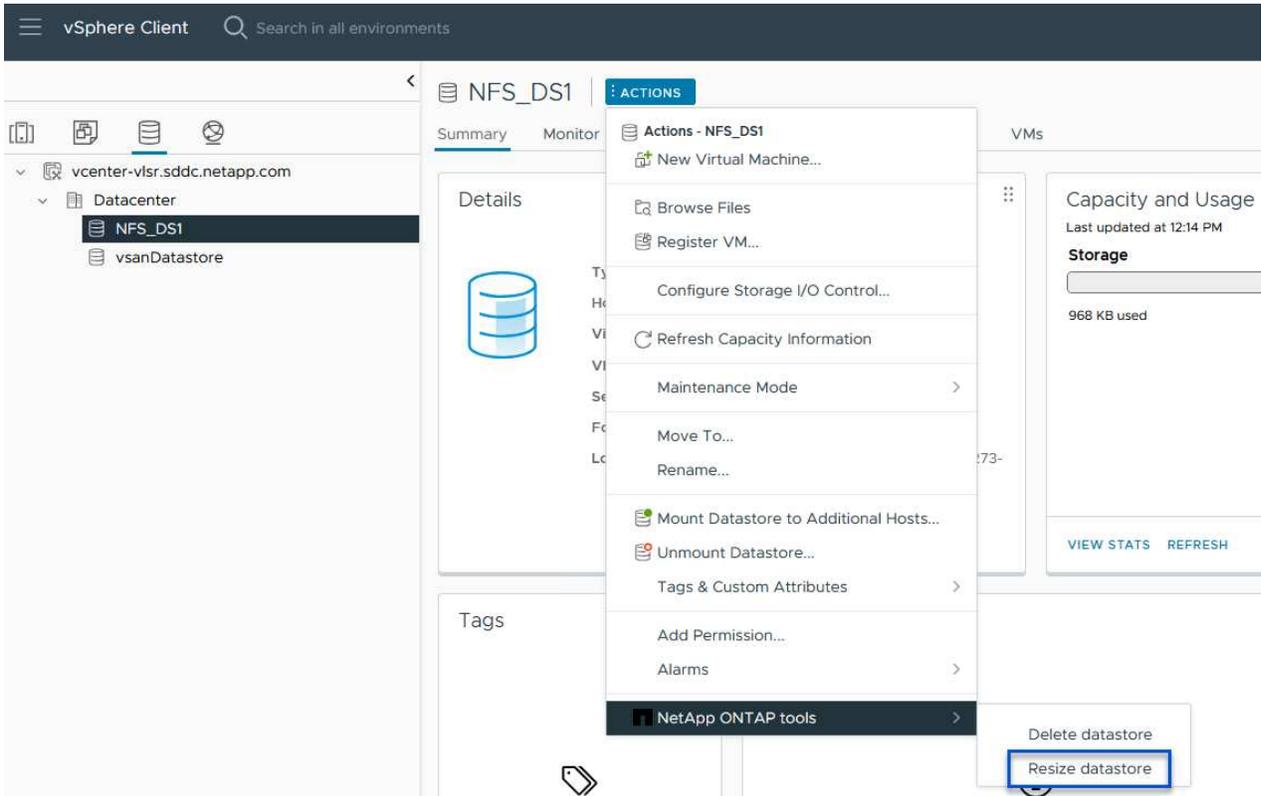
BACK

FINISH

Cambie el tamaño de un almacén de datos NFS con ONTAP Tools 10

Complete los siguientes pasos para cambiar el tamaño de un almacén de datos NFS existente con ONTAP Tools 10.

1. En el cliente de vSphere, desplácese hasta el inventario de almacenamiento. En el menú **ACCIONES**, seleccione **Herramientas de NetApp ONTAP > Cambiar tamaño de almacén de datos**.



2. En el asistente de **Resize Datastore**, rellena el nuevo tamaño del almacén de datos en GB y haz clic en **Resize** para continuar.

Resize Datastore | NFS_DS1

Volume Details

Volume Name:	NFS_DS1
Total Size:	2.1 TB
Used Size:	968 KB
Snapshot Reserve (%):	5
Thin Provisioned:	Yes

Size

Current Datastore Size:	2 TB
New Datastore Size (GB): *	3000

3. Supervise el progreso del trabajo de cambio de tamaño en el panel **Tareas recientes**.

Task Name	Target	Status	Details
Expand Datastore	vcenter-vlsr.sddc.net app.com	<div style="width: 100%; background-color: #0070C0; height: 10px;"></div> 100%	Expand datastore initiated with job id 2807

Información adicional

Para obtener una lista completa de las herramientas de ONTAP para los recursos de VMware vSphere 10, consulte ["Recursos de documentación de las herramientas de ONTAP para VMware vSphere"](#).

Para obtener más información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte ["Documentación de ONTAP 10"](#) el centro.

Utilice Site Recovery Manager de VMware para la recuperación ante desastres de almacenes de datos NFS

El uso de herramientas de ONTAP para VMware vSphere 10 y el adaptador de replicación de sitio (SRA) junto con el administrador de recuperación de sitio (SRM) de VMware aporta un valor importante a los procesos de recuperación ante desastres. Las herramientas de ONTAP 10 proporcionan sólidas funciones de almacenamiento, entre las que se incluyen alta disponibilidad y escalabilidad nativas para el proveedor VASA, y son compatibles con vVols iSCSI y NFS. Esto garantiza la disponibilidad de datos y

simplifica la gestión de múltiples servidores de VMware vCenter y clústeres de ONTAP. Mediante el SRA con VMware Site Recovery Manager, las organizaciones pueden lograr una replicación y una conmutación por error fluidas de máquinas virtuales y datos entre sitios, lo que permite procesos de recuperación ante desastres eficientes. La combinación de las herramientas de ONTAP y el SRA permite a las empresas proteger las cargas de trabajo cruciales, minimizar los tiempos de inactividad y mantener la continuidad del negocio ante desastres o eventos imprevistos.

Las herramientas de ONTAP 10 simplifican las funciones de eficiencia y gestión del almacenamiento, mejora la disponibilidad y reduce los costes de almacenamiento y la sobrecarga operativa, tanto si utiliza SAN como NAS. Utiliza prácticas recomendadas para aprovisionar almacenes de datos y optimiza la configuración de host ESXi para entornos de almacenamiento en bloques y NFS. Para todas estas ventajas, NetApp recomienda este plugin cuando se usa vSphere en sistemas que ejecutan el software ONTAP.

El SRA se usa junto con el SRM para gestionar la replicación de datos de máquinas virtuales entre sitios de producción y recuperación ante desastres para almacenes de datos VMFS tradicionales y NFS, y también para las pruebas no disruptivas de réplicas de recuperación ante desastres. Ayuda a automatizar las tareas de identificación, recuperación y protección.

En este escenario, demostraremos cómo poner en marcha y utilizar el administrador de recuperación de sitios de VMware para proteger los almacenes de datos y ejecutar tanto una prueba como una conmutación por error final a un sitio secundario. La reprotcción y la conmutación por recuperación también se tratan.

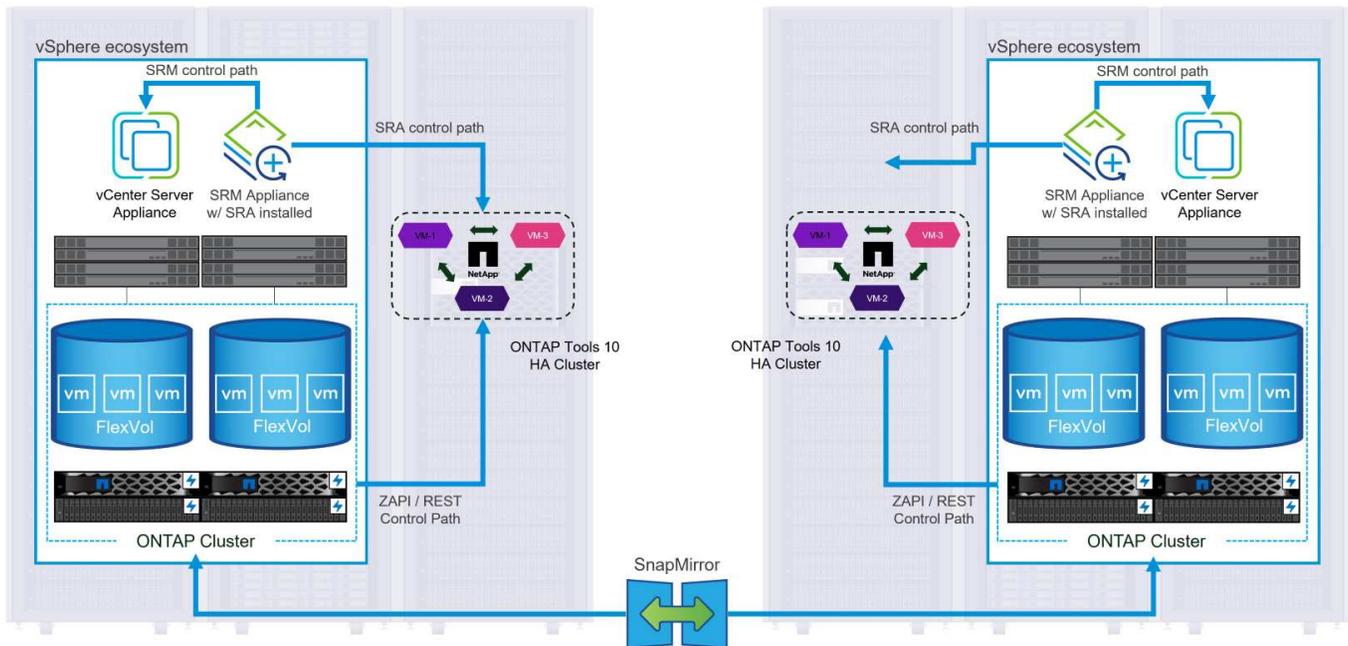
Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Configurar SRM con servidores de vCenter en sitios principales y secundarios.
- Instale las herramientas del adaptador SRA para ONTAP para VMware vSphere 10 y regístrelo en vCenters.
- Crear relaciones de SnapMirror entre los sistemas de almacenamiento de ONTAP de origen y de destino
- Configurar Site Recovery para SRM.
- Realizar pruebas y recuperación tras fallos final.
- Habla sobre la reprotcción y la conmutación tras recuperación.

Arquitectura

El siguiente diagrama muestra una arquitectura típica de VMware Site Recovery con herramientas ONTAP para VMware vSphere 10 configuradas en una configuración de alta disponibilidad de 3 nodos.



Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Clústeres de vSphere 8 instalados en las ubicaciones principales y secundarias con redes adecuadas para las comunicaciones entre entornos.
- Sistemas de almacenamiento de ONTAP en la ubicación principal y secundaria, con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento NFS.
- Se han instalado las herramientas de ONTAP para VMware vSphere 10 y tienen registrados ambos servidores vCenter.
- Se han instalado dispositivos VMware Site Recovery Manager para los sitios primarios y secundarios.
 - Se configuraron las asignaciones de inventario (red, carpeta, recurso, política de almacenamiento) para SRM.

NetApp recomienda diseños de red redundantes para NFS, lo que proporciona tolerancia a fallos para sistemas de almacenamiento, switches, adaptadores de red y sistemas host. Es común poner en marcha NFS con una única subred o varias subredes, en función de los requisitos de la arquitectura.

Consulte "[Prácticas recomendadas para ejecutar NFS con VMware vSphere](#)" Para obtener información detallada específica de VMware vSphere.

Para obtener orientación de red sobre el uso de ONTAP con VMware vSphere, consulte la "[Configuración de red: NFS](#)" De la documentación de aplicaciones empresariales de NetApp.

Para obtener documentación de NetApp sobre el uso del almacenamiento de ONTAP con VMware SRM, consulte "[VMware Site Recovery Manager con ONTAP](#)"

Pasos de despliegue

Las siguientes secciones describen los pasos de puesta en marcha para implementar y probar una configuración de VMware Site Recovery Manager con el sistema de almacenamiento de ONTAP.

Crear una relación de SnapMirror entre los sistemas de almacenamiento de ONTAP

Debe establecerse una relación de SnapMirror entre los sistemas de almacenamiento ONTAP de origen y de destino para que los volúmenes de almacenes de datos estén protegidos.

Consulte la documentación de ONTAP en la que comienza ["AQUÍ"](#) para obtener información completa sobre la creación de relaciones de SnapMirror para volúmenes de ONTAP.

Las instrucciones paso a paso se describen en el siguiente documento, ubicado ["AQUÍ"](#). Estos pasos describen cómo crear relaciones entre iguales de clústeres y SVM y, a continuación, relaciones de SnapMirror para cada volumen. Estos pasos pueden llevarse a cabo en ONTAP System Manager o mediante la CLI de ONTAP.

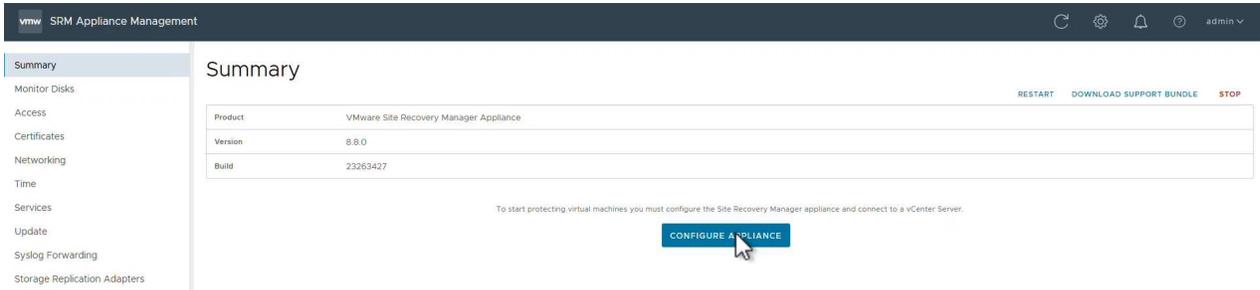
Configure el dispositivo SRM

Complete los siguientes pasos para configurar el dispositivo SRM y el adaptador de SRA.

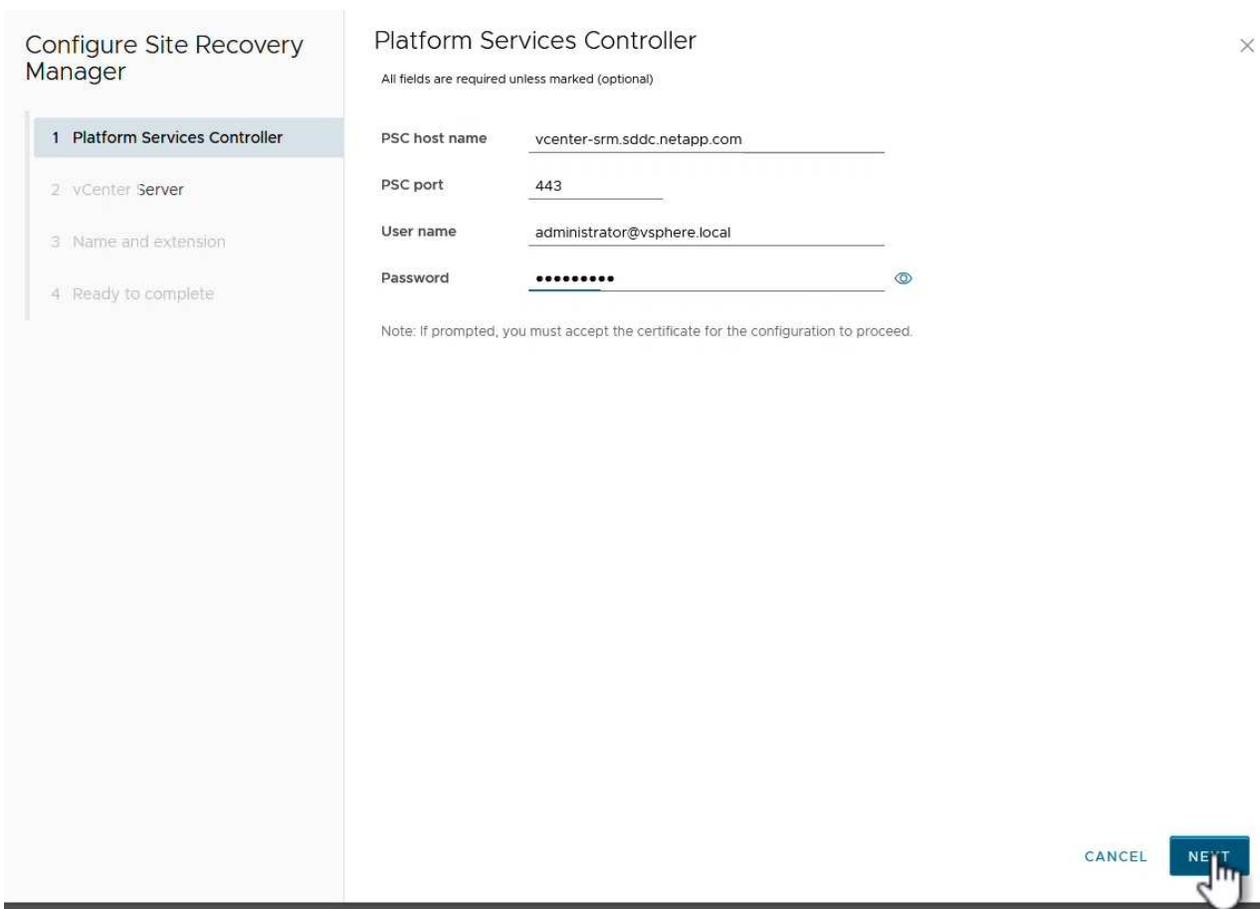
Conecte el dispositivo SRM para sitios primarios y secundarios

Deben completarse los siguientes pasos tanto para el sitio primario como para el secundario.

1. En un navegador web, navegue https://<SRM_appliance_IP>:5480 e inicie sesión. Haga clic en **Configurar dispositivo** para comenzar.



2. En la página **Platform Services Controller** del asistente Configure Site Recovery Manager, rellene las credenciales del servidor vCenter en el que se registrará SRM. Haga clic en **Siguiente** para continuar.



3. En la página **vCenter Server**, vea el vServer conectado y haga clic en **Siguiente** para continuar.

4. En la página **Nombre y extensión**, introduzca un nombre para el sitio SRM, una dirección de correo electrónico de los administradores y el host local que utilizará SRM. Haga clic en **Siguiente** para continuar.

The screenshot shows a configuration wizard titled "Configure Site Recovery Manager" with a sidebar on the left containing four steps: 1 Platform Services Controller, 2 vCenter Server, 3 Name and extension (highlighted), and 4 Ready to complete. The main area is titled "Name and extension" and includes a close button (X) in the top right. Below the title, it states "All fields are required unless marked (optional)". The form contains the following fields and options:

- Site name:** "Site 2" (with a note: "A unique display name for this Site Recovery Manager site.")
- Administrator email:** "josh.powell@netapp.com" (with a note: "An email address to use for system notifications.")
- Local host:** "srm-site2.sddc.netapp.com" (with a note: "The address on the local host to be used by Site Recovery Manager.")
- Extension ID:** Radio buttons for "Default extension ID (com.vmware.vcDr)" (selected) and "Custom extension ID". A note below states: "The default extension ID is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom extension ID for each SRM pair."
- Extension ID:** "com.vmware.vcDr-"
- Organization:** (empty field)
- Description:** (empty field)

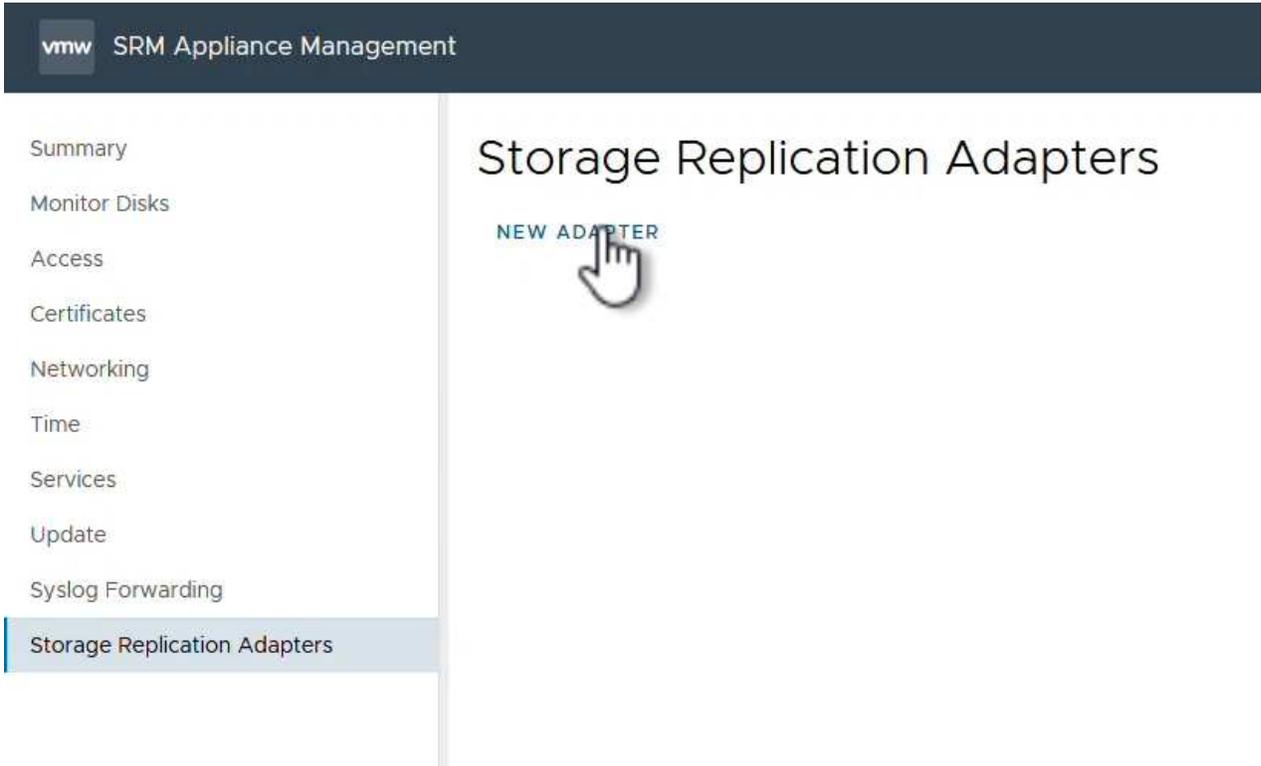
At the bottom right, there are three buttons: "CANCEL", "BACK", and "NEXT". A mouse cursor is clicking on the "NEXT" button.

5. En la página **Listo para completar** revise el resumen de los cambios

Configure el SRA en el dispositivo SRM

Complete los siguientes pasos para configurar el SRA en el dispositivo SRM:

1. Descargue las herramientas SRA para ONTAP 10 en el "[Sitio de soporte de NetApp](#)" y guarde el archivo tar.gz en una carpeta local.
2. Desde el dispositivo de gestión SRM, haga clic en **Adaptadores de replicación de almacenamiento** en el menú de la izquierda y luego en **Nuevo adaptador**.



3. Siga los pasos descritos en el sitio de documentación de ONTAP Tools 10 en "[Configure el SRA en el dispositivo SRM](#)". Una vez que se haya completado, el SRA puede comunicarse con el SRA mediante la dirección IP proporcionada y las credenciales del servidor de vCenter.

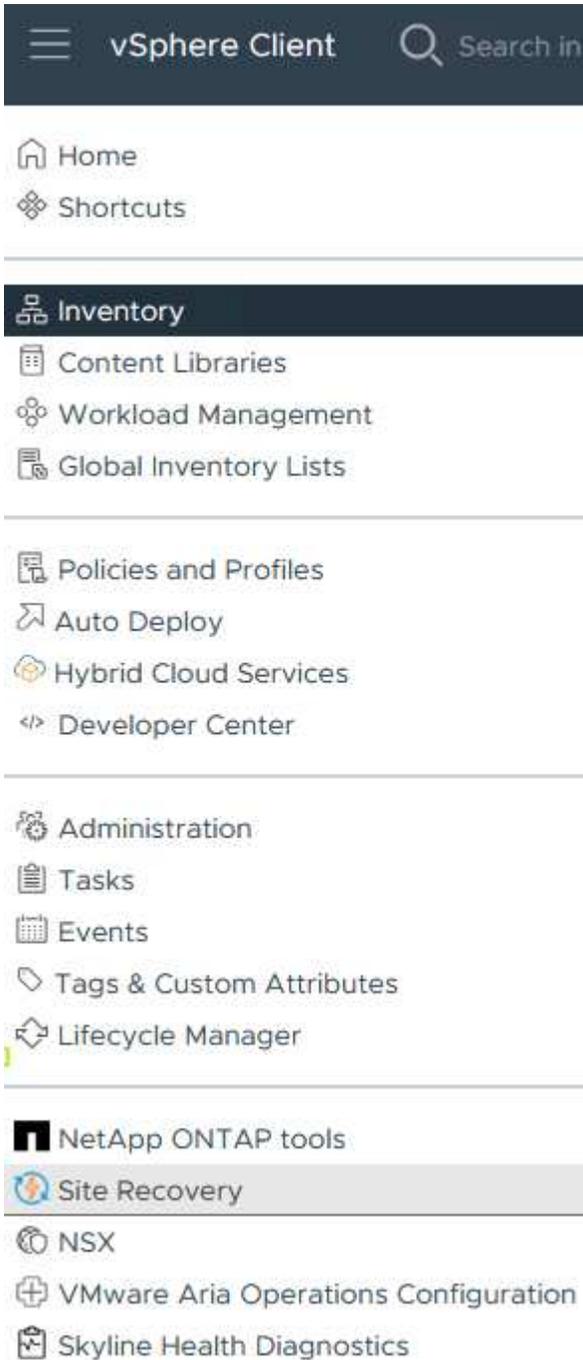
Configurar Site Recovery para SRM

Realice los siguientes pasos para configurar el emparejamiento de sitios, crear grupos de protección,

Configure Site Pairing para SRM

El siguiente paso se completa en el cliente vCenter del sitio primario.

1. En el cliente vSphere haga clic en **Site Recovery** en el menú de la izquierda. Se abre una nueva ventana del explorador en la interfaz de usuario de gestión de SRM en el sitio principal.



2. En la página **Site Recovery**, haz clic en **NEW SITE PAIR**.

Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.

[NEW SITE PAIR](#)[Learn More](#)

3. En la página **Pair type** del asistente **New Pair**, verifique que el servidor vCenter local esté seleccionado y seleccione el **Pair type**. Haga clic en **Siguiente** para continuar.

The screenshot shows the 'New Pair' wizard with the 'Pair type' step selected. The wizard has four steps: 1. Pair type, 2. Peer vCenter Server, 3. Services, and 4. Ready to complete. The 'Pair type' step is active and shows a list of vCenter Servers. The first server, 'vcenter-vlsr.sddc.netapp.com', is selected. Below the list, there are two radio button options for the pair type: 'Pair with a peer vCenter Server located in a different SSO domain' (selected) and 'Pair with a peer vCenter Server located in the same SSO domain'. At the bottom right, there are 'CANCEL' and 'NEXT' buttons, with a mouse cursor clicking on 'NEXT'.

4. En la página **Peer vCenter**, rellene las credenciales de vCenter en el sitio secundario y haga clic en **Buscar instancias de vCenter**. Compruebe que la instancia de vCenter se ha detectado y haga clic en **Siguiente** para continuar.

New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

Peer vCenter Server



All fields are required unless marked (optional)

Enter the Platform Services Controller details for the peer vCenter Server.

PSC host name

PSC port

User name

Password

FIND VCENTER SERVER INSTANCES

Select a vCenter Server you want to pair.

vCenter Server

- vcenter-srm.sddc.netapp.com

CANCEL

BACK

NEXT

5. En la página **Servicios**, marque la casilla junto al emparejamiento de sitios propuesto. Haga clic en **Siguiente** para continuar.

New Pair

- 1 Pair type
- 2 Peer vCenter Server
- 3 Services
- 4 Ready to complete

Services

The following services were identified on the selected vCenter Server instances. Select the ones you want to pair.

Service	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com
<input checked="" type="checkbox"/> Site Recovery Manager (com.vmware.vc...	Site 1	Site 2

CANCEL

BACK

NEXT

6. En la página **Listo para completar**, revise la configuración propuesta y luego haga clic en el botón **Finalizar** para crear el Emparejamiento del sitio
7. El nuevo par de sitios y su resumen se pueden ver en la página Resumen.

Summary

RECONNECT

BREAK SITE PAIR



vCenter Server: vcenter-vlsr.sddc.netapp.com vcenter-srm.sddc.netapp.com
vCenter Version: 8.0.2, 22385739 8.0.2, 22385739
vCenter Host Name: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443
Platform Services Controller: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443

Site Recovery Manager

EXPORT/IMPORT SRM CONFIGURATION

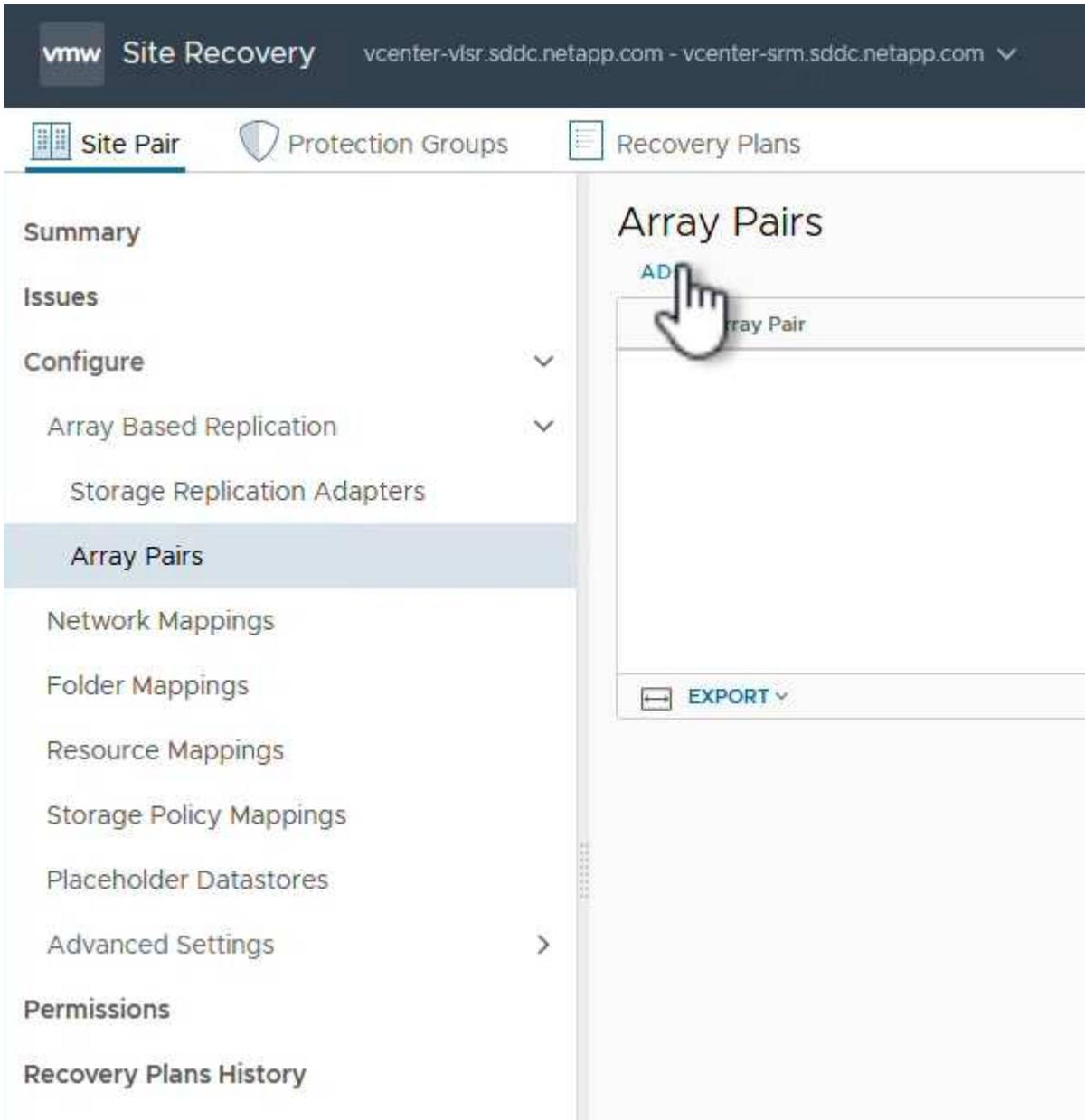
Protection Groups:0 Recovery Plans:0

Name	Site 1 RENAME	Site 2 RENAME
Server	srm-site1.sddc.netapp.com:443 ACTIONS	srm-site2.sddc.netapp.com:443 ACTIONS
Version	8.8.0, 23263429	8.8.0, 23263429
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

Añada un par de cabinas para SRM

El siguiente paso se completa en la interfaz de recuperación del sitio principal.

1. En la interfaz de recuperación del sitio, vaya a **Configure > Array Based Replication > Array Pairs** en el menú de la izquierda. Haga clic en **ADD** para comenzar.



2. En la página **Storage replication adapter** del asistente **Add Array Pair**, verifique que el adaptador SRA esté presente para el sitio principal y haga clic en **Next** para continuar.

Add Array Pair

1 Storage replication adapter

2 Local array manager

3 Remote array manager

4 Array pairs

5 Ready to complete

Storage replication adapter

Select a storage replication adapter (SRA):

	Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
	NetApp Storage Replication Ada...	OK	NetApp	10.1	Not Support...

Items per page: AUTO 1 items

CANCEL

NEXT

3. En la página **Local array manager**, introduzca un nombre para la cabina en el sitio primario, el FQDN del sistema de almacenamiento, las direcciones IP de SVM que sirven NFS y, opcionalmente, los nombres de volúmenes específicos que se van a detectar. Haga clic en **Siguiente** para continuar.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Local array manager

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vcenter-vlsr.sddc.netapp.com":

Array_1

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname ontap-source.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses 172.21.118.49

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name SQL_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list SQL_NFS

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT

4. En el **Remote array manager**, rellene la misma información que el último paso para el sistema de almacenamiento ONTAP en el sitio secundario.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Remote array manager



Do not create a remote array manager now.

Enter a name for the array manager on "vcenter-srm.sddc.netapp.com":

Array_2

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname

ontap-destination.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses

172.21.118.51

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name

SRM_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list

|

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT



5. En la página **Matrices**, seleccione los pares de matrices que desea habilitar y haga clic en **Siguiente** para continuar.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs**
- 5 Ready to complete

Array pairs

Select the array pairs to enable:

<input checked="" type="checkbox"/>	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com	Status
<input checked="" type="checkbox"/>	ontap-source:SQL_NFS (Array_1)	ontap-destination:SRM_NFS (Array_2)	Ready to be enabled

1 1 items

CANCEL

BACK

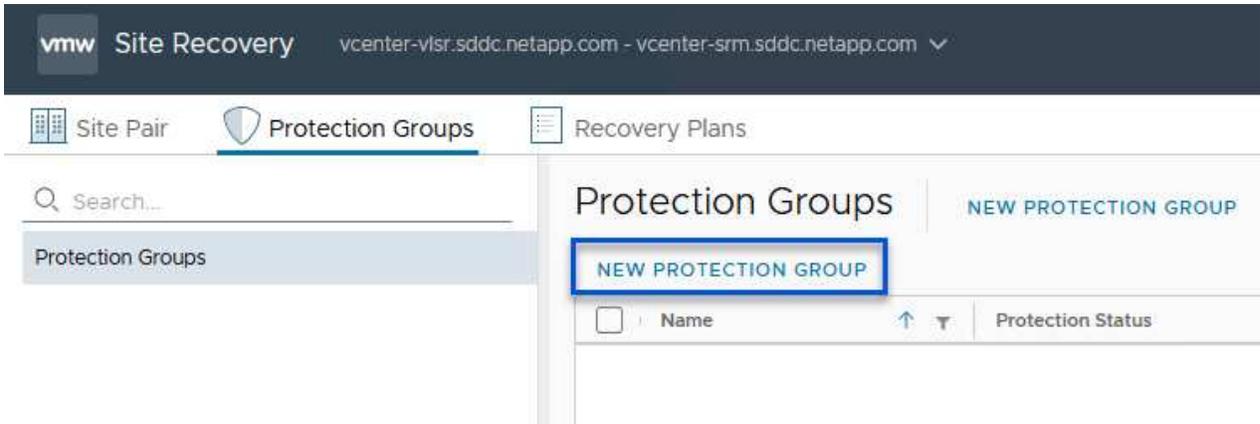
NEXT

6. Revise la información en la página **Ready to Complete** y haga clic en **Finish** para crear el par de matrices.

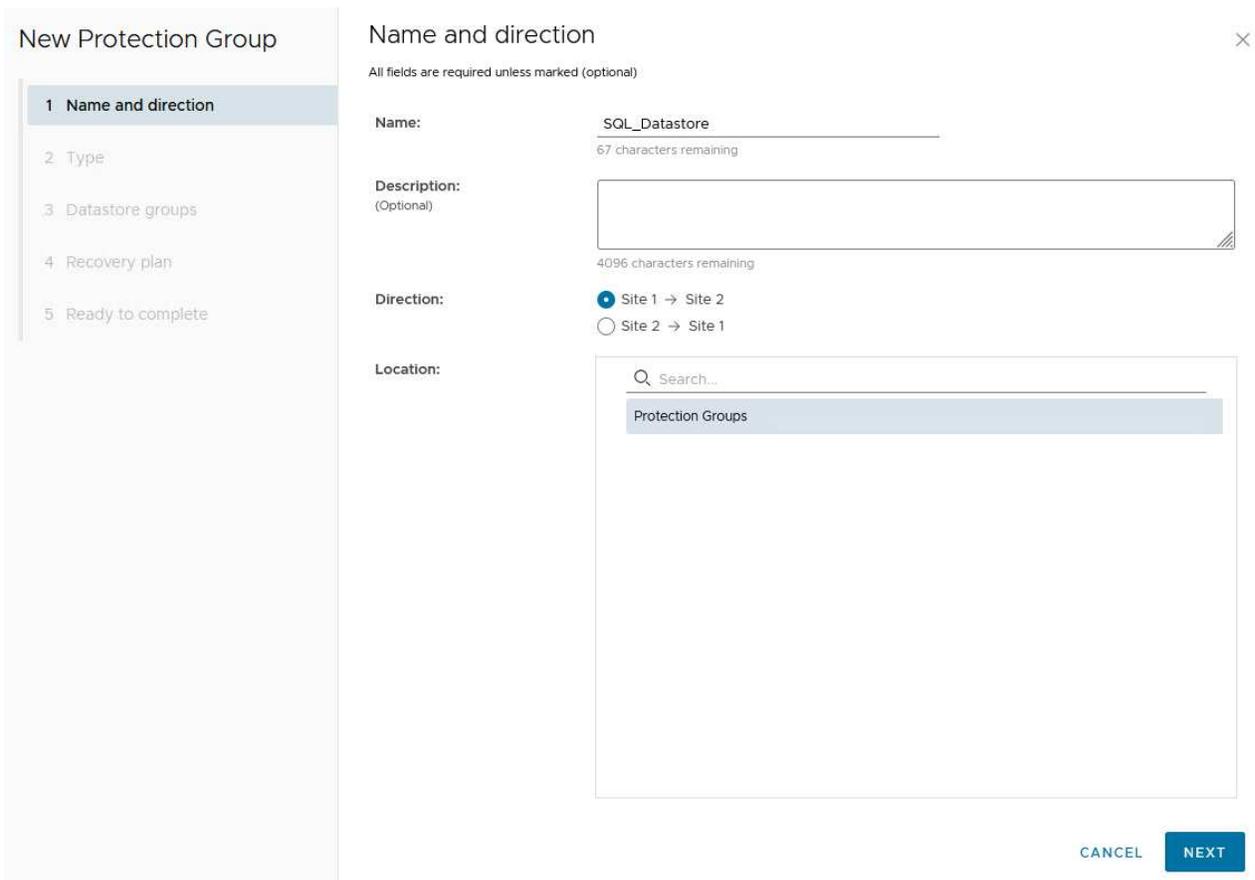
Configure los grupos de protección para el SRM

El siguiente paso se completa en la interfaz de recuperación del sitio principal.

1. En la interfaz de recuperación del sitio, haga clic en la pestaña * Grupos de protección * y luego en * Nuevo grupo de protección * para comenzar.



2. En la página **Nombre y dirección** del asistente **New Protection Group**, proporcione un nombre para el grupo y elija la dirección del sitio para la protección de los datos.

The screenshot shows the 'New Protection Group' wizard in the 'Name and direction' step. On the left, there's a sidebar with steps: 1. Name and direction (selected), 2. Type, 3. Datastore groups, 4. Recovery plan, and 5. Ready to complete. The main area has the following fields:

- Name:** A text input field containing 'SQL_Datastore' with a character count of '67 characters remaining'.
- Description:** An optional text input field that is currently empty, with a character count of '4096 characters remaining'.
- Direction:** Two radio button options: 'Site 1 -> Site 2' (which is selected) and 'Site 2 -> Site 1'.
- Location:** A search input field with a dropdown menu showing 'Protection Groups'.

At the bottom right, there are 'CANCEL' and 'NEXT' buttons.

3. En la página **Type**, seleccione el tipo de grupo de protección (almacén de datos, VM o VVol) y seleccione el par de cabinas. Haga clic en **Siguiente** para continuar.

New Protection Group

- 1 Name and direction
- 2 Type**
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Type

Select the type of protection group you want to create:

- Datastore groups (array-based replication)**
Protect all virtual machines which are on specific datastores.
- Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.
- Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

Select array pair

Array Pair	Array Manager Pair
<input checked="" type="radio"/> ✓ ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2	nfs_array1 ↔ nfs_Array2
<input type="radio"/> ✓ ontap-source:SQL_NFS ↔ ontap-destination:SRM_NFS	Array_1 ↔ Array_2

Items per page: AUTO 2 array pairs

CANCEL BACK NEXT

4. En la página **Datastore groups**, seleccione los almacenes de datos que desea incluir en el grupo de protección. Las máquinas virtuales que residen actualmente en el almacén de datos se muestran para cada almacén de datos seleccionado. Haga clic en **Siguiente** para continuar.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups**
- 4 Recovery plan
- 5 Ready to complete

Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together.

[SELECT ALL](#) [CLEAR SELECTION](#)

<input checked="" type="checkbox"/>	Datastore Group	Status
<input checked="" type="checkbox"/>	NFS_DS1	Add to this protection group

1 Items per page: [AUTO](#) 1 datastore groups

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
SQLSRV-01	NFS_DS1	Add to this protection group
SQLSRV-03	NFS_DS1	Add to this protection group
SQLSRV-02	NFS_DS1	Add to this protection group

[CANCEL](#) [BACK](#) [NEXT](#)

5. En la página **Recovery plan**, opcionalmente, elija agregar el grupo de protección a un plan de recuperación. En este caso, el plan de recuperación aún no se ha creado, por lo que se selecciona **NO AÑADIR AL PLAN DE RECUPERACIÓN**. Haga clic en **Siguiente** para continuar.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Recovery plan

You can optionally add this protection group to a recovery plan.

- Add to existing recovery plan
- Add to new recovery plan
- Do not add to recovery plan now

 The protection group cannot be recovered unless it is added to a recovery plan.

CANCEL

BACK

NEXT

6. En la página **Listo para completar**, revise los nuevos parámetros del grupo de protección y haga clic en **Finalizar** para crear el grupo.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Ready to complete



Review your selected settings.

Name	SQL_Datastore
Description	
Protected site	Site 1
Recovery site	Site 2
Location	Protection Groups
Protection group type	Datastore groups (array-based replication)
Array pair	ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_array2)
Datastore groups	NFS_DS1
Total virtual machines	3
Recovery plan	none

CANCEL

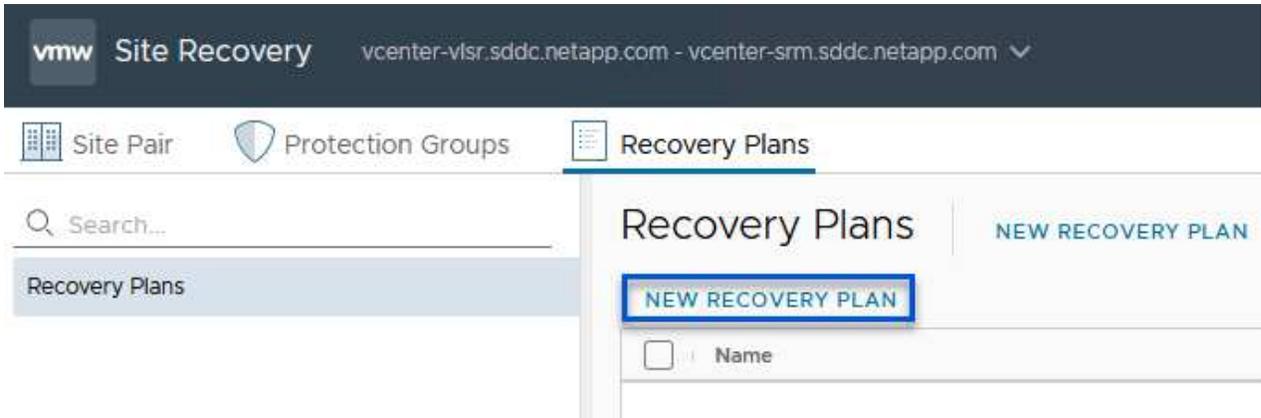
BACK

FINISH

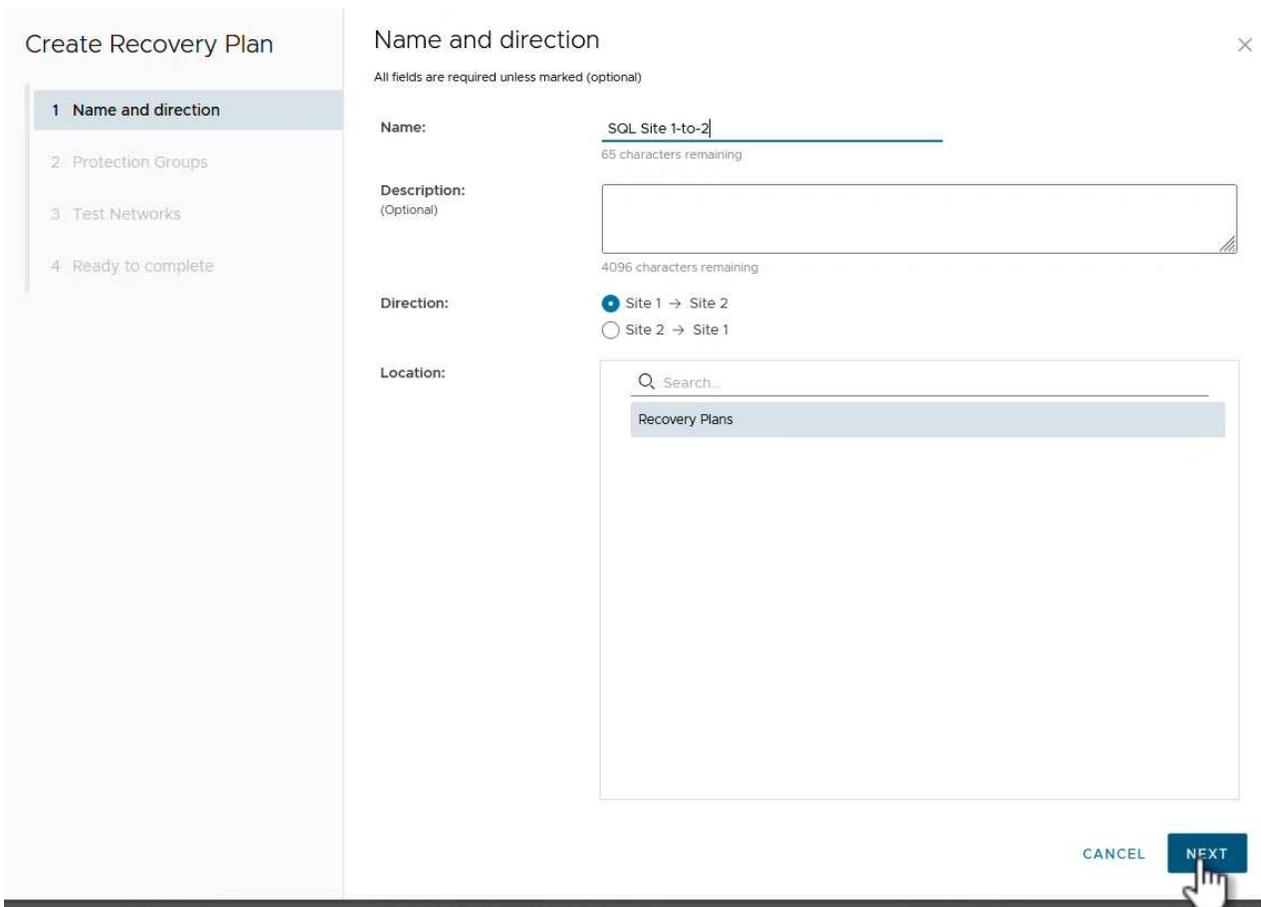
Configurar el plan de recuperación para SRM

El siguiente paso se completa en la interfaz de recuperación del sitio principal.

1. En la interfaz de recuperación del sitio haga clic en la pestaña **Plan de recuperación** y luego en **Nuevo plan de recuperación** para comenzar.



2. En la página **Nombre y dirección** del asistente **Crear plan de recuperación**, proporcione un nombre para el plan de recuperación y elija la dirección entre los sitios de origen y destino. Haga clic en **Siguiente** para continuar.



3. En la página **Grupos de protección**, seleccione los grupos de protección creados previamente para incluir en el plan de recuperación. Haga clic en **Siguiente** para continuar.

The screenshot displays the 'Create Recovery Plan' wizard in step 2, 'Protection Groups'. On the left, a sidebar lists the steps: 1 Name and direction, 2 Protection Groups (highlighted), 3 Test Networks, and 4 Ready to complete. The main area is titled 'Protection Groups' and shows a table with columns 'Name' and 'Description'. One group, 'SQL_Datastore', is selected. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT', with a mouse cursor clicking on 'NEXT'.

Name	Description
SQL_Datastore	

4. En las **Redes de prueba** configure redes específicas que se utilizarán durante la prueba del plan. Si no existe ninguna asignación o si no se selecciona ninguna red, se creará una red de prueba aislada. Haga clic en **Siguiente** para continuar.

Create Recovery Plan

- 1 Name and direction
- 2 Protection Groups
- 3 Test Networks
- 4 Ready to complete

Test Networks

Select the networks to use while running tests of this plan.

i If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.

Recovery Network	↑ ↓	Test Network	
Datacenter > DPortGroup	☰	Use site-level mapping	CHANGE
Datacenter > Mgmt 3376	☰	Mgmt 3376	CHANGE
Datacenter > NFS 3374	☰	NFS 3374	CHANGE
Datacenter > VLAN 181	☰	Use site-level mapping	CHANGE
Datacenter > VM Network	☰	Use site-level mapping	CHANGE
Datacenter > vMotion 3373	☰	Use site-level mapping	CHANGE
Datacenter > vSAN 3422	☰	Use site-level mapping	CHANGE

7 network(s)

CANCEL
BACK
NEXT

5. En la página **Listo para completar**, revise los parámetros elegidos y luego haga clic en **Finalizar** para crear el plan de recuperación.

Operaciones de recuperación ante desastres con SRM

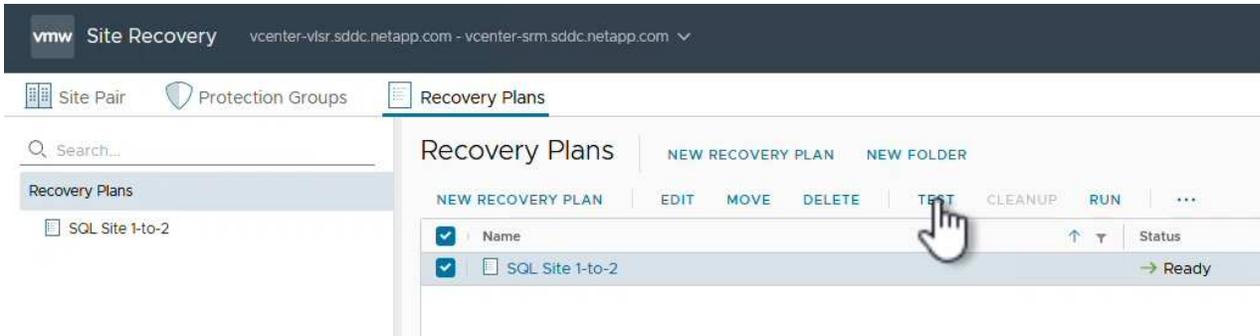
En esta sección se tratarán varias funciones de uso de la recuperación ante desastres con SRM, como la prueba de recuperación tras fallos, la realización de recuperación tras fallos, la realización de reprotección y la conmutación tras recuperación.

Consulte "[Mejores prácticas operativas](#)" si desea más información sobre cómo usar el almacenamiento de ONTAP con operaciones de recuperación ante desastres de SRM.

Pruebas de recuperación tras fallos con SRM

El siguiente paso se completa en la interfaz de recuperación del sitio.

1. En la interfaz de recuperación del sitio haga clic en la pestaña **Plan de recuperación** y luego seleccione un plan de recuperación. Haga clic en el botón **Test** para comenzar a probar la conmutación por error en el sitio secundario.

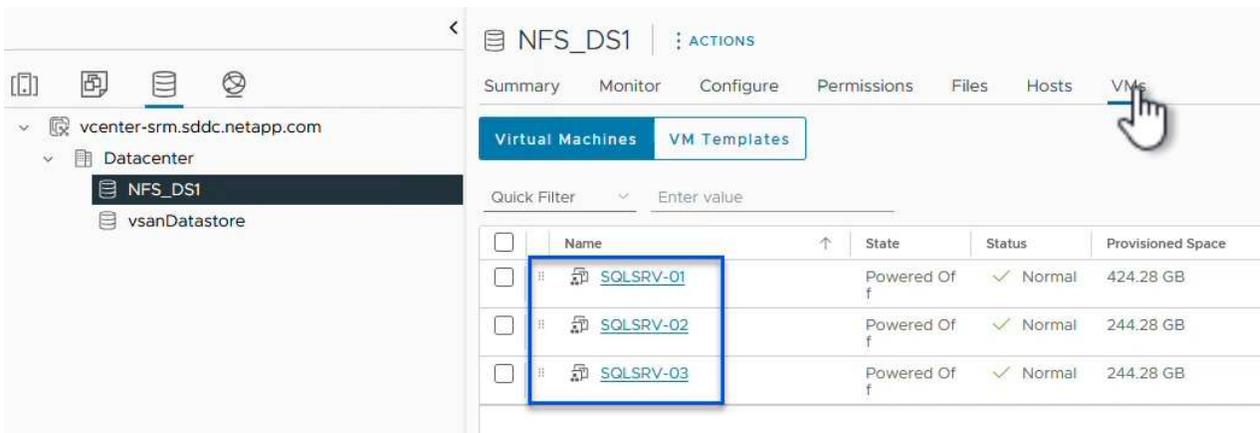


2. Es posible ver el progreso de la prueba desde el panel de tareas Site Recovery y el panel de tareas de vCenter.

The screenshot shows the vCenter Site Recovery Manager interface. At the top, there are tabs for 'Recent Tasks' and 'Alarms'. The 'Recent Tasks' tab is active. Below it, there's a table of recent tasks with columns for 'Task Name', 'Target', 'Status', 'Initiator', and 'Queued For'. The 'Test Recovery Plan' task is highlighted, showing a progress bar at 6%. Other tasks include 'Create Recovery Plan', 'Set virtual machine custom value', and 'Set virtual machine custom value'.

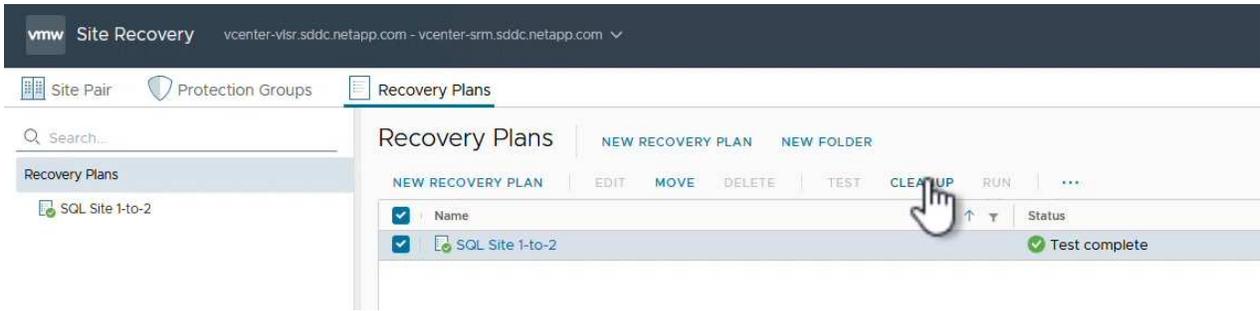
Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	4 ms
Set virtual machine custom value	SQLSRV-01	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	3 ms

3. El SRM envía comandos a través del SRA al sistema de almacenamiento de ONTAP secundario. Se crea y se monta una FlexClone de la snapshot más reciente en el clúster de vSphere secundario. El almacén de datos recién montado puede verse en el inventario de almacenamiento.



4. Una vez completada la prueba, haga clic en **Cleanup** para desmontar el almacén de datos y volver al

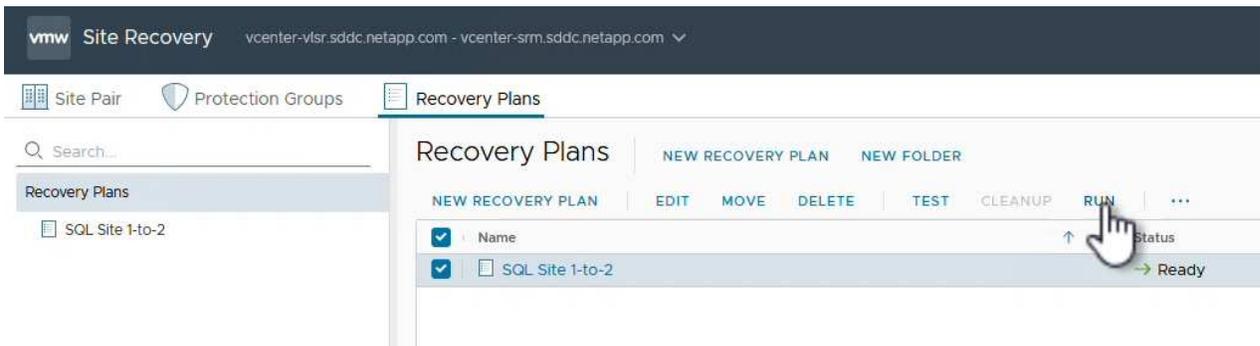
entorno original.



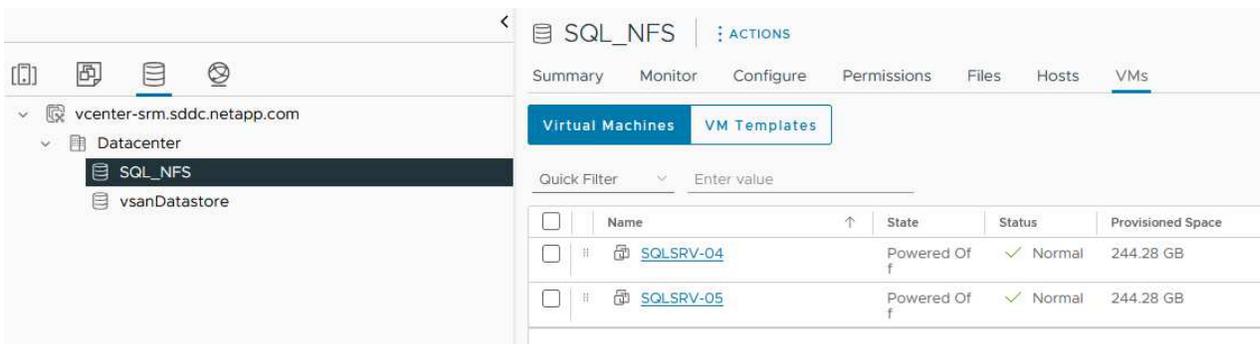
Ejecute el plan de recuperación con SRM

Realice una recuperación completa y una conmutación al nodo de respaldo en el sitio secundario.

1. En la interfaz de recuperación del sitio haga clic en la pestaña **Plan de recuperación** y luego seleccione un plan de recuperación. Haga clic en el botón **Run** para iniciar la conmutación por error al sitio secundario.



2. Una vez finalizada la conmutación al respaldo, puede ver el almacén de datos montado y las máquinas virtuales registradas en el sitio secundario.



SRM ofrece funciones adicionales una vez completada una recuperación tras fallos.

Reprotección: Una vez completado el proceso de recuperación, el sitio de recuperación previamente designado asume el papel del nuevo sitio de producción. Sin embargo, es importante tener en cuenta que la replicación de SnapMirror se interrumpe durante la operación de recuperación, lo que deja al nuevo sitio de

producción vulnerable a futuros desastres. Para garantizar la protección continua, se recomienda establecer una nueva protección para el nuevo sitio de producción replicándola en otro sitio. En los casos en que el sitio de producción original siga funcionando, el administrador de VMware puede reorganizarlo como un nuevo centro de recuperación, invirtiendo efectivamente la dirección de la protección. Es crucial destacar que la reprotcción solo es factible en caso de fallos no catastróficos, lo que requiere la capacidad de recuperación eventual de los servidores vCenter Server originales, los servidores ESXi, los servidores SRM y sus bases de datos respectivas. Si estos componentes no están disponibles, es necesario crear un nuevo grupo de protección y un nuevo plan de recuperación.

Failback: Una operación de failback es una conmutación por error inversa, devolviendo las operaciones al sitio original. Es crucial asegurarse de que el sitio original ha recuperado la funcionalidad antes de iniciar el proceso de conmutación por error. Para garantizar una conmutación por error sin problemas, se recomienda realizar una conmutación por error de prueba después de completar el proceso de reprotcción y antes de ejecutar la conmutación por error final. Esta práctica sirve como un paso de verificación, confirmando que los sistemas en el sitio original son totalmente capaces de manejar la operación. Si sigue este enfoque, puede minimizar los riesgos y garantizar una transición más fiable de vuelta al entorno de producción original.

Información adicional

Para obtener documentación de NetApp sobre el uso del almacenamiento de ONTAP con VMware SRM, consulte ["VMware Site Recovery Manager con ONTAP"](#)

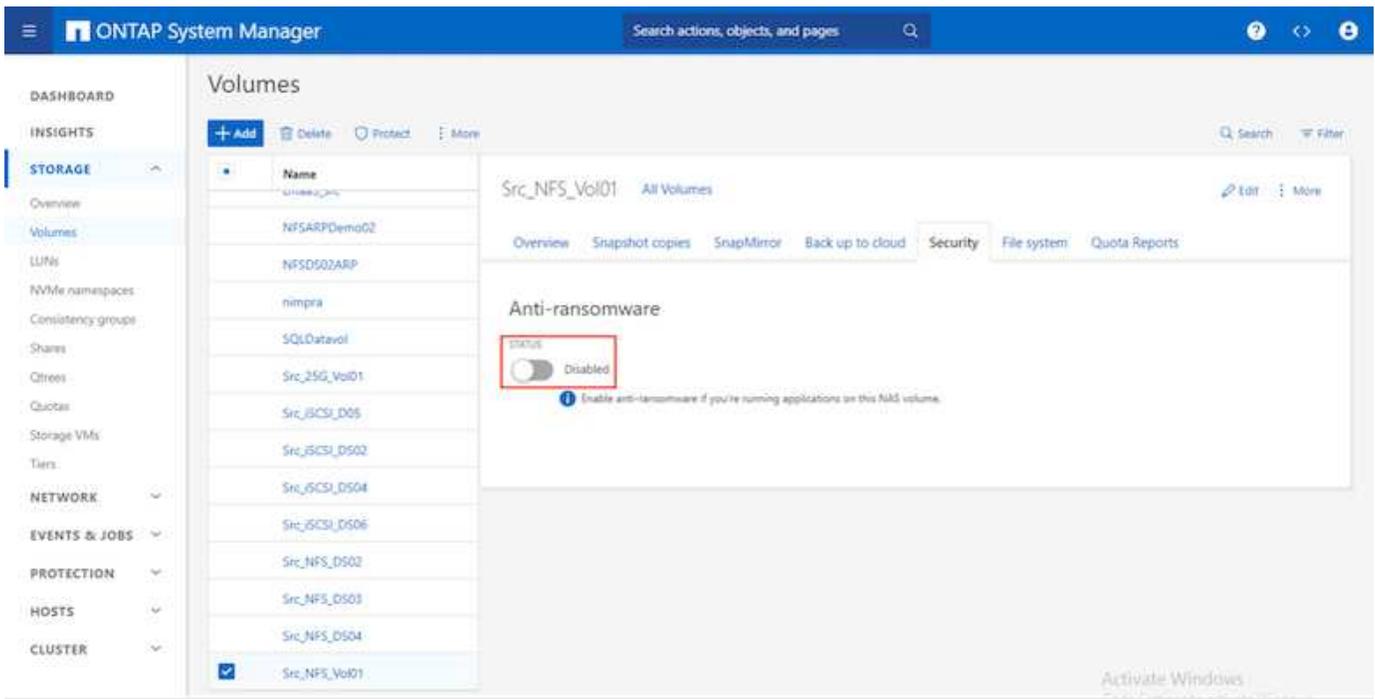
Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

Protección autónoma frente al ransomware para almacenamiento NFS

Detectar el ransomware lo antes posible es crucial para evitar su propagación y evitar costosos tiempos de inactividad. Una estrategia de detección de ransomware eficaz debe incorporar múltiples capas de protección en los niveles de host ESXi y máquina virtual invitada. Aunque se implementan múltiples medidas de seguridad para crear una defensa completa contra ataques de ransomware, ONTAP permite incorporar más capas de protección al enfoque de defensa general. Para nombrar algunas funcionalidades, lo primero es copias Snapshot, protección autónoma frente a ransomware, copias Snapshot a prueba de manipulaciones, etc.

Veamos cómo las funciones anteriores funcionan con VMware para proteger y recuperar los datos contra el ransomware. Para proteger vSphere y las máquinas virtuales invitadas contra ataques, es esencial tomar varias medidas, como la segmentación, el uso de EDR/XDR/SIEM para terminales e la instalación de actualizaciones de seguridad y el cumplimiento de las directrices de endurecimiento 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 de servidor empresarial se instalan y se actualizan regularmente en ellos, lo que es un componente esencial de la estrategia de protección contra ransomware de varias capas. Además, habilite la protección autónoma frente a ransomware (ARP) en el volumen NFS que alimenta el almacén de datos. ARP aprovecha EL APRENDIZAJE automático integrado que analiza la actividad de las cargas de trabajo del volumen más la entropía de los datos para detectar automáticamente el ransomware. ARP es configurable a través de la interfaz de gestión incorporada de ONTAP o System Manager y se habilita para cada volumen.

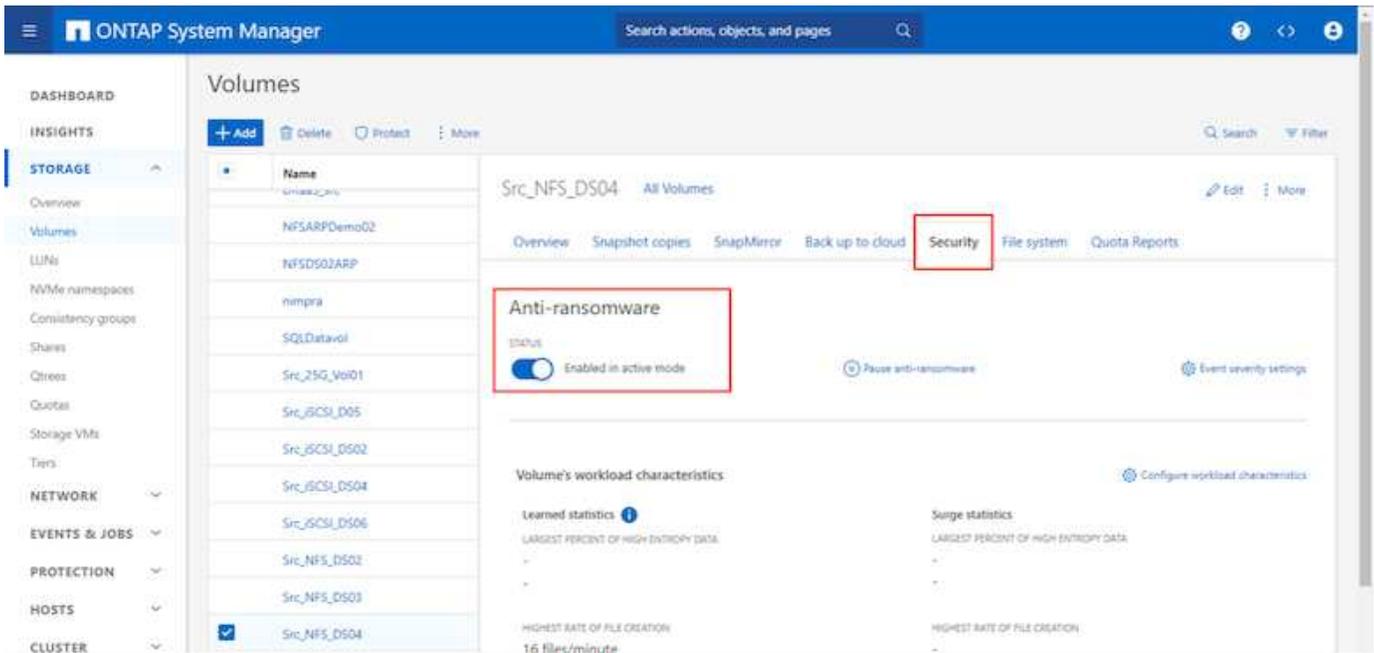


Con el nuevo ARP/AI de NetApp, que actualmente se encuentra en versión preliminar tecnológica, no es necesario un modo de aprendizaje. En su lugar, puede pasar directamente al modo activo con su función de detección de ransomware impulsada por la IA.



Con ONTAP One, todos estos conjuntos de características son completamente gratuitos. Acceda a NetApp la sólida suite de protección de datos, seguridad y todas las funciones que ofrece ONTAP sin tener que preocuparse por las barreras de las licencias.

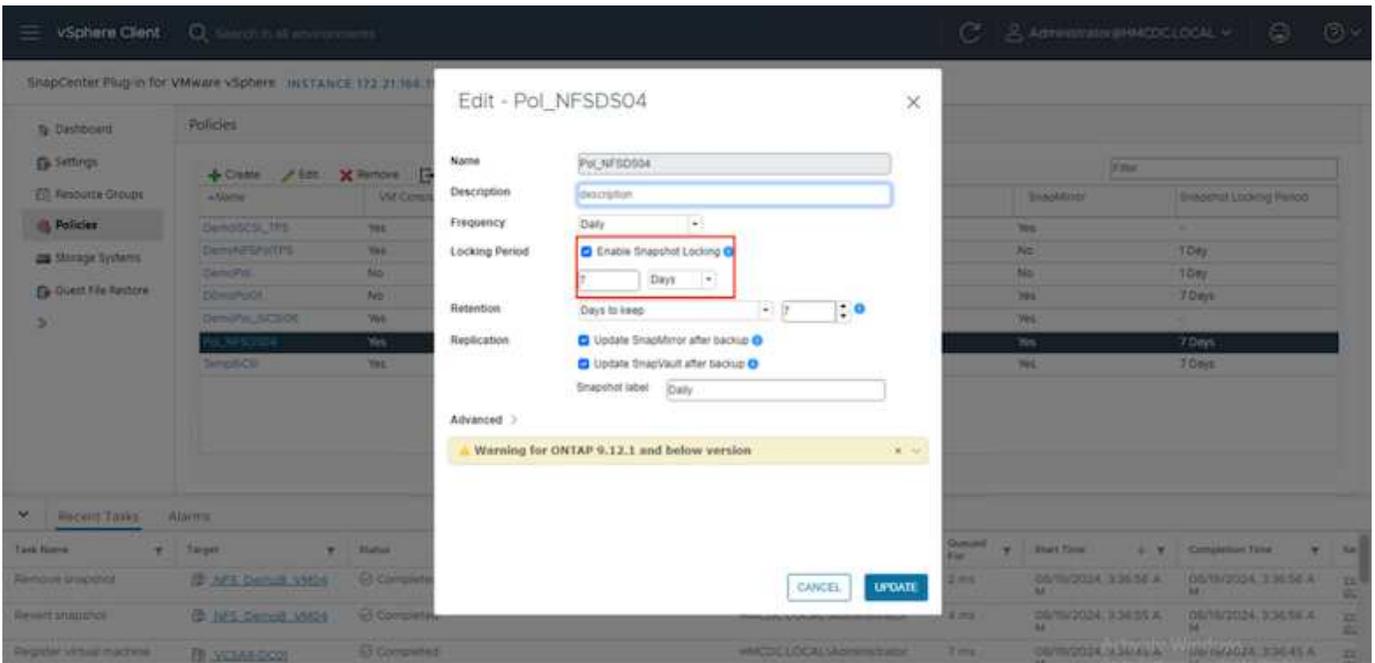
Una vez en el modo activo, se inicia a buscar la actividad anormal del volumen que podría ser potencialmente ransomware. Si se detecta una actividad anormal, se realiza inmediatamente una copia snapshot automática que proporciona un punto de restauración lo más cercano posible a la infección del archivo. ARP puede detectar cambios en las extensiones de archivos específicas de la máquina virtual en un volumen NFS ubicado fuera de la máquina virtual cuando se agrega una nueva extensión al volumen cifrado o se modifica la extensión de un archivo.



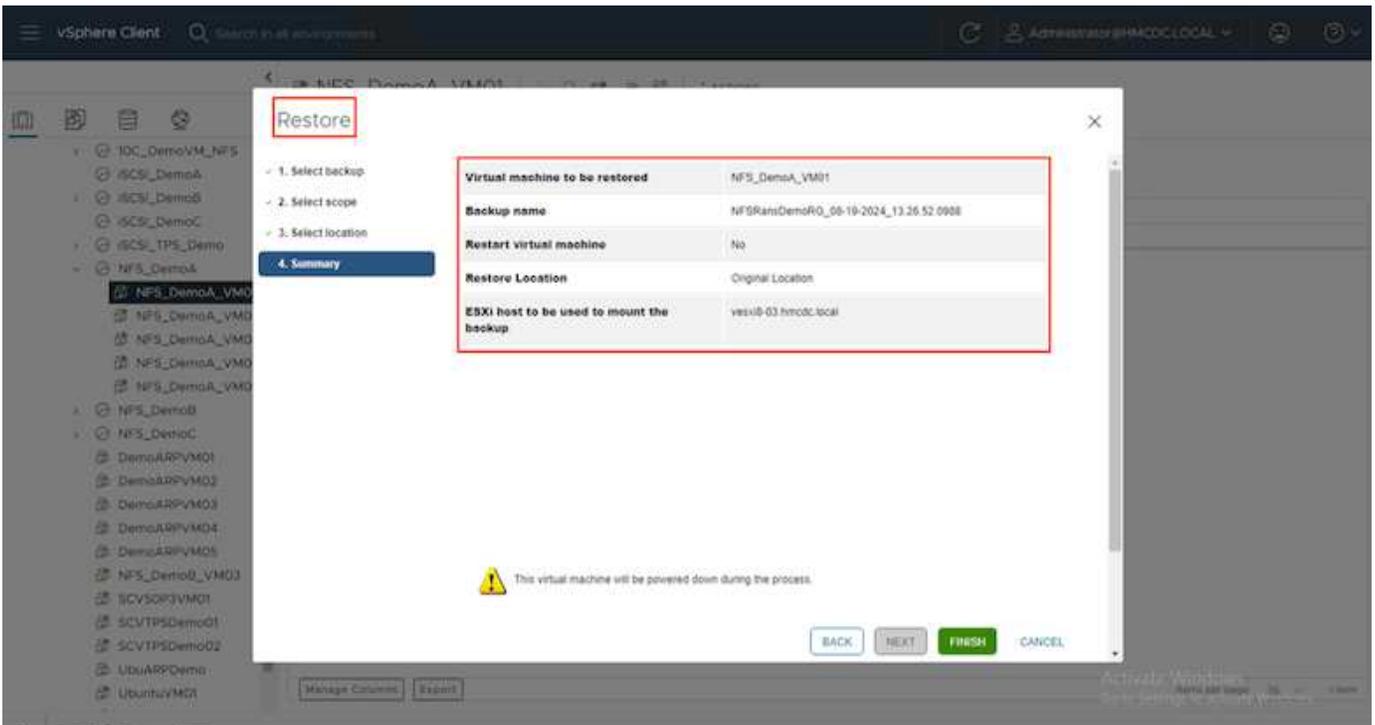
Si un ataque de ransomware se dirige a la máquina virtual (VM) y altera los archivos dentro de la máquina virtual sin hacer cambios fuera de la máquina virtual, la protección avanzada contra ransomware (ARP) seguirá detectando la amenaza si la entropía predeterminada de la máquina virtual es baja, por ejemplo, para tipos de archivos como .txt, .docx o .mp4. Aunque ARP crea una instantánea de protección en este escenario, no genera una alerta de amenaza porque las extensiones de archivo fuera de la VM no se han manipulado. En tales escenarios, las capas iniciales de defensa identificarían la anomalía, sin embargo ARP ayuda en la creación de una instantánea basada en la entropía.

Para obtener información detallada, consulte la sección “ARP and Virtual Machines” en ["Casos de uso y consideraciones ARP"](#).

Al pasar de los archivos a los datos de backup, los ataques de ransomware se dirigen cada vez más a los backups y los puntos de recuperación de snapshots 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 NetApp SnapShot™"](#).



Estas copias de SnapVault no se pueden eliminar ni modificar por atacantes de ransomware ni administradores malintencionados, por lo que están disponibles incluso después de un ataque. Si el almacén de datos o las máquinas virtuales específicas se ven afectados, SnapCenter puede recuperar los datos de máquinas virtuales en segundos, lo que minimiza el tiempo de inactividad de la organización.



La prueba anterior demuestra cómo el almacenamiento de ONTAP suma una capa adicional a las técnicas existentes, con lo que mejora la prueba del entorno para el futuro.

Para obtener más información, consulte la guía de ["Soluciones de NetApp para ransomware"](#).

Ahora, si todo esto necesita orquestarse e integrarse con herramientas de SIEM, se puede usar un servicio OFFTAP como la protección contra ransomware de BlueXP . Se trata de un servicio diseñado para proteger

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 el almacenamiento NFS local.

En este ejemplo, el almacén de datos NFS «src_nfs_DS04» está protegido con protección contra ransomware de BlueXP .

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	
Src_nfs_ds02	VM datastore	GISABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Draas_src_test_3130	VM file share	GISABXPConn	Standard	At risk	None	None	None	n/a	Protect
Nfsds02zrp_804	VM file share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection
Draas_src_7027	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_vol01_7948	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_ds03	VM datastore	GISABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	Protect
Src_nfs_ds04	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Src_nfs_ds04	File share	GISABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	Edit protection
Testvol_1787	File share	GISABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	Edit protection
Nfsarpdemo02_3419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection

Datastore protected and No Alerts reported

✔ **Protected**
 Protection health
[Edit protection](#)

Standard Importance

These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

- Pol_NFSDS04 Snapshot policy
- 1 Year Daily LTR Backup policy

VM datastore

Location: urn:acvs:scvmUI:Resou...

vCenter server: vvcas01-01.hmcidc.local

Connector: GISABXPConn

Storage

Cluster id: add38d26-348c-11ef-8...

Working Env name: NTAP915_Src

Storage VM name: svm_NFS

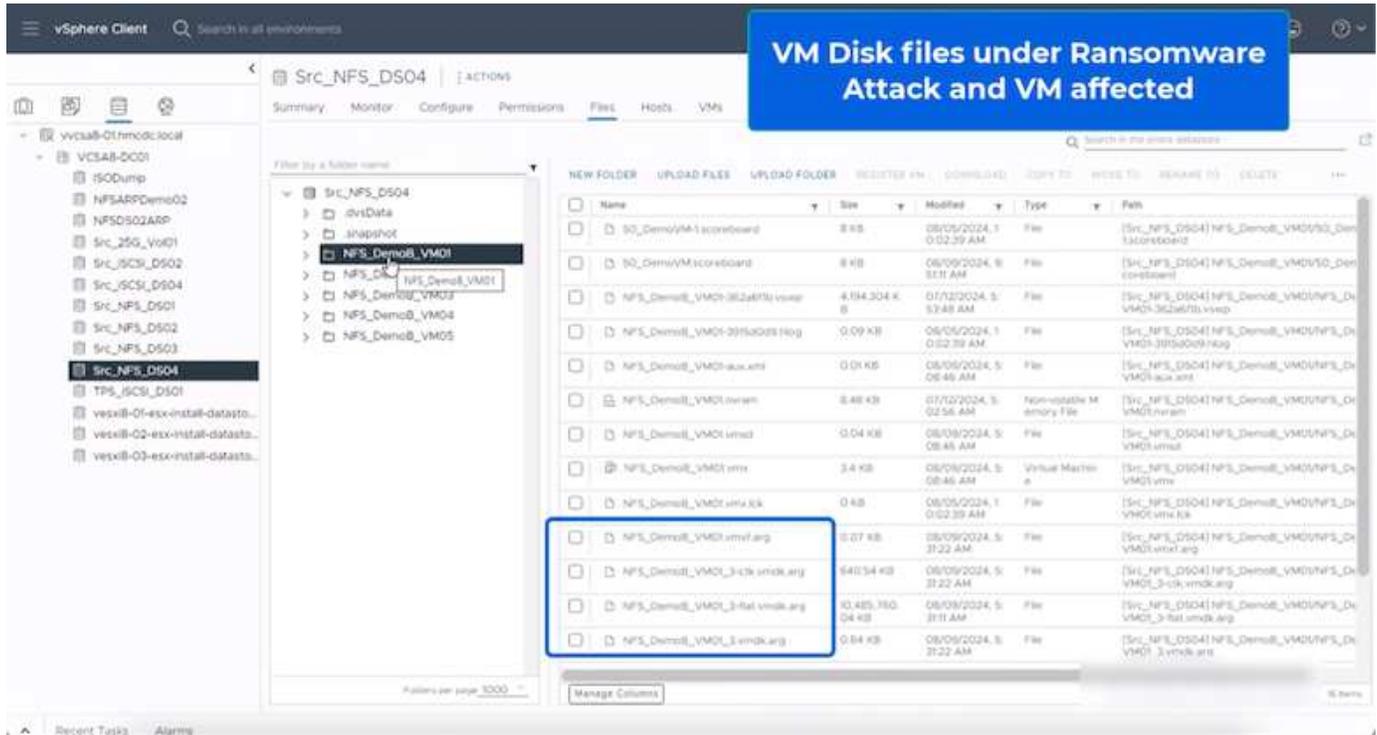
Volume name: Src_NFS_DS04

Used size: 29 GiB

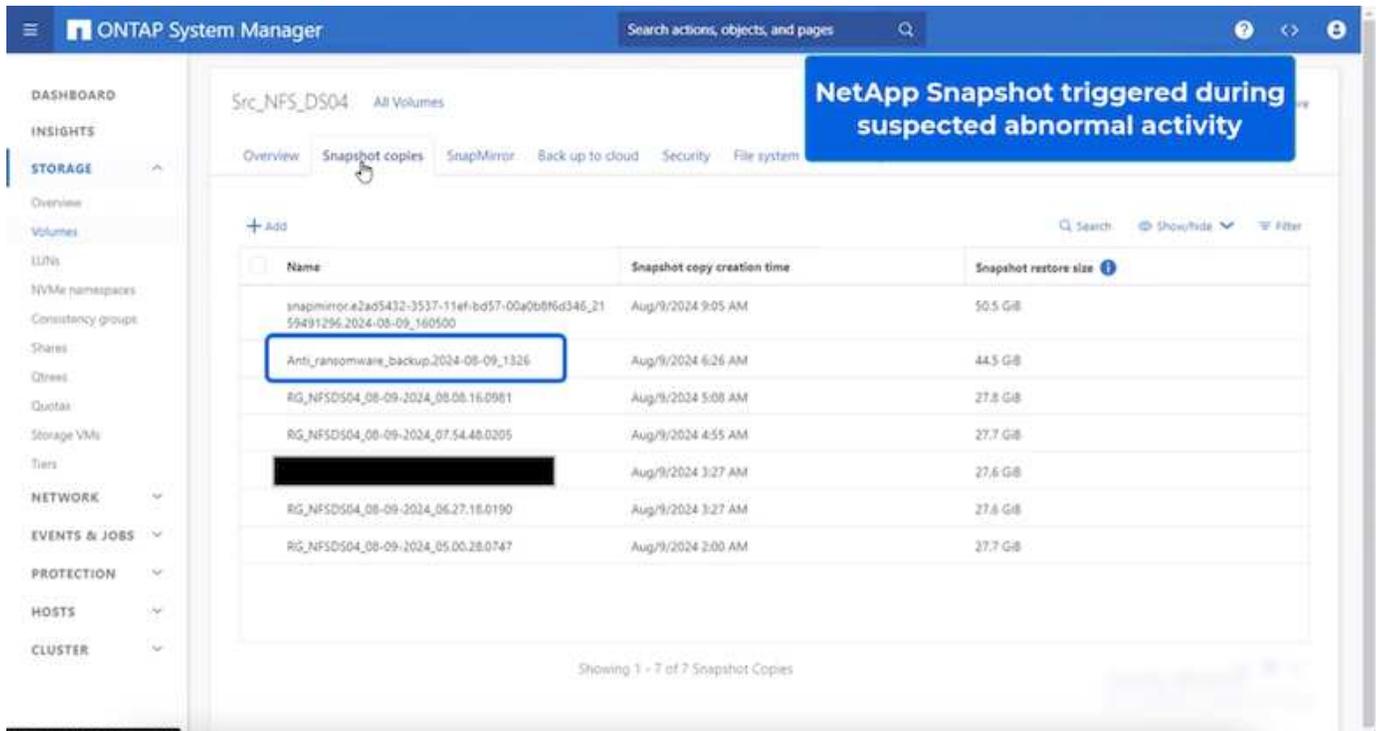
Para obtener información detallada sobre cómo configurar la protección contra ransomware de BlueXP , consulte "Configura la protección frente al ransomware de BlueXP" y "Configura las opciones de protección

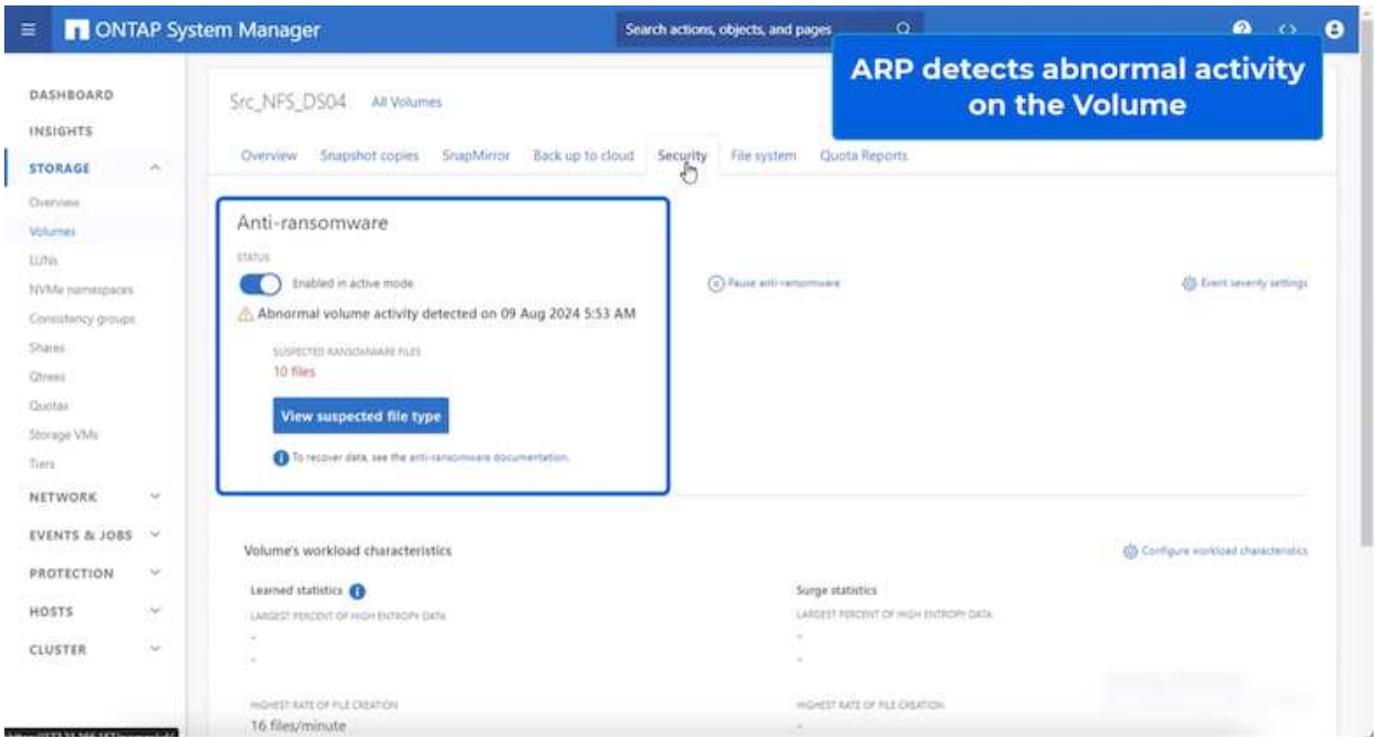
contra ransomware de BlueXP".

Es hora de caminar a través de esto con un ejemplo. En este tutorial, el almacén de datos "src_nfs_DS04" se ve afectado.

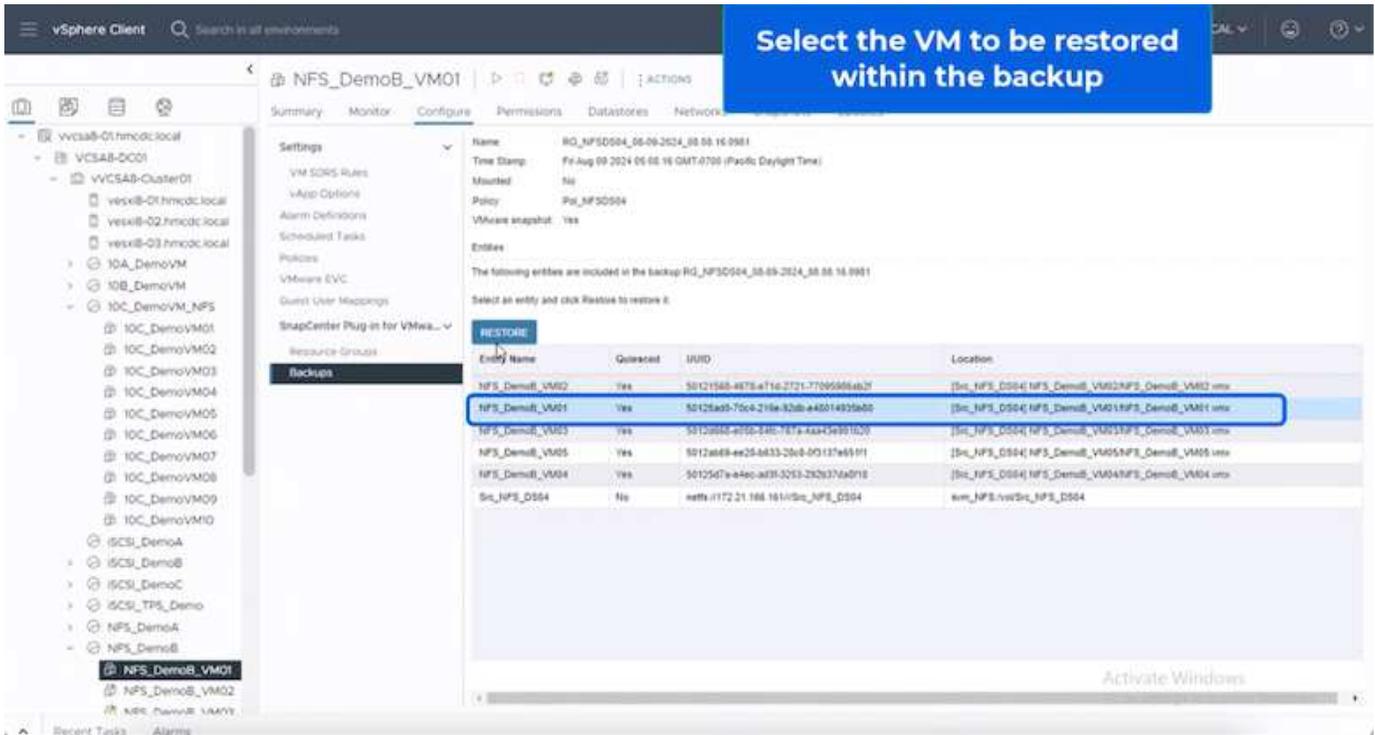


ARP activó inmediatamente una instantánea en el volumen después de la detección.





Una vez que se ha completado el análisis forense, las restauraciones pueden realizarse de forma rápida y sin problemas gracias a SnapCenter o la protección frente al ransomware de BlueXP . Con SnapCenter, vaya a las máquinas virtuales afectadas y seleccione la snapshot que desee restaurar.

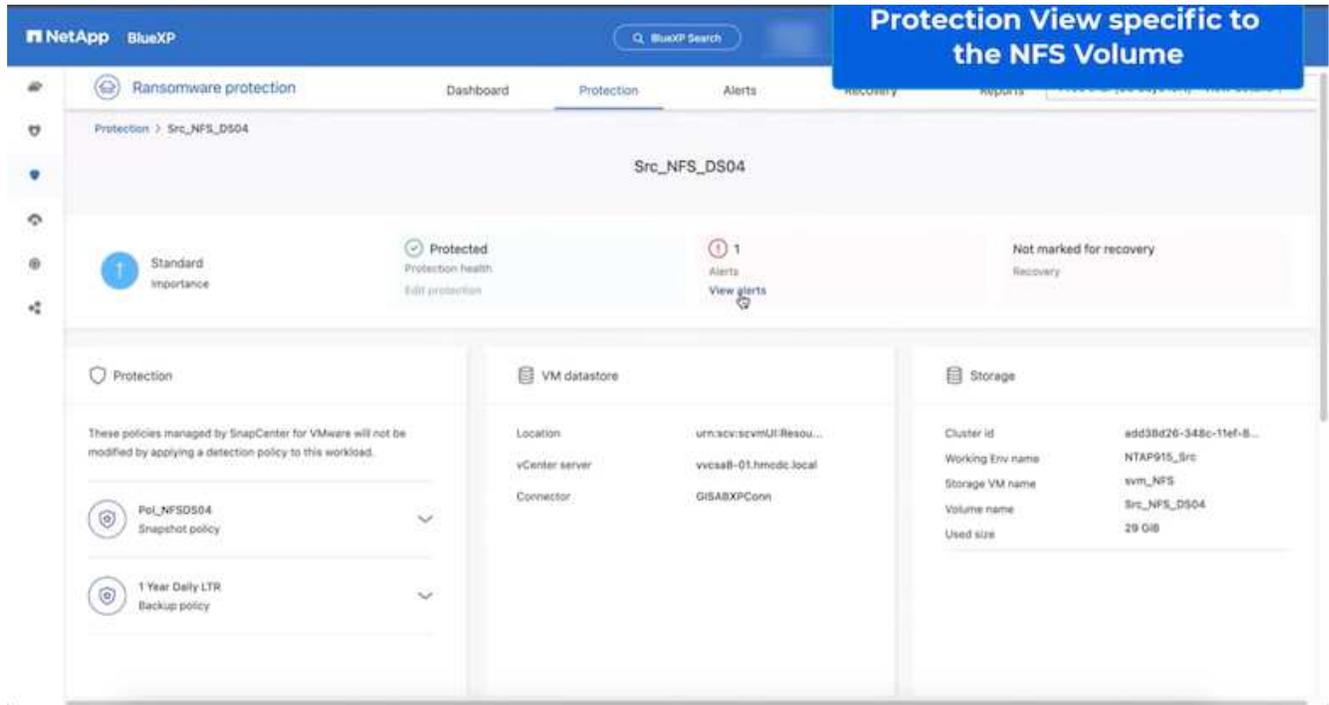


Esta sección muestra cómo la protección contra ransomware de BlueXP orquesta la recuperación de un incidente de ransomware en el que los archivos de VM están cifrados.

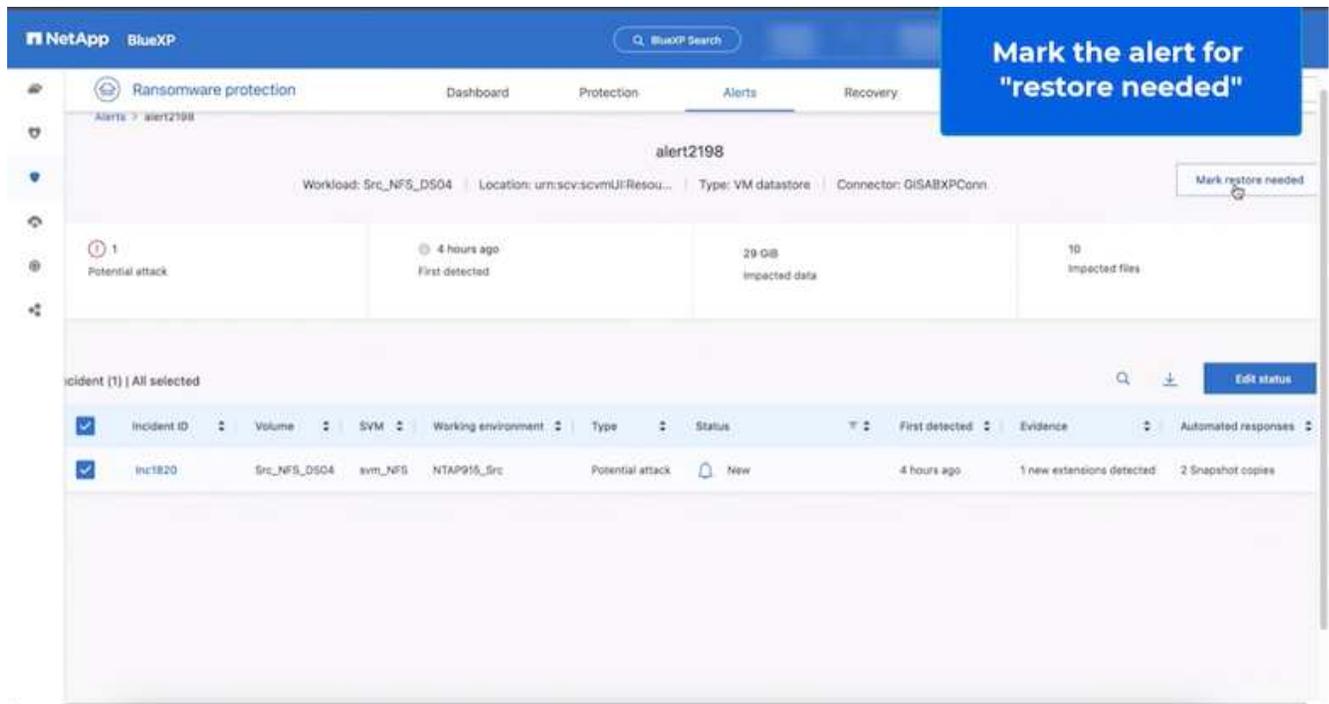


Si SnapCenter gestiona la máquina virtual, la protección frente al ransomware de BlueXP restaura la máquina virtual a su estado anterior mediante el proceso consistente con la máquina virtual.

1. Acceda a la protección contra ransomware de BlueXP y aparece una alerta en la consola de protección contra ransomware de BlueXP .
2. Haga clic en la alerta para revisar los incidentes en ese volumen específico para la alerta generada



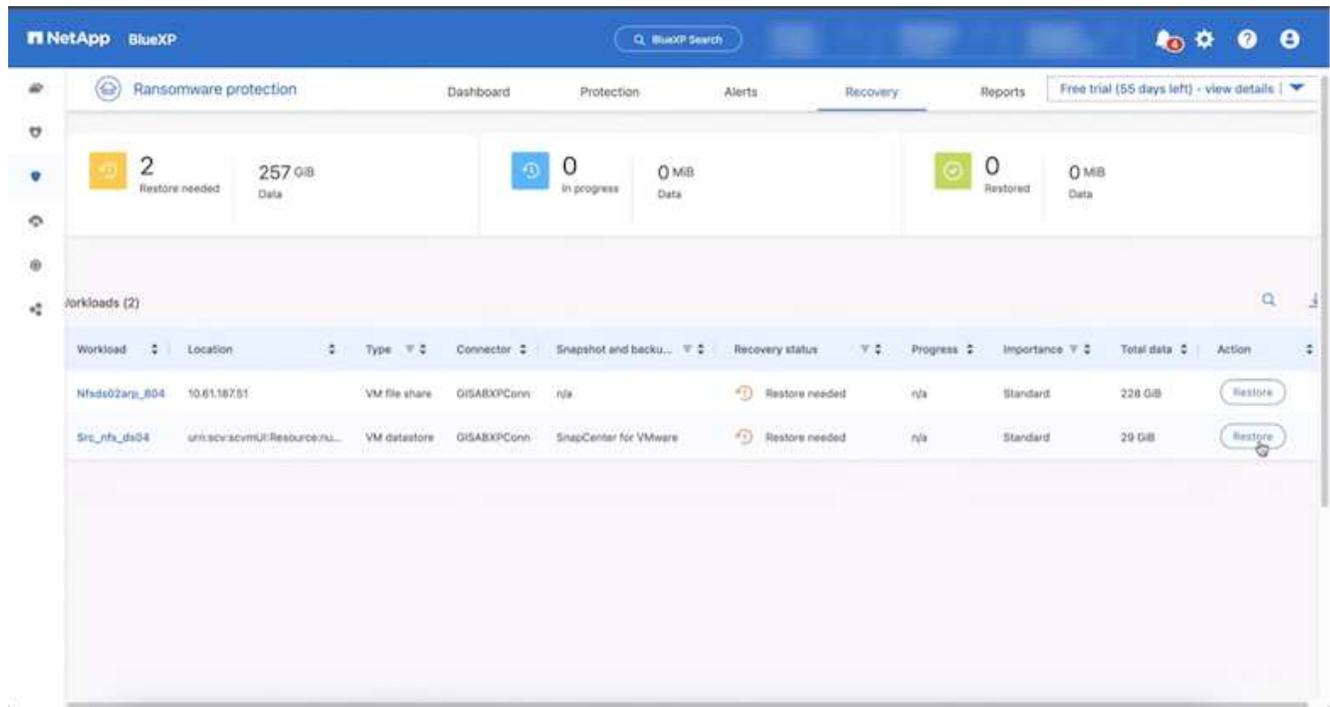
3. Marque el incidente de ransomware como listo para la recuperación (después de que se neutralicen los incidentes) seleccionando «Mark restore needed» (Mark restore needed).



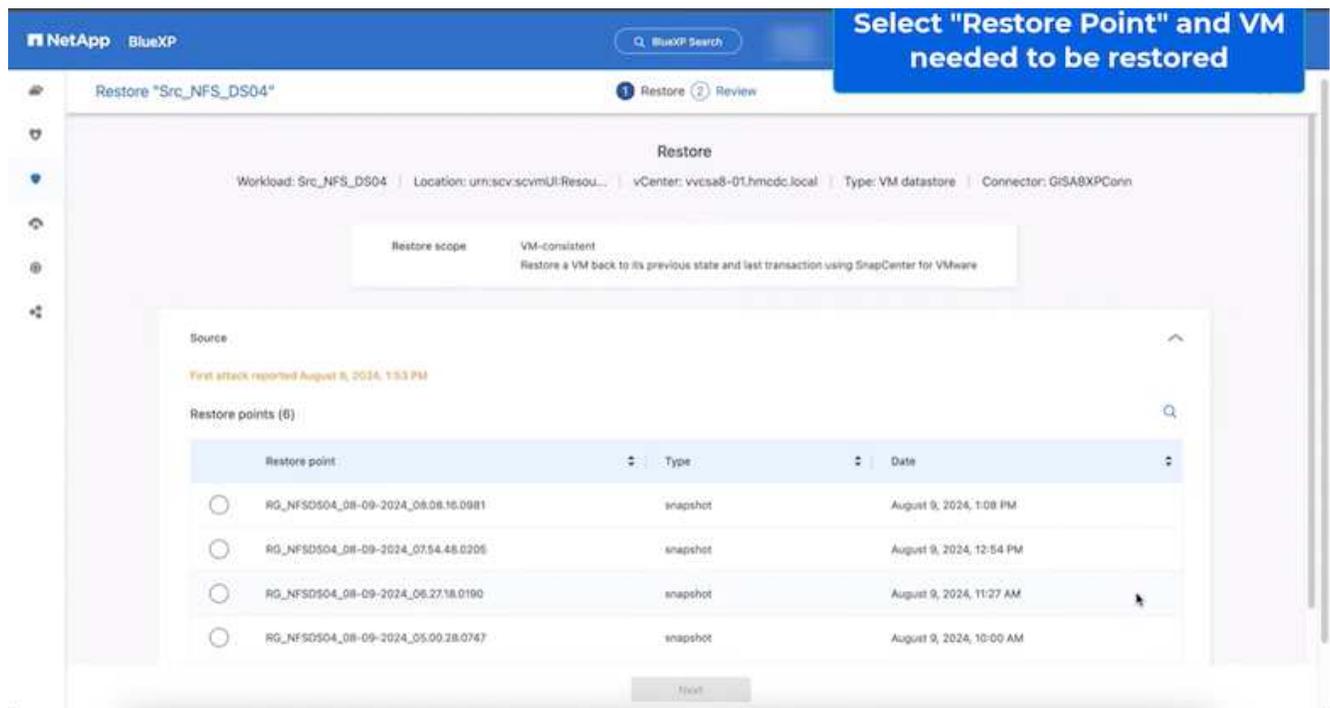


La alerta se puede descartar si el incidente resulta ser falso positivo.

- Tengo que acceder a la pestaña Recovery y revisar la información de la carga de trabajo en la página Recovery y seleccionar el volumen del almacén de datos que está en el estado «Restore needed» y seleccionar Restore.

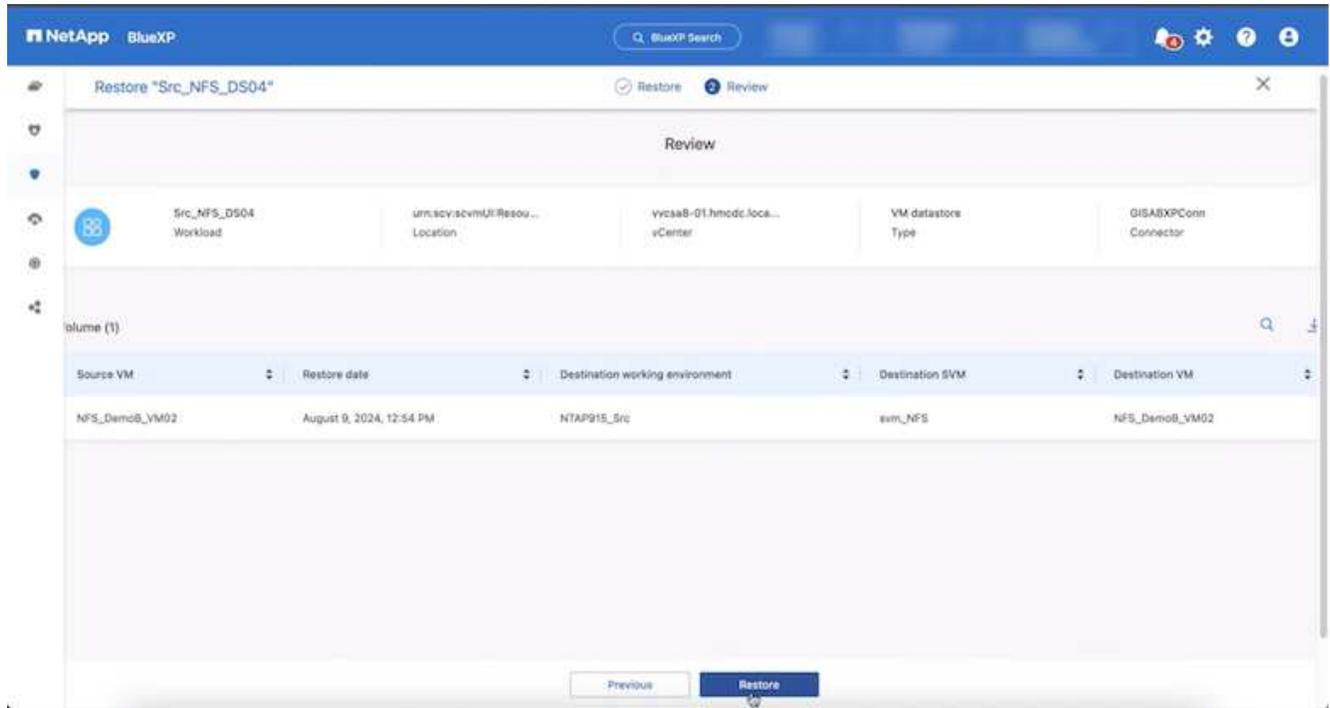


- En este caso, el ámbito de la restauración es «por equipo virtual» (para SnapCenter en los equipos virtuales, el ámbito de la restauración se establece «por equipo virtual»).

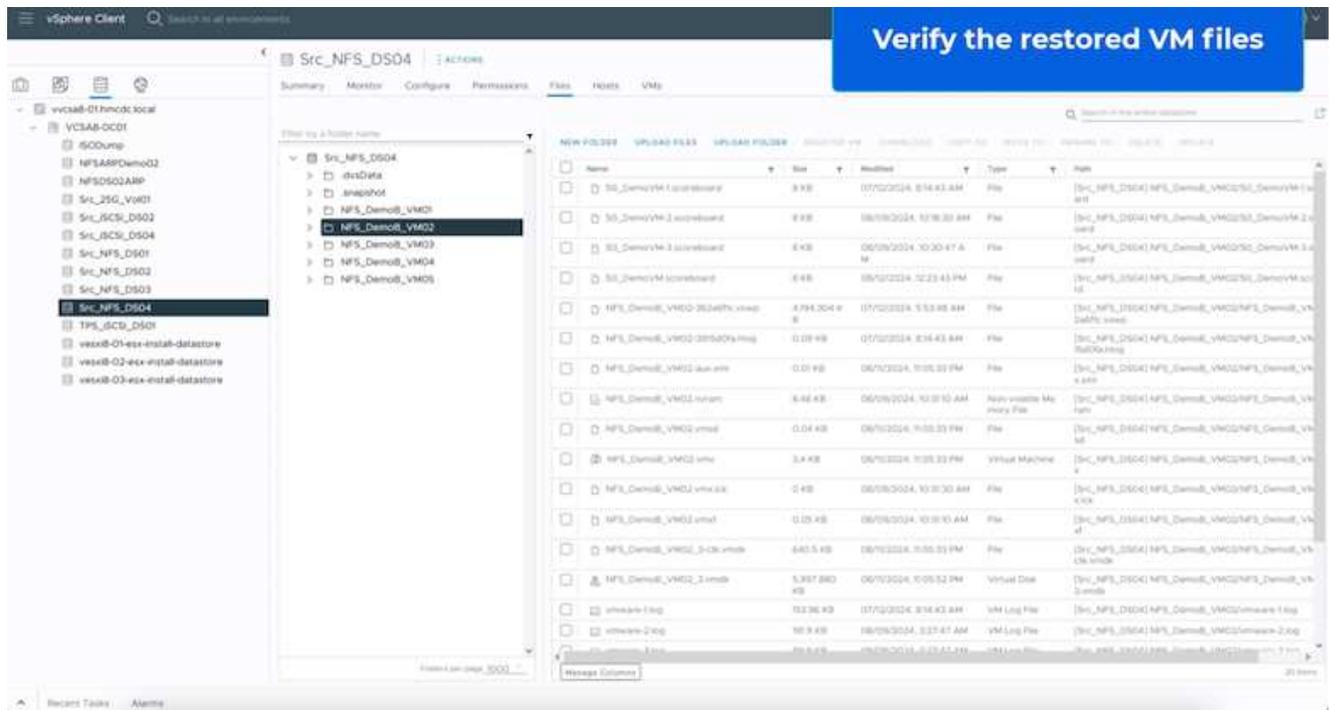


- Elija el punto de restauración que desea utilizar para restaurar los datos y seleccione Destino y haga clic

en Restaurar.



7. En el menú superior, seleccione Recovery para revisar la carga de trabajo en la página Recovery, en la que el estado de la operación se mueve por los estados. Una vez completada la restauración, los archivos del equipo virtual se restauran como se muestra a continuación.



La recuperación se puede llevar a cabo desde SnapCenter para VMware o desde el complemento SnapCenter según la aplicación.

La solución de NetApp proporciona varias herramientas eficaces para la visibilidad, la detección y la

corrección, lo que le ayuda a detectar el ransomware de forma temprana, prevenir esta propagación y recuperarse rápidamente, si es necesario, para evitar costosos tiempos de inactividad. Las soluciones tradicionales de defensa en capas siguen siendo comunes, como las que utilizan las soluciones de terceros y de socios para la visibilidad y la detección. La corrección efectiva sigue siendo una parte crucial de la respuesta a cualquier amenaza.

VMware Virtual Volumes con ONTAP

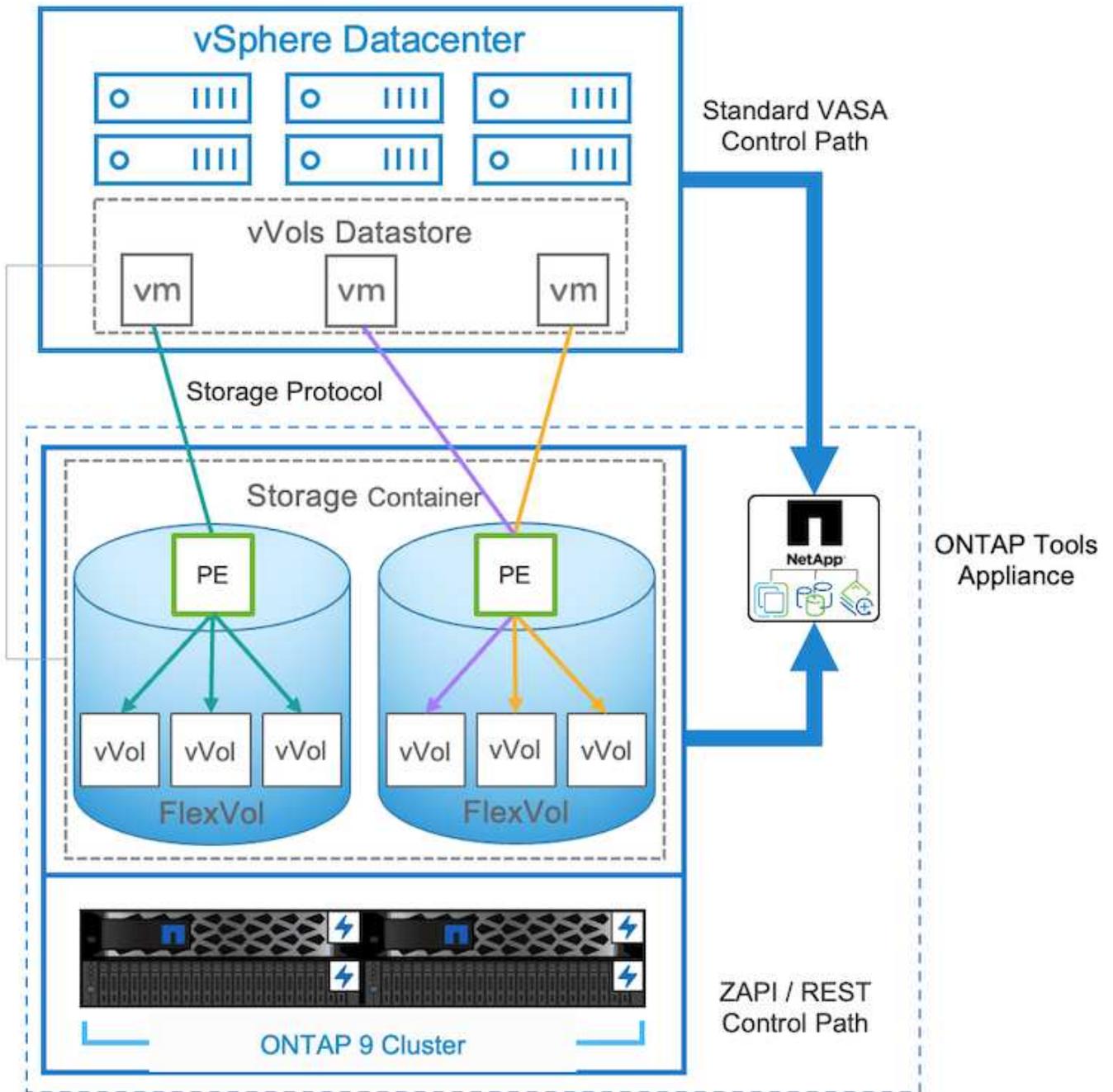
VMware Virtual Volumes (vVols) hace posible que los requisitos específicos de las aplicaciones dirijan las decisiones de aprovisionamiento de almacenamiento al tiempo que se aprovecha el amplio conjunto de funcionalidades que proporcionan los arrays de almacenamiento. La API de vSphere for Storage Awareness (VASA) facilita que un administrador de máquinas virtuales utilice cualquier capacidad de almacenamiento necesaria para aprovisionar máquinas virtuales sin tener que interactuar con su equipo de almacenamiento. Antes de VASA, los administradores de máquinas virtuales podían definir políticas de almacenamiento de máquinas virtuales, pero debían trabajar con sus administradores de almacenamiento para identificar los almacenes de datos adecuados, a menudo mediante la documentación o las convenciones de nomenclatura. Con VASA, los administradores de vCenter con los permisos adecuados pueden definir una serie de funcionalidades de almacenamiento que los usuarios de vCenter pueden usar luego para aprovisionar máquinas virtuales. La asignación entre la política de almacenamiento de las máquinas virtuales y el perfil de funcionalidades de almacenamiento de almacenes de datos permite a vCenter mostrar una lista de almacenes de datos compatibles para su selección, además de permitir que otras tecnologías, como Aria (antes conocida como vRealize) Automation o Tanzu Kubernetes Grid, seleccionen automáticamente el almacenamiento de una política asignada. Este enfoque se conoce como gestión basada en políticas de almacenamiento. Si bien las políticas y perfiles de la capacidad de almacenamiento también se pueden utilizar con almacenes de datos tradicionales, nuestro enfoque se centra en los almacenes de datos vVols. El proveedor VASA para ONTAP se incluye como parte de las herramientas de ONTAP para VMware vSphere.

Las ventajas de tener un proveedor VASA fuera de la cabina de almacenamiento incluyen:

- Una instancia única puede gestionar varias cabinas de almacenamiento.
- El ciclo de lanzamiento no tiene por qué depender de la versión del SO de almacenamiento.
- Los recursos de la cabina de almacenamiento son mucho caros.

Cada almacén de datos VVol se respalda mediante Storage Container, que es una entrada lógica en el proveedor de VASA para definir la capacidad de almacenamiento. El contenedor de almacenamiento con las herramientas de ONTAP se crea con los volúmenes de ONTAP. El contenedor de almacenamiento se puede ampliar añadiendo volúmenes de ONTAP en la misma SVM.

El extremo de protocolo (PE) se gestiona principalmente mediante herramientas de ONTAP. En el caso de vVols basados en iSCSI, se crea un PE para cada volumen ONTAP que forma parte de ese contenedor de almacenamiento o almacén de datos VVOL. El PE para iSCSI es un LUN de pequeño tamaño (4MiB para 9.x y 2GiB para 10.x) presentado al host vSphere y se aplican políticas multivía al PE.



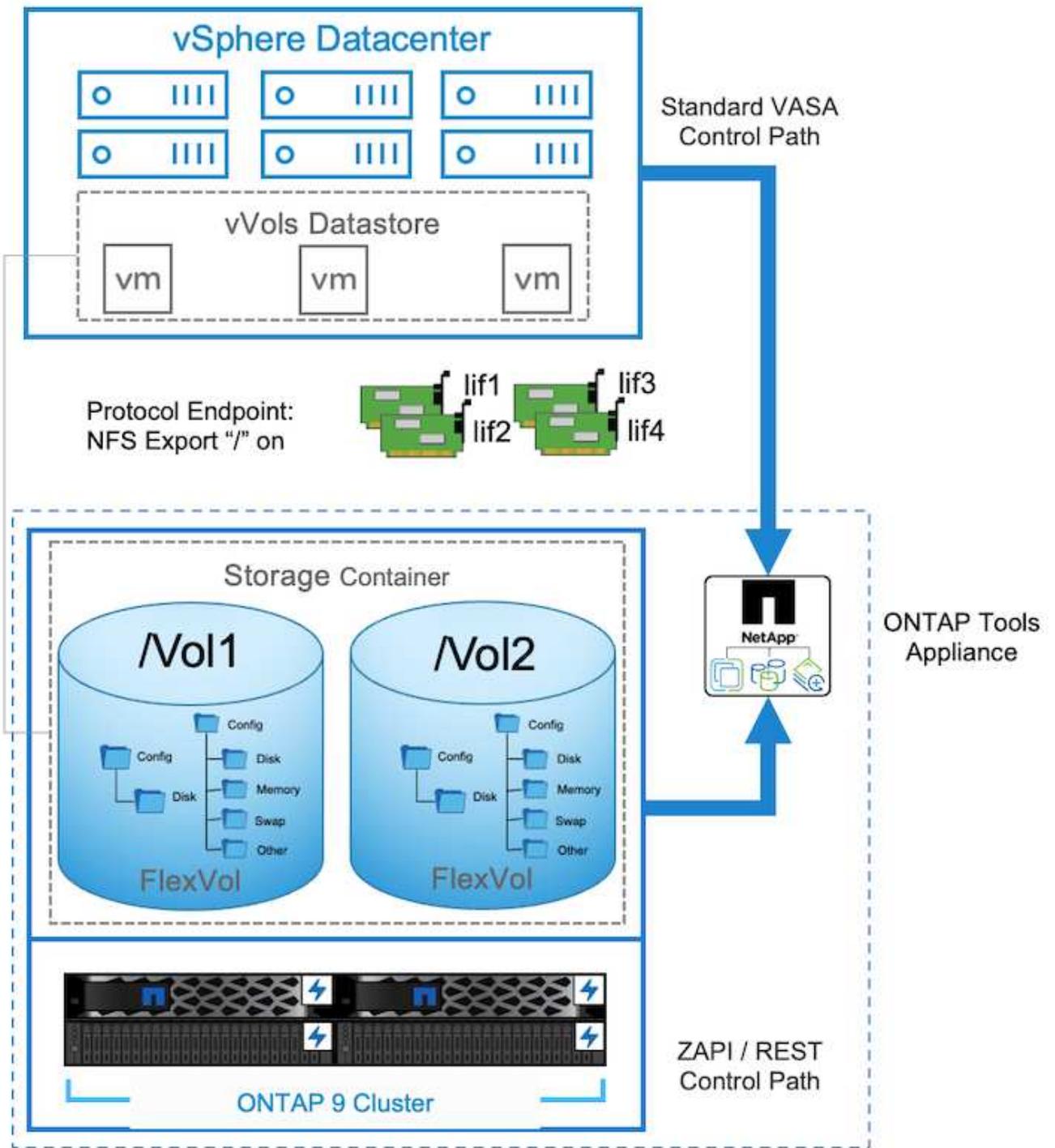
```

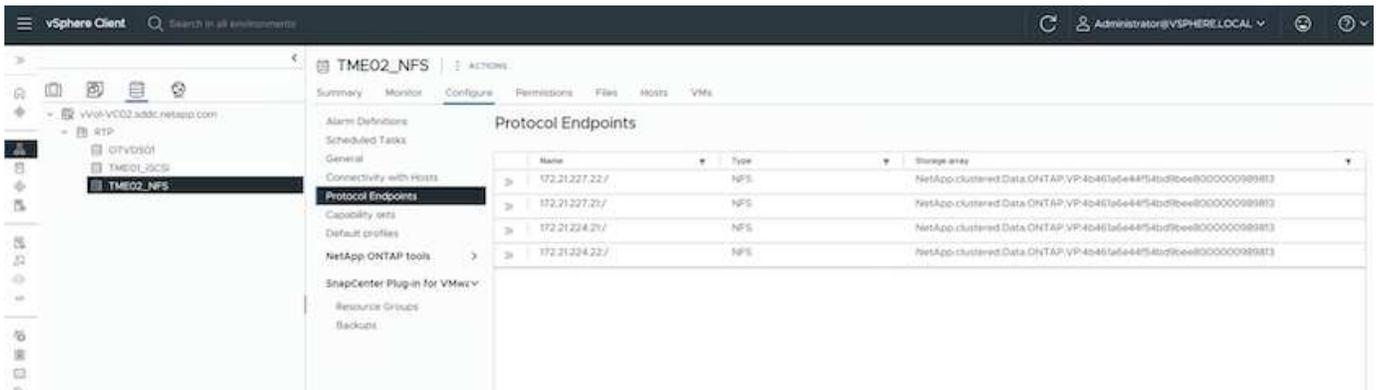
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint -fields size
vserver path size
-----
zoneb /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217 2GB
zoneb /vol/TME01_iSCSI_01/vvolPE-1723727751956 4MB
zoneb /vol/TME01_iSCSI_02/vvolPE-1723727751970 4MB
4 entries were displayed.

```

Para NFS, se crea un PE para la exportación del sistema de archivos raíz con cada LIF de datos NFS en la

SVM en la que reside el contenedor de almacenamiento o el almacén de datos VVOL.





Las herramientas de ONTAP gestionan el ciclo de vida de PE y también para la comunicación con hosts de vSphere con la expansión y la reducción del clúster de vSphere. La API de herramientas de ONTAP está disponible para integrarse con una herramienta de automatización existente.

Actualmente, las herramientas de ONTAP para VMware vSphere están disponibles con dos versiones.

Herramientas de ONTAP 9.x

- Cuando se requiere la compatibilidad con VVOL para NVMe/FC
- Requisitos normativos de la UE o federales de EE. UU
- Más casos de uso integrados con el plugin de SnapCenter para VMware vSphere

Herramientas de ONTAP 10.x

- Alta disponibilidad
- Soporte para múltiples usuarios
- Gran escala
- Soporte de sincronización activa de SnapMirror para almacén de datos VMFS
- Próxima integración para determinados casos de uso con el complemento de SnapCenter para VMware vSphere

¿Por qué vVols?

Virtual Volumes de VMware (vVols) ofrece los siguientes beneficios:

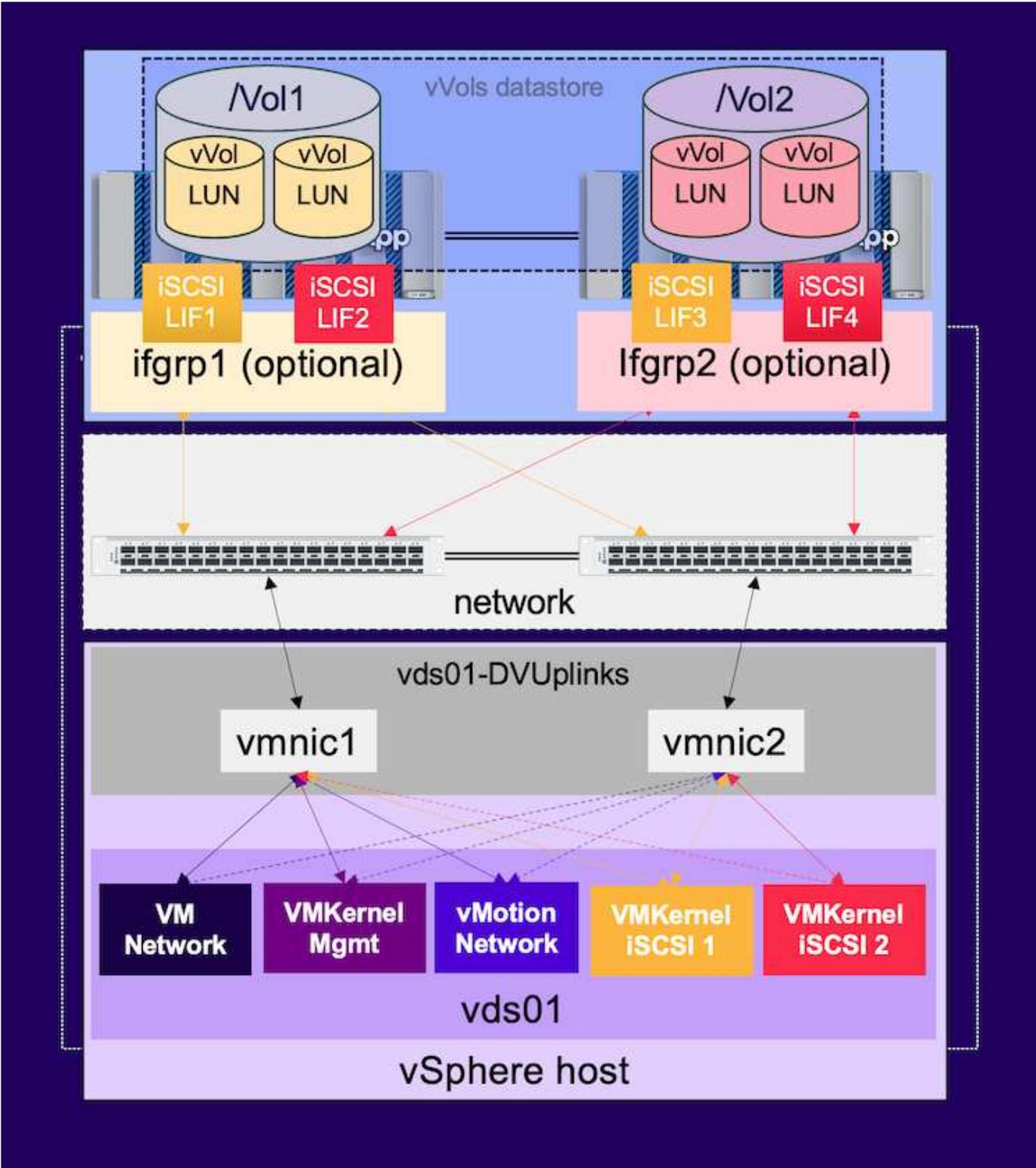
- Aprovisionamiento simplificado (no hay que preocuparse por los límites máximos de LUN por host vSphere ni es necesario crear las exportaciones NFS para cada volumen).
- Minimiza el número de rutas de iSCSI/FC (para VVOL basados en SCSI en bloques)
- Las snapshots, clones y otras operaciones de almacenamiento normalmente se descargan en la cabina de almacenamiento y se ejecutan mucho más rápido.
- Migraciones de datos simplificadas de los equipos virtuales (no es necesario coordinarse con otros propietarios de máquinas virtuales en el mismo LUN)
- Las políticas de calidad de servicio se aplican a nivel de disco de máquina virtual, en lugar de a nivel de volumen.
- Simplicidad operativa (los proveedores de almacenamiento ofrecen sus funciones diferenciadas en el proveedor de VASA)

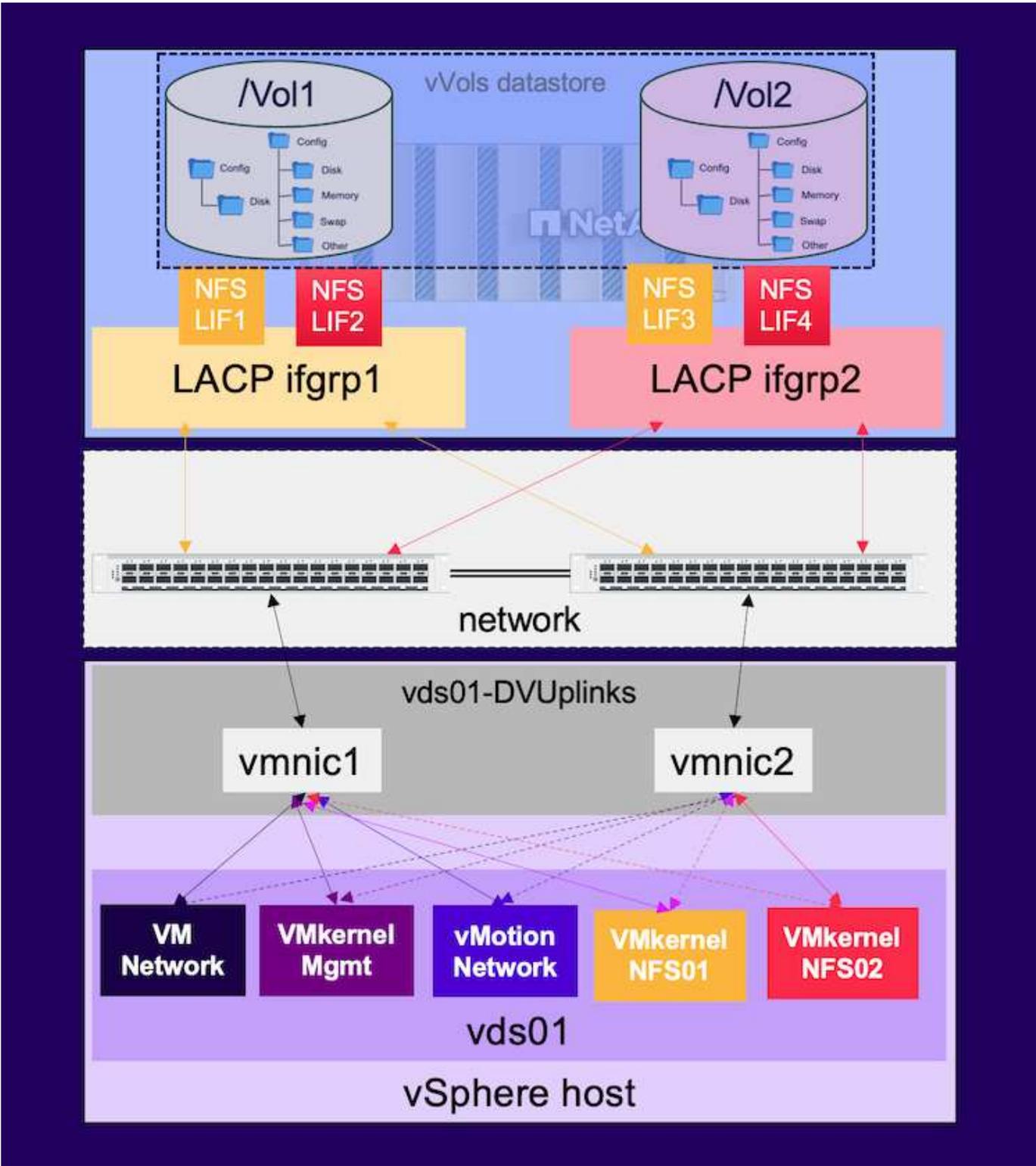
- Admite una gran escala de máquinas virtuales.
- Soporte de replicación de VVol para migrar entre vCenter.
- Los administradores de almacenamiento tienen la opción de supervisar a nivel de disco de máquina virtual.

Opciones de conectividad

El entorno de estructura doble se suele recomendar para que las redes de almacenamiento aborden la alta disponibilidad, el rendimiento y la tolerancia a fallos. Los vVols son compatibles con iSCSI, FC, NFSv3 GbE y NVMe/FC. NOTA: Consulte "[Herramienta de matriz de interoperabilidad \(IMT\)](#)" la versión compatible de la herramienta ONTAP

La opción de conectividad sigue siendo consistente con las opciones de almacén de datos VMFS o NFS. A continuación se muestra un ejemplo de red vSphere de referencia para iSCSI y NFS.





Aprovisionar mediante las herramientas de ONTAP para VMware vSphere

El almacén de datos de VVOL se puede aprovisionar de manera similar a un almacén de datos VMFS o NFS utilizando herramientas de ONTAP. Si el complemento de herramientas de ONTAP no está disponible en la interfaz de usuario del cliente de vSphere, consulte la sección Cómo empezar a continuación.

Con las herramientas de ONTAP 9,13

1. Haga clic con el botón derecho en el clúster o el host de vSphere y seleccione Provision Datastore en NetApp ONTAP tools.
2. Mantenga el tipo como vVols, proporcione el nombre para el almacén de datos y seleccione el protocolo deseado

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

General

Specify the details of the datastore to provision ⓘ

Provisioning destination: Cluster01 BROWSE

Type: NFS VMFS vVols

Name: TME01_ISCSI

Description:

Protocol: NFS ISCSI FC / FCoE NVMe/FC

CANCEL NEXT

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

General

Specify the details of the datastore to provision ⓘ

Provisioning destination: Cluster01 BROWSE

Type: NFS VMFS vVols

Name: TME02_NFS

Description:

Protocol: NFS ISCSI FC / FCoE NVMe/FC

CANCEL NEXT

3. Seleccione el perfil de funcionalidad de almacenamiento deseado, seleccione el sistema de almacenamiento y la SVM.

New Datastore

- 1 General
- 2 Storage system**
- 3 Storage attributes
- 4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles: **Default profiles**

- Platinum_AFF_A
- Platinum_AFF_C
- Platinum_ASA_A
- Platinum_ASA_C

[Create storage capability profile](#)

Storage system:

Storage VM:

[CANCEL](#) [BACK](#) [NEXT](#)

4. Cree volúmenes de ONTAP nuevos o seleccione uno existente para el almacén de datos de VVol.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes**
- 4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
TME01_ISCSI_01	250 GB	Platinum_AFF_A	EHCAGgr01
TME01_ISCSI_02	250 GB	Platinum_AFF_A	EHCAGgr02

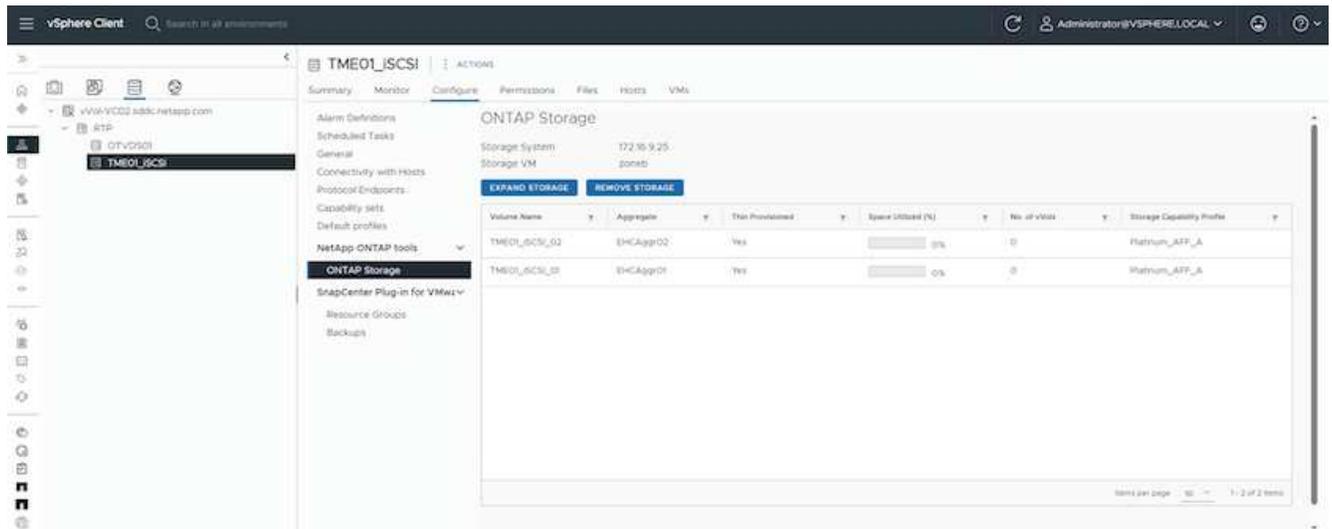
1 - 2 of 2 items

Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
<input type="text"/>	<input type="text"/>	<input type="text" value="Platinum_AFF_A"/>	<input type="text" value="EHCAGgr02 - (17109.63 Gi)"/>	<input type="text" value="Thin"/>

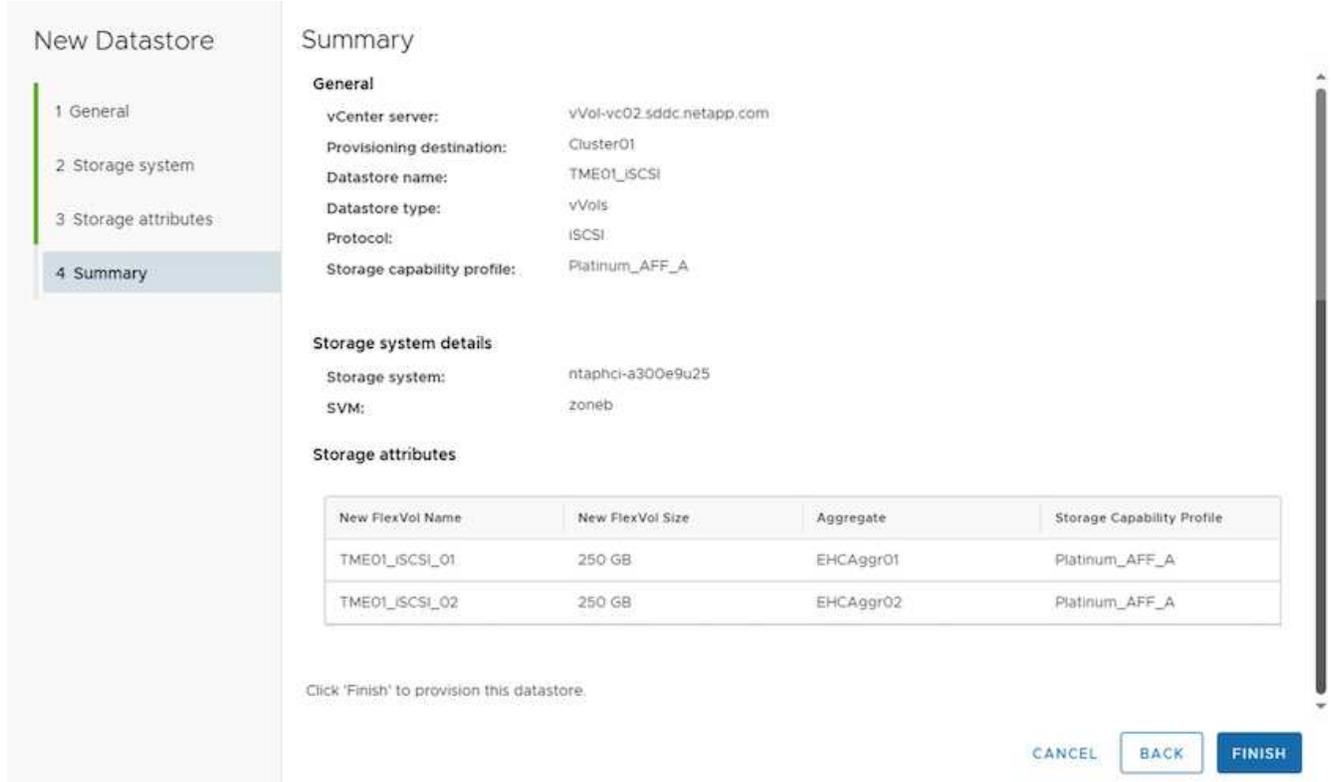
[ADD](#)

[CANCEL](#) [BACK](#) [NEXT](#)

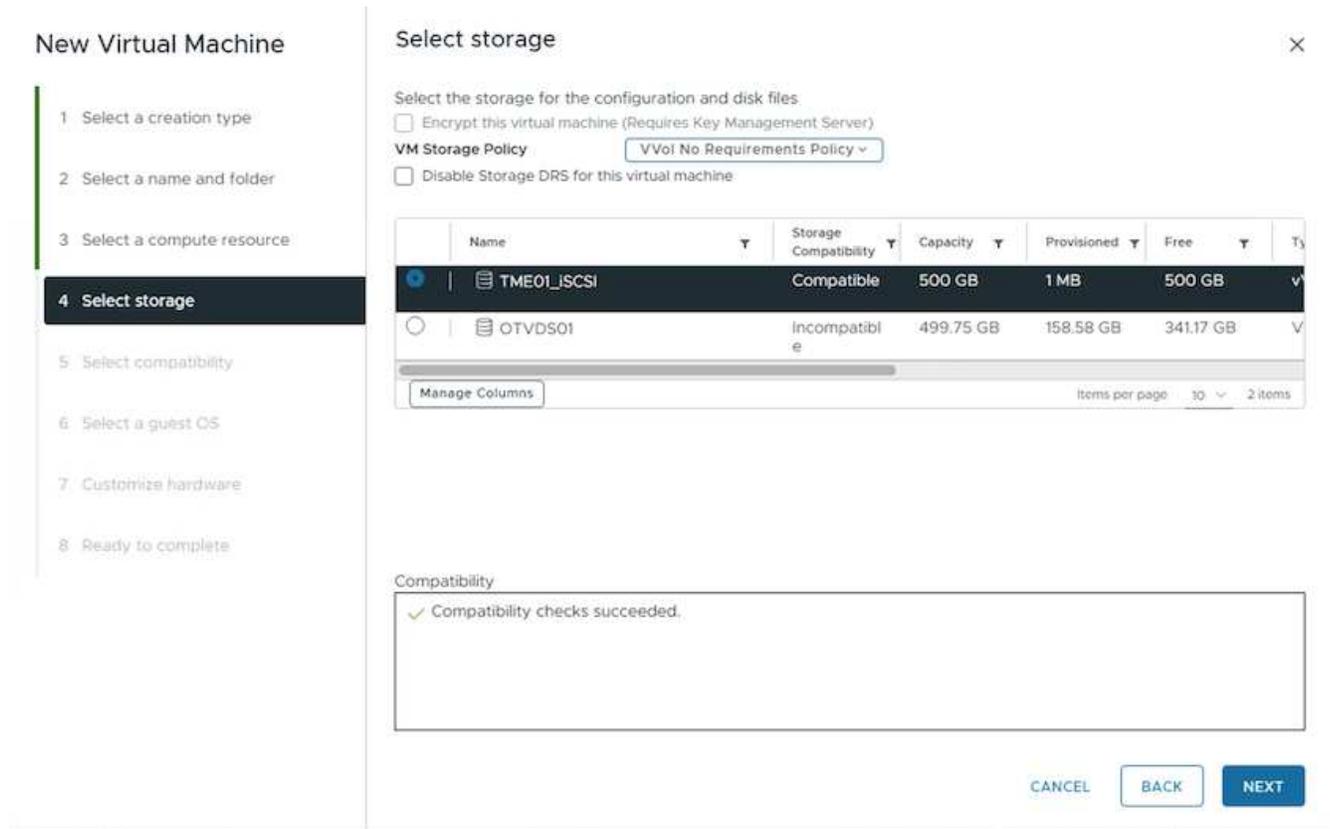
Los volúmenes de ONTAP se pueden ver o modificar más tarde desde la opción datastore.



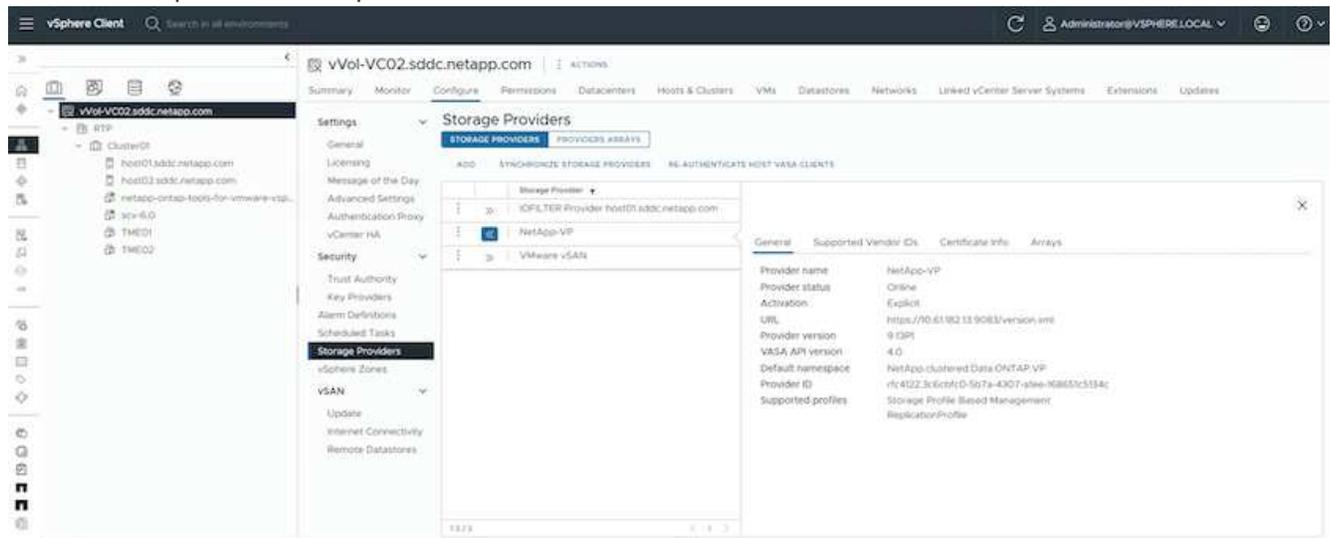
5. Revise el resumen y haga clic en On Finish para crear el almacén de datos de VVol.



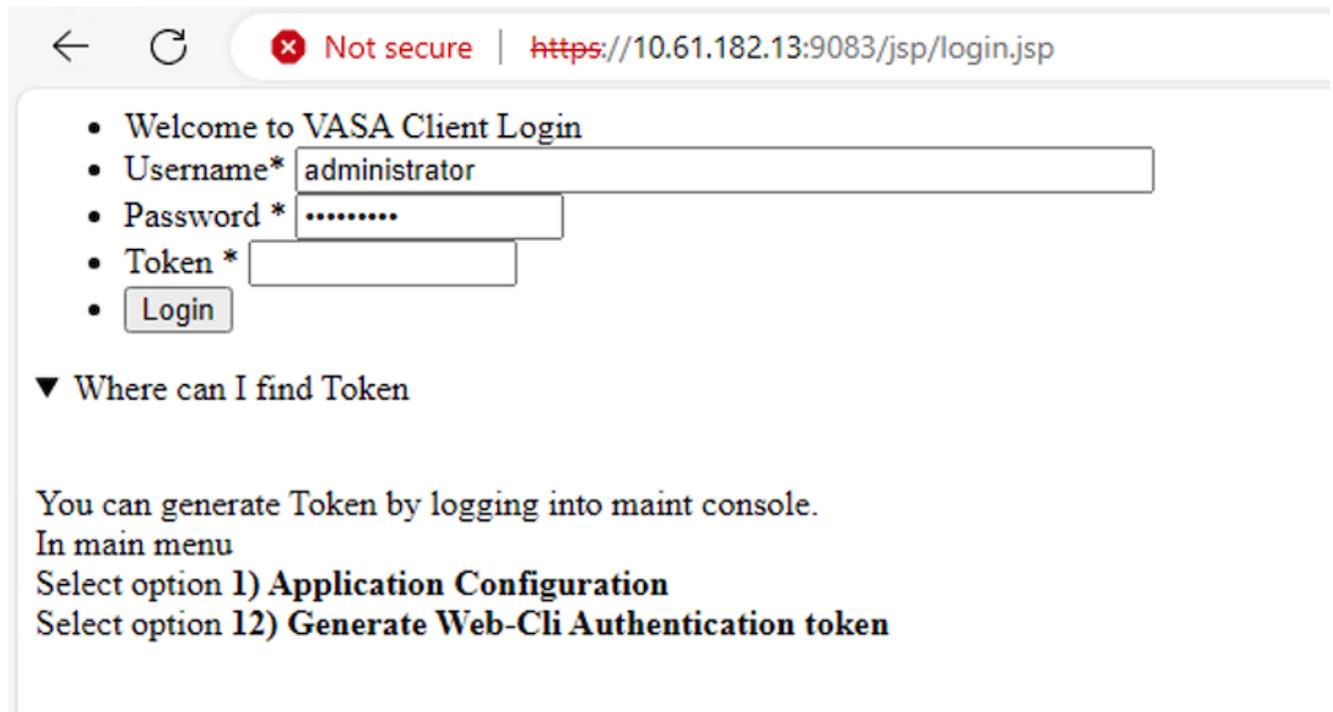
6. Una vez que se crea el almacén de datos VVol, puede consumirse igual que cualquier otro almacén de datos. A continuación se muestra un ejemplo de asignación de almacén de datos según política de almacenamiento de máquinas virtuales a una máquina virtual que se está creando.



7. Los detalles de VVol se pueden recuperar mediante una interfaz de CLI basada en web. La URL del portal es la misma que la URL del proveedor VASA sin el nombre de archivo version.xml.



La credencial debe coincidir con la información utilizada durante la provisión de herramientas de ONTAP



O utilice la contraseña actualizada con la consola de mantenimiento de las herramientas de ONTAP.

Application Configuration Menu:

- 1) Display server status summary
 - 2) Start Virtual Storage Console service
 - 3) Stop Virtual Storage Console service
 - 4) Start VASA Provider and SRA service
 - 5) Stop VASA Provider and SRA service
 - 6) Change 'administrator' user password
 - 7) Re-generate certificates
 - 8) Hard reset database
 - 9) Change LOG level for Virtual Storage Console service
 - 10) Change LOG level for VASA Provider and SRA service
 - 11) Display TLS configuration
 - 12) Generate Web-CLI Authentication token
 - 13) Start ONTAP tools plug-in service
 - 14) Stop ONTAP tools plug-in service
 - 15) Start Log Integrity service
 - 16) Stop Log Integrity service
 - 17) Change database password
-
- b) Back
 - x) Exit

Enter your choice: 12

Starting token creation
Your webcli auth token is :668826

This token is for one time use only.Its valid for 20 minutes.

Press ENTER to continue.

Seleccione Interfaz CLI basada en web.

NetApp ONTAP tools for VMware vSphere - Control Panel:

Operation	Description
Web based CLI interface	Web based access to the command line interface for administrative tasks
Inventory	Listing of all objects and information currently known in Unified Virtual Appliance database
Statistics	Listing of all counters and information regarding internal state
Right Now	See what operations are in flight right now
Logout	Logout

Build Release 9.13P1
Build Timestamp 03/08/2024 11:11:42 AM
System up since Thu Aug 15 02:23:18 UTC 2024
Current time Thu Aug 15 17:59:26 UTC 2024

Escriba el comando deseado en la lista de comandos disponibles. Para enumerar los detalles de VVol junto con información sobre almacenamiento subyacente, pruebe `vvol list -verbose=true`

```

Command: vvol list --verbose=true [Execute]
Executed:
vvol list --verbose=true
Returned:
[{"LUNID": "naa.600a0980383043595a2b506b67783041", "METADATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk", "Binds": [{"LUNID": "naa.600a0980383043595a2b506b67783041", "DATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk", "Binds": [{"LUNID": "naa.600a0980383043595a2b506b67783041", "KEY": "keyValuePairs={\"VMS_VolNameSpace\": \"vms/vol/naa.600a0980383043595a2b506b67783041\"}"}]}, {"LUNID": "naa.600a0980383043595a2b506b67783042", "METADATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk", "Binds": [{"LUNID": "naa.600a0980383043595a2b506b67783042", "KEY": "keyValuePairs={\"VMS_VolNameSpace\": \"vms/vol/naa.600a0980383043595a2b506b67783042\"}"}]}, {"LUNID": "naa.600a0980383043595a2b506b67783043", "METADATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk", "Binds": [{"LUNID": "naa.600a0980383043595a2b506b67783043", "KEY": "keyValuePairs={\"VMS_VolNameSpace\": \"vms/vol/naa.600a0980383043595a2b506b67783043\"}"}]}, {"LUNID": "naa.600a0980383043595a2b506b67783044", "METADATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783044.vmdk", "Binds": [{"LUNID": "naa.600a0980383043595a2b506b67783044", "KEY": "keyValuePairs={\"VMS_VolNameSpace\": \"vms/vol/naa.600a0980383043595a2b506b67783044\"}"}]}]}]

```

para LUN basada en LUN, también pueden utilizarse la cli o System Manager de ONTAP.

```

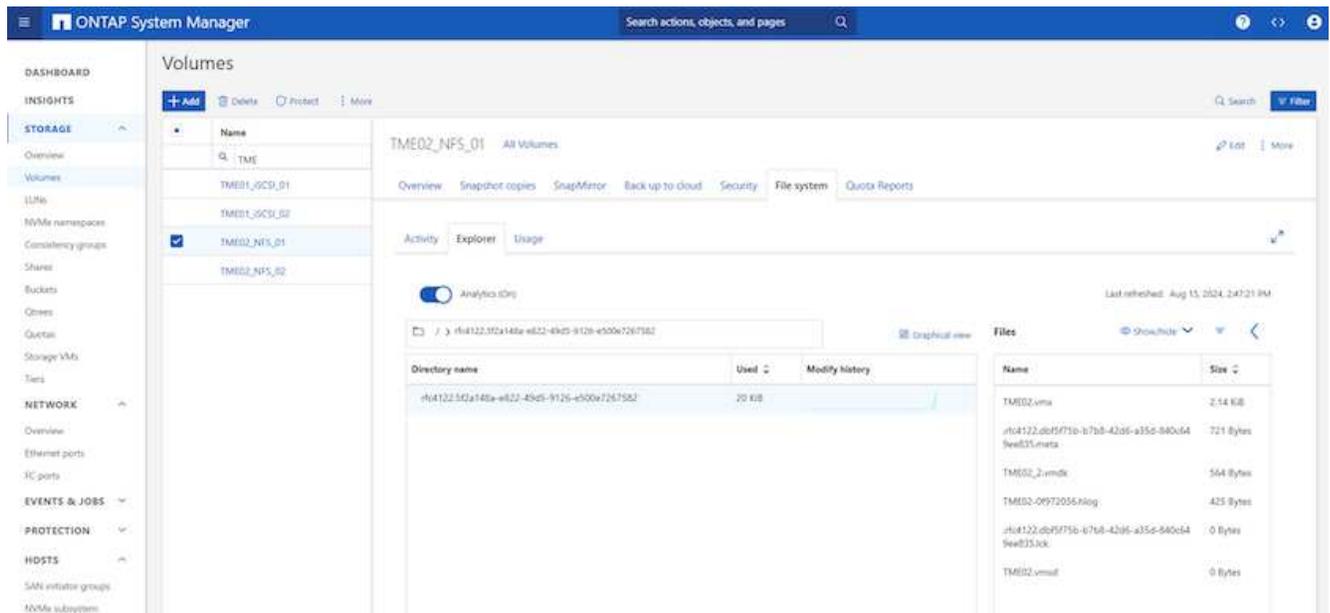
ntaphci-a300e9u25::> lun show -vserver zoneb -class vvol -fields comment,size
vserver path size comment
-----
zoneb /vol/Demo01_fv01/naa.600a0980383043595a2b506b67783038.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683735.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683736.vmdk 16GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683737.vmdk 16GB
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk
255GB TME01 - METADATA
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk
16GB TME01.vmdk - DATA
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk
16GB TME01.vmdk - DATA

```

The screenshot shows the ONTAP System Manager interface. The 'LUNs' section is active, displaying a table of LUNs. The table has columns for Name, Storage VM, Volume, Size, IOPS, Latency (ms), and Throughput (MB/s). Below the table, detailed information for a specific LUN is shown, including its status (Online), volume (TME01_iSCSI_01), description (TME01.vmdk - DATA), and snapshot policy (Protected).

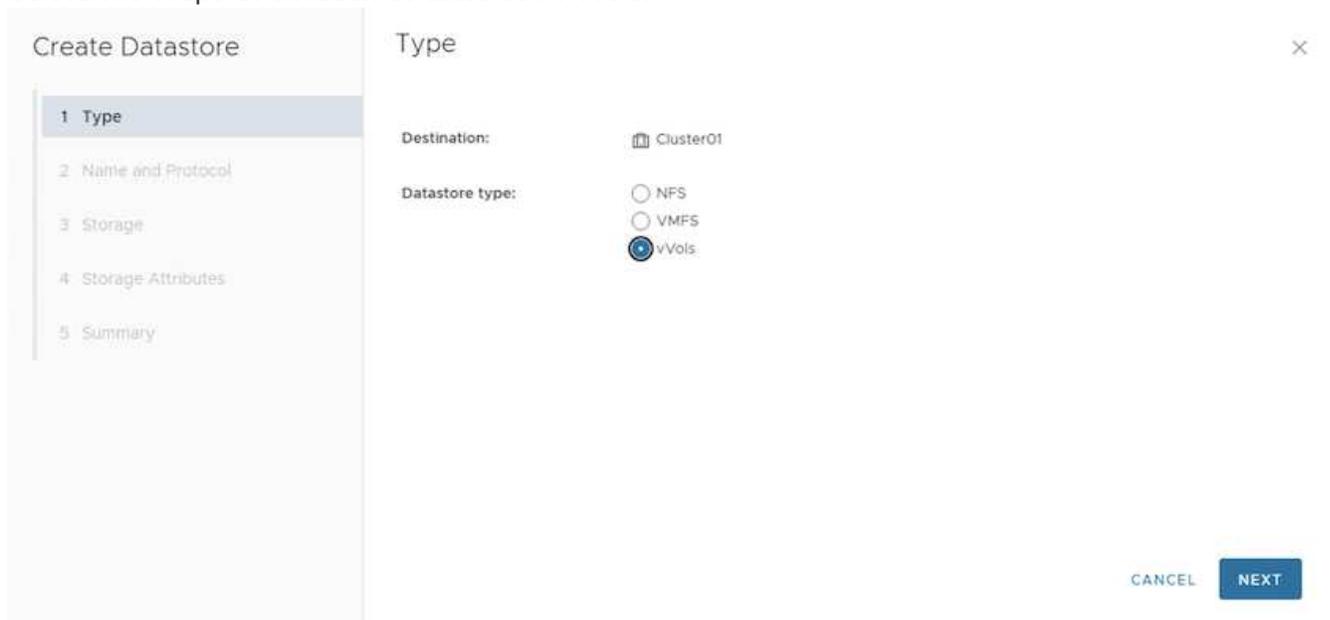
Name	Storage VM	Volume	Size	IOPS	Latency (ms)	Throughput (MB/s)
vvolPE-1723727751970	zoneb	TME01_iSCSI_02	4 MB	0	0	0
naa.600a0980383043595a2b506b67783041.vmdk	zoneb	TME01_iSCSI_01	16 GB	-	-	-
vvolPE-1723727751956	zoneb	TME01_iSCSI_01	4 MB	0	0	0
naa.600a0980383043595a2b506b67783041.vmdk	zoneb	TME01_iSCSI_01	255 GB	0	0	0

Para NFS, System Manager se puede usar para explorar el almacén de datos.

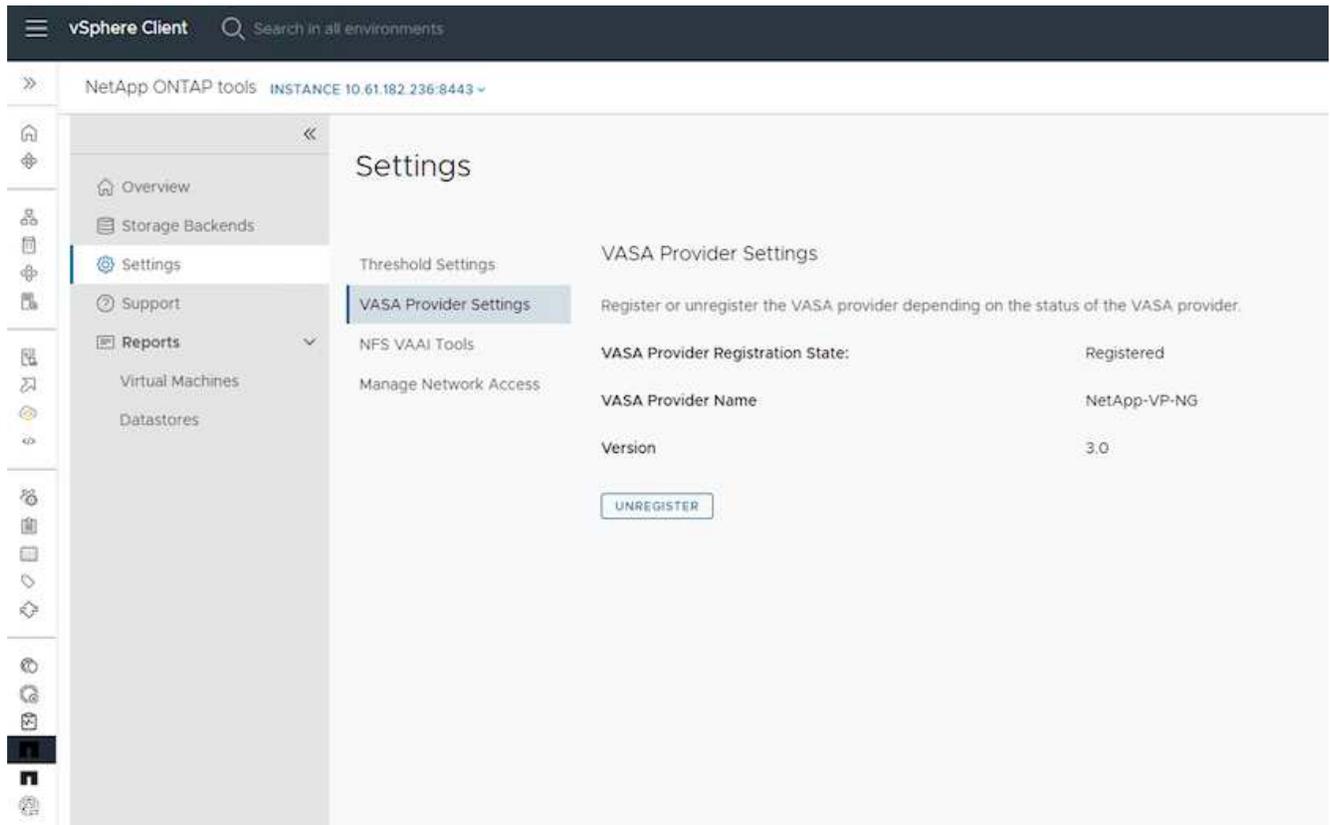


Con las herramientas de ONTAP 10.1

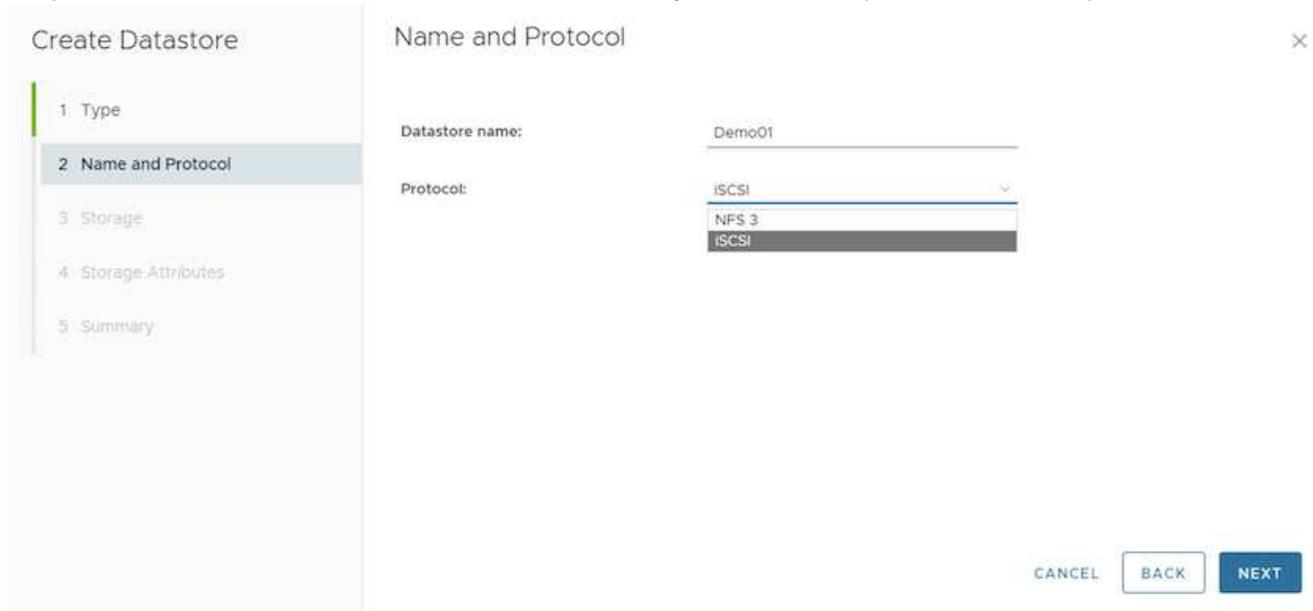
1. Haga clic con el botón derecho en el clúster o el host de vSphere y seleccione Create Datastore (10,1) en NetApp ONTAP tools.
2. Seleccione el tipo de almacén de datos como vVols.



Si la opción vVols no está disponible, asegúrese de que el proveedor de VASA esté registrado.



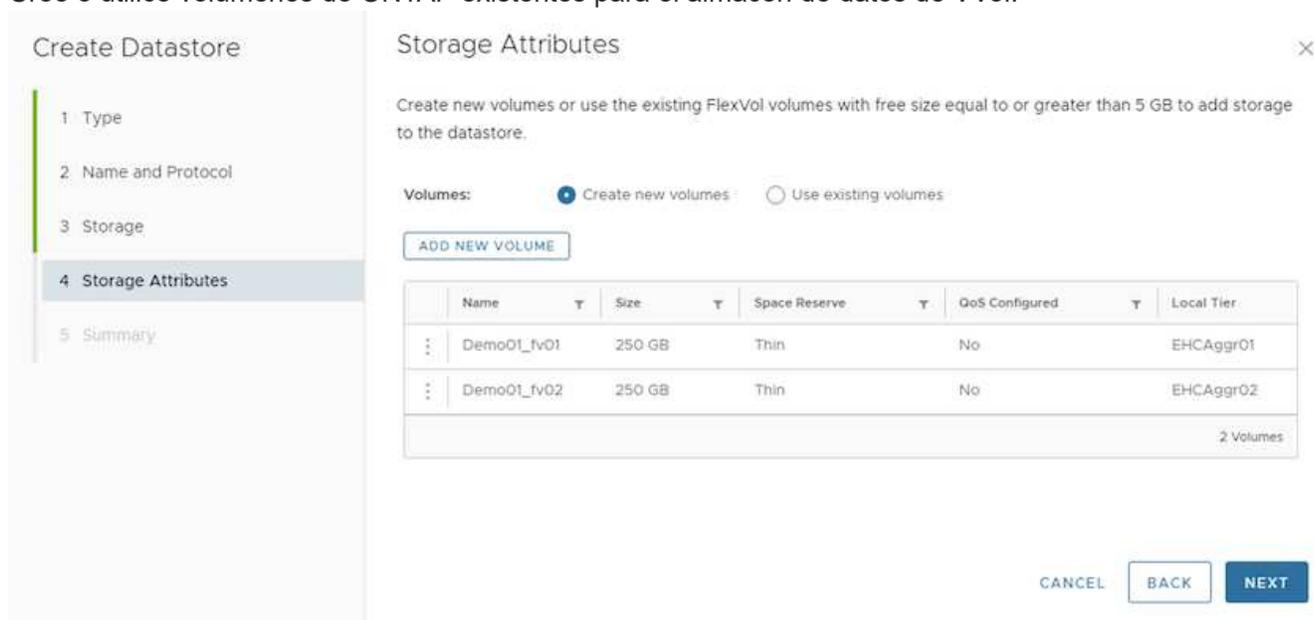
3. Proporcione el nombre del almacén de datos de VVol y seleccione el protocolo de transporte.



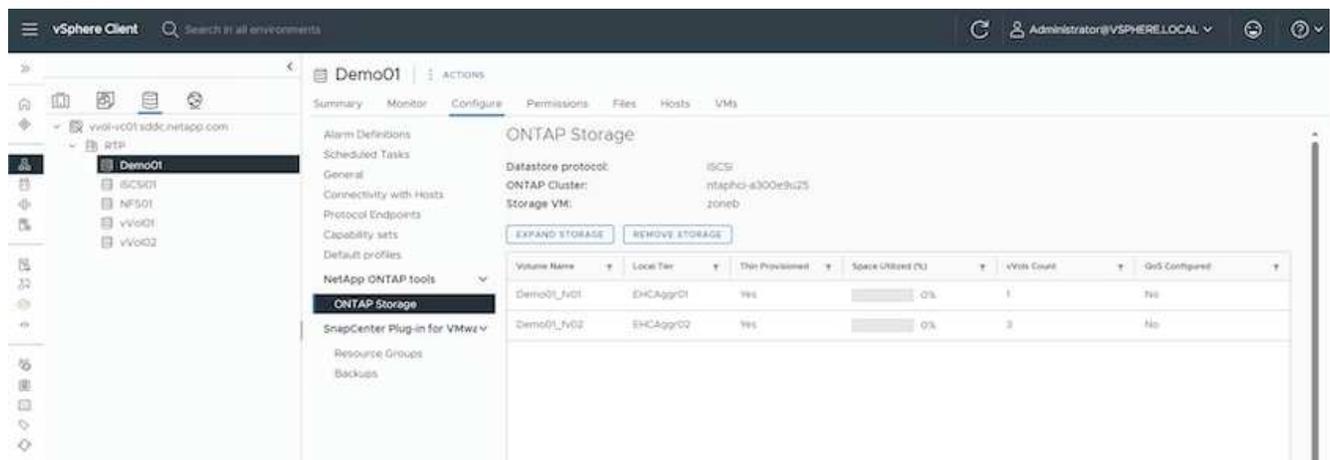
4. Seleccione la plataforma y Storage VM.



5. Cree o utilice volúmenes de ONTAP existentes para el almacén de datos de VVol.



Los volúmenes de ONTAP se pueden ver o actualizar posteriormente desde la configuración del almacén de datos.



6. Después de aprovisionar el almacén de datos VVol, es posible consumir de forma similar a cualquier otro

almacén de datos.

7. Las herramientas de ONTAP proporcionan el informe VM y Datastore.

The first screenshot shows the 'Virtual Machines' report in the vSphere Client. The table lists three VMs: 'scv', 'Demo01', and 'Demo02'. The 'scv' VM is using VMFS storage, while 'Demo01' and 'Demo02' are using VVOLs. The 'scv' VM has a space utilization of 37.21% and is in an 'On' state. The 'Demo01' VM has a space utilization of 0.03% and is in an 'Off' state. The 'Demo02' VM has a space utilization of 0.01% and is in an 'Off' state.

VM Name	Primary Data Store Type	Primary Data Store Name	vCenter VM Latency	Max Latency	Total Datastore IOPS	Average Datastore Throughput	Total Datastore Capacity	Uptime	Power State	vCenter VM Committed Capacity
scv	VMFS	dcsc01	0 ms	189 µs	3	10.89 KB/s	37.21%	16 hours	On	96 GB OS
Demo01	VVOLs	Demo01	-	53 µs	1	86 Bytes/s	0.03%	-	Off	287 GB
Demo02	VVOLs	VVOL02	-	0 µs	0	0 Bytes/s	0.01%	-	Off	271 GB

The second screenshot shows the 'Datastores' report in the vSphere Client. The table lists five datastores: 'dcsc01', 'NFSD1', 'VVOL1', 'VVOL2', and 'Demo01'. The 'dcsc01' datastore is using VMFS storage and has a space utilization of 37.21%. The 'NFSD1' datastore is using NFS storage and has a space utilization of 0.01%. The 'VVOL1' and 'VVOL2' datastores are using VVOLs storage and have space utilizations of 3.02% and 5.01% respectively. The 'Demo01' datastore is using VVOLs storage and has a space utilization of 5.03%.

Name	Space Utilized (%)	Type	IOPS	Latency	Throughput	Storage VM	Storage Controller
dcsc01	37.21%	VMFS	3	189 µs	10.89 KB/s	demo	ntaprci-4300w9u25
NFSD1	0.01%	NFS	0	297 µs	21 Bytes/s	demo	ntaprci-4300w9u25
VVOL1	3.02%	VVOLs	2	48 µs	81 Bytes/s	demo	ntaprci-4300w9u25
VVOL2	5.01%	VVOLs	0	0 µs	0 Bytes/s	demo	ntaprci-4300w9u25
Demo01	5.03%	VVOLs	1	53 µs	86 Bytes/s	demo	ntaprci-4300w9u25

Protección de datos de máquinas virtuales en almacenes de datos de VVOL

En "Protección de vVols".

1. Registre el sistema de almacenamiento que aloja el almacén de datos VVol y cualquier partner de replicación.

vSphere Client Search in all environments Administrator@VSPHERE.LOCAL

SnapCenter Plug-in for VMware vSphere INSTANCE 10.81.192.32-8144

Dashboard Settings Resource Groups Policies **Storage Systems** Guest File Restore

Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and ONTAP as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to recognize changes to ONTAP user login methods. Click here to know more.

Name	Display Name	Type	Protocol	Port	Username	SVM	TimeOutSec	Cache
B:RTH-C503-5403-orig.e...	nasadm-4300e9a25	ONTAP Cluster	HTTPS	443	admin	0	60	No
VCF_SCSI	VCF_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
isur0	isur0	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.228.20	isur0	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_SCSI_3510	HMC_SCSI_3510	ONTAP SVM	HTTPS	443	-	-	60	No
JL_SHC_SCSI	JL_SHC_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
030192.217	psdriv-smb-SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_3E7	HMC_3E7	ONTAP SVM	HTTPS	443	-	-	60	No
VCF_3422	VCF_3422	ONTAP SVM	HTTPS	443	-	-	60	No
VCF_NVM	VCF_NVM	ONTAP SVM	HTTPS	443	-	-	60	No
demo	demo	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.254.120	Temp_3510_N1	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.35.19	HYPERV-SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
EHC_NFS	EHC_NFS	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.19.203	EHC_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.19.19	VCF_NFS	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_3510	HMC_3510	ONTAP SVM	HTTPS	443	-	-	60	No
00fa_smb_4300	00fa_smb_4300	ONTAP SVM	HTTPS	443	-	-	60	No
B:ontap-destination-s43c-ne...	ontap-destination	ONTAP Cluster	HTTPS	443	admin	1	90	No
030192.147	sym2	ONTAP SVM	HTTPS	443	-	-	90	No

2. Crear una política con atributos necesarios.

New Backup Policy



Name

Description

Frequency

Locking Period Enable Snapshot Locking

Retention

Replication Update SnapMirror after backup
 Update SnapVault after backup

Snapshot label

Advanced

VM consistency

Include datastores with independent disks

Scripts

CANCEL

ADD

3. Cree un grupo de recursos y asócielo a una política (o políticas).

Create Resource Group



1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope:

Virtual Machines

Parent entity:

Datastores

Virtual Machines

Tags

Folders

Enter available entity name

Available entities

TME01

Selected entities

BACK

NEXT

FINISH

CANCEL

NOTA: Para el almacén de datos de VVol, debe protegerse con una máquina virtual, una etiqueta o una carpeta. El almacén de datos de VVol no se puede incluir en el grupo de recursos.

4. Se puede ver el estado específico de backup de la máquina virtual en su pestaña de configuración.

Name	Status	Locations	Snapshot lock Expression	Created Time	Mounted	Policy	VMware Snapshot
TME_00-05-2024_10.4	Completed	Primary & Secondary	-	8/15/2024 10:44:10 AM	No	hourly	No
TME_00-05-2024_10.2	Completed	Primary & Secondary	-	8/15/2024 10:24:52 AM	No	hourly	No
TME_00-05-2024_10.5	Completed	Primary	-	8/15/2024 9:53:15 AM	No	hourly	No
TME_00-05-2024_09.4	Completed	Primary	-	8/15/2024 9:47:24 AM	No	hourly	No
TME_00-05-2024_09.4	Completed	Primary	-	8/15/2024 9:44:50 AM	No	hourly	No
TME_00-05-2024_09.4	Completed	Primary	-	8/15/2024 9:44:08 AM	No	hourly	No
TME_00-05-2024_09.3	Completed	Primary	-	8/15/2024 9:40:04 AM	No	hourly	No

5. La máquina virtual se puede restaurar desde su ubicación primaria o secundaria.

Consulte "[Documentación del plugin de SnapCenter](#)" para obtener más casos de uso.

Migración de máquinas virtuales desde almacenes de datos tradicionales a almacenes de datos de VVOL

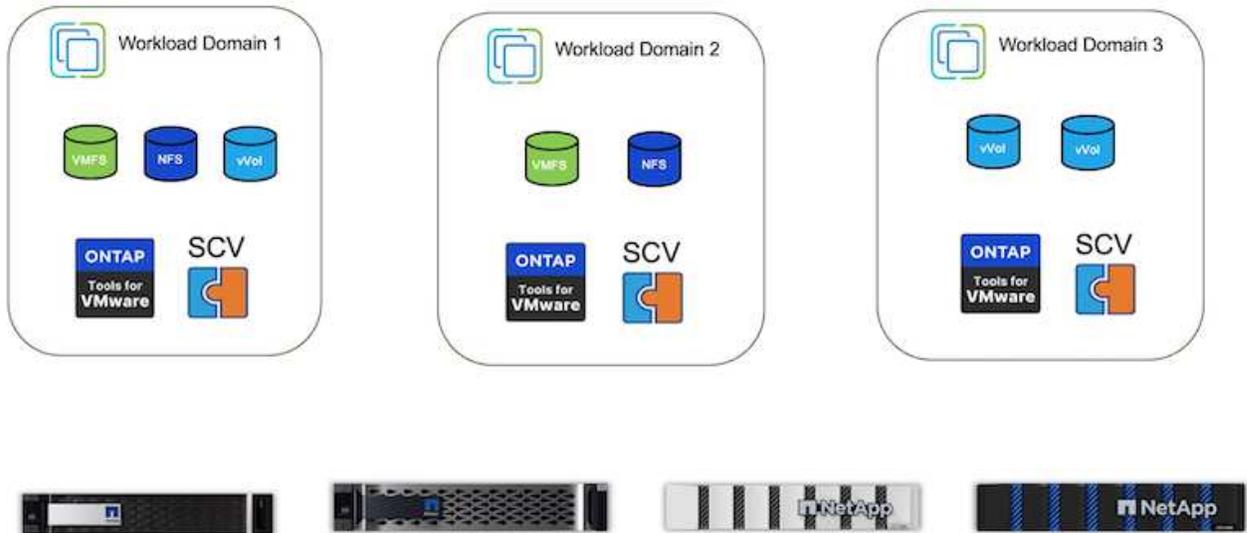
Para migrar máquinas virtuales desde otros almacenes de datos a un almacén de datos VVOL, se ofrecen varias opciones en función del escenario. Puede variar de una operación de vMotion de almacenamiento simple a la migración mediante HCX. Consulte "[Migrar máquinas virtuales a almacén de datos de ONTAP](#)" para obtener más información.

Migración de máquinas virtuales entre almacenes de datos de VVOL

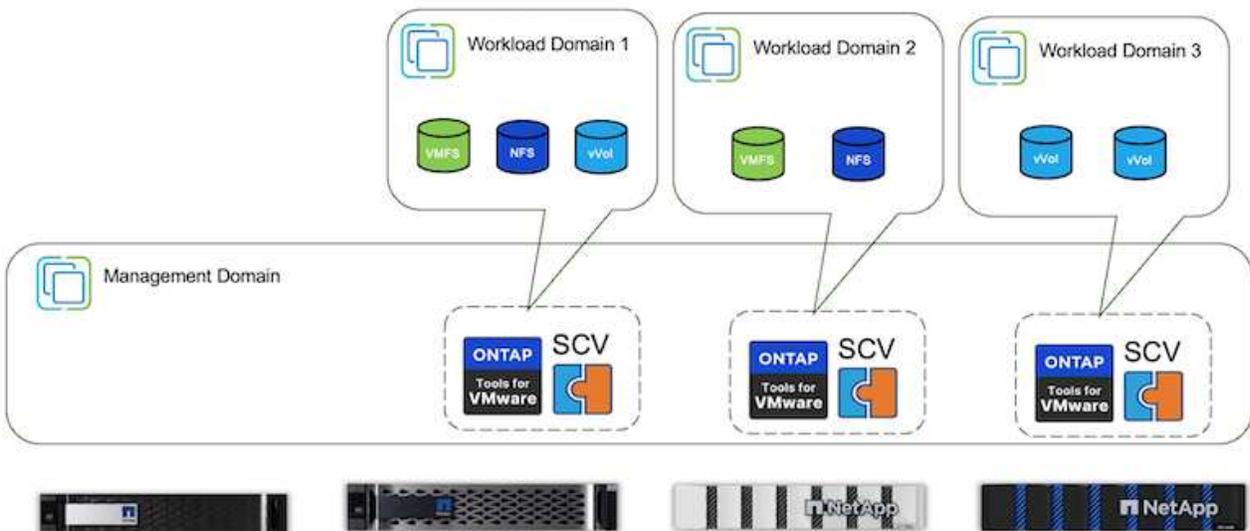
Para la migración masiva de máquinas virtuales entre almacenes de datos de VVol, compruebe "[Migrar máquinas virtuales a almacén de datos de ONTAP](#)".

Ejemplo de arquitectura de referencia

Se pueden instalar las herramientas de ONTAP para VMware vSphere y SCV en la misma instancia de vCenter que gestiona o en un servidor vCenter diferente. Es mejor evitar alojar en el almacén de datos de VVol que gestiona.

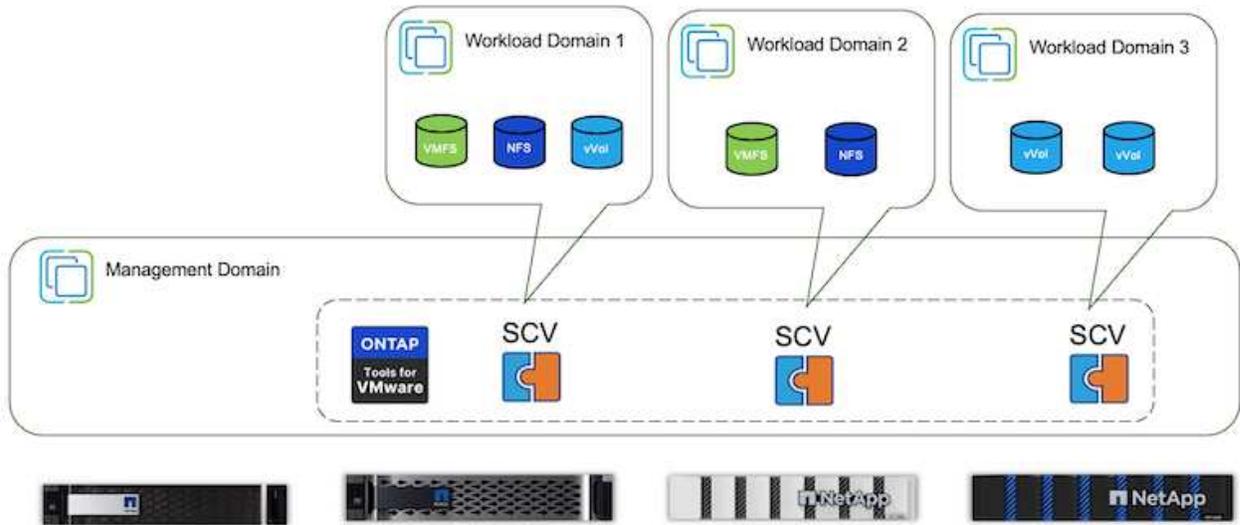


Como muchos clientes alojan sus servidores vCenter en uno diferente en lugar de gestionarlos, se aconseja un enfoque similar para ONTAP TOOLS y SCV también.

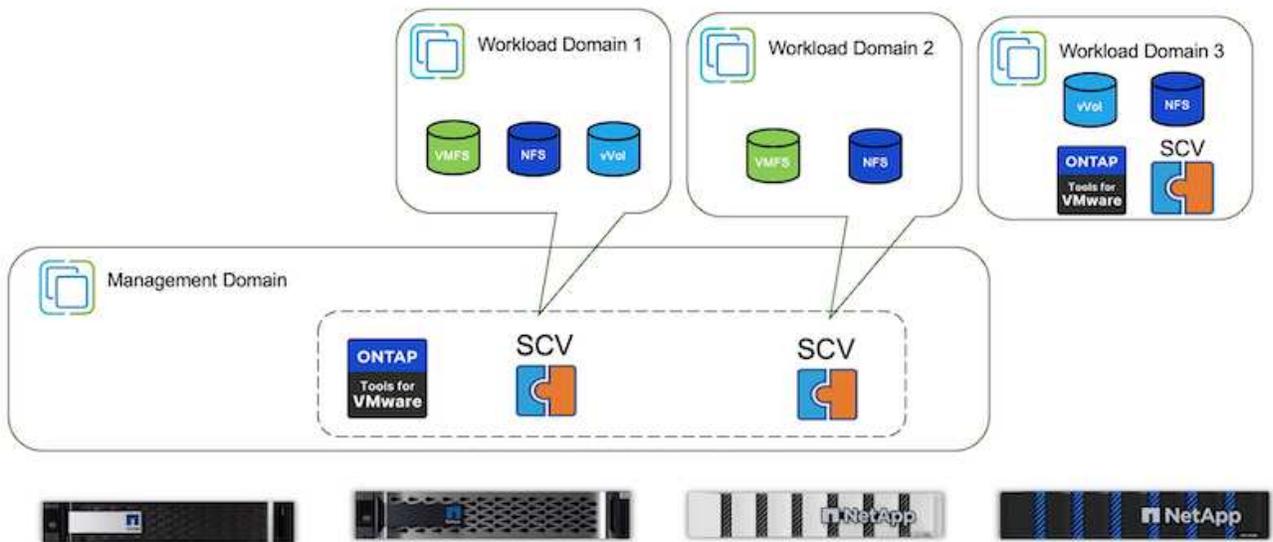


Con las herramientas de ONTAP 10.x, una sola instancia puede gestionar varios entornos vCenter. Los sistemas de almacenamiento se registran a nivel global con credenciales de clúster y se asignan SVM a cada

inquilino de vCenter Server.



También se admite la combinación de modelos dedicados y compartidos.



Cómo comenzar

Si las herramientas de ONTAP no están instaladas en el entorno, descárguelas de ["Sitio de soporte de NetApp"](#) y siga las instrucciones disponibles en ["Usar vVols con ONTAP"](#).

Guía de puesta en marcha para VMFS

Las soluciones y la oferta de almacenamiento de NetApp dan a los clientes todo lo que necesitan para aprovechar al máximo las ventajas de una infraestructura virtualizada. Con las soluciones de NetApp, los clientes pueden implementar con eficacia un software integral de gestión de datos que garantice las funcionalidades de automatización,

eficiencia, protección de datos y seguridad con el fin de satisfacer con eficacia los requisitos de rendimiento más exigentes. La combinación del software ONTAP con VMware vSphere permite reducir los gastos de licencia de VMware y el hardware host, garantizar la protección de los datos a un menor coste y ofrecer un alto rendimiento constante.

Introducción

Las cargas de trabajo virtualizadas son móviles. Por lo tanto, los administradores utilizan VMware Storage vMotion para mover equipos virtuales entre almacenes de datos de VMware Virtual Machine File System (VMFS), NFS o vVols, todos ellos ubicados en el mismo sistema de almacenamiento, y, por lo tanto, exploran distintos métodos de almacenamiento si se usa un sistema all-flash o se usan los modelos de ASA más recientes con innovación de SAN para obtener una mayor eficiencia de costes.

El mensaje clave es que la migración a ONTAP mejora la experiencia del cliente y el rendimiento de las aplicaciones a la vez que ofrece la flexibilidad para migrar datos y aplicaciones entre FCP, iSCSI, NVMe/FC y NVMe/TCP. Para las empresas que han invertido profundamente en VMware vSphere, el uso del almacenamiento de ONTAP es una opción rentable dadas las condiciones actuales del mercado, una oportunidad única. Hoy en día, las empresas se enfrentan a nuevos imperativos que puede abordar con rapidez y sencillez un enfoque SAN moderno. A continuación se muestran algunas de las formas en que los clientes de NetApp, nuevos y actuales, añaden valor con ONTAP.

- **Rentabilidad:** La eficiencia del almacenamiento integrada permite a ONTAP reducir significativamente los costes de almacenamiento. Los sistemas NetApp ASA pueden ejecutar todas las funcionalidades de eficiencia del almacenamiento en producción sin que se vea afectado el rendimiento. NetApp simplifica la planificación de estas ventajas de eficiencia con la garantía más eficiente disponible.
- **Protección de datos:** El software SnapCenter mediante copias Snapshot proporciona protección de datos a nivel de aplicación y máquina virtual avanzada para diversas aplicaciones empresariales puestas en marcha en una configuración de máquina virtual.
- **Seguridad:** Utilice copias de Snapshot para protegerse frente al malware y el ransomware. Mejore la protección al hacer que las copias snapshot sean inmutables mediante el bloqueo de instantáneas y el software NetApp SnapLock®.
- **Cloud:** ONTAP proporciona una amplia gama de opciones de cloud híbrido que permiten a las empresas combinar clouds públicos y privados, lo que ofrece flexibilidad y reduce los gastos generales de gestión de la infraestructura. El soporte complementario de almacenes de datos basado en las ofertas de ONTAP permite utilizar VMware Cloud en Azure, AWS y Google para la puesta en marcha optimizada del TCO, protección de datos y continuidad del negocio, evitando el bloqueo del proveedor.
- **Flexibilidad -** ONTAP está bien equipado para satisfacer las necesidades cambiantes de las organizaciones modernas. Con ONTAP One, todas estas funcionalidades se incluyen de serie con un sistema ONTAP sin coste adicional.

Ajusta el tamaño y optimiza

Con los próximos cambios en las licencias, las organizaciones están abordando de forma proactiva el aumento potencial del coste total de propiedad (TCO). Están optimizando estratégicamente su infraestructura de VMware mediante la agresiva gestión de recursos y el dimensionamiento para mejorar la utilización de recursos y optimizar la planificación de la capacidad. Gracias al uso eficaz de herramientas especializadas, las organizaciones pueden identificar y recuperar de manera eficiente los recursos desperdiciados, lo que permite reducir el número de núcleos y los gastos generales de licencias. Es importante destacar que muchas organizaciones ya están integrando estas prácticas en sus evaluaciones de cloud, lo que demuestra cómo estos procesos y herramientas mitigan de manera efectiva las preocupaciones sobre los costes de los entornos locales y eliminan los gastos de migración innecesarios a otros hipervisores.

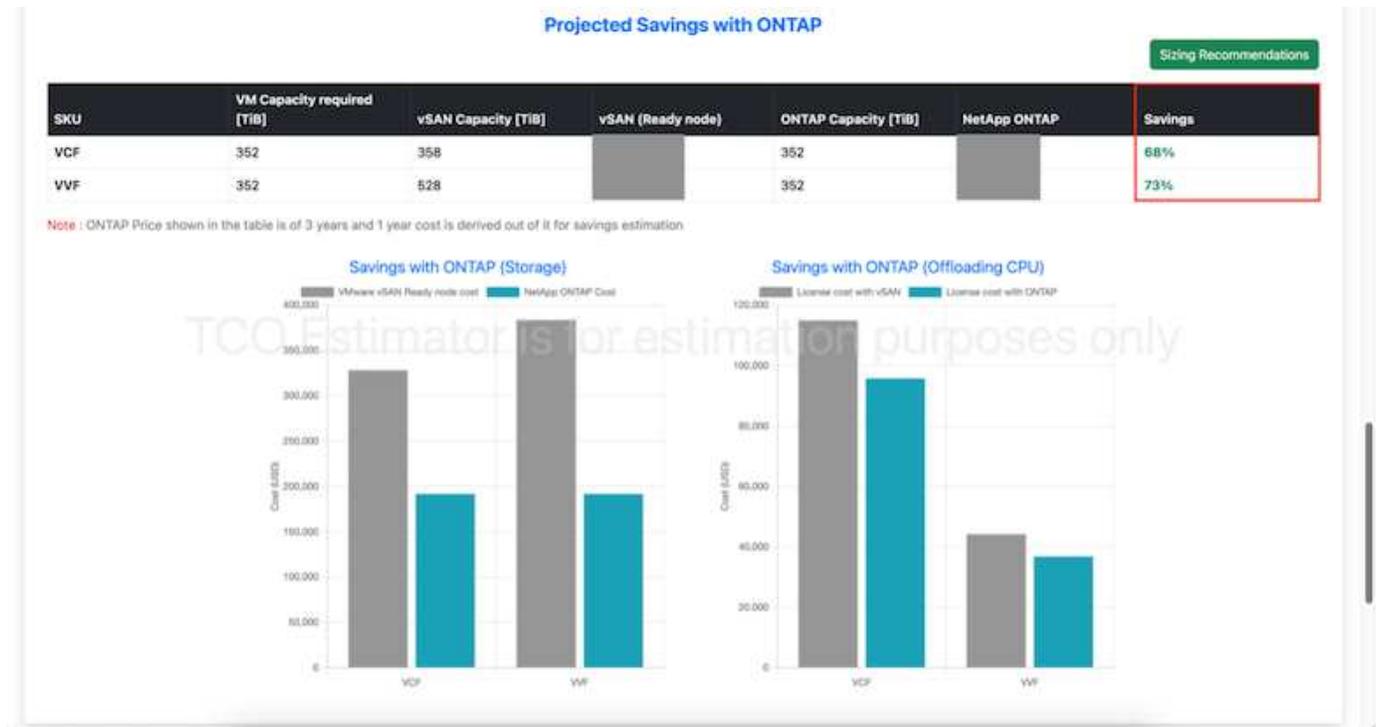
Estimación de TCO

NetApp ha creado un estimador simple del TCO que actuaría como un paso adelante para iniciar este viaje de optimización. El estimador del coste total de propiedad utiliza herramientas RVtools o métodos de entrada manuales para proyectar fácilmente cuántos hosts se necesitan para una implementación determinada y calcular el ahorro a fin de optimizar la implementación mediante los sistemas de almacenamiento de NetApp ONTAP. Tenga en cuenta que este es el escalón.



Los equipos y partners de campo de NetApp solo pueden acceder al estimador de TCO. Trabaje con los equipos de cuenta de NetApp para evaluar su entorno actual.

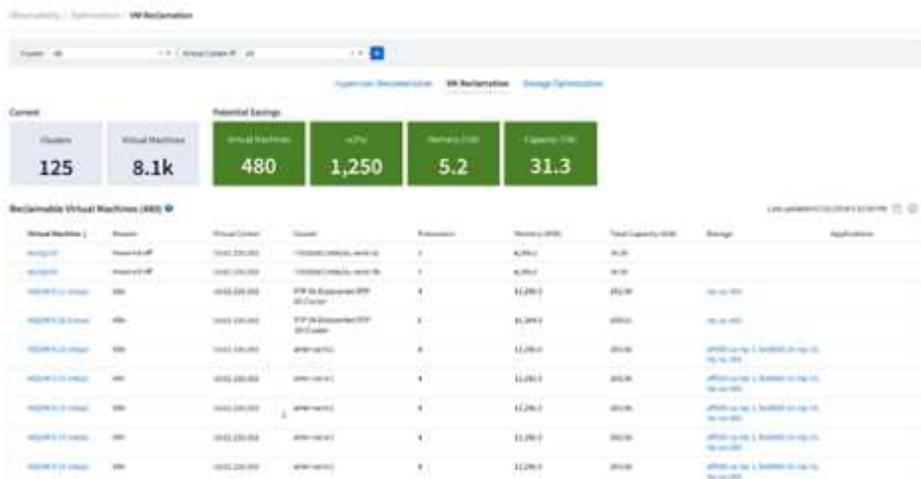
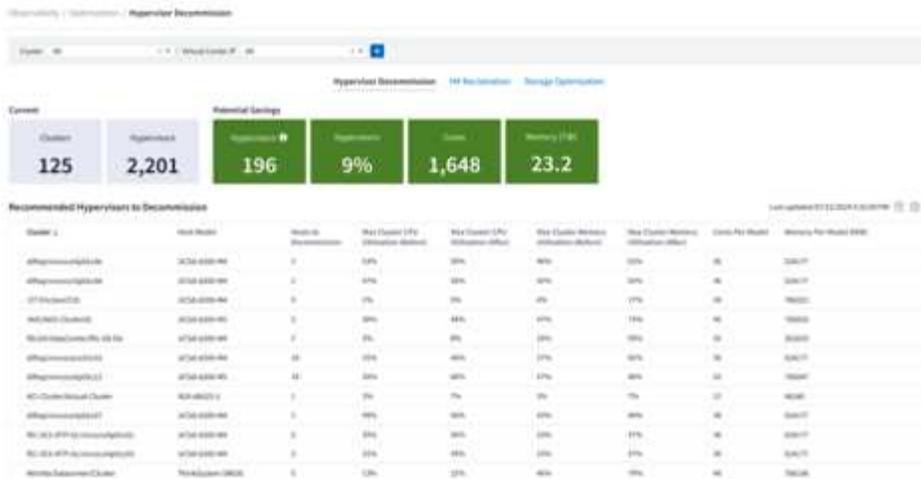
Aquí tiene una captura de pantalla del estimador de TCO.



Cloud Insights

Una vez que el evaluador muestre el ahorro posible (que será el caso de una organización determinada), es el momento de profundizar en el análisis de los perfiles de E/S de la carga de trabajo en las máquinas virtuales utilizando métricas en tiempo real. Para ello, NetApp proporciona Cloud Insights. Al ofrecer análisis y recomendaciones detallados para la recuperación de máquinas virtuales, Cloud Insights puede ayudar a las empresas a tomar decisiones informadas sobre la optimización de su entorno de máquinas virtuales. Puede identificar dónde se pueden reclamar los recursos o dónde se pueden retirar los hosts con un impacto mínimo en la producción, lo que ayuda a las empresas a navegar por los cambios provocados por la adquisición de VMware por Broadcom de forma reflexiva y estratégica. En otras palabras, Cloud Insight ayuda a las empresas a eliminar la emoción de la decisión. En lugar de reaccionar a los cambios con pánico o frustración, pueden usar la información proporcionada por la herramienta Cloud Insights para tomar decisiones estratégicas y racionales que equilibren la optimización de costes con la eficiencia operativa y la productividad.

A continuación se muestran las capturas de pantalla de Cloud Insights.



Realice evaluaciones periódicas para detectar los recursos infrutilizados, aumentar la densidad de los equipos virtuales y su utilización en clústeres de VMware para controlar los crecientes costes asociados con las nuevas licencias de suscripción. Considere la posibilidad de reducir el número de núcleos por CPU a 16 GHz en compras de nuevos servidores para alinearlo con los cambios en los modelos de licencia de VMware.

Con NetApp, ajusta el tamaño adecuado de tus entornos virtualizados e introduce un rendimiento rentable del almacenamiento flash, junto con una gestión de datos simplificada y soluciones de ransomware para garantizar que las organizaciones están preparadas para el nuevo modelo de suscripción, mientras optimizan los recursos TECNOLÓGICOS que se encuentran en la actualidad.

Herramientas de ONTAP de NetApp para VMware vSphere

Para mejorar y simplificar aún más la integración de VMware, NetApp ofrece varias herramientas de ONTAP que se pueden utilizar con NetApp ONTAP y VMware vSphere para gestionar de forma eficiente entornos virtualizados. Esta sección se centrará en las herramientas de ONTAP para VMware. Las herramientas de ONTAP para VMware vSphere 10 proporcionan un completo conjunto de herramientas para la gestión del ciclo de vida de las máquinas virtuales, simplifican la gestión del almacenamiento, mejoran las funciones de eficiencia, mejoran la disponibilidad y reducen los costes de almacenamiento y la sobrecarga operativa. Estas herramientas se integran a la perfección con el ecosistema de VMware, lo que facilita el aprovisionamiento de almacenes de datos y ofrece protección básica para máquinas virtuales. La versión 10.x de las herramientas de ONTAP para VMware vSphere incluye microservicios basados en eventos y escalables horizontalmente implementados como dispositivo Open Virtual Appliance (OVA), siguiendo las mejores prácticas para

aprovisionar almacenes de datos y optimizar la configuración de hosts ESXi para entornos de almacenamiento NFS y bloques. Teniendo en cuenta estos beneficios, se recomienda OTV como una práctica recomendada para usar con sistemas que ejecutan software ONTAP.

Primeros pasos

Antes de implementar y configurar las herramientas de ONTAP para VMware, asegúrese de que se cumplen los requisitos previos. Una vez hecho esto, ponga en marcha una configuración de nodo único.



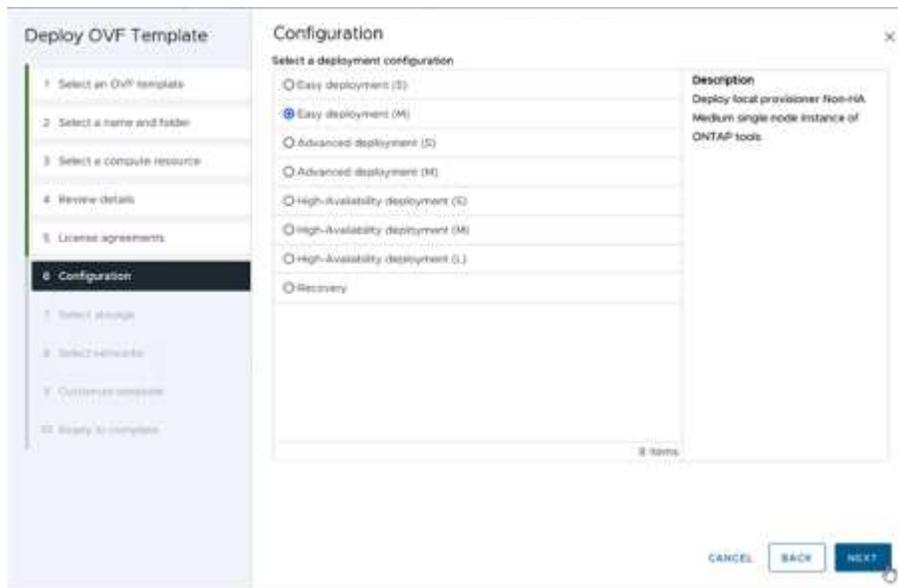
Se requieren tres direcciones IP para la implementación: Una dirección IP para el balanceador de carga, una dirección IP para el plano de control de Kubernetes y una para el nodo.

Pasos

1. Inicie sesión en vSphere Server.
2. Desplácese hasta el clúster o el host en el que desea implementar el OVA.
3. Haga clic con el botón derecho del ratón en la ubicación deseada y seleccione Desplegar plantilla OVF.
 - a. Introduzca la URL del archivo .ova o vaya a la carpeta donde se guarda el archivo .ova y, a continuación, seleccione Siguiente.
4. Seleccione un nombre, carpeta, clúster / host para la máquina virtual y seleccione Siguiente.
5. En la ventana Configuration, seleccione Easy deployment(S), Easy deployment(M) o Advanced deployment(S) o Advanced deployment(M) configuration.



La opción de fácil implementación se utiliza en este tutorial.



6. Seleccione el almacén de datos para implementar el OVA, la red de origen y destino. Cuando haya terminado, seleccione Siguiente.
7. Es hora de personalizar la plantilla > la ventana de configuración del sistema.

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 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Customize template

Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only [a-z, 0-9, -, _] special characters are supported. <input type="text" value="admin"/>
Administrator password(*)	Password to assign to the Administrator. Password <input type="password" value="*****"/> 👁 Confirm Password <input type="password" value="*****"/> 👁
NTP servers	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware Tools based time synchronization will be used. <input type="text" value="172.21.166.1"/>
Maintenance user password(*)	Password to assign to maint user account. Password <input type="password" value="*****"/> 👁 Confirm Password <input type="password" value="*****"/> 👁

CANCEL BACK NEXT

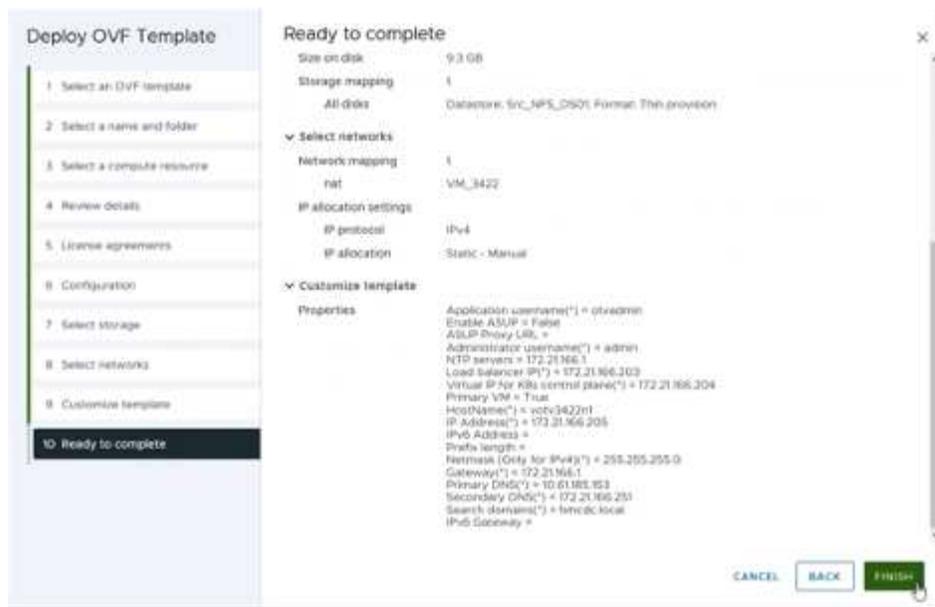
Deploy OVF Template

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

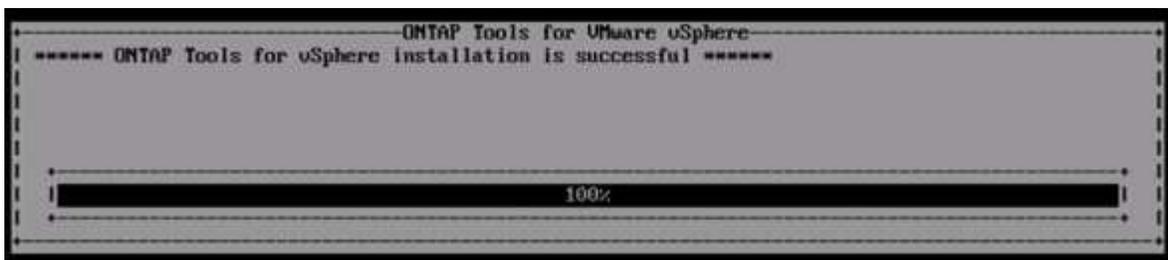
Customize template

Deployment Configuration	3 settings
Load balancer IP(*)	Load balancer IP (*) <input type="text" value="172.21.166.203"/>
Virtual IP for K8s control plane(*)	Provides the virtual IP address for K8s control plane. <input type="text" value="172.21.166.204"/>
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. <input checked="" type="checkbox"/>
Node Configuration	10 settings
HostName(*)	Specify the hostname for the VM. <input type="text" value="vst-0422r1"/>
IP Address(*)	Specify the IP address for the appliance. <input type="text" value="172.21.166.205"/>
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack. <input type="text"/>
Prefix length	Specify the prefix length. <input type="text"/>

CANCEL BACK NEXT



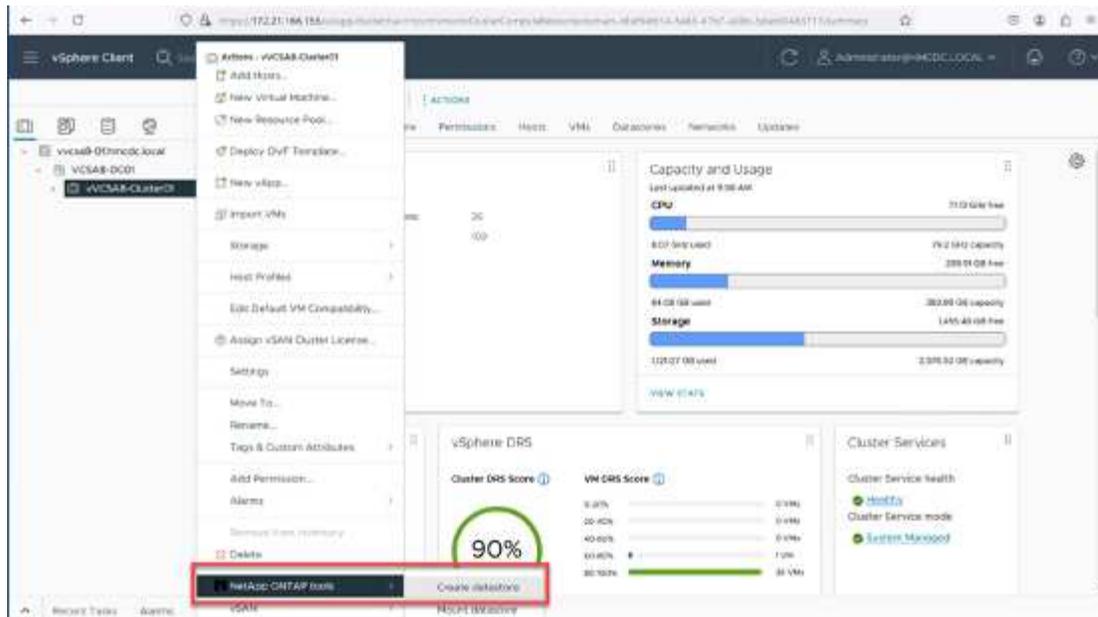
Después de la instalación correcta, la consola web muestra el estado de las herramientas de ONTAP para VMware vSphere.



El asistente de creación de almacenes de datos admite el aprovisionamiento de almacenes de datos VMFS, NFS y vVols.

Es hora de aprovisionar almacenes de datos VMFS basados en iSCSI para este tutorial.

1. Inicie sesión en el cliente de vSphere mediante <https://<vcenterip>/ui>
2. Haga clic con el botón derecho en un host, un clúster de hosts o un almacén de datos y, a continuación, seleccione Herramientas de NetApp ONTAP > Crear almacén de datos.



3. En el panel Type, seleccione VMFS en Datastore Type.



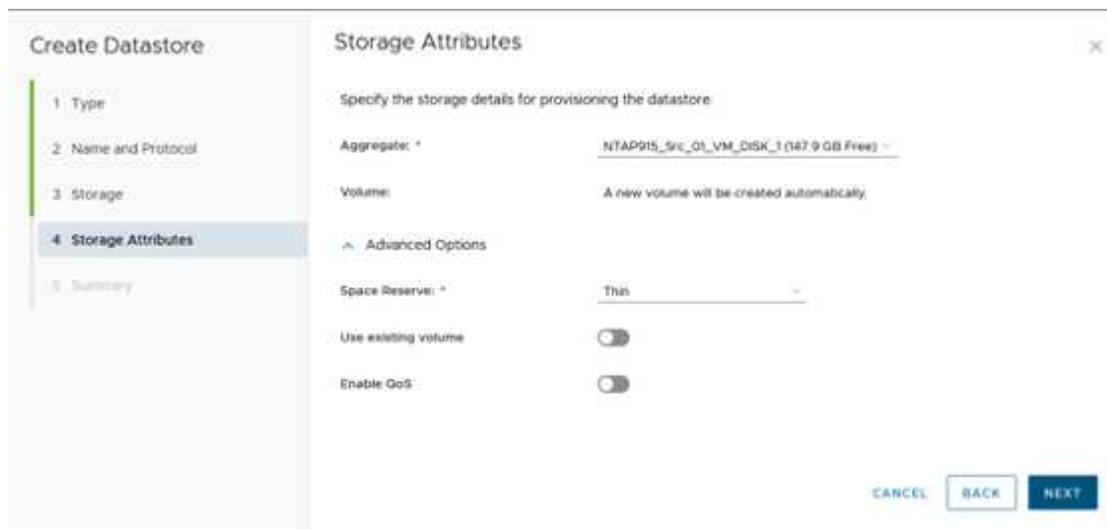
4. En el panel Name and Protocol, introduzca el nombre, el tamaño y la información del protocolo del almacén de datos. En la sección Advanced options del panel, seleccione el clúster del almacén de datos si desea añadir este almacén de datos.



5. Seleccione Plataforma y almacenamiento VM en el panel Almacenamiento. Proporcione el nombre de iGroup personalizado en la sección Advanced Options del panel (opcional). Puede seleccionar un iGroup existente para el almacén de datos o crear un iGroup nuevo con un nombre personalizado.



6. En el panel de atributos de almacenamiento, seleccione el agregado en el menú desplegable. Seleccione las opciones Space Reserve, volume Option y Enable QoS según sea necesario en la sección Advanced options.



7. Revise los detalles del almacén de datos en el panel Summary y haga clic en Finish. El almacén de datos de VMFS se crea y se monta en todos los hosts.



Consulte estos enlaces para el aprovisionamiento de almacén de datos VVOL, FC, NVMe/TCP.

VAAI independiente

Los primitivos VAAI se usan en operaciones rutinarias de vSphere, como la creación, el clonado, la migración, el inicio y la detención de máquinas virtuales. Estas operaciones se pueden ejecutar a través del cliente vSphere para mayor simplicidad o desde la línea de comandos para el scripting o para obtener tiempos más precisos. VAAI para SAN es compatible de forma nativa con ESX. VAAI está siempre habilitado en los sistemas de almacenamiento NetApp compatibles y proporciona compatibilidad nativa para las siguientes operaciones VAAI en el almacenamiento SAN:

- Descarga de copias
- Bloqueo de prueba y ajuste atómico (ATS)
- Escriba igual
- Gestión de condiciones de falta de espacio
- Recuperación de espacio

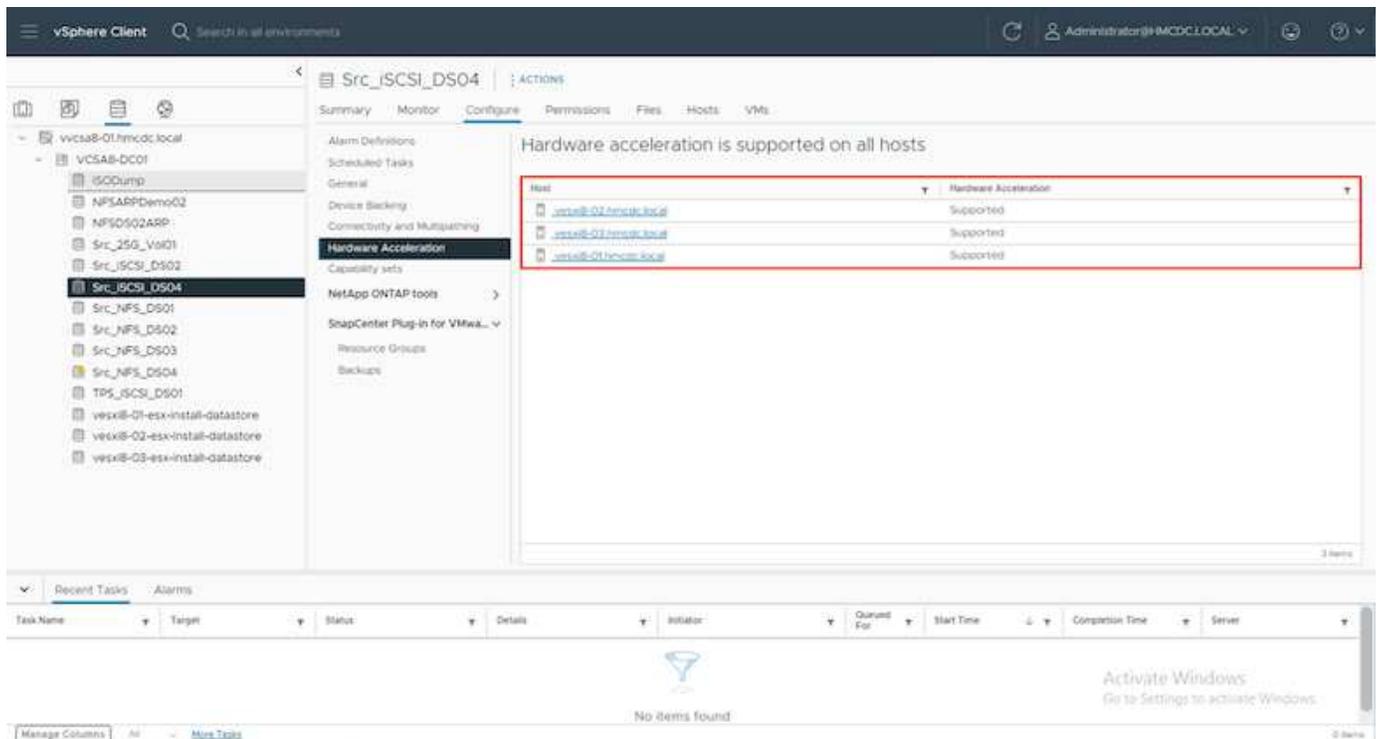
```
[root@vesxi8-02:~] esxcli storage core device vaai status get -d=naa.600a09805a506576495d576a57553455
naa.600a09805a506576495d576a57553455
VAAI Plugin Name: VMW_VAAIP_NETAPP
ATS Status: supported
Clone Status: supported
Zero Status: supported
Delete Status: supported
```



Asegúrese de que HardwareAcceleratedMove está habilitado a través de las opciones de configuración avanzadas de ESX.



Asegúrese de que la LUN tiene habilitada la «asignación de espacio». Si no está habilitada, habilite la opción y vuelva a analizar todos los HBA.





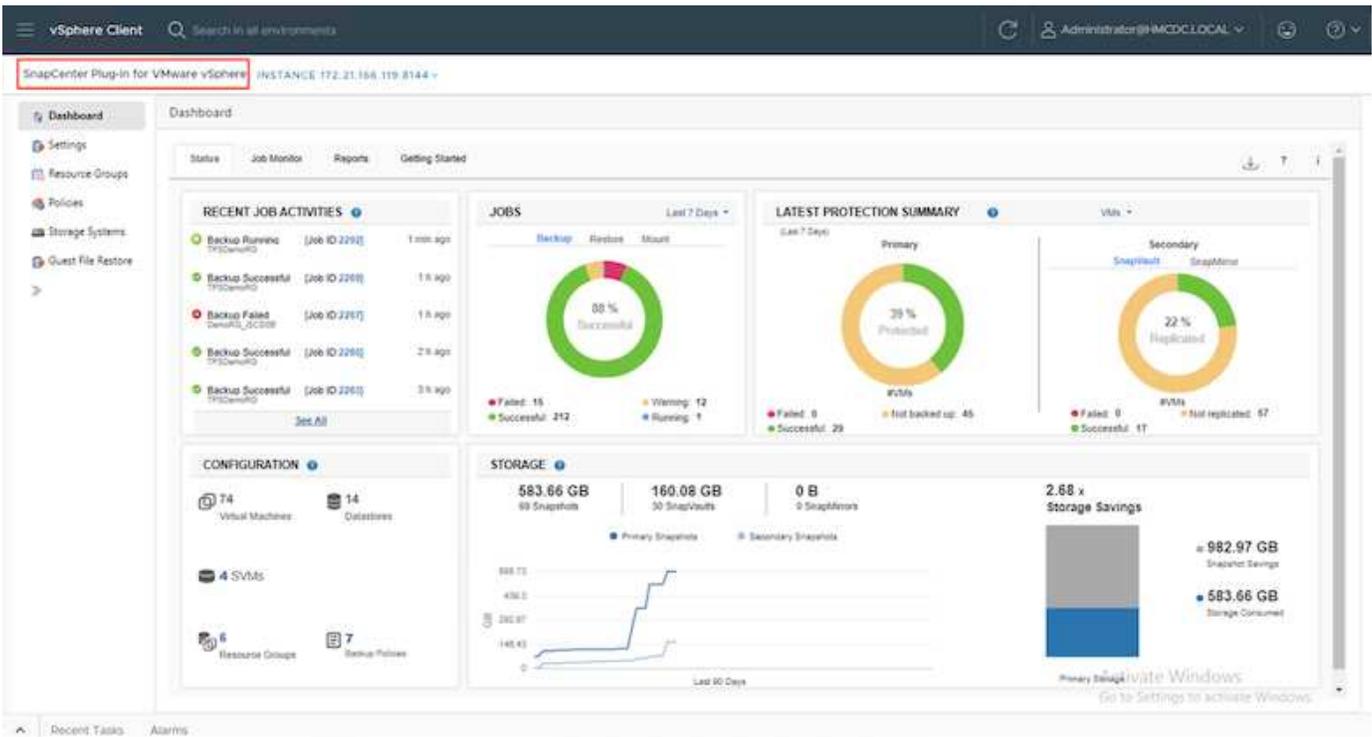
Estos valores se establecen fácilmente mediante las herramientas de ONTAP para VMware vSphere. En la consola Overview, vaya a Tarjeta de cumplimiento de host ESXi y seleccione la opción Apply Recommended Settings. En la ventana Aplicar configuración de host recomendada, seleccione los hosts y haga clic en Siguiente para aplicar la configuración de host recomendada por NetApp.



Ver orientación detallada para ["Host ESXi recomendado y otra configuración de ONTAP"](#).

Protección de datos

Realizar backups eficientes de máquinas virtuales en almacenes de datos VMFS y recuperarlas rápidamente son algunas de las ventajas clave de ONTAP para vSphere. Al integrarse con vCenter, el software NetApp SnapCenter® ofrece una amplia gama de funciones de copia de seguridad y recuperación para máquinas virtuales. Proporciona operaciones de backup y restauración rápidas, eficientes en cuanto al espacio, consistentes con los fallos y consistentes con las máquinas virtuales para máquinas virtuales, almacenes de datos y VMDK. También funciona con el servidor de SnapCenter para admitir operaciones de backup y restauración basadas en aplicaciones en entornos VMware usando plugins específicos de la aplicación de SnapCenter. El aprovechamiento de las copias snapshot permite realizar copias rápidas de la máquina virtual o del almacén de datos sin ningún impacto en el rendimiento y utilizar la tecnología NetApp SnapMirror® o NetApp SnapVault® para la protección de datos a largo plazo fuera del sitio.



El flujo de trabajo es sencillo. Añada los sistemas de almacenamiento principales y SVM (y secundario si se

requiere SnapMirror/SnapVault).

Pasos de alto nivel para la implementación y configuración:

1. Descargue SnapCenter para el OVA del plugin de VMware
2. Inicie sesión con las credenciales de vSphere Client
3. Implemente la plantilla OVF para iniciar el asistente de implementación de VMware y completar la instalación
4. Para acceder al plugin, seleccione SnapCenter Plug-in for VMware vSphere en el menú
5. Agregar almacenamiento
6. Cree políticas de backup
7. Crear grupos de recursos
8. Grupos de recursos de backup
9. Restaure toda la máquina virtual o un disco virtual determinado

Configurar el plugin de SnapCenter para VMware para máquinas virtuales

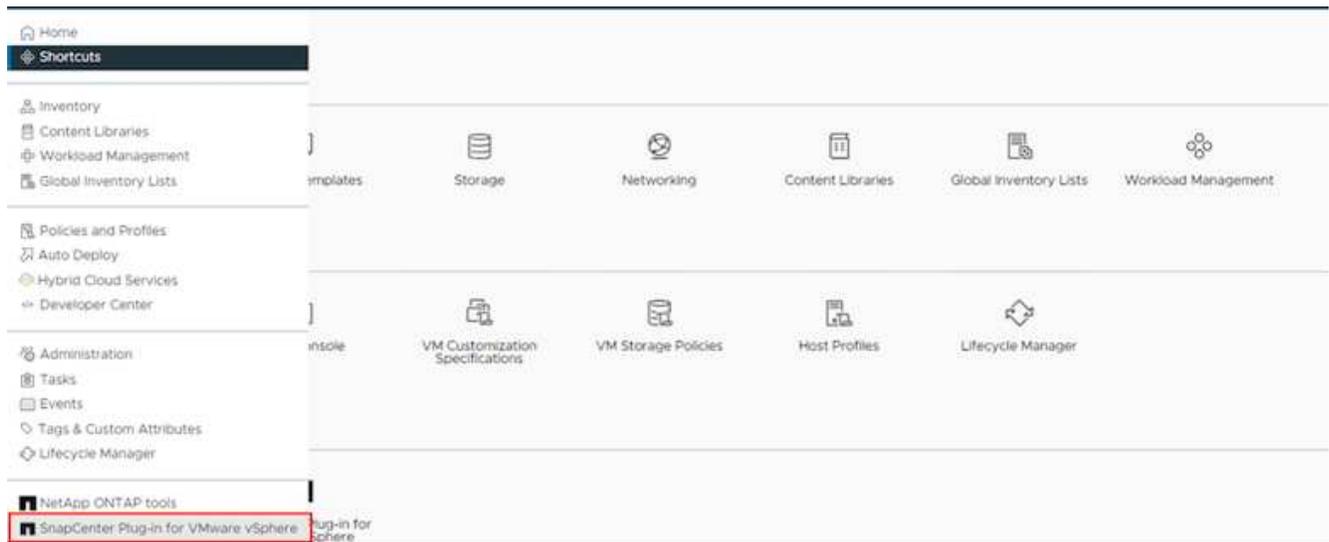
Para proteger máquinas virtuales y almacenes de datos iSCSI que las alojan, se debe implementar el plugin de SnapCenter para VMware. Es una importación de OVF simple.

Los pasos para desplegar son los siguientes:

1. Descargue el dispositivo Open Virtual Appliance (OVA) del sitio de soporte de NetApp.
2. Inicie sesión en vCenter.
3. En vCenter, haga clic con el botón derecho en cualquier objeto de inventario, como un centro de datos, una carpeta, un clúster o un host, y seleccione Deploy OVF template.
4. Seleccione la configuración adecuada, incluido el almacenamiento y la red, y personalice la plantilla para actualizar el para vCenter y sus credenciales. Una vez revisado, haga clic en Finalizar.
5. Espere a que se completen las tareas de importación y despliegue de OVF.
6. Una vez que el plugin de SnapCenter para VMware se ponga en marcha correctamente, se registrará en vCenter. Lo mismo se puede verificar accediendo a Administration > Client Plugins



7. Para acceder al plugin, desplácese hasta el lateral izquierdo de la página Web Client de vCenter, seleccione SnapCenter Plug-in for VMware.



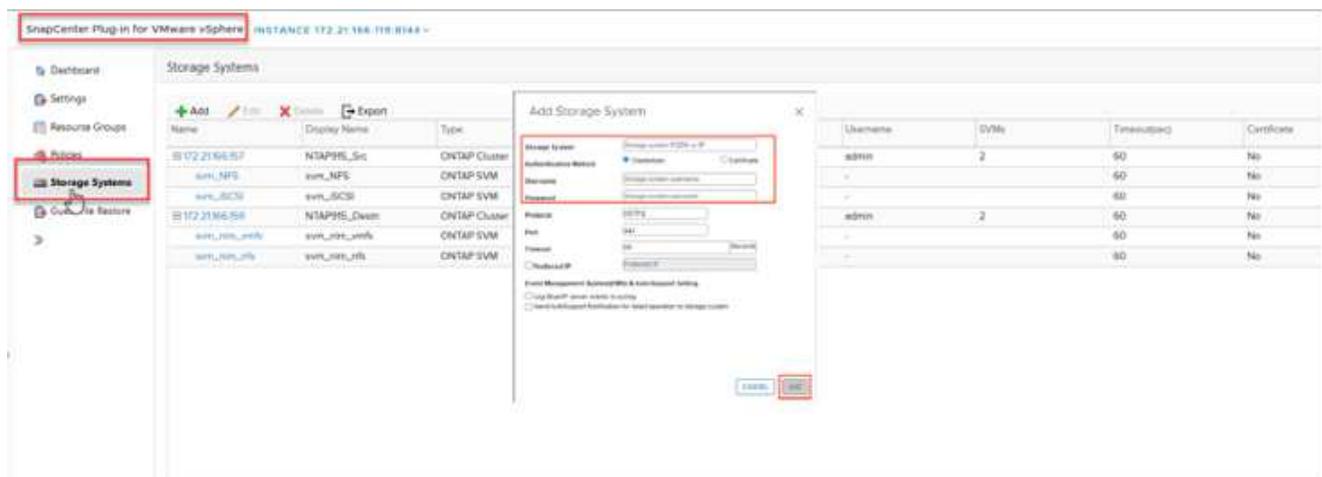
Añada almacenamiento, cree políticas y grupo de recursos

Añadir sistema de almacenamiento

El siguiente paso es añadir el sistema de almacenamiento. El extremo de gestión de clústeres o la IP del extremo de administración de máquinas virtuales de almacenamiento (SVM) se deben añadir como un sistema de almacenamiento para realizar copias de seguridad o restaurar máquinas virtuales. Añadir almacenamiento permite que el plugin de SnapCenter para VMware reconozca y gestione las operaciones de backup y restauración en vCenter.

El proceso es directo.

1. En el menú de navegación de la izquierda, seleccione SnapCenter Plug-in for VMware.
2. Seleccione almacenamiento sistemas.
3. Seleccione Agregar para agregar los detalles de «almacenamiento».
4. Utilice Credenciales como método de autenticación e introduzca el nombre de usuario y su contraseña y, a continuación, haga clic en Agregar para guardar la configuración.



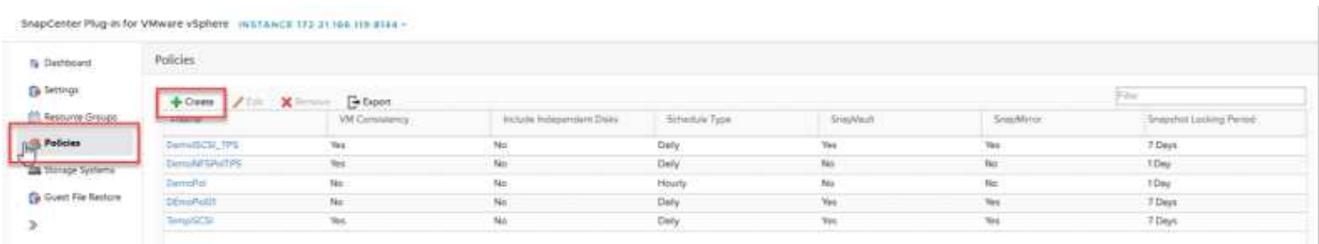


Crear política de backup

Una estrategia de backup completa incluye factores como cuándo, qué hacer backup y cuánto tiempo conservar los backups. Las Snapshot pueden activarse por horas o diariamente para realizar backups de almacenes de datos completos. Este enfoque no solo captura los almacenes de datos, sino que también permite realizar backups y restaurar las máquinas virtuales y VMDK dentro de esos almacenes de datos.

Antes de realizar un backup de las máquinas virtuales y los almacenes de datos, debe crearse una política de backup y un grupo de recursos. Una política de backup incluye configuración como la programación y la política de retención. Siga estos pasos para crear una política de backup.

1. En el panel de navegación de la izquierda del plugin de SnapCenter para VMware, haga clic en Políticas.
2. En la página Políticas, haga clic en Create para iniciar el asistente.



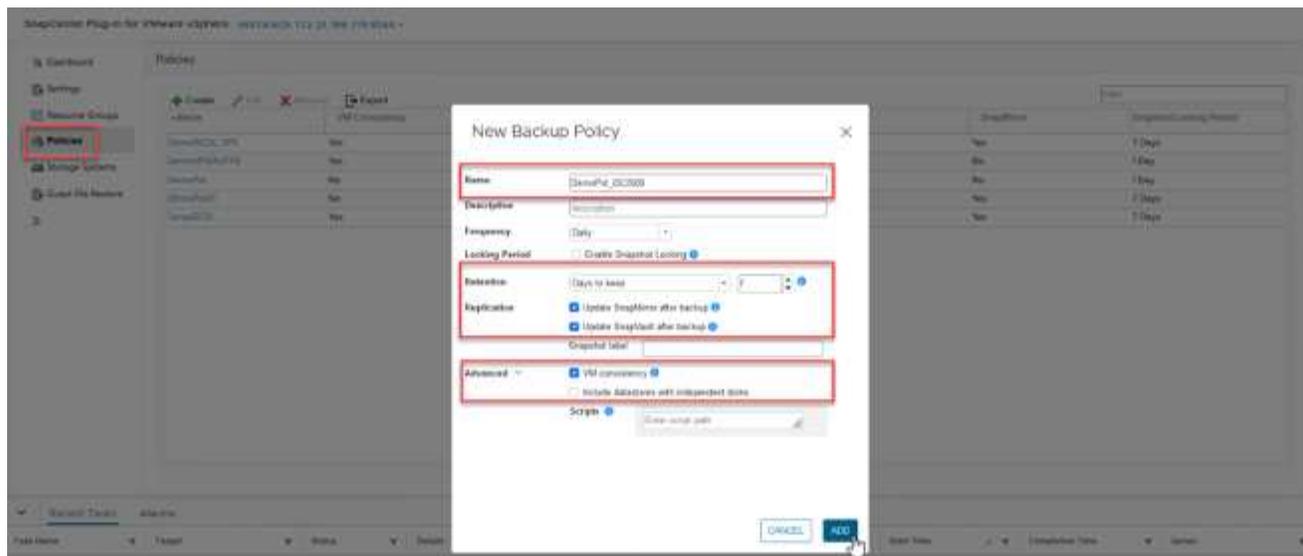
3. En la página New Backup Policy, escriba el nombre de la política.
4. Especifique la retención, la configuración de frecuencia y la replicación.



Para replicar copias Snapshot en un sistema de almacenamiento secundario reflejado o en almacén, las relaciones deben configurarse de antemano.



Para permitir los backups coherentes con los equipos virtuales, las herramientas de VMware deben instalarse y ejecutarse. Cuando se marca la casilla de consistencia de máquina virtual, las máquinas virtuales primero se ponen en modo inactivo, VMware ejecuta una Snapshot consistente de máquina virtual (excepto la memoria) y, a continuación, el plugin de SnapCenter para VMware ejecuta su operación de backup y, a continuación, se reanudan las operaciones de máquina virtual.



Una vez creada la política, el siguiente paso es crear el grupo de recursos que definirá los almacenes de datos iSCSI y las máquinas virtuales correspondientes que deben respaldarse. Una vez creado el grupo de recursos, es hora de activar los backups.

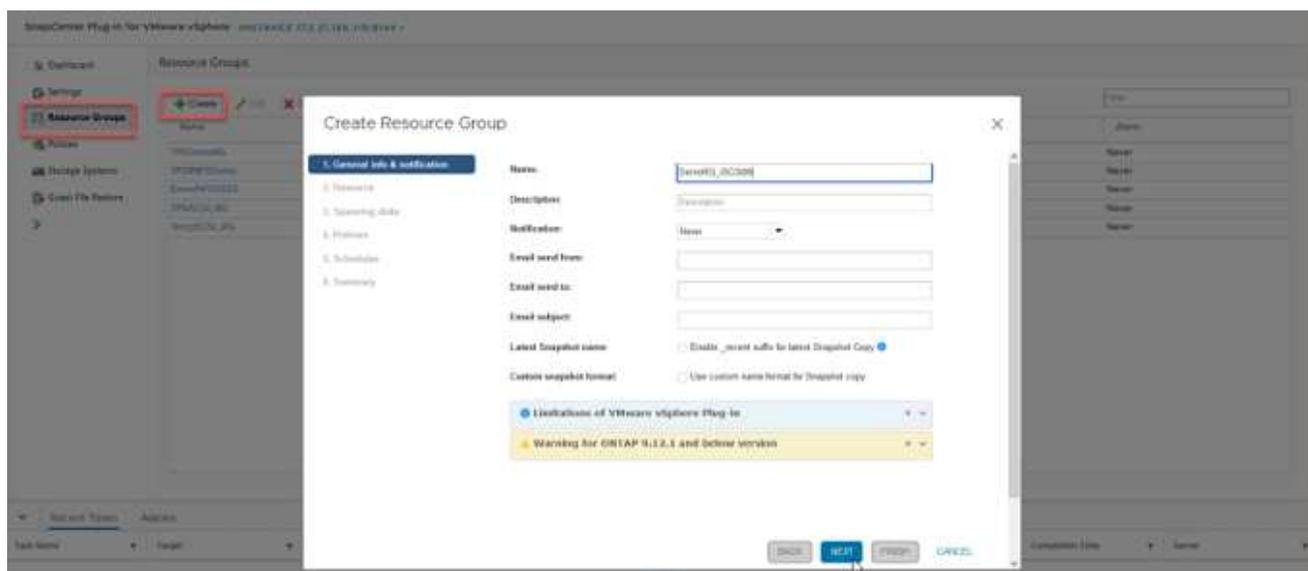
Crear grupo de recursos

Un grupo de recursos es el contenedor para máquinas virtuales y almacenes de datos que deben protegerse. Los recursos se pueden agregar o eliminar a grupos de recursos en cualquier momento.

Siga los pasos a continuación para crear un grupo de recursos.

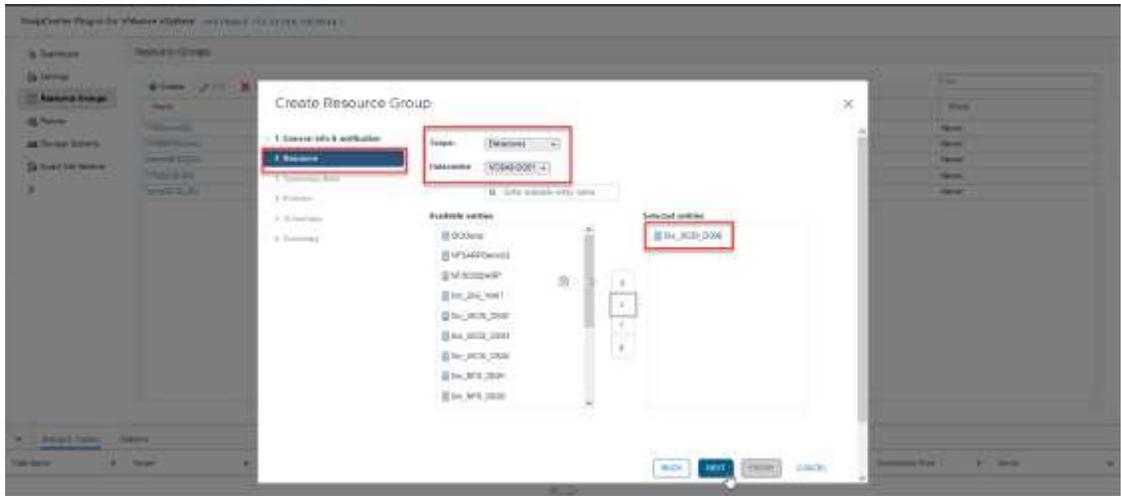
1. En el panel de navegación de la izquierda del plugin de SnapCenter para VMware, haga clic en Resource Groups.
2. En la página Resource Groups, haga clic en Create para iniciar el asistente.

Otra opción para crear un grupo de recursos es seleccionar la máquina virtual o el almacén de datos individual y crear un grupo de recursos respectivamente.

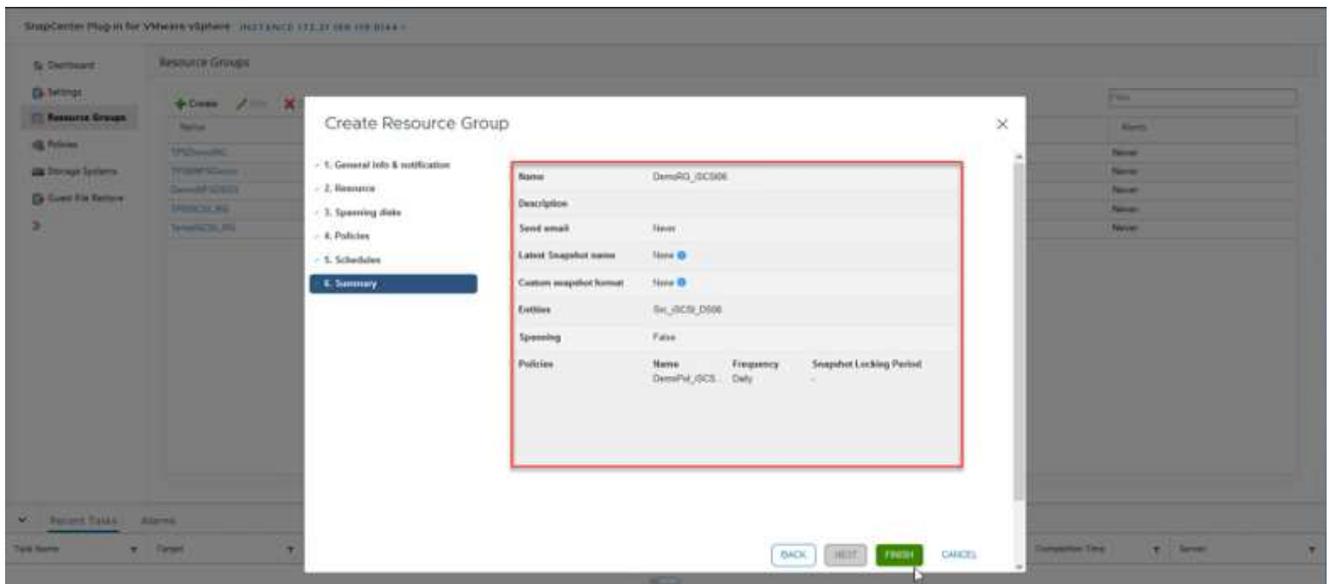


3. En la página Resources, seleccione el alcance (máquinas virtuales o almacenes de datos) y el centro de

datos.

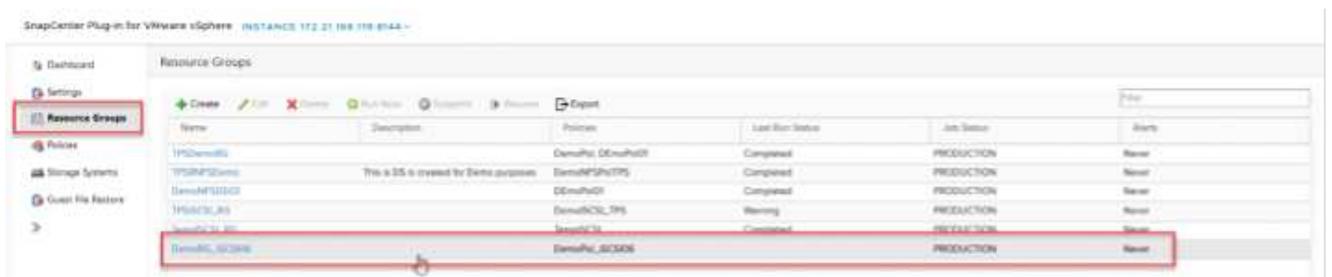


4. En la página Spanning Disks, seleccione una opción para Virtual Machines con varios VMDK en diferentes almacenes de datos
5. El siguiente paso es asociar una política de backup. Seleccione una política existente o cree una nueva.
6. En la página Schedules, configure la programación de backup para cada política seleccionada.



7. Una vez realizadas las selecciones adecuadas, haga clic en Finalizar.

Esto creará un nuevo grupo de recursos y lo añadirá a la lista de grupos de recursos.



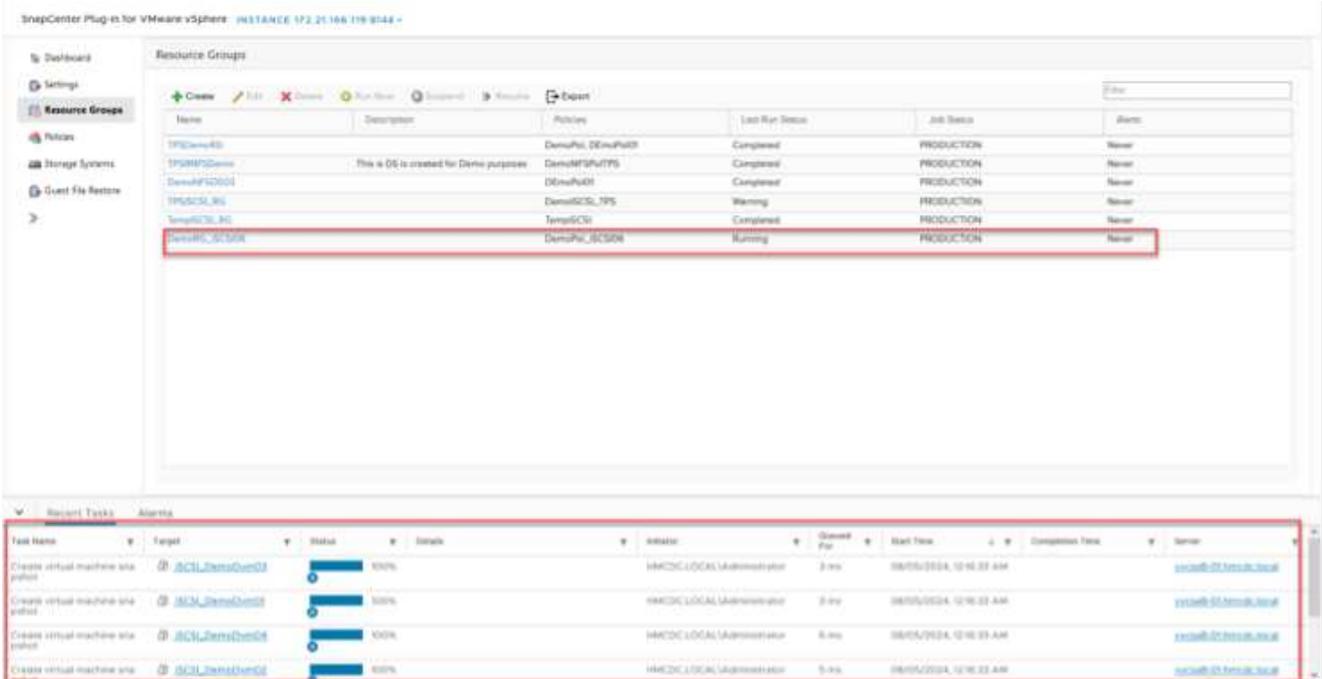
Realice un backup de los grupos de recursos

Ahora es el momento de activar un backup. Las operaciones de backup se ejecutan en todos los recursos definidos en un grupo de recursos. Si el grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

1. En la navegación izquierda de la página de cliente web de vCenter, seleccione SnapCenter Plug-in for VMware > Resource Groups y, a continuación, seleccione el grupo de recursos designado. Seleccione Run now para iniciar el backup ad-hoc.



2. Si el grupo de recursos tiene varias políticas configuradas, seleccione la política para la operación de backup en el cuadro de diálogo Backup Now.
3. Seleccione OK para iniciar el backup.

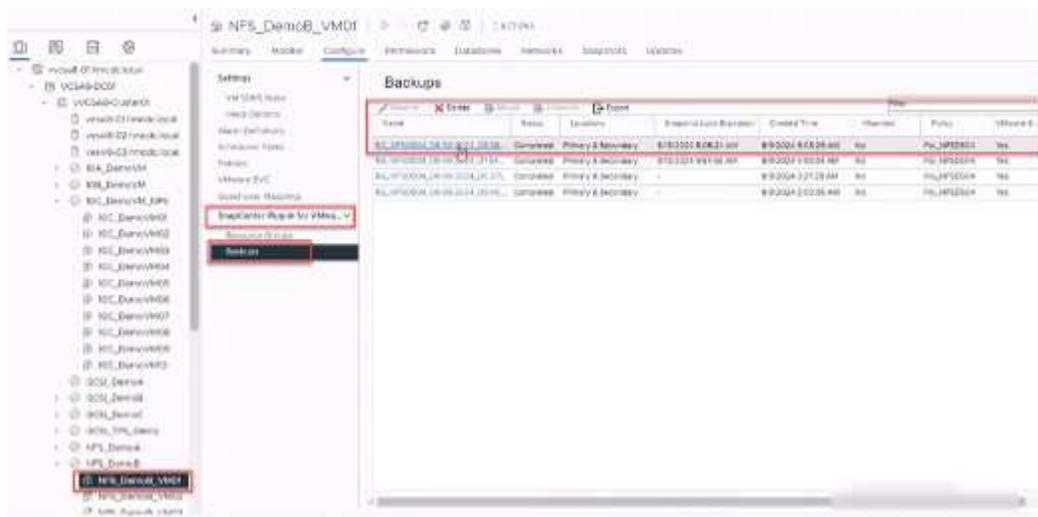


Supervise el progreso de las operaciones seleccionando Recent Tasks en la parte inferior de la ventana o en la consola Job Monitor para obtener más detalles.

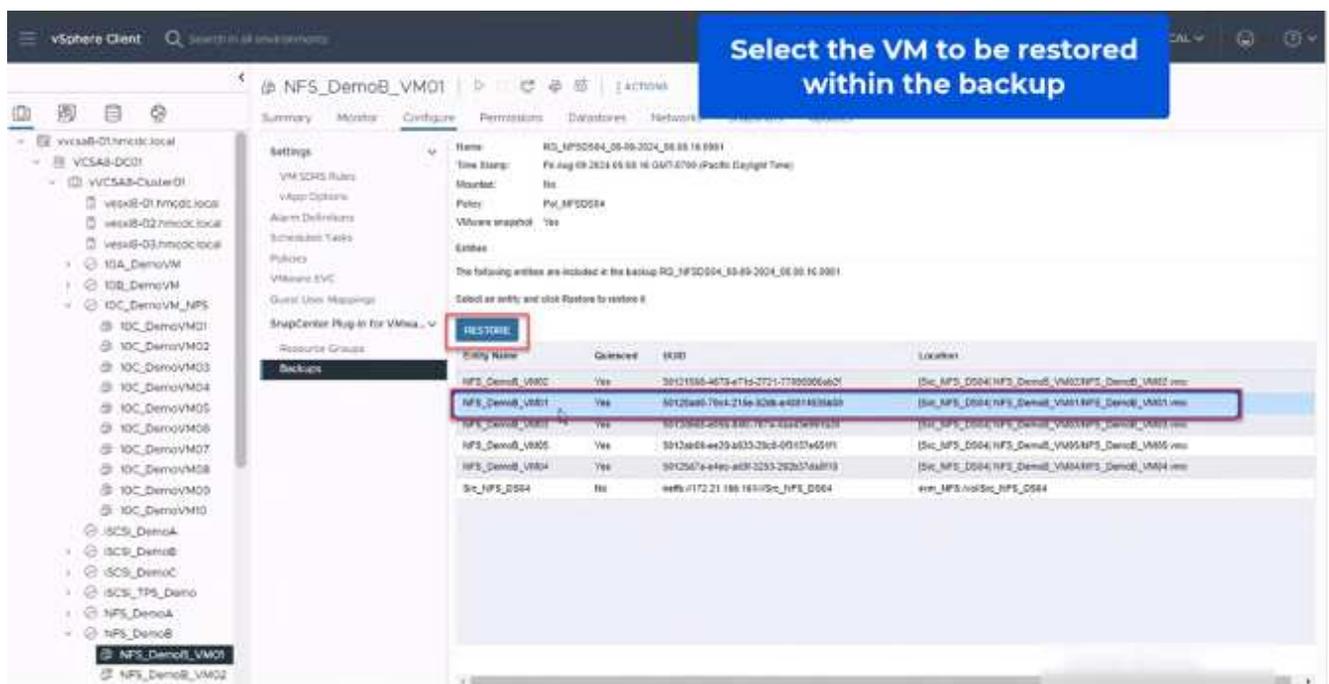
Restaurar máquinas virtuales desde backup

El plugin de SnapCenter para VMware permite restaurar máquinas virtuales (VM) en vCenter. Durante la restauración de una máquina virtual, se puede restaurar al almacén de datos original montado en el host ESXi original, que sobrescribirá el contenido existente con la copia de backup que se selecciona o se puede restaurar una máquina virtual eliminada/renombrada desde una copia de backup (la operación sobrescribe los datos en los discos virtuales originales). Para realizar la restauración, siga estos pasos:

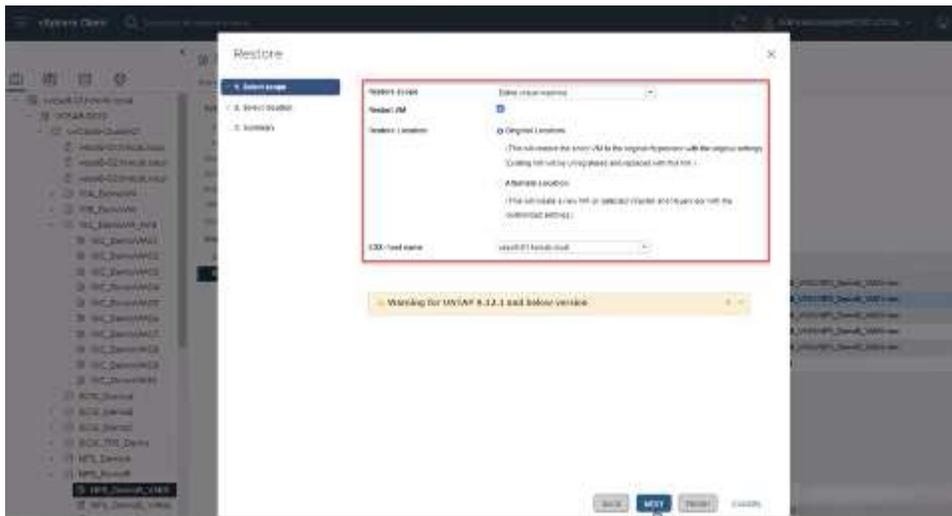
1. En la GUI de VMware vSphere Web Client, seleccione Menu en la barra de herramientas. Seleccione Inventory y, a continuación, Virtual Machines and Templates.
2. En la navegación de la izquierda, seleccione la máquina virtual y, a continuación, seleccione Configure, seleccione Backups en SnapCenter Plug-in for VMware. Haga clic en el trabajo de backup desde el que debe restaurarse la máquina virtual.



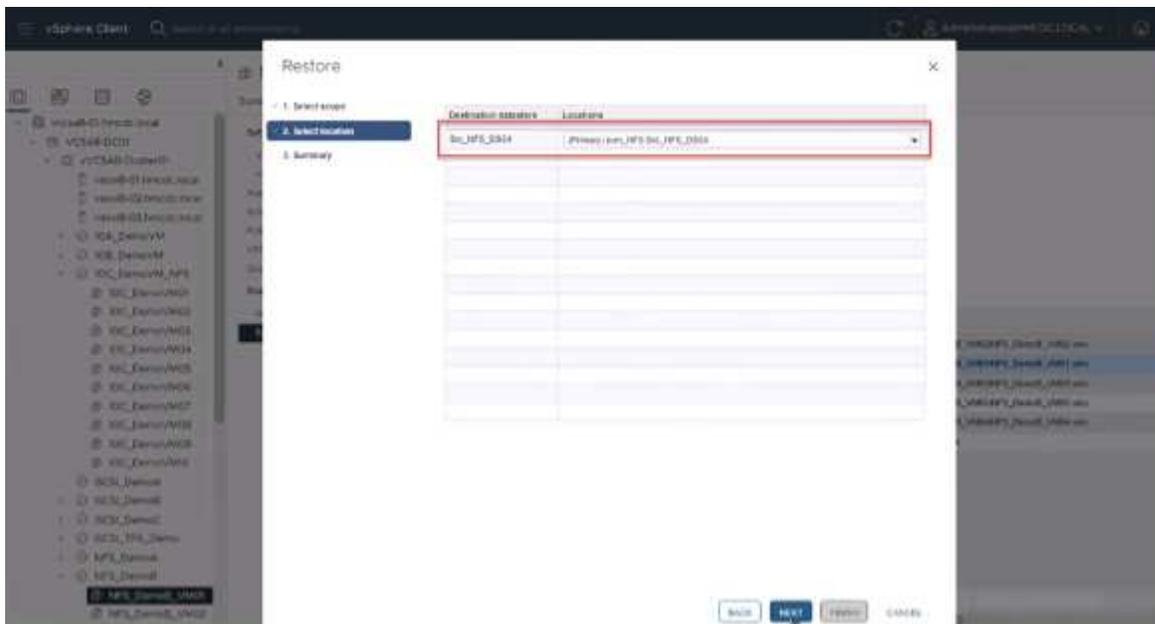
3. Seleccione la máquina virtual que necesita restaurar desde el backup.



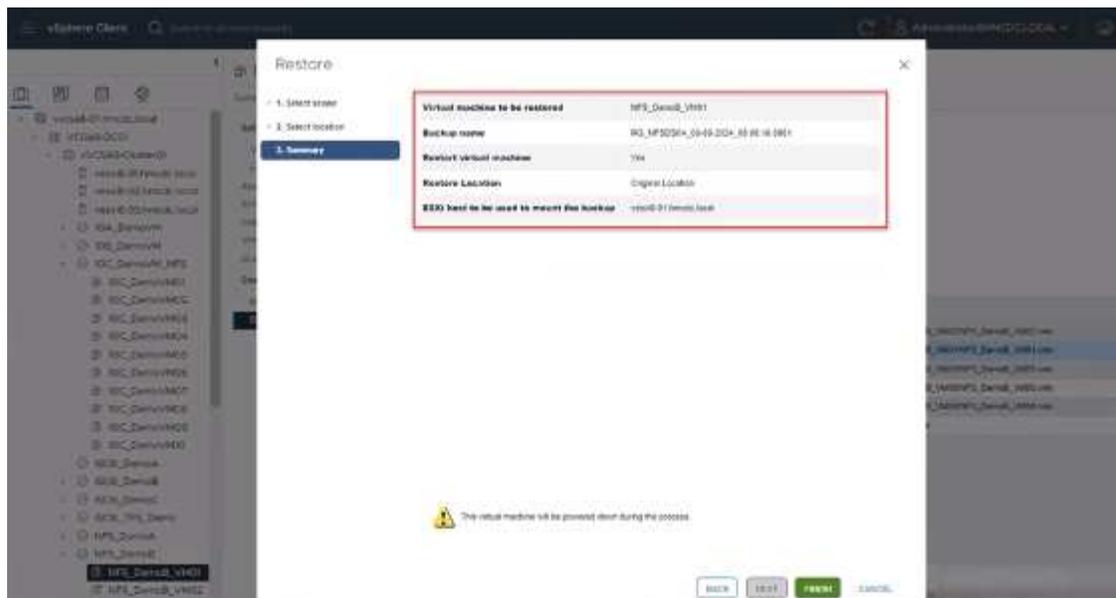
4. En la página Select Scope, seleccione Entire Virtual Machine en el campo Restore scope, a continuación, seleccione Restore location y, a continuación, introduzca la información ESXi de destino donde debe montarse el backup. Habilite la casilla de comprobación Restart VM si la máquina virtual debe encenderse después de la operación de restauración.



5. En la página Selección de ubicación, seleccione la ubicación de la ubicación principal.



6. Revise la página Summary y seleccione Finish.

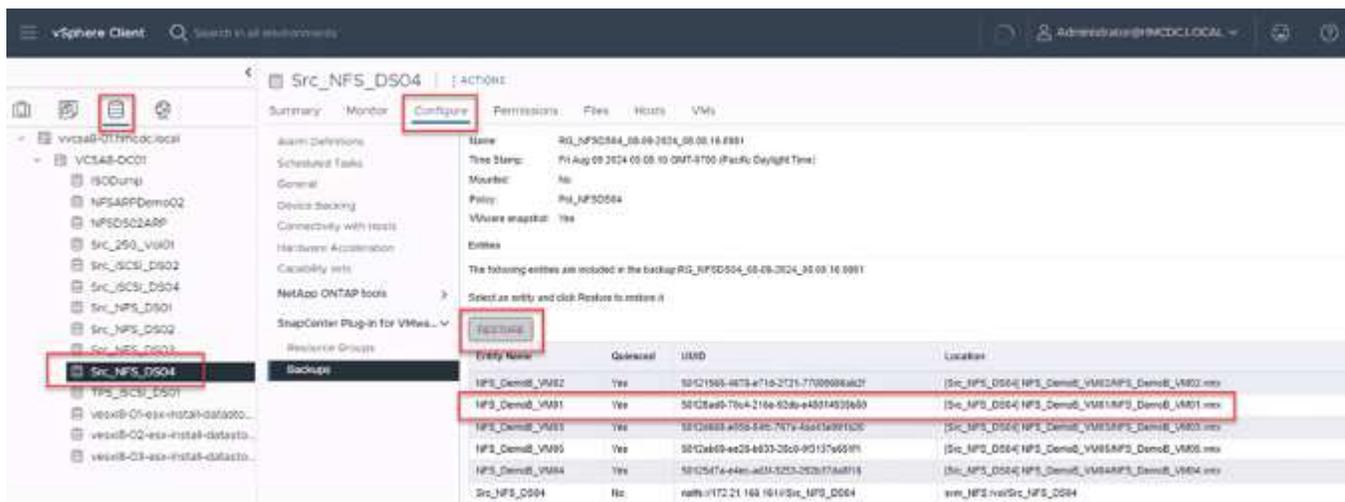


Supervise el progreso de las operaciones seleccionando Recent Tasks, en la parte inferior de la pantalla.



Aunque las máquinas virtuales se restauran, no se agregan automáticamente a sus primeros grupos de recursos. Por lo tanto, añada manualmente las máquinas virtuales restauradas a los grupos de recursos adecuados si requiere la protección de esas máquinas virtuales.

Ahora, ¿qué sucede si se eliminó la VM original? Es una tarea sencilla con el plug-in de SnapCenter para VMware. La operación de restauración para una máquina virtual eliminada puede ejecutarse desde el nivel de almacén de datos. Vaya a respectivo Datastore > Configure > Backups y seleccione la máquina virtual eliminada y seleccione Restore.

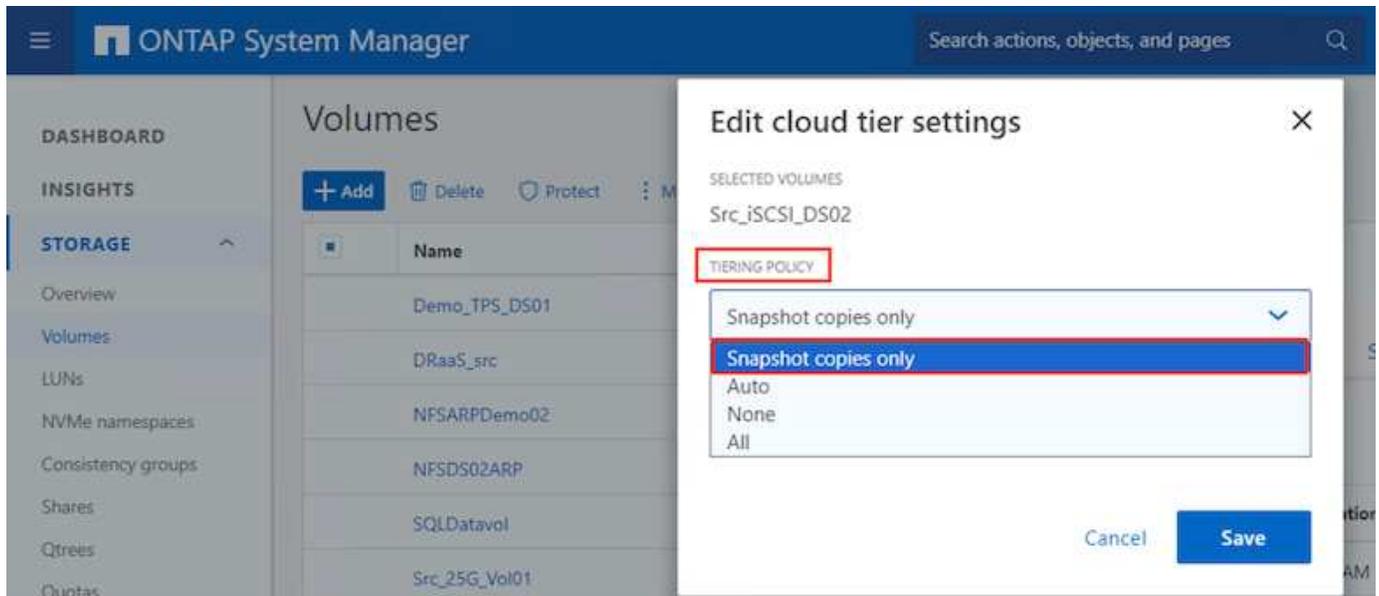


En resumen, al usar almacenamiento de ONTAP ASA para optimizar el TCO para una puesta en marcha de VMware, use el complemento SnapCenter para VMware como un método sencillo y eficiente para realizar backups de máquinas virtuales. Permite realizar backups y restauraciones de máquinas virtuales de una manera rápida y fluida, ya que los backups de copias Snapshot tardan literalmente segundos en completarse.

Consulte esto "[guía de soluciones](#)" y "[documentación de productos](#)" descubra más detalles sobre la configuración de SnapCenter, el backup, la restauración desde sistemas de almacenamiento principal o secundario, o incluso a partir de backups almacenados en un almacenamiento de objetos para retención a

largo plazo.

Para reducir los costes de almacenamiento, se puede permitir la organización en niveles de volúmenes de FabricPool para mover datos automáticamente para copias Snapshot a un nivel de almacenamiento de menor coste. Las copias Snapshot suelen utilizar más del 10 % del almacenamiento asignado. Si bien son importantes para la protección de datos y la recuperación ante desastres, estas copias puntuales rara vez se utilizan y no suponen un uso eficiente del almacenamiento de alto rendimiento. Con la normativa «solo Snapshot» para FabricPool, puede liberar espacio fácilmente en almacenamiento de alto rendimiento. Cuando se habilita esta política, los bloques de copia de Snapshot inactivos del volumen que no está usando el sistema de archivos activo se mueven al nivel de objetos y, una vez leída, la copia de Snapshot se mueve al nivel local para recuperar una máquina virtual o un almacén de datos entero. Este nivel de objetos puede estar en la forma de un cloud privado (como NetApp StorageGRID) o un cloud público (como AWS o Azure).

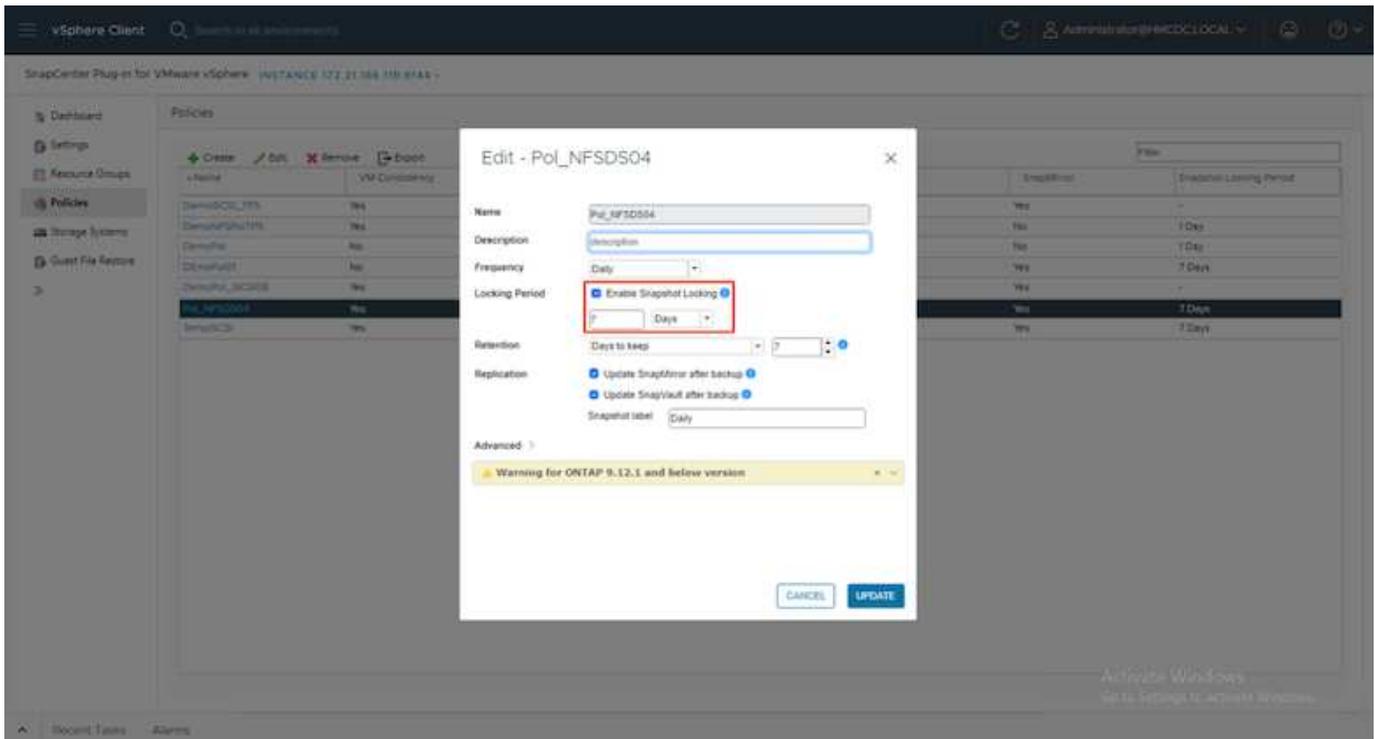


Ver orientación detallada para ["VMware vSphere con ONTAP"](#).

Protección contra ransomware

Una de las formas más efectivas para la protección contra ataques de ransomware es mediante la implementación de medidas de seguridad de múltiples capas. Cada máquina virtual que reside en un almacén de datos aloja un sistema operativo estándar. Asegúrese de que los paquetes de productos antimalware de servidor empresarial se instalan y se actualizan regularmente en ellos, lo que es un componente esencial de la estrategia de protección contra ransomware de varias capas. Además, implemente la protección de datos aprovechando la tecnología de copias Snapshot de NetApp para garantizar una recuperación rápida y fiable tras el ataque de ransomware.

Los ataques de ransomware se dirigen cada vez más a los backups y los puntos de recuperación de snapshots al intentar eliminarlos antes de empezar a cifrar archivos. Sin embargo, con ONTAP, esto se puede evitar creando snapshots a prueba de manipulaciones en sistemas primarios o secundarios ["Bloqueo de copia NetApp SnapShot™"](#) con en ONTAP. Estas copias de SnapVault no se pueden eliminar ni modificar por atacantes de ransomware ni administradores malintencionados, por lo que están disponibles incluso después de un ataque. Puede recuperar los datos de máquinas virtuales en segundos, lo que minimiza el tiempo de inactividad de la organización. Además, tiene la flexibilidad de elegir la programación de Snapshot y la duración del bloqueo que mejor se adapte a su organización.



Como parte de la adición de un método compuesto por varias capas, también existe una solución de ONTAP nativa incorporada para proteger la eliminación no autorizada de copias Snapshot de backup. Se conoce como verificación multiadmin o MAV, que está disponible en ONTAP 9.11,1 y versiones posteriores. El enfoque ideal será utilizar consultas para operaciones específicas de MAV.

Para obtener más información sobre MAV y cómo configurar sus capacidades de protección, consulte la ["Información general de verificación de varios administradores"](#).

Migración

Muchas ORGANIZACIONES DE TECNOLOGÍA adoptan un enfoque donde se prioriza el cloud híbrido cuando se someten a una fase de transformación. Los clientes están evaluando su INFRAESTRUCTURA TECNOLÓGICA actual y trasladando sus cargas de trabajo a la nube en función de esta evaluación y detección. Los motivos para migrar al cloud varían y pueden incluir factores como elasticidad y ráfaga, salida del centro de datos, consolidación del centro de datos, escenarios de fin de vida, fusiones, adquisiciones, etc. El razonamiento de migración de cada organización depende de sus prioridades empresariales específicas, siendo la optimización de costes la prioridad más alta. Seleccionar el almacenamiento en cloud adecuado es crucial para la transición al cloud híbrido, ya que libera el potencial de la puesta en marcha y la elasticidad del cloud.

Al integrarse con servicios 1P impulsados por NetApp en cada hiperescala, las organizaciones pueden lograr una solución cloud basada en vSphere con un método de migración sencillo, sin necesidad de volver a crear la plataforma, cambios de IP ni cambios en la arquitectura. Asimismo, esta optimización le permite escalar el espacio de almacenamiento a la vez que mantiene el número de hosts al menor tiempo necesario en vSphere, pero sin cambios en la jerarquía de almacenamiento, la seguridad ni los archivos que se han puesto a disposición.

- Ver orientación detallada para ["Migra cargas de trabajo al almacén de datos de FSx ONTAP"](#).
- Ver orientación detallada para ["Migre cargas de trabajo a un almacén de datos de Azure NetApp Files"](#).
- Ver orientación detallada para ["Migre cargas de trabajo al almacén de datos de Google Cloud NetApp Volumes"](#).

Recuperación ante desastres

Recuperación ante desastres entre sitios locales

Si desea obtener más información, visite ["Recuperación ante desastres mediante DRaaS de BlueXP para almacenes de datos de VMFS"](#)

Recuperación ante desastres entre on-premises y VMware Cloud en cualquier hiperescalador

Para aquellos clientes que buscan usar VMware Cloud en cualquier hiperescala como destino de recuperación ante desastres, se pueden usar almacenes de datos con tecnología de almacenamiento de ONTAP (Azure NetApp Files, FSx ONTAP, Google Cloud NetApp Volumes) para replicar datos de las instalaciones mediante cualquier solución de terceros validada que proporcione funcionalidad de replicación de máquinas virtuales. Al añadir almacenes de datos basados en el almacenamiento de ONTAP, se permitirá una recuperación ante desastres de costes optimizados en el destino con menos cantidad de hosts ESXi. Esto también permite retirar el sitio secundario en el entorno local, lo que ayuda a ahorrar significativamente en costes.

- Ver orientación detallada para ["Recuperación ante desastres para el almacén de datos ONTAP FSx"](#).
- Ver orientación detallada para ["Recuperación ante desastres en el almacén de datos de Azure NetApp Files"](#).
- Ver orientación detallada para ["Recuperación ante desastres en el almacén de datos de Google Cloud NetApp Volumes"](#).

Conclusión

Esta solución demuestra el enfoque óptimo para usar las tecnologías SAN de ONTAP y las herramientas de OFFTAP para proporcionar SERVICIOS TECNOLÓGICOS esenciales a las empresas, tanto ahora como en el futuro. Estas ventajas son especialmente beneficiosas para entornos virtualizados que ejecutan VMware vSphere en una configuración SAN. Gracias a la flexibilidad y la escalabilidad de los sistemas de almacenamiento de NetApp, las organizaciones pueden establecer la base para la actualización y ajuste de su infraestructura, lo que les permite satisfacer las cambiantes necesidades del negocio a lo largo del tiempo. Este sistema puede gestionar las cargas de trabajo actuales y mejorar la eficiencia de la infraestructura, reduciendo los costes operativos y preparando las cargas de trabajo futuras.

Cabina All-Flash SAN de NetApp con VMware vSphere 8

Cabina All-Flash SAN de NetApp con VMware vSphere 8

Durante casi dos décadas, el software NetApp ONTAP se ha situado como una solución de almacenamiento de primera categoría para entornos vSphere de VMware, introduciendo continuamente funciones innovadoras que simplifican la gestión y reducen los costes. NetApp es un líder establecido en el desarrollo de NAS y plataformas de almacenamiento unificado que ofrecen una amplia gama de compatibilidad con protocolos y conectividad. Junto con este segmento del mercado, hay muchos clientes que prefieren la simplicidad y las ventajas de coste de las plataformas de almacenamiento SAN basadas en bloques centradas en optimizar su trabajo. La cabina all-flash SAN (ASA) de NetApp cumple esa promesa con sencillez a escala y con funciones de gestión y automatización consistentes para todas las aplicaciones y los proveedores de cloud.

Autor: Josh Powell: Ingeniería de soluciones de NetApp

Descripción general de la solución

Objetivo de este documento

En este documento, trataremos el valor exclusivo del uso de sistemas de almacenamiento de NetApp ASA con vSphere de VMware y proporcionaremos una descripción general de la tecnología de la cabina SAN all-flash de NetApp. Además, veremos herramientas adicionales para simplificar el aprovisionamiento de almacenamiento y la protección de datos y la supervisión de tu centro de datos de VMware y ONTAP.

Las secciones de puesta en marcha de este documento tratan la creación de almacenes de datos VVOL con herramientas de ONTAP para VMware vSphere y la observabilidad del centro de datos moderno con NetApp Cloud Insights.

Visión general de la tecnología

Esta solución incluye tecnologías innovadoras de VMware y NetApp.

VMware vSphere 8,0

VMware vSphere es una plataforma de virtualización que transforma los recursos físicos en pools de informática, red y almacenamiento que se pueden utilizar para satisfacer los requisitos de las aplicaciones y las cargas de trabajo de los clientes. Entre los principales componentes de VMware vSphere se incluyen:

- **ESXi** - Hipervisor de VMware que permite la abstracción de procesadores de cómputo, memoria, red y otros recursos y los pone a disposición de máquinas virtuales y cargas de trabajo de contenedores.
- **VCenter** - VMware vCenter es una plataforma de gestión centralizada para interactuar con recursos informáticos, redes y almacenamiento como parte de una infraestructura virtual. VCenter desempeña un papel crucial en la simplificación de la administración de infraestructura virtualizada.

Nuevas mejoras en vSphere 8,0

vSphere 8,0 introduce algunas mejoras nuevas, entre las que se incluyen:

Escalabilidad - vSphere 8,0 es compatible con las CPU Intel y AMD más recientes y tiene límites extendidos para dispositivos vGPU, hosts ESXi, VM por clúster y dispositivos de E/S DirectPath de VM.

Distributed Services Engine - Descarga de red con NSX a unidades de procesamiento de datos (DPU).

- Eficiencia mejorada de dispositivos * - vSphere 8,0 aumenta las capacidades de administración de dispositivos con funciones como grupos de dispositivos y extensiones de virtualización de dispositivos (DVX).
- Seguridad mejorada * - La inclusión de un tiempo de espera SSH y la Política de provisión TPM fortalece el marco de seguridad.

Integración con servicios de nube híbrida - Esta característica facilita la transición sin interrupciones entre las cargas de trabajo en las instalaciones y en la nube.

- Tiempo de ejecución de Kubernetes integrado * - Con la inclusión de Tanzu, vSphere 8,0 simplifica la orquestación de contenedores.

Para obtener más información, consulte el blog, "[¿Qué novedades hay en vSphere 8?](#)".

Volúmenes virtuales de VMware (vVols)

vVols es un nuevo y revolucionario método de la gestión del almacenamiento en clústeres de vSphere que ofrece una gestión simplificada y un control más granular de los recursos de almacenamiento. En un almacén de datos vVols, cada disco virtual es un vVOL y se convierte en un objeto LUN nativo del sistema de almacenamiento. La integración del sistema de almacenamiento y vSphere se lleva a cabo a través del proveedor de la API de VMware para el conocimiento del almacenamiento (VASA)* y permite que el sistema de almacenamiento sea consciente de los datos de la VM y lo gestione en consecuencia. Las políticas de almacenamiento, definidas en vCenter Client, se utilizan para asignar y gestionar recursos de almacenamiento.

Los vVols constituyen un método simplificado de la gestión del almacenamiento y son preferibles en algunos casos prácticos.

Para obtener más información sobre vVols, consulte la ["Guía de inicio de vVols"](#).

NVMe sobre entramados

Con el lanzamiento de vSphere 8,0, ahora se admite NVMe integral, con compatibilidad total con vVols con NVMe-TCP y NVMe-FC.

Para obtener información detallada sobre el uso de NVMe con vSphere, consulte ["Acerca del almacenamiento NVMe de VMware"](#) En la documentación de vSphere Storage.

ONTAP de NetApp

El software ONTAP de NetApp lleva casi dos décadas siendo una solución de almacenamiento líder para entornos VMware vSphere y sigue agregando funcionalidades innovadoras que simplifican la gestión y reducen los costes. El uso de ONTAP junto con vSphere es una excelente combinación que le permite reducir los gastos en hardware del host y software de VMware. También puede proteger sus datos con un coste menor y un alto rendimiento uniforme, al tiempo que aprovecha las eficiencias del almacenamiento nativo.

Funciones básicas de ONTAP

Copias Snapshot de NetApp: Copias Snapshot de una máquina virtual o un almacén de datos, lo que garantiza que el rendimiento no afecte a la creación o utilización de una snapshot. Estas réplicas pueden servir como puntos de restauración para equipos virtuales o como una sencilla protección de datos. Estas copias Snapshot basadas en cabina son diferentes de las copias Snapshot de VMware (coherencia). El método más sencillo para generar una copia Snapshot de ONTAP es mediante el plugin de SnapCenter para VMware vSphere, que realiza backups de máquinas virtuales y almacenes de datos.

- **Eficiencia de almacenamiento** - ONTAP proporciona deduplicación y compresión en tiempo real y en segundo plano, deduplicación de bloques cero y compactación de datos.
- *** Volumen y movimiento de LUN *** - Permite el movimiento no disruptivo de volúmenes y LUN que admiten almacenes de datos de vSphere y vVols dentro del clúster de ONTAP para equilibrar el rendimiento y la capacidad o admitir mantenimiento y actualizaciones no disruptivas.
- **Reubicación de volumen y LUN** - ONTAP permite el movimiento no disruptivo de volúmenes y LUN que alojan almacenes de datos vSphere y vVols dentro del clúster de ONTAP. De este modo, se consigue equilibrar el rendimiento y la capacidad, y se pueden realizar actualizaciones sin interrupciones.
- **Calidad de servicio** - QoS es una característica que permite la administración del rendimiento en un LUN, volumen o archivo individual. Puede utilizarse para limitar una máquina virtual agresiva o para garantizar que una máquina virtual crítica reciba suficientes recursos de rendimiento.

- **Cifrado** - Cifrado de volumen NetApp y Cifrado agregado NetApp. Estas opciones proporcionan un enfoque sencillo basado en software para cifrar los datos en reposo y garantizar su protección.
- **Fabric Pool** - Esta función organiza en niveles los datos a los que se accede con menos frecuencia en un almacén de objetos separado, liberando valioso almacenamiento flash. Al operar a nivel de bloque, se identifican y clasifican en niveles los datos más inactivos de manera eficiente, lo que ayuda a optimizar los recursos de almacenamiento y reducir los costes.
- *** Automatización *** - Simplifica las tareas de almacenamiento y gestión de datos utilizando las API REST DE ONTAP para la automatización y aprovechando los módulos de Ansible para una gestión de configuración perfecta de los sistemas de ONTAP. Los módulos de Ansible ofrecen una solución práctica para gestionar de manera eficiente las configuraciones de los sistemas ONTAP. La combinación de estas potentes herramientas permite agilizar los flujos de trabajo y mejorar la gestión global de la infraestructura de almacenamiento.

Funcionalidades de recuperación ante desastres de ONTAP

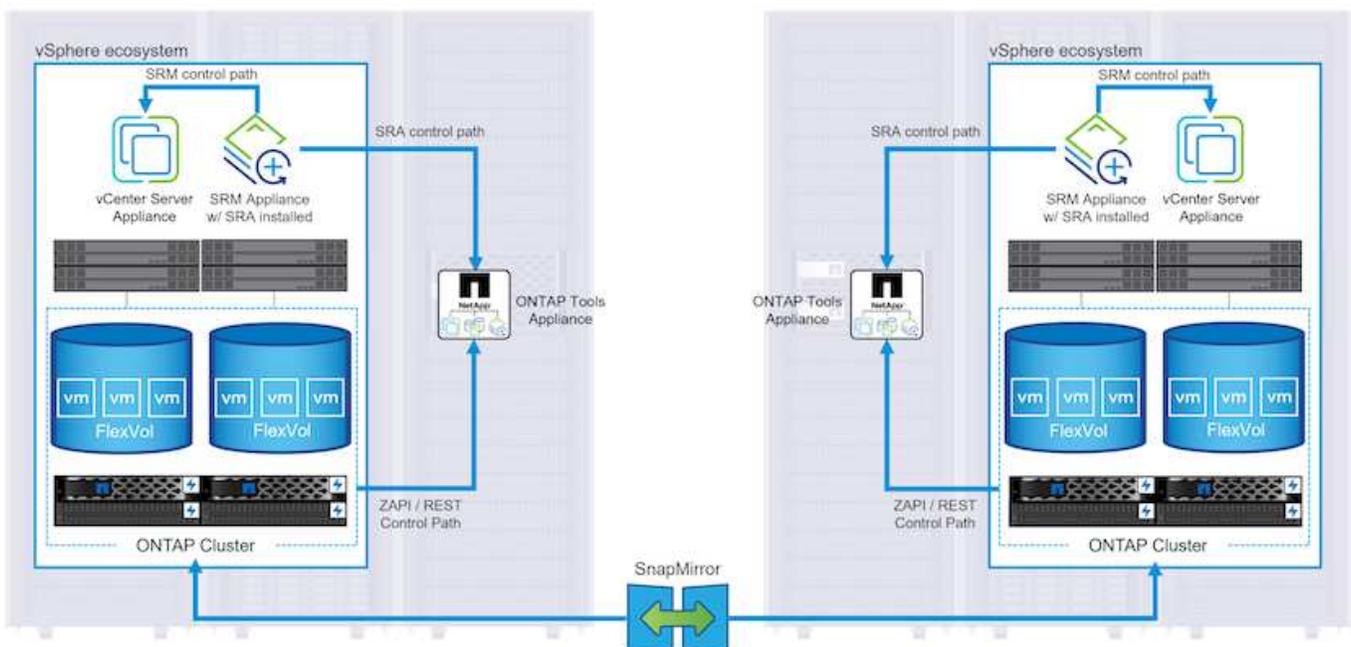
NetApp ONTAP ofrece soluciones sólidas de recuperación ante desastres para entornos VMware. Estas soluciones aprovechan las tecnologías de replicación de SnapMirror entre los sistemas de almacenamiento primario y secundario para permitir la recuperación tras fallos y una rápida recuperación en caso de fallo.

Adaptador de Replicación de Almacenamiento:

El adaptador de replicación de almacenamiento (SRA) de NetApp es un componente de software que ofrece integración entre los sistemas de almacenamiento de NetApp y el administrador de recuperación de sitio (SRM) de VMware. Facilita la replicación de datos de máquinas virtuales (VM) en las cabinas de almacenamiento de NetApp y ofrece funcionalidades sólidas de protección de datos y recuperación ante desastres. El SRA utiliza SnapMirror y SnapVault para lograr la replicación de datos de VM en sistemas de almacenamiento dispares o ubicaciones geográficas.

El adaptador proporciona replicación asíncrona en el nivel de máquina virtual de almacenamiento (SVM) mediante la tecnología SnapMirror y amplía la compatibilidad con VMFS en entornos de almacenamiento SAN (iSCSI y FC) y NFS en entornos de almacenamiento NAS.

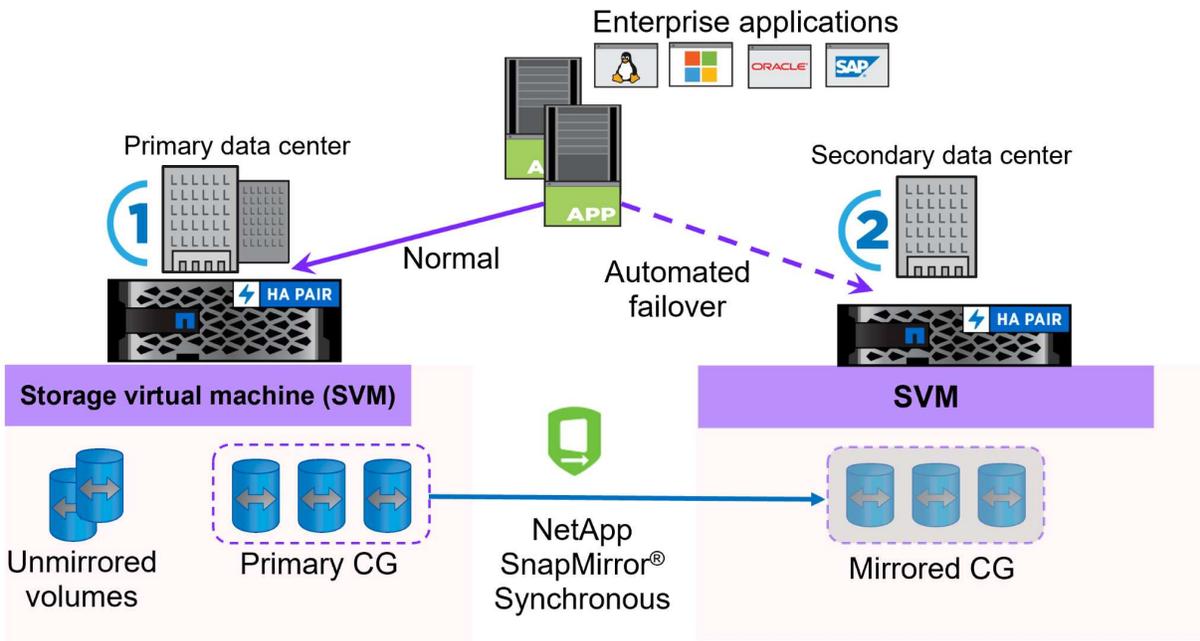
El SRA de NetApp se instala como parte de las herramientas de ONTAP para VMware vSphere.



Para obtener información sobre el adaptador de replicación de almacenamiento de NetApp para SRM, consulte ["VMware Site Recovery Manager con NetApp ONTAP"](#).

Continuidad del negocio de SnapMirror:

SnapMirror es una tecnología de replicación de datos de NetApp que proporciona replicación síncrona de datos entre sistemas de almacenamiento. Permite la creación de varias copias de los datos en ubicaciones diferentes, proporcionando la posibilidad de recuperar los datos en caso de desastre o pérdida de datos. SnapMirror ofrece flexibilidad en términos de frecuencia de replicación y permite la creación de copias de un momento específico de datos para fines de backup y recuperación de datos. SM-BC replica los datos a nivel del grupo de consistencia.



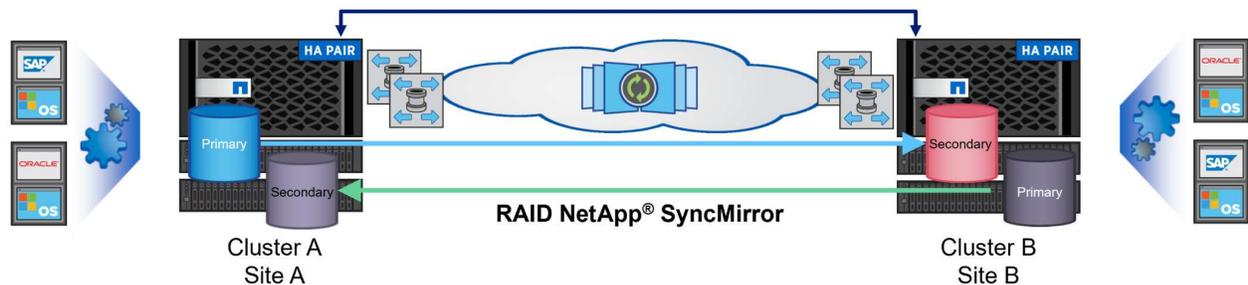
Si quiere más información, consulte SnapMirror ["Información general sobre la continuidad del negocio"](#).

NetApp MetroCluster:

NetApp MetroCluster es una solución de alta disponibilidad y de recuperación ante desastres que ofrece replicación de datos síncrona entre dos sistemas de almacenamiento de NetApp distribuidos geográficamente. Está diseñado para garantizar la disponibilidad y la protección continuas de los datos en caso de que se produzca un fallo en todo el site.

MetroCluster utiliza SyncMirror para replicar datos de manera síncrona justo por encima del nivel de RAID. SyncMirror se ha diseñado para realizar una transición eficiente entre modos síncronos y asíncronos. Esto permite que el clúster de almacenamiento principal siga funcionando en un estado no replicado en situaciones en las que el sitio secundario quede temporalmente inaccesible. SyncMirror también se volverá a replicar en un estado RPO = 0 cuando se restaure la conectividad.

MetroCluster puede funcionar sobre redes basadas en IP o utilizando Fibre Channel.



Para obtener información detallada sobre la arquitectura y configuración de MetroCluster, consulte la "[Sitio de documentación de MetroCluster](#)".

Modelo de licencias de ONTAP One

ONTAP One es un completo modelo de licencias que proporciona acceso a todas las funciones de ONTAP sin necesidad de licencias adicionales. Esto incluye la protección de datos, recuperación ante desastres, alta disponibilidad, integración del cloud, eficiencia del almacenamiento, rendimiento y seguridad. Los clientes con sistemas de almacenamiento de NetApp con licencias Flash, Core más Data Protection o Premium pueden obtener licencias de ONTAP One y así maximizar el aprovechamiento de sus sistemas de almacenamiento.

La licencia de ONTAP One incluye todas las siguientes funciones:

NVMeoF – Permite el uso de NVMe over Fabrics para la E/S de cliente front-end, tanto NVMe/FC como NVMe/TCP.

FlexClone – Permite la creación rápida de la clonación eficiente del espacio de datos basada en instantáneas.

S3 – Permite el protocolo S3 para la E/S del cliente front-end.

SnapRestore – Permite la rápida recuperación de datos de instantáneas.

Protección contra ransomware autónoma - Permite la protección automática de los recursos compartidos de archivos del NAS cuando se detecta una actividad anormal del sistema de archivos.

- Multi Tenant Key Manager * - Permite la capacidad de tener varios administradores de claves para diferentes inquilinos en el sistema.

SnapLock – Permite la protección de los datos contra la modificación, eliminación o corrupción en el sistema.

SnapMirror Cloud – Permite la replicación de volúmenes del sistema a objetivos de objetos.

S3 SnapMirror – Permite la replicación de objetos de ONTAP S3 para alternar destinos compatibles con S3.

Cabina All-Flash SAN NetApp

La cabina all-flash SAN (ASA) de NetApp es una solución de almacenamiento de alto rendimiento diseñada para satisfacer los requisitos más exigentes de los centros de datos modernos. Combina la velocidad y la fiabilidad del almacenamiento flash con las funciones avanzadas de gestión de datos de NetApp para ofrecer un rendimiento, una escalabilidad y una protección de datos excepcionales.

La gama ASA está compuesta por los modelos A-Series y C-Series.

Las cabinas flash all-NVMe NetApp A-Series están diseñadas para cargas de trabajo de alto rendimiento, con una latencia ultrabaja y una alta resiliencia, lo que las convierte en adecuadas para aplicaciones de misión crítica.



Las cabinas flash QLC de C-Series se dirigen a casos de uso de mayor capacidad, y ofrecen la velocidad de la tecnología flash con la economía del flash híbrido.



Para obtener información detallada, consulte ["Página de destino de NetApp ASA"](#).

Funciones de NetApp ASA

La cabina all-flash SAN NetApp incluye las siguientes funciones:

Rendimiento - La cabina SAN All-Flash aprovecha las unidades de estado sólido (SSD), con una arquitectura NVMe integral, para proporcionar un rendimiento increíblemente rápido, reduciendo significativamente la latencia y mejorando los tiempos de respuesta de las aplicaciones. Ofrece una alta tasa constante de IOPS y baja latencia, lo que lo convierte en adecuado para cargas de trabajo sensibles a la latencia, como bases de datos, virtualización y análisis.

- Escalabilidad * - Las cabinas SAN All-Flash de NetApp se crean con una arquitectura de escalado horizontal, lo que permite a las organizaciones escalar sin problemas su infraestructura de almacenamiento a medida que crecen sus necesidades. Gracias a la capacidad de añadir nodos de almacenamiento adicionales, las organizaciones pueden ampliar la capacidad y el rendimiento sin interrupciones, lo que garantiza que su almacenamiento pueda satisfacer las crecientes demandas de datos.
- Gestión de datos *: El sistema operativo Data ONTAP de NetApp incorpora la cabina All-Flash SAN, que ofrece un conjunto completo de funciones de gestión de datos. Estas incluyen thin provisioning, la deduplicación, la compresión y la compactación de datos, que optimizan el aprovechamiento del

almacenamiento y reducen los costes. Las funciones de protección de datos avanzadas, como snapshots, replicación y cifrado, garantizan la integridad y la seguridad de los datos almacenados.

Integración y flexibilidad: La cabina SAN All-Flash se integra con el ecosistema más amplio de NetApp, lo que permite una integración perfecta con otras soluciones de almacenamiento de NetApp, como implementaciones de clouds híbridos con NetApp Cloud Volumes ONTAP. Además, admite protocolos estándares del sector como Fibre Channel (FC) e iSCSI, lo que permite la integración fácil en las infraestructuras SAN existentes.

- **Análisis y automatización*:** El software de gestión de NetApp, incluido NetApp Cloud Insights, proporciona funcionalidades completas de supervisión, análisis y automatización. Estas herramientas permiten a los administradores obtener información sobre su entorno de almacenamiento, optimizar el rendimiento y automatizar las tareas rutinarias, simplificar la gestión del almacenamiento y mejorar la eficiencia operativa.
- **Protección de datos y continuidad empresarial *:** La cabina SAN All-Flash ofrece funciones integradas de protección de datos, como instantáneas puntuales, replicación y capacidades de recuperación ante desastres. Estas funciones garantizan la disponibilidad de datos y facilitan una rápida recuperación en caso de pérdida de datos o de fallos del sistema.

Compatibilidad con protocolos

ASA admite todos los protocolos SAN estándar, incluidos iSCSI, Fibre Channel (FC), Fibre Channel sobre Ethernet (FCoE) y NVMe over Fabrics.

iSCSI - NetApp ASA proporciona una sólida compatibilidad con iSCSI, lo que permite el acceso a nivel de bloque a dispositivos de almacenamiento a través de redes IP. Ofrece una integración perfecta con iniciadores iSCSI, lo que permite aprovisionar y gestionar LUN iSCSI de manera eficaz. Funciones avanzadas de ONTAP, como rutas múltiples, autenticación CHAP y compatibilidad con ALUA.

Para obtener una guía de diseño sobre configuraciones de iSCSI, consulte .

Canal de fibra - NetApp ASA ofrece soporte integral para el canal de fibra (FC), una tecnología de red de alta velocidad comúnmente utilizada en redes de área de almacenamiento (SAN). ONTAP se integra sin problemas con la infraestructura de FC y proporciona un acceso por bloques fiable y eficiente a los dispositivos de almacenamiento. Ofrece funciones como la división en zonas, las rutas múltiples y el inicio de sesión estructural (FLOGI) para optimizar el rendimiento, mejorar la seguridad y garantizar una conectividad perfecta en entornos FC.

Para obtener directrices de diseño sobre configuraciones de Fibre Channel, consulte ["Documentación de referencia de configuración de SAN"](#).

NVMe over Fabrics - NetApp ONTAP y ASA admiten NVMe over Fabrics. NVMe/FC permite utilizar dispositivos de almacenamiento NVMe sobre infraestructura Fibre Channel y NVMe/TCP sobre redes IP de almacenamiento.

Para obtener directrices de diseño en NVMe, consulte ["Configuración, compatibilidad y limitaciones de NVMe"](#).

Tecnología activo-activo

Las cabinas NetApp All-Flash SAN permiten rutas activo-activo que pasan por ambas controladoras, por lo que no es necesario que el sistema operativo host espere a que se produzca un error en una ruta activa antes de activar la ruta alternativa. Esto significa que el host puede utilizar todas las rutas disponibles en todas las controladoras, asegurando que las rutas activas siempre estén presentes sin importar si el sistema está en estado constante o si se debe someter a una operación de conmutación por error de la controladora.

Además, NetApp ASA ofrece una función distintiva que mejora significativamente la velocidad de la conmutación por error de SAN. Cada controladora replica continuamente los metadatos LUN esenciales con su asociado. Como resultado, cada controladora está preparada para asumir las responsabilidades del servicio de datos en caso de un fallo repentino de su compañero. Esta preparación es posible debido a que la controladora ya posee la información necesaria para comenzar a utilizar las unidades que se gestionaron previamente por la controladora con el error.

Con rutas activo-activo, las tomas de control planificadas y sin planificar tienen tiempos de reanudación de I/O de 2-3 segundos.

Para obtener más información, consulte ["TR-4968, cabina All-SAS NetApp: Disponibilidad e integridad de los datos con NetApp ASA"](#).

Garantías de almacenamiento

NetApp ofrece un conjunto único de garantías de almacenamiento con cabinas SAN All-Flash NetApp. Sus ventajas únicas incluyen:

- **Garantía de eficiencia de almacenamiento:** * Consiga un alto rendimiento al tiempo que minimiza el costo de almacenamiento con la Garantía de Eficiencia de Almacenamiento. 4:1 para cargas de trabajo SAN.

Garantía de disponibilidad de datos de 6 Nines (99,9999%): garantiza la corrección de los tiempos de inactividad no planificados en más de 31,56 segundos al año.

Garantía de recuperación de ransomware: Recuperación de datos garantizada en caso de un ataque de ransomware.

Consulte ["Portal de productos de NetApp ASA"](#) si quiere más información.

Complementos de NetApp para VMware vSphere

Los servicios de almacenamiento de NetApp se integran perfectamente con VMware vSphere mediante el uso de los siguientes plugins:

Herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware permiten a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Las herramientas de ONTAP incluyen los siguientes componentes:

Virtual Storage Console (VSC): El VSC incluye la interfaz integrada con el cliente vSphere, donde puede agregar controladores de almacenamiento, aprovisionar almacenes de datos, supervisar el rendimiento de los almacenes de datos y ver y actualizar la configuración del host ESXi.

- **Proveedor VASA:** * El proveedor de API de VMware vSphere para ONTAP envía información sobre el almacenamiento utilizado por VMware vSphere al servidor vCenter, lo que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidad de

almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

Adaptador de replicación de almacenamiento (SRA): Cuando se habilita y se usa con VMware Site Recovery Manager (SRM), SRA facilita la recuperación de los almacenes de datos de vCenter Server y las máquinas virtuales en caso de fallo, lo que permite la configuración de sitios protegidos y sitios de recuperación para recuperación ante desastres.

Para obtener más información sobre las herramientas de NetApp ONTAP para VMware, consulte ["Herramientas de ONTAP para documentación de VMware vSphere"](#).

Plugin de SnapCenter para VMware vSphere

El plugin de SnapCenter para VMware vSphere (SCV) es una solución de software de NetApp que ofrece una protección de datos completa para entornos VMware vSphere. Está diseñado para simplificar y agilizar el proceso de protección y gestión de máquinas virtuales y almacenes de datos.

El plugin de SnapCenter para VMware vSphere ofrece las siguientes funcionalidades en una interfaz unificada, integrada con el cliente de vSphere:

Instantáneas basadas en políticas - SnapCenter le permite definir políticas para crear y administrar instantáneas consistentes con aplicaciones de máquinas virtuales (VM) en VMware vSphere.

- Automatización * - La creación y gestión automatizada de instantáneas basadas en políticas definidas ayudan a garantizar una protección de datos consistente y eficiente.

VM-Level Protection - La protección granular a nivel de VM permite una gestión y recuperación eficientes de máquinas virtuales individuales.

- Características de eficiencia del almacenamiento * - La integración con las tecnologías de almacenamiento de NetApp proporciona funciones de eficiencia del almacenamiento como deduplicación y compresión para instantáneas, minimizando los requisitos de almacenamiento.

El complemento de SnapCenter orquesta el modo inactivo de máquinas virtuales junto con los snapshots basados en hardware en las cabinas de almacenamiento de NetApp. La tecnología SnapMirror se utiliza para replicar copias de backups en sistemas de almacenamiento secundarios, incluso en el cloud.

Para obtener más información, consulte ["Documentación del plugin de SnapCenter para VMware vSphere"](#).

La integración de BlueXP habilita estrategias de backup de 3-2-1 que amplían las copias de datos en el almacenamiento de objetos en el cloud.

Para obtener más información sobre estrategias de backup 3-2-1 con BlueXP, visita ["3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales"](#).

Cloud Insights de NetApp

NetApp Cloud Insights simplifica la observación de la infraestructura on-premises y de nube, y proporciona funcionalidades de análisis y solución de problemas para ayudar a resolver problemas complejos. Cloud Insights funciona recogiendo datos de un entorno de centro de datos y enviándolos al cloud. Esto se realiza con un software instalado localmente denominado Unidad de adquisición y con recopiladores específicos habilitados para los activos en el centro de datos.

Los activos de Cloud Insights se pueden etiquetar con anotaciones que proporcionan un método de organizar y clasificar los datos. El panel de control se puede crear utilizando una amplia variedad de widgets para mostrar los datos y se pueden crear consultas de métricas para obtener vistas tabulares detalladas de los datos.

Cloud Insights viene con un gran número de paneles de control listos para usar que ayudan a centrarse en tipos específicos de áreas problemáticas y categorías de datos.

Cloud Insights es una herramienta heterogénea diseñada para recopilar datos de una amplia gama de dispositivos. Sin embargo, existe una biblioteca de plantillas, llamada ONTAP Essentials, que permite a los clientes de NetApp empezar a trabajar rápidamente.

Si desea obtener información detallada sobre cómo empezar a usar Cloud Insights, consulte la ["Página de inicio de BlueXP y Cloud Insights de NetApp"](#).

Cabina All-Flash SAN de NetApp con VMware vSphere 8

Las herramientas de ONTAP para VMware permiten a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Autor: Josh Powell: Ingeniería de soluciones de NetApp

Gestión del almacenamiento en bloques con las herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP incluyen los siguientes componentes:

Virtual Storage Console (VSC): El VSC incluye la interfaz integrada con el cliente vSphere, donde puede agregar controladores de almacenamiento, aprovisionar almacenes de datos, supervisar el rendimiento de los almacenes de datos y ver y actualizar la configuración del host ESXi.

- **Proveedor VASA:** * El proveedor de API de VMware vSphere para ONTAP envía información sobre el almacenamiento utilizado por VMware vSphere al servidor vCenter, lo que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidad de almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

Adaptador de replicación de almacenamiento (SRA): Cuando se habilita y se usa con VMware Site Recovery Manager (SRM), SRA facilita la recuperación de los almacenes de datos de vCenter Server y las máquinas virtuales en caso de fallo, lo que permite la configuración de sitios protegidos y sitios de recuperación para recuperación ante desastres.

Para obtener más información sobre las herramientas de NetApp ONTAP para VMware, consulte ["Herramientas de ONTAP para documentación de VMware vSphere"](#).

Descripción general de la puesta en marcha de soluciones

En esta solución demostraremos el uso de las herramientas ONTAP para VMware vSphere para aprovisionar almacenes de datos de VMware Virtual Volumes (VVOL) y crear una máquina virtual en un almacén de datos

de VVOL.

En un almacén de datos vVols, cada disco virtual es un VVOL y se convierte en un objeto LUN nativo del sistema de almacenamiento. La integración del sistema de almacenamiento y vSphere se realiza a través del proveedor VASA (que se instala con las herramientas de ONTAP) de las API de VMware y permite al sistema de almacenamiento conocer los datos de los equipos virtuales y gestionarlos de la forma correspondiente. Las políticas de almacenamiento, definidas en vCenter Client, se utilizan para asignar y gestionar recursos de almacenamiento.

Para obtener información detallada sobre vVols con ONTAP, consulte ["Volúmenes virtuales vVols\) con ONTAP"](#).

Esta solución cubre los siguientes pasos generales:

1. Añadir un sistema de almacenamiento en Herramientas de ONTAP.
2. Crear un perfil de capacidad de almacenamiento en las herramientas de ONTAP.
3. Cree un almacén de datos vVols en Herramientas de ONTAP.
4. Cree una política de almacenamiento de máquinas virtuales en el cliente de vSphere.
5. Cree una máquina virtual nueva en el almacén de datos de VVol.

Requisitos previos

En esta solución se utilizaron los siguientes componentes:

1. Cabina All-Flash SAN A400 de NetApp con ONTAP 9,13.
2. ISCSI SVM creada en la ASA con conectividad de red a los hosts ESXi.
3. Herramientas de ONTAP para VMware vSphere 9,13 (proveedor VASA habilitado de forma predeterminada).
4. Clúster 8,0 de vSphere (dispositivo de vCenter y hosts ESXi).

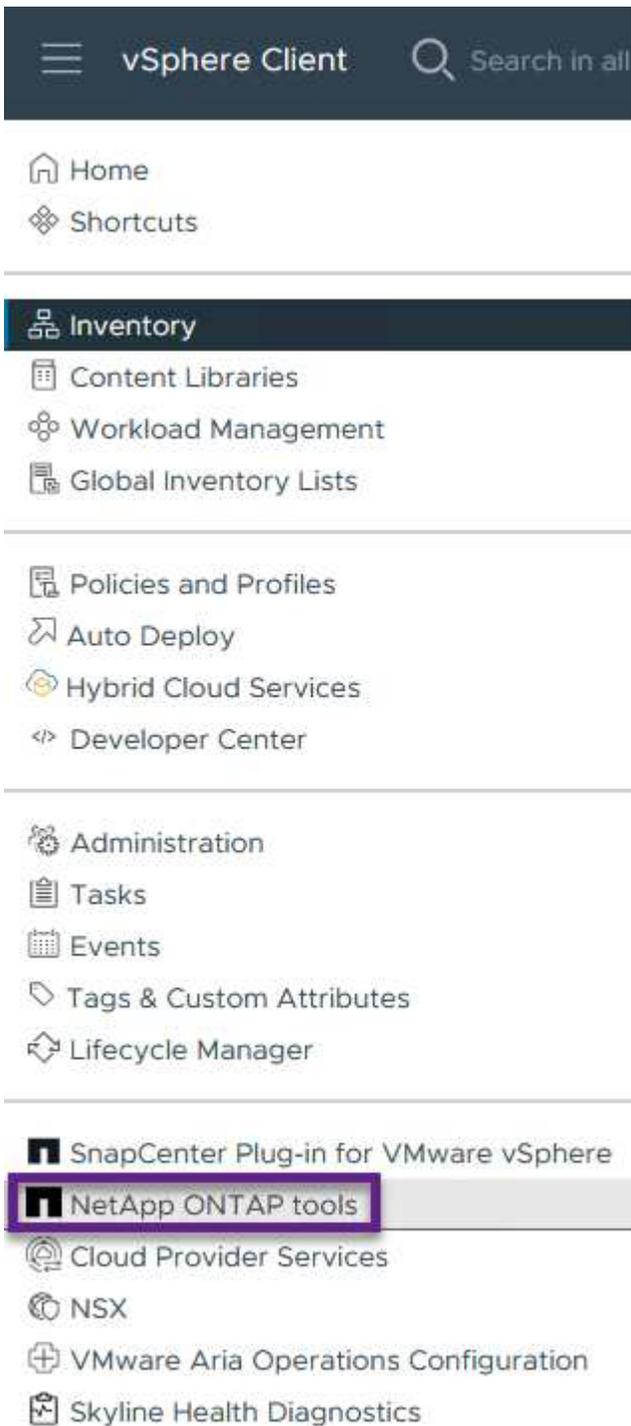
Puesta en marcha de la solución

Cree un almacén de datos vVols en Herramientas de ONTAP

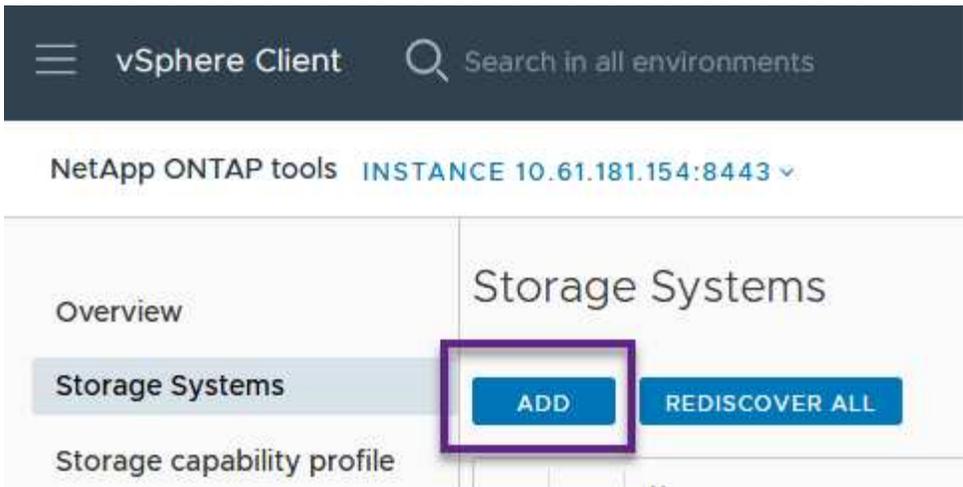
Para crear un almacén de datos vVols en Herramientas de ONTAP, lleve a cabo los siguientes pasos:

Agregar un sistema de almacenamiento a las herramientas de ONTAP.

1. Acceda a herramientas de NetApp ONTAP seleccionándolo en el menú principal del vSphere Client.



2. En Herramientas de ONTAP seleccione **Sistemas de almacenamiento** en el menú de la izquierda y luego presione **Añadir**.



3. Rellene la dirección IP, las credenciales del sistema de almacenamiento y el número de puerto. Haga clic en **Add** para iniciar el proceso de descubrimiento.

Add Storage System

i Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

Name or IP address:

Username:

Password:

Port:

Advanced options **^**

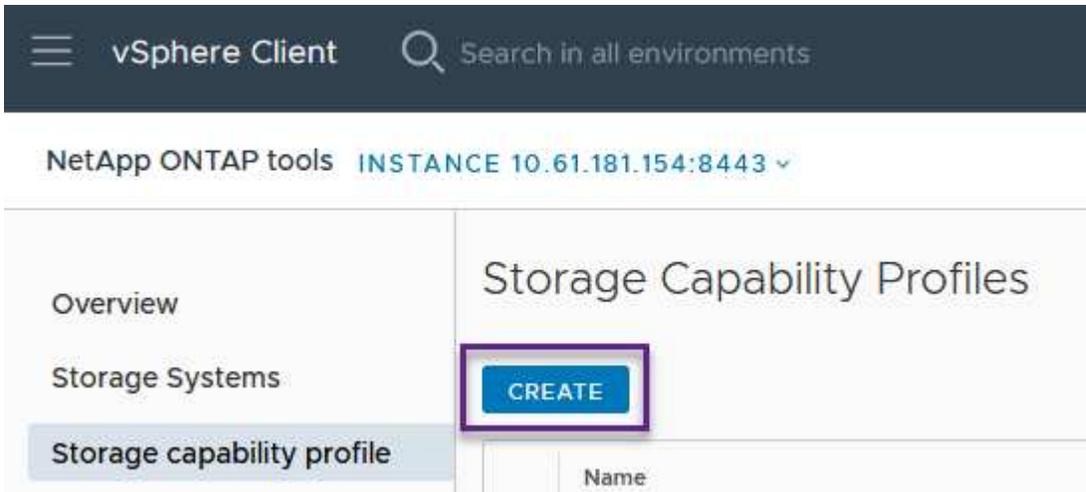
ONTAP Cluster Certificate: Automatically fetch Manually upload

Crear un perfil de capacidad de almacenamiento en las herramientas de ONTAP

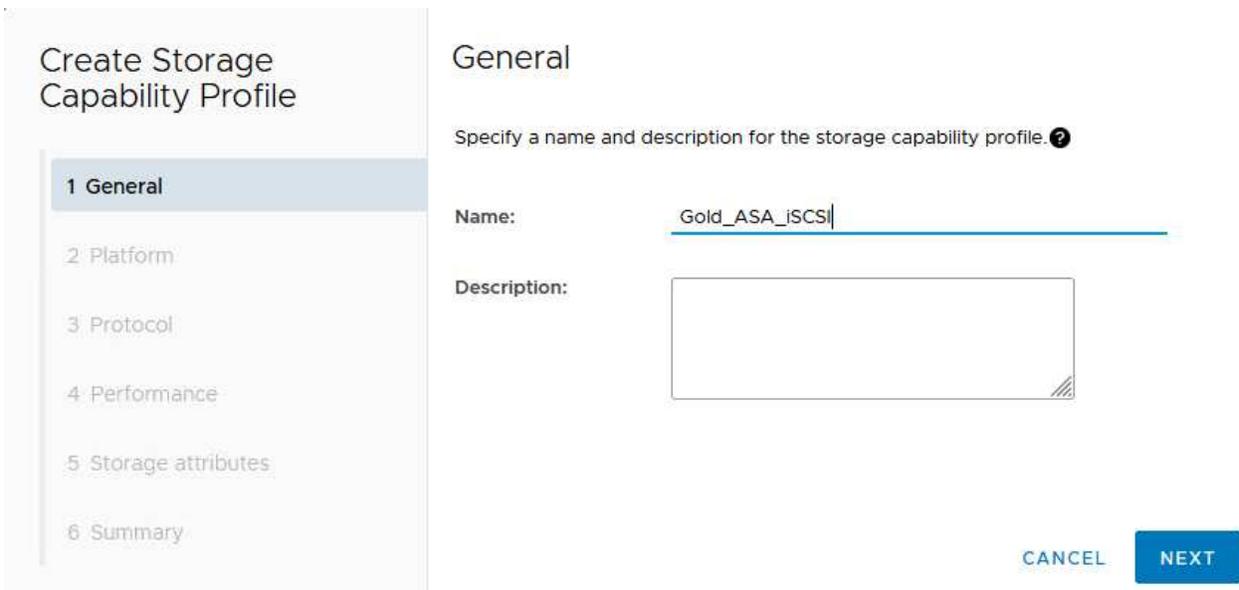
Los perfiles de funcionalidad de almacenamiento describen las funciones de una cabina de almacenamiento o un sistema de almacenamiento. Incluyen definiciones de calidad de servicio y se utilizan para seleccionar sistemas de almacenamiento que cumplan con los parámetros definidos en el perfil.

Para crear un perfil de funcionalidad del almacenamiento en las herramientas de ONTAP, 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 de **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 debe ser una cabina SAN All-Flash establecida en **asimétrica** en false.

Create Storage Capability Profile

- 1 General
- 2 Platform**
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

4. A continuación, seleccione la opción de protocolo o * cualquiera * para permitir todos los protocolos posibles. Haga clic en **Siguiente** para continuar.

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

5. La página **PERFORMANCE** permite establecer la calidad del servicio en forma de IOPS mínima y máxima permitida.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Storage attributes

Deduplication:

Yes



Compression:

Yes



Space reserve:

Thin



Encryption:

No



Tiering policy (FabricPool):

None



CANCEL

BACK

NEXT

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
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	No
Tiering policy (FabricPool):	None

CANCEL

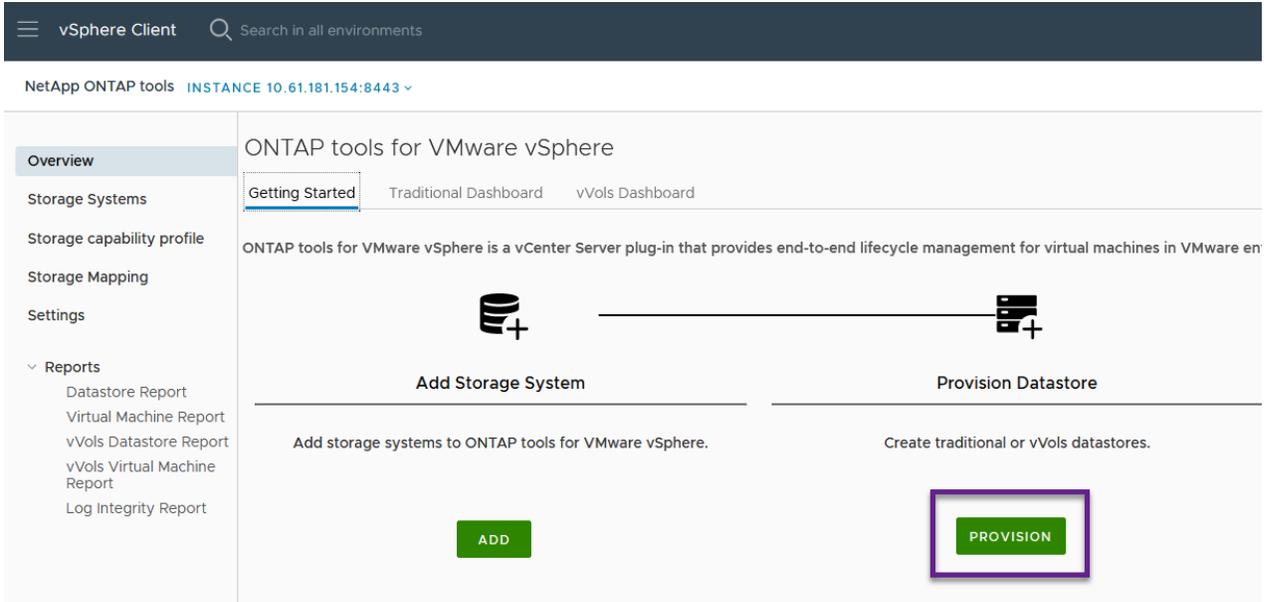
BACK

FINISH

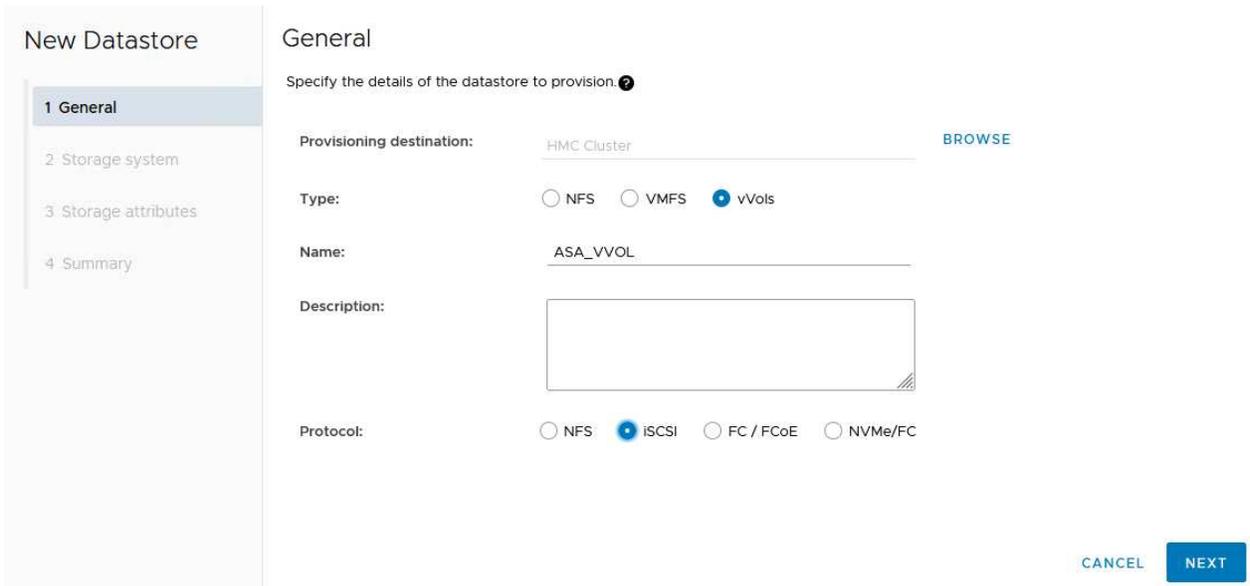
Cree un almacén de datos vVols en Herramientas de ONTAP

Para crear un almacén de datos vVols en Herramientas de ONTAP, lleve a cabo los siguientes pasos:

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



2. En la página **General** del asistente New Datastore, seleccione el centro de datos de vSphere o el destino del clúster. Seleccione **vVols** como tipo de datastore, rellene un nombre para el almacén de datos y seleccione el protocolo.



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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

FAS_Default
FAS_Max20
Custom profiles
Gold_ASA_JSCSI
Gold_ASA

Storage system:

HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM:

svml

CANCEL

BACK

NEXT

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
ASA_VVOL	2000	Gold_ASA	HCG_A400_E3u3b_NVMe	Thin

ADD

CANCEL

BACK

NEXT

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

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

General

vCenter server: 10.61.181.205

Provisioning destination: HMC Cluster

Datastore name: ASA_VVOL

Datastore type: vVols

Protocol: iSCSI

Storage capability profile: Gold_ASA

Storage system details

Storage system: HCG-NetApp-A400-E3U03

SVM: svm1

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL
BACK
FINISH

Cree una política de almacenamiento de máquinas virtuales en el cliente de vSphere

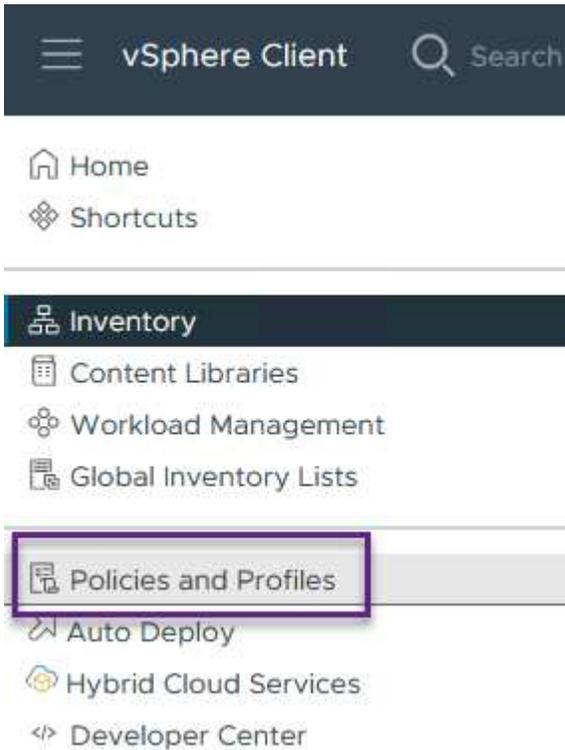
Una política de almacenamiento de máquina virtual es un conjunto de reglas y requisitos que definen cómo deben almacenarse y gestionarse los datos de máquinas virtuales (VM). Especifica las características de almacenamiento deseadas, como el rendimiento, la disponibilidad y los servicios de datos, para una máquina virtual determinada.

En este caso, la tarea implica crear una normativa de almacenamiento de máquinas virtuales para especificar que se generará una máquina virtual en almacenes de datos de VVol y establecer una asignación uno a uno con el perfil de funcionalidad de almacenamiento generado previamente.

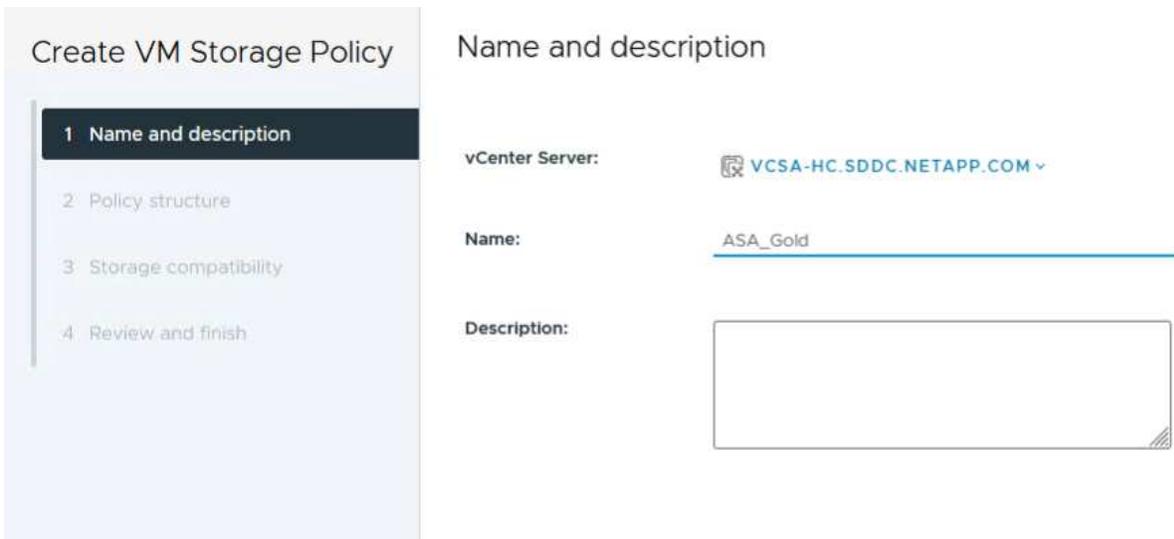
Cree una normativa de almacenamiento de equipos virtuales

Para crear una política de almacenamiento de VM, complete los siguientes pasos:

1. En el menú principal de vSphere Clients, seleccione **Políticas y perfiles**.



2. En el asistente de **Create VM Storage Policy**, primero complete un nombre y una descripción para la política y haga clic en **Next** para continuar.

The image shows the 'Create VM Storage Policy' wizard. On the left, there is a sidebar with four steps: '1 Name and description' (active), '2 Policy structure', '3 Storage compatibility', and '4 Review and finish'. The main area is titled 'Name and description' and contains three fields: 'vCenter Server' with a dropdown menu showing 'VCSA-HC.SDDC.NETAPP.COM', 'Name' with a text input field containing 'ASA_Gold', and 'Description' with a large empty text area.

3. En la página **Estructura de políticas**, seleccione habilitar las reglas para el almacenamiento de VVOL de Clustered Data ONTAP de NetApp y haga clic en **Siguiente**.

- En la siguiente página, específica de la estructura de políticas elegida, seleccione el perfil de funcionalidad de almacenamiento que describe los sistemas de almacenamiento que se utilizarán en la normativa de almacenamiento de los equipos virtuales. Haga clic en **Siguiente** para continuar.

- En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos vSAN que coincidan con esta política y haga clic en **Siguiente**.
- Por último, revise la política a implementar y haga clic en **Finalizar** para crear la política.

Cree una política de almacenamiento de máquinas virtuales en el cliente de vSphere

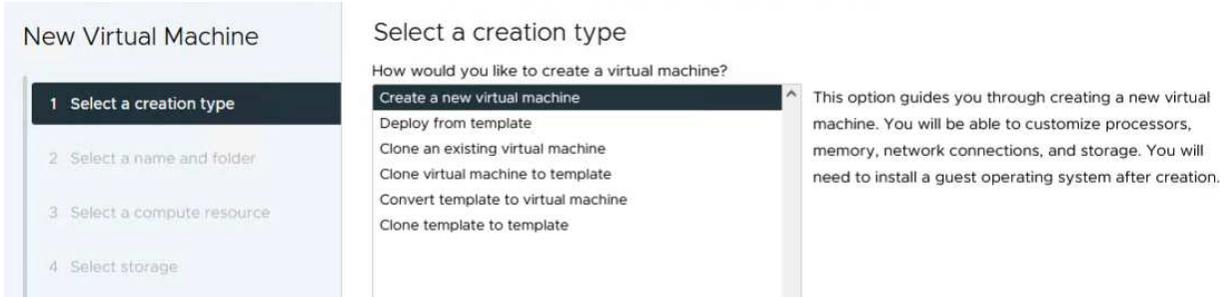
Una política de almacenamiento de máquina virtual es un conjunto de reglas y requisitos que definen cómo deben almacenarse y gestionarse los datos de máquinas virtuales (VM). Especifica las características de almacenamiento deseadas, como el rendimiento, la disponibilidad y los servicios de datos, para una máquina virtual determinada.

En este caso, la tarea implica crear una normativa de almacenamiento de máquinas virtuales para especificar que se generará una máquina virtual en almacenes de datos de VVol y establecer una asignación uno a uno con el perfil de funcionalidad de almacenamiento generado previamente.

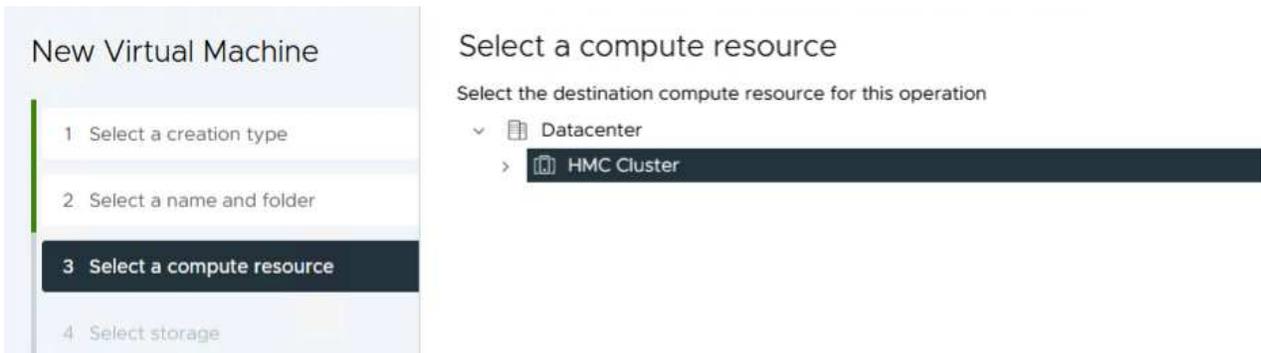
Cree una máquina virtual en un almacén de datos de VVol

El último paso es crear una máquina virtual utilizando las políticas de almacenamiento de VM creadas previamente:

1. Desde el asistente de **Nueva máquina virtual**, selecciona **Crear una nueva máquina virtual** y selecciona **Siguiente** para continuar.



2. Introduzca un nombre y seleccione una ubicación para la máquina virtual y haga clic en **Siguiente**.
3. En la página **Seleccionar un recurso de cálculo** seleccione un destino y haga clic en **Siguiente**.



4. En la página **Select storage** seleccione una política de almacenamiento de VM y el almacén de datos vVols que será el destino de la VM. Haga clic en **Siguiente**.

New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

VM Storage Policy ASA_Gold ▾

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	9 MB	1.95 TB	v
<input type="radio"/>	ASA400_ISCSI01	Incompatible	2 TB	185.32 GB	1.9 TB	v
<input type="radio"/>	DemoDS	Incompatible	800 GB	6.99 GB	793.01 GB	N
<input type="radio"/>	destination	Incompatible	250 GB	32.66 MB	249.97 GB	N
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	133.27 GB	956.83 GB	N
<input type="radio"/>	esxi-hc-01 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	v
<input type="radio"/>	esxi-hc-02 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	v
<input type="radio"/>	esxi-hc-03 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	v

Manage Columns Items per page 10 ▾ 1 - 10 of 15 items < < < 1 / 2 > > >

Compatibility

Validating...

CANCEL

BACK

NEXT

5. En la página **Seleccionar compatibilidad**, seleccione las versiones de vSphere con las que será compatible la VM.
6. Seleccione la familia y la versión del SO invitado para la nueva VM y haga clic en **Next**.
7. Rellene la página **Personalizar hardware**. Tenga en cuenta que puede seleccionarse una normativa de almacenamiento de equipos virtuales independiente para cada disco duro (archivo VMDK).

New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Customize hardware ✕

Configure the virtual machine hardware

Virtual Hardware VM Options Advanced Parameters

[ADD NEW DEVICE ▾](#)

> CPU *	4	▼	(i)
> Memory *	32	▼	GB ▼
> New Hard disk *	150	▼	GB ▼

Maximum Size 1.95 TB

VM storage policy ASA_Gold ▼

Location Store with the virtual machine ▼

Disk Provisioning Thin Provision ▼

Sharing Unspecified ▼

Disk Mode Dependent ▼

Virtual Device Node New SCSI controller ▼ SCSI(0:0) New Hard disk ▼

> New SCSI controller LSI Logic SAS

> New Network VM Network Connected

CANCEL
BACK
NEXT

8. Por último, revise la página de resumen y haga clic en **Finish** para crear la VM.

En resumen, Herramientas de NetApp ONTAP automatiza el proceso de creación de almacenes de datos VVOL en sistemas de almacenamiento de ONTAP. Los perfiles de funcionalidades de almacenamiento no solo definen los sistemas de almacenamiento que deben usarse para la creación de almacenes de datos, sino que también dictan las políticas de calidad de servicio que se pueden implementar sobre una base individual de VMDK. VVols proporciona un paradigma de gestión del almacenamiento simplificado y una estrecha integración entre NetApp y VMware hacen de esta solución una solución práctica para un control optimizado, eficiente y granular sobre entornos virtualizados.

Cabina All-Flash SAN de NetApp con VMware vSphere 8

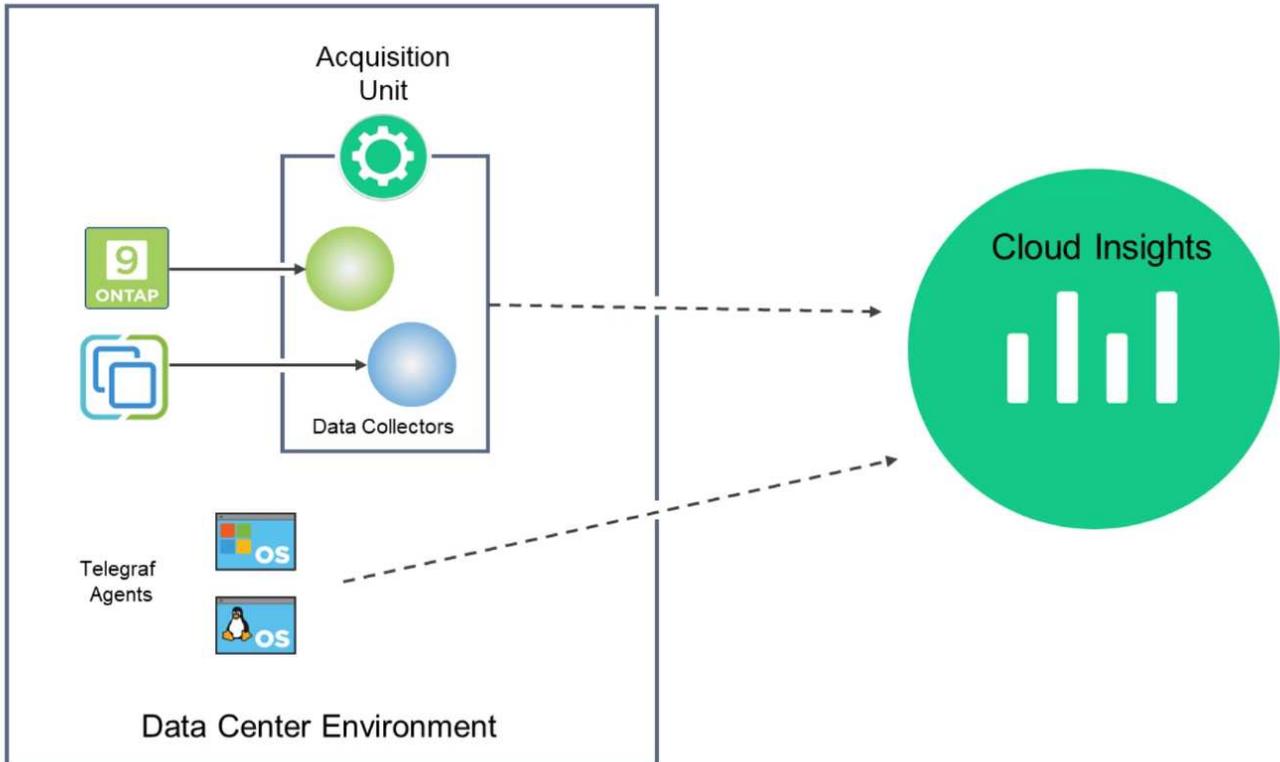
NetApp Cloud Insights es una plataforma de supervisión y análisis de infraestructuras basada en la nube diseñada para proporcionar una visibilidad e información exhaustiva sobre el rendimiento, el estado y los costes de las INFRAESTRUCTURAS TECNOLÓGICAS, tanto on-premises como en la nube. Las funciones clave de NetApp Cloud Insights incluyen supervisión en tiempo real, consolas personalizables, análisis predictivo y herramientas de optimización de costes, lo que permite a las organizaciones gestionar y optimizar con eficiencia sus entornos en las instalaciones y en el cloud.

Autor: Josh Powell: Ingeniería de soluciones de NetApp

Supervisión del almacenamiento en las instalaciones con NetApp Cloud Insights

NetApp Cloud Insights funciona a través del software Acquisition Unit, configurado con recopiladores de datos para activos como VMware vSphere y sistemas de almacenamiento NetApp ONTAP. Estos recolectores recopilan datos y los transmiten a Cloud Insights. A continuación, la plataforma utiliza una variedad de paneles de control, widgets y consultas de métricas para organizar los datos en análisis perspicaces para que los usuarios los interpreten.

Diagrama de la arquitectura de Cloud Insights:



Descripción general de la puesta en marcha de soluciones

Esta solución proporciona una introducción a la supervisión de los sistemas de almacenamiento ONTAP y VMware vSphere en las instalaciones mediante NetApp Cloud Insights.

Esta lista proporciona los pasos generales que se tratan en esta solución:

1. Configure el recopilador de datos para un clúster de vSphere.
2. Configurar el Recopilador de datos para un sistema de almacenamiento de ONTAP
3. Utilice reglas de anotación para etiquetar activos.
4. Explorar y correlacionar activos.
5. Utilice una consola Top VM Latency para aislar los vecinos ruidosos.
6. Identifique oportunidades para ajustar el tamaño de los equipos virtuales.
7. Utilice consultas para aislar y ordenar métricas.

Requisitos previos

Esta solución usa los siguientes componentes:

1. Cabina All-Flash SAN A400 de NetApp con ONTAP 9,13.
2. Clúster de vSphere 8,0 de VMware.
3. Cuenta de NetApp Cloud Insights.
4. Software de unidad de adquisición NetApp Cloud Insights instalado en una VM local con conectividad de red a activos para la recopilación de datos.

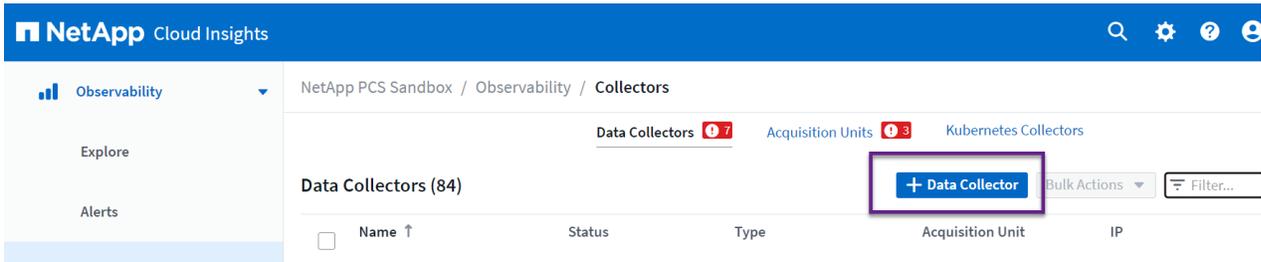
Puesta en marcha de la solución

Configurar colectores de datos

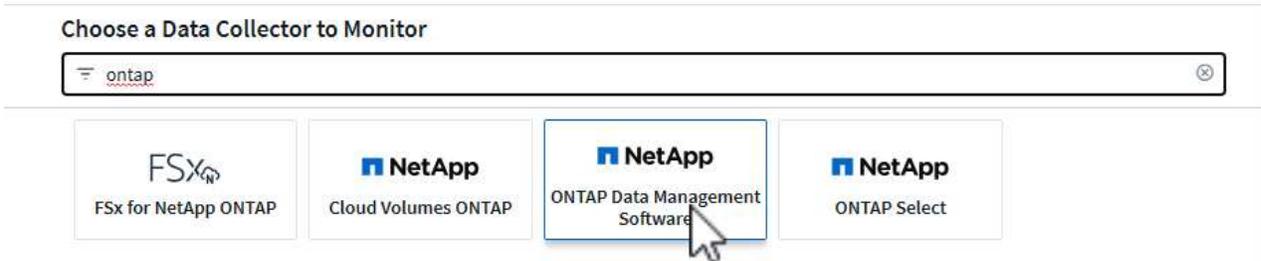
Para configurar los recopiladores de datos para los sistemas de almacenamiento VMware vSphere y ONTAP, lleve a cabo los siguientes pasos:

Agregar un recopilador de datos para un sistema de almacenamiento de ONTAP

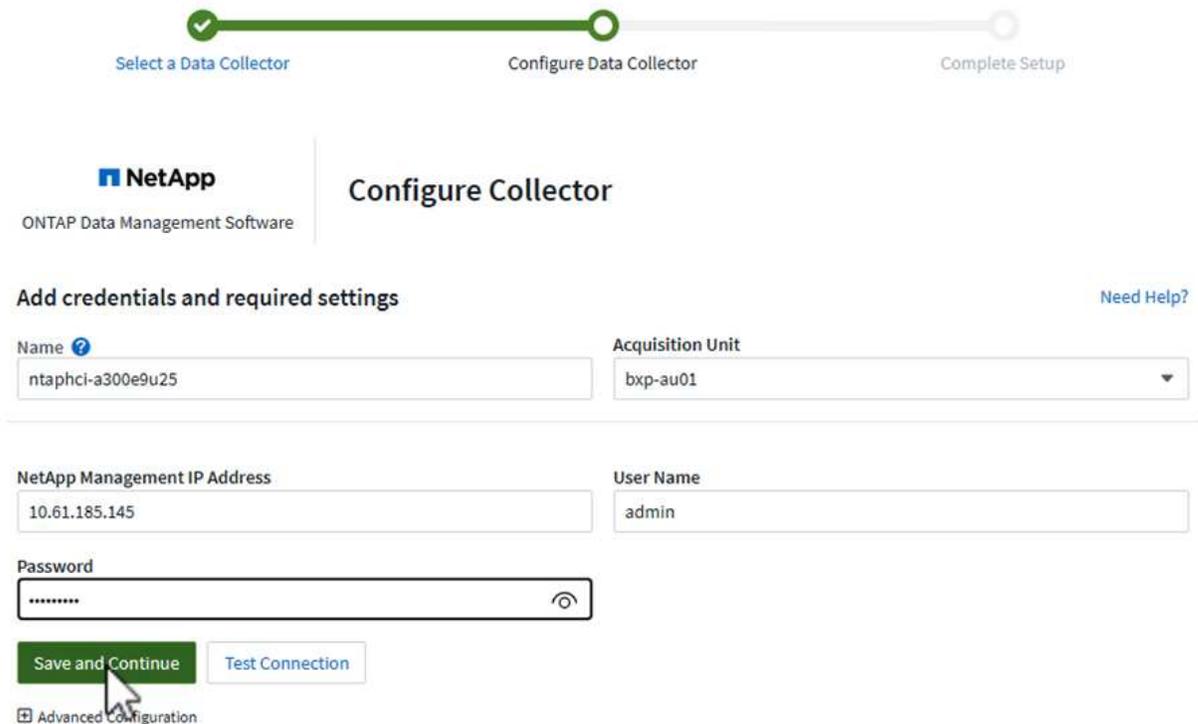
1. Una vez que haya iniciado sesión en Cloud Insights, vaya a **Observabilidad > Recopiladores > Recopiladores de datos** y pulse el botón para instalar un nuevo Recopilador de datos.



2. Desde aquí busque **ONTAP** y haga clic en **Software de gestión de datos ONTAP**.

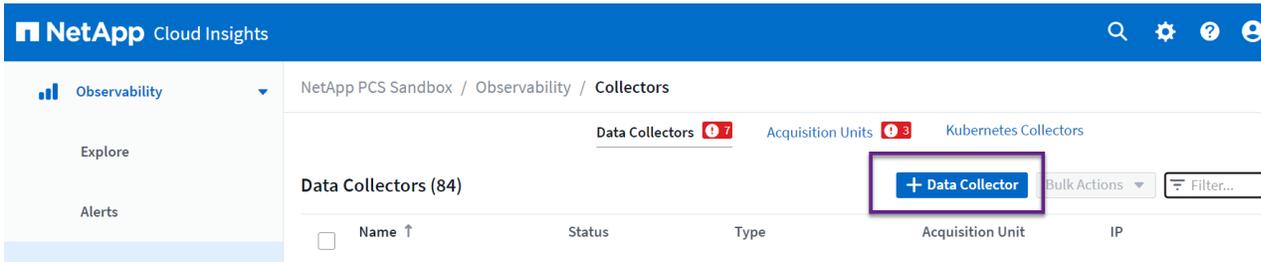


3. En la página **Configurar recopilador**, rellene un nombre para el recopilador, especifique la **Unidad de adquisición** correcta y proporcione las credenciales para el sistema de almacenamiento ONTAP. Haga clic en **Guardar y continuar** y luego en **Completar configuración** en la parte inferior de la página para completar la configuración.

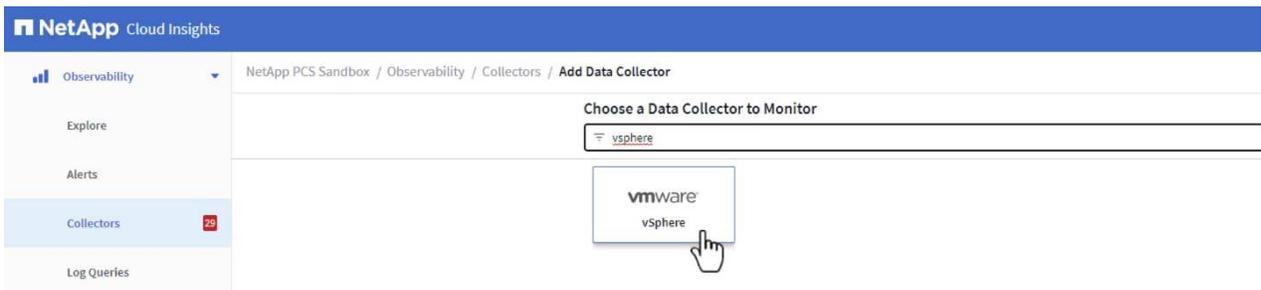


Añadir un recopilador de datos para un clúster de VMware vSphere

1. Una vez más, navegue hasta **Observabilidad > Recopiladores > Recopiladores de datos** y pulse el botón para instalar un nuevo Recopilador de datos.



2. Desde aquí busca **vsphere** y haz clic en **vmware vsphere**.



3. En la página **Configure Collector**, rellene un nombre para el recopilador, especifique la **Acquisition Unit** 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.



Configure Collector

Add credentials and required settings [Need Help?](#)

Name ? VCSA7	Acquisition Unit bxp-au01
---------------------------------	------------------------------

Virtual Center IP Address 10.61.181.210	User Name administrator@vsphere.local
--	--

Password *****

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
---	--

Advanced Configuration

Collecting:

- Inventory
- VM Performance

Inventory Poll Interval (min) 20	Communication Port 443
-------------------------------------	---------------------------

Filter VMs by ESX_HOST	Choose 'Exclude' or 'Include' to Specify a List Exclude
---------------------------	--

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only)	Performance Poll Interval (sec) 300
---	--

Collect basic performance metrics only

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
---	--

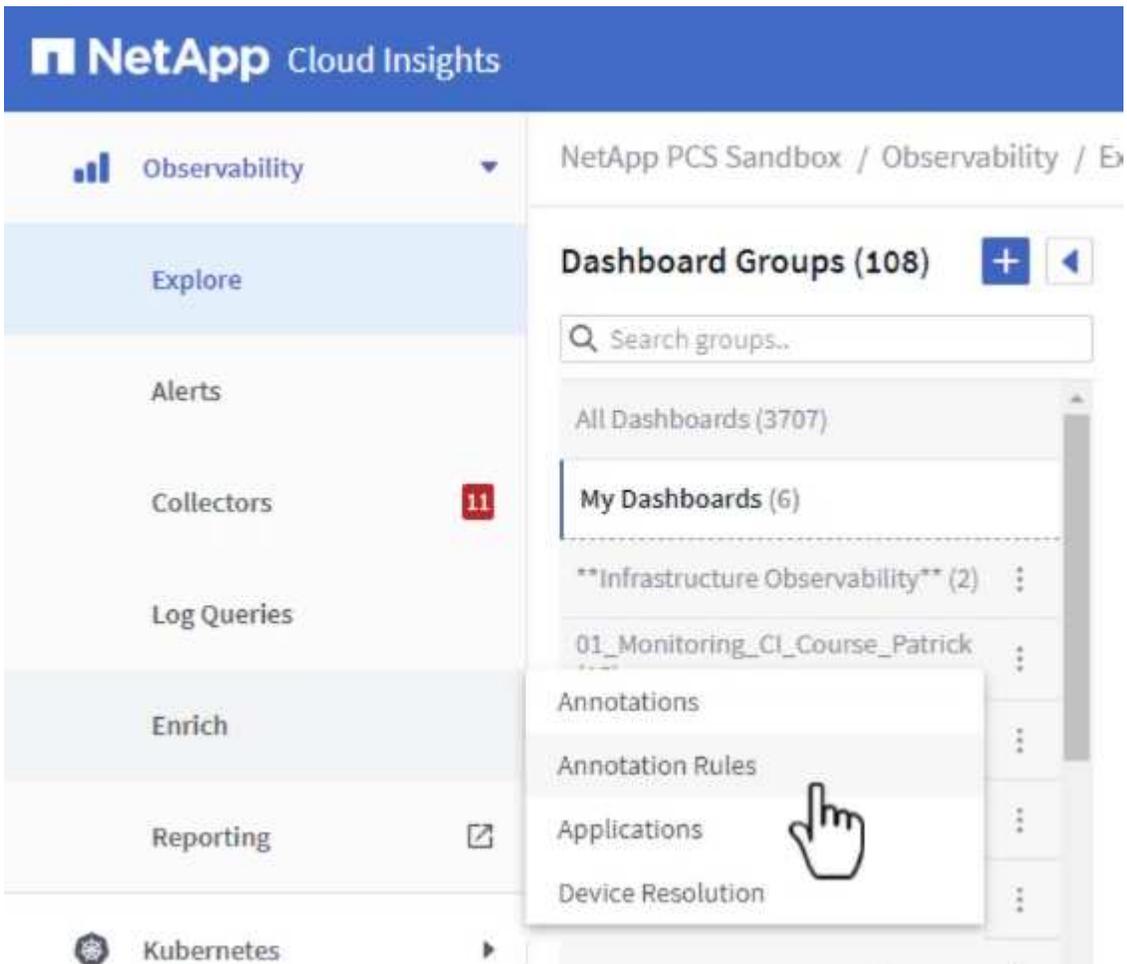
Agregar anotaciones a activos

Las anotaciones son un método útil para etiquetar activos para que se puedan filtrar e identificar 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 filtrarlos por **Data Center**.

Utilice reglas de anotación para etiquetar activos

1. En el menú de la izquierda, navegue hasta **Observabilidad > Enriquecimiento > Reglas de anotación** y haga clic en el botón **+ Regla** en la parte superior derecha para agregar una nueva regla.



2. En el cuadro de diálogo **Agregar regla**, rellene un nombre para la regla, localice una consulta a la que se aplicará la regla, el campo de anotación afectado y el valor que se va a rellenar.

Add Rule
✕

Name

Query

Annotation

Value

- Por último, 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.

NetApp PCS Sandbox / Observability / Enrich / **Annotation Rules**

Rules running... **Run All Rules**

Annotation rules (217)

Name	Resource Type	Query	Annotation	Value
Annotate Tier 1 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 1
Annotate Tier 2 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 2

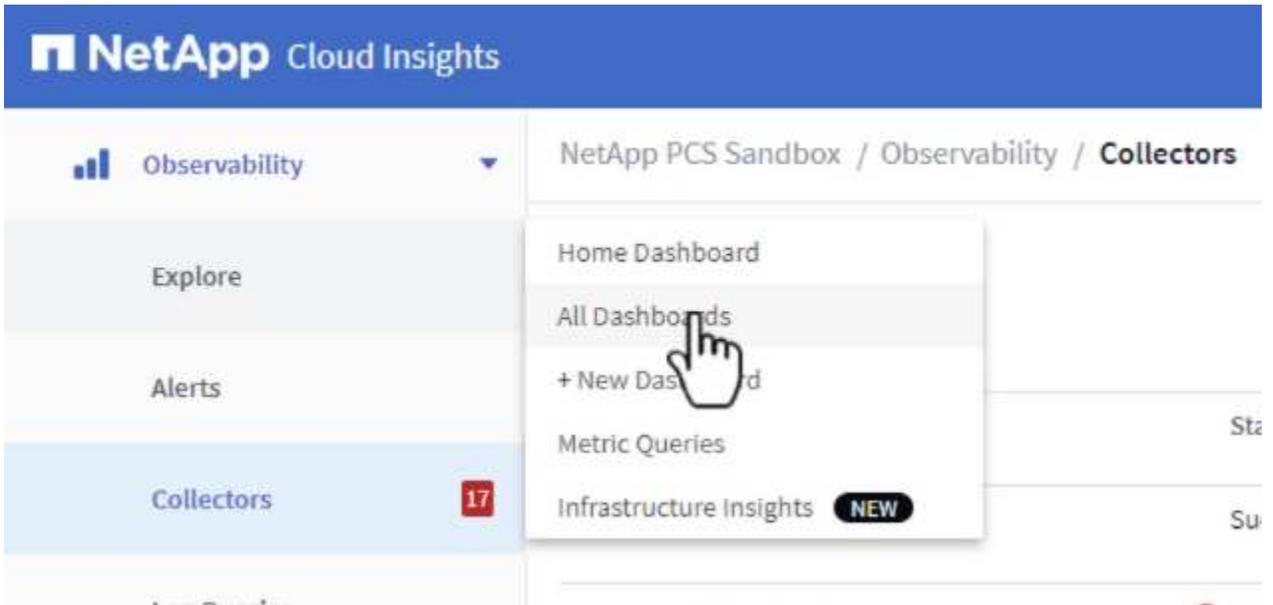
Explorar y correlacionar activos

Cloud Insights saca conclusiones lógicas sobre los activos que se ejecutan juntos en los sistemas de almacenamiento y clústeres de vsphere.

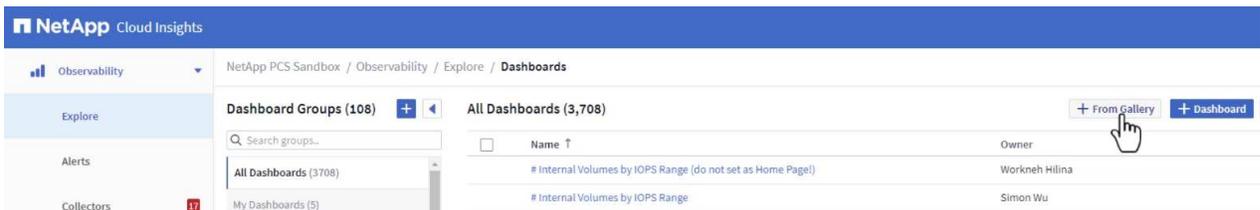
En esta sección se muestra cómo utilizar paneles de control para correlacionar activos.

Correlación de activos de una consola de rendimiento del almacenamiento

1. En el menú de la izquierda, navegue hasta **Observabilidad > Explorar > Todos los paneles**.



2. Haga clic en el botón **+ From Gallery** para ver una lista de los paneles de control ya preparados que se pueden importar.



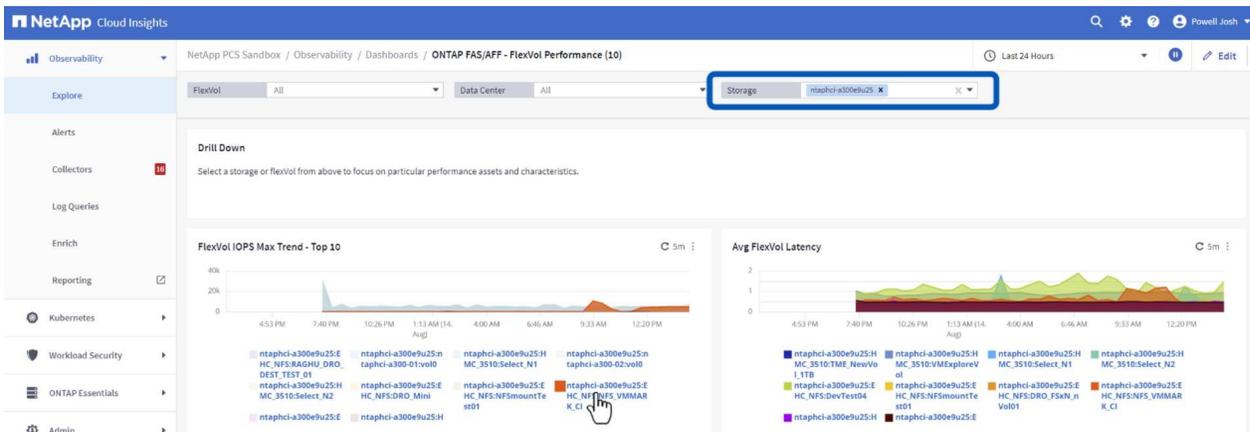
3. Elija un panel de control para el rendimiento de FlexVol de la lista y haga clic en el botón **Agregar paneles de control** en la parte inferior de la página.

- ONTAP FAS/AFF - Cluster Capacity
- ONTAP FAS/AFF - Efficiency
- ONTAP FAS/AFF - FlexVol Performance
- ONTAP FAS/AFF - Node Operational/Optimal Points
- ONTAP FAS/AFF - PrePost Capacity Efficiencies
- Storage Admin - Which nodes are in high demand?
- Storage Admin - Which pools are in high demand?
- StorageGRID - Capacity Summary
- StorageGRID - ILM Performance Monitoring
- StorageGRID - MetaData Usage
- StorageGRID - S3 Performance Monitoring
- VMware Admin - ESX Hosts Overview
- VMware Admin - Overview
- VMware Admin - VM Performance
- VMware Admin - Where are opportunities to right size?
- VMware Admin - Where can I potentially reclaim waste?
- VMware Admin - Where do I have VM Latency?

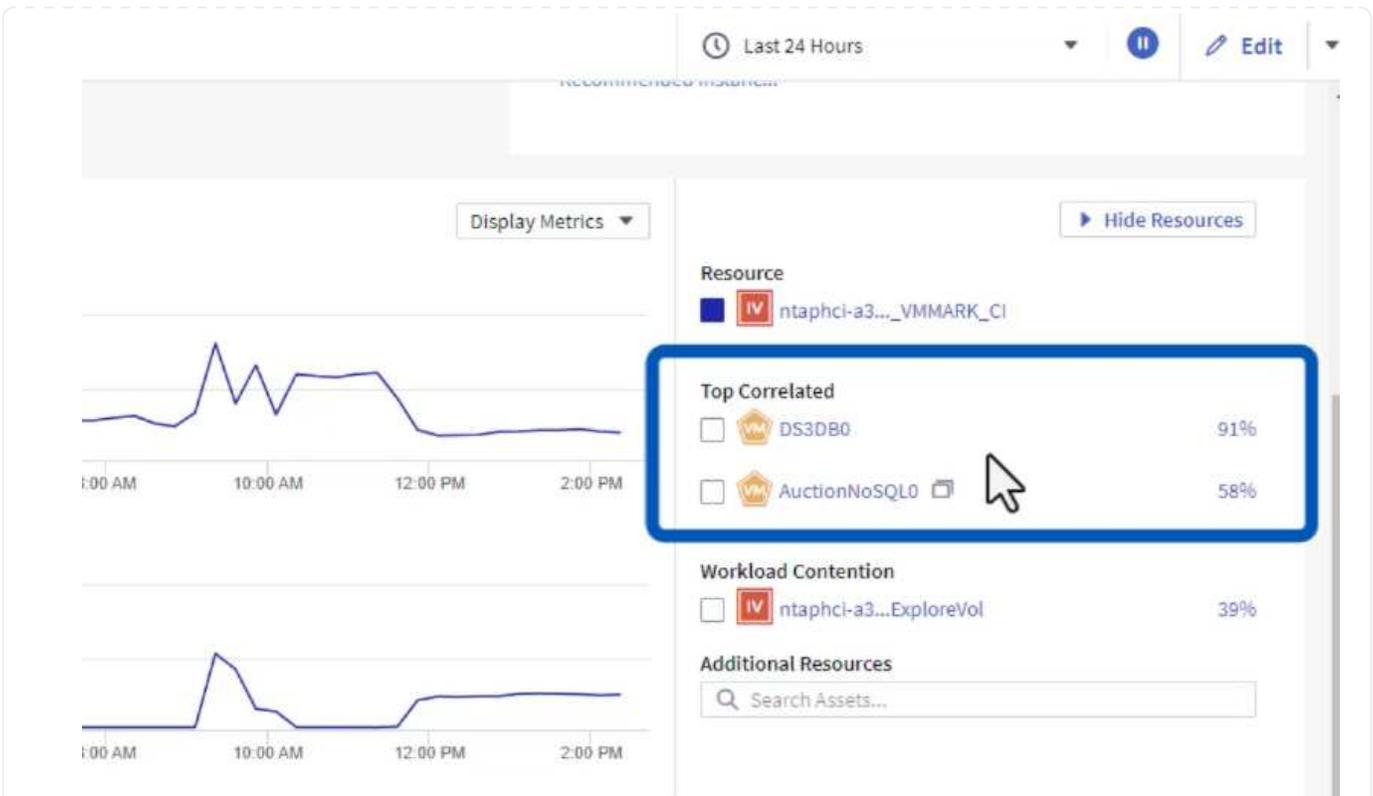
+ Additional Dashboards (13)
 These dashboards require additional data collectors to be installed. [Add More](#)

Add Dashboards Go Back

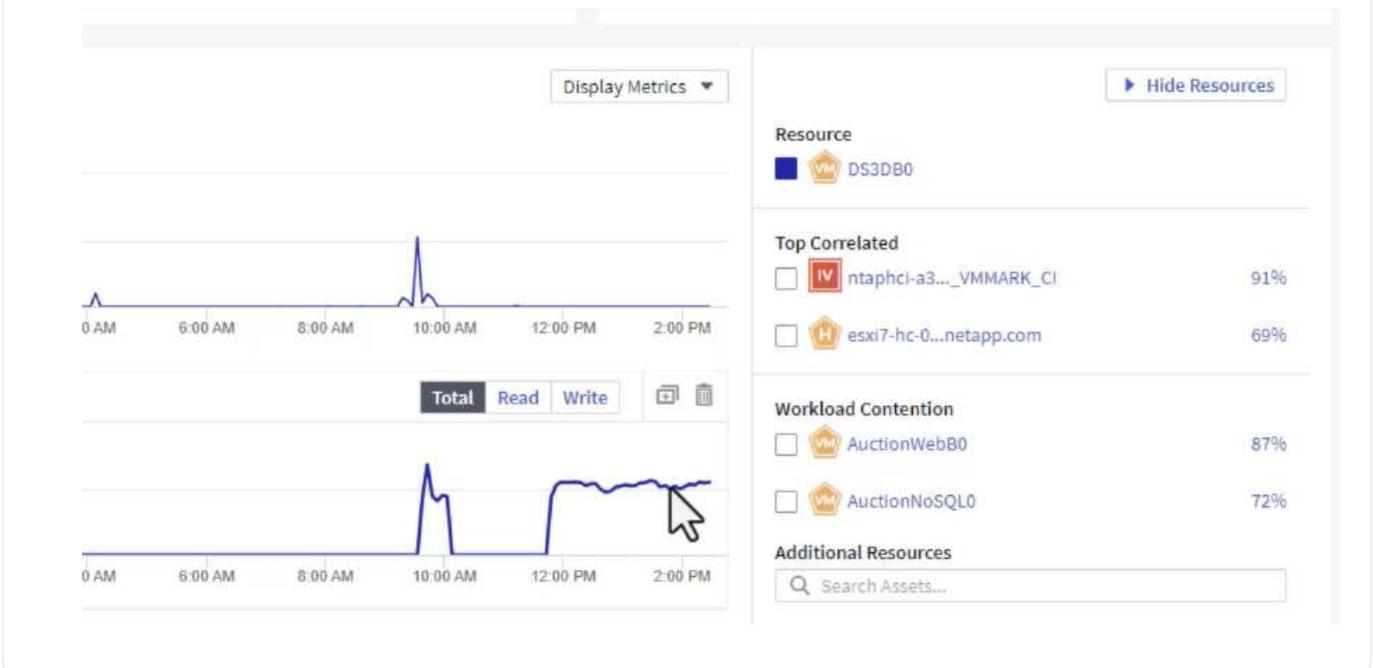
4. Una vez importado, abra el panel de control. Desde aquí puede ver varios widgets con datos de rendimiento detallados. Añada un filtro para ver un único sistema de almacenamiento y seleccione un volumen de almacenamiento para examinar sus detalles.



5. Desde esta vista, se pueden observar diferentes métricas relacionadas con este volumen de almacenamiento y los equipos virtuales más utilizados y correlacionados que se ejecutan en el volumen.



6. Al hacer clic en el VM con la mayor utilización, se profundiza en las métricas para ese VM para ver cualquier problema potencial.



Use Cloud Insights para identificar los vecinos ruidosos

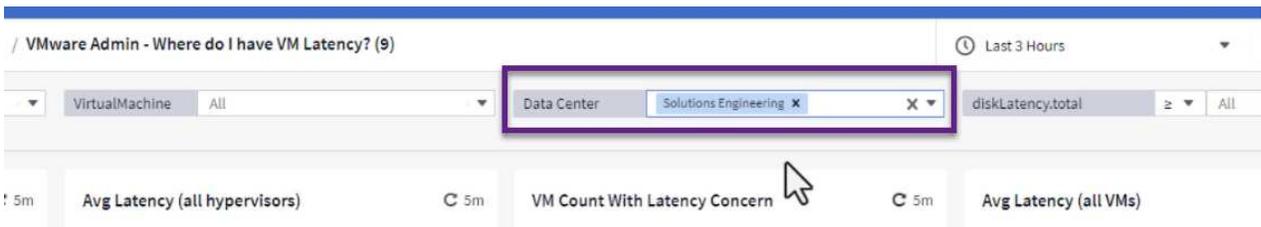
Cloud Insights incluye consolas que pueden aislar fácilmente máquinas virtuales iguales que afectan negativamente a otras máquinas virtuales que se ejecutan en el mismo volumen de almacenamiento.

Utilice una consola Top VM Latency para aislar los vecinos ruidosos

1. En este ejemplo, acceda a un panel de control disponible en la **Galería** llamado **VMware Admin - ¿Dónde tengo la latencia de VM?**



2. A continuación, filtra por la anotación **Data Center** creada en un paso anterior para ver un subconjunto de activos.



3. Esta consola muestra una lista de las 10 máquinas virtuales principales por latencia media. A partir de aquí, haga clic en la VM de la preocupación para profundizar en sus detalles.

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

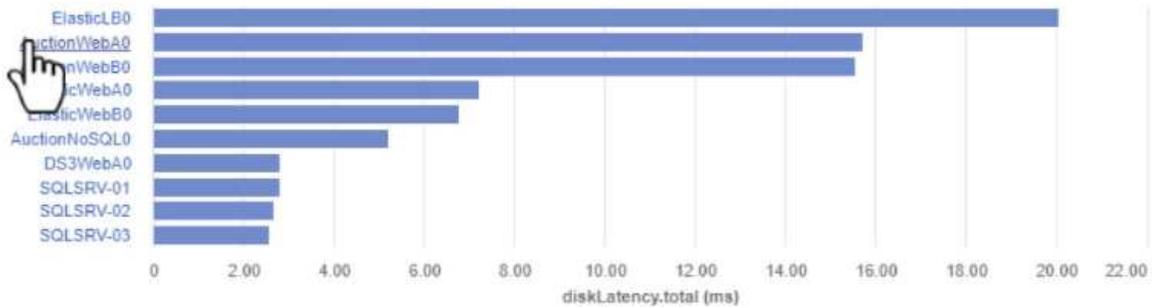
5m

1.55 ms

diskLatency.total

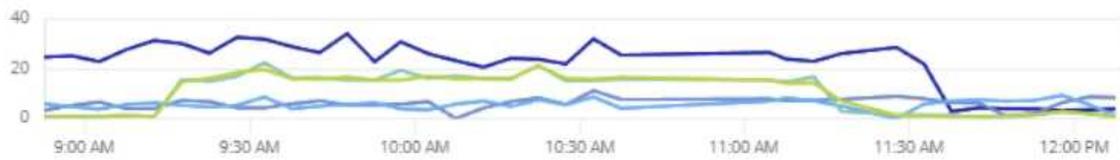
Avg VM Latency - Top 10

5m

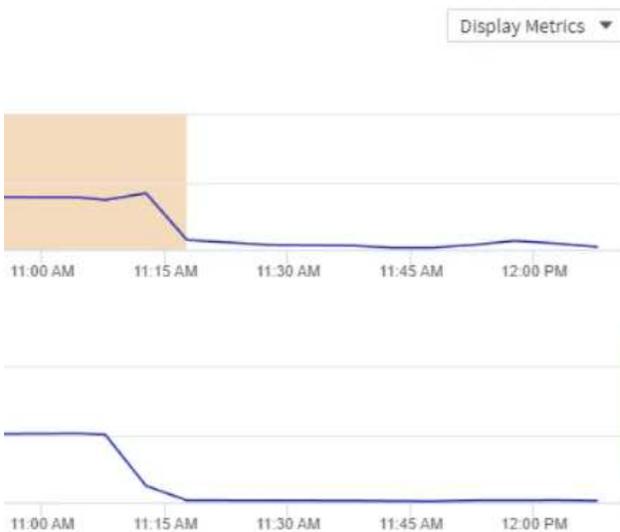


Top 5 Avg VM Latency Trend

30s



4. Las máquinas virtuales que potencialmente causan la contención de las cargas de trabajo aparecen y están disponibles. Examine estas métricas de rendimiento de las máquinas virtuales para investigar cualquier posible problema.



Display Metrics

Hide Resources

Resource

VM AuctionWebA0

Top Correlated

esxi7-hc-0...netapp.com 91%

ntaphci-a3..._VMMARK_CI 84%

Workload Contention

AuctionNoSQL0 92%

AuctionWebB0 57%

Additional Resources

Search Assets...

Visualice los recursos infrautilizados en Cloud Insights

Al adecuar los recursos de las máquinas virtuales a los requisitos reales de la carga de trabajo, se puede optimizar la utilización de recursos, lo que genera ahorros de costes de la infraestructura y los servicios en cloud. Los datos de Cloud Insights se pueden personalizar para mostrar fácilmente sobre o infrautilizados equipos virtuales.

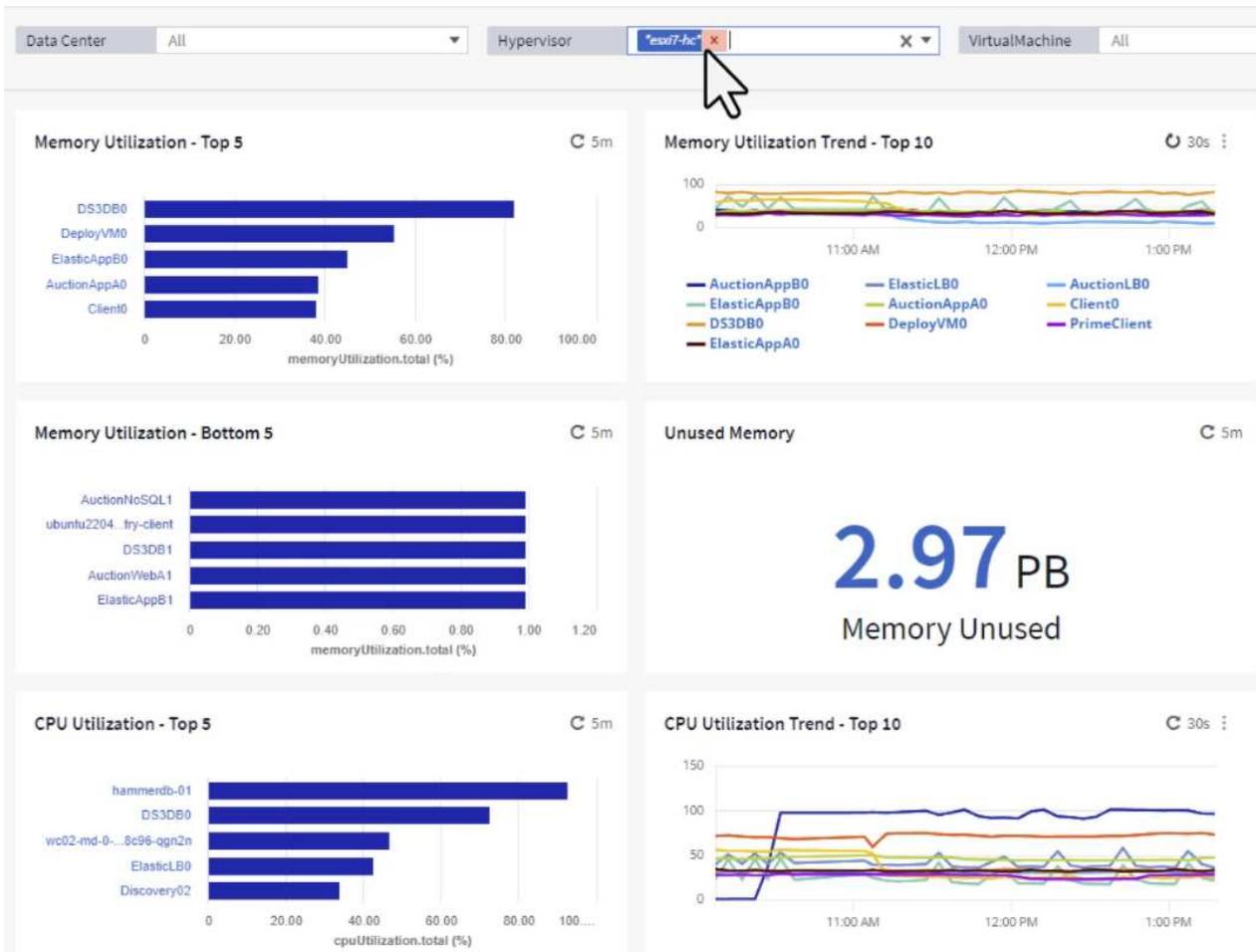
Identifique oportunidades para ajustar el tamaño de los equipos virtuales

1. En este ejemplo, acceda a un panel de control disponible en la **Galería** llamado **VMware Admin - ¿Dónde están las oportunidades para el tamaño adecuado?**

My Dashboards (6)

<input type="checkbox"/>	Name ↑
	All SAN Array Status (2)
	Cloud Volumes ONTAP - FlexVol Performance (6)
	ONTAP - Volume Workload Performance (Frontend) (7)
<input type="checkbox"/> ★	VMware Admin - Where are opportunities to right size? (37)
	VMware Admin - Where do I have VMs that potentially reclaim waste? (11)
	VMware Admin - Where do I have VM Latency? (9)

2. Primer filtro por todos los hosts ESXi del clúster. Entonces puede ver clasificación de los equipos virtuales principales e inferiores por uso de la memoria y la CPU.



3. Las tablas permiten ordenar y proporcionar más detalles en función de las columnas de datos elegidas.

Memory Usage

5m

121 items found

Virtual Machine	memory (MiB)	memoryUt... ↓
DS3DB0	768.0	81.64
DeployVM0	92.0	55.06
ElasticAppB0	92.0	44.91
AuctionAppA0	336.0	38.42
Client0	480.0	37.98
AuctionAppB0	336.0	37.83
ElasticAppA0	92.0	35.63
ElasticLB0	96.0	35.13
user-cluster1-8872k-78c65dd794...	92.0	32.47
PrimeClient	48.0	30.30

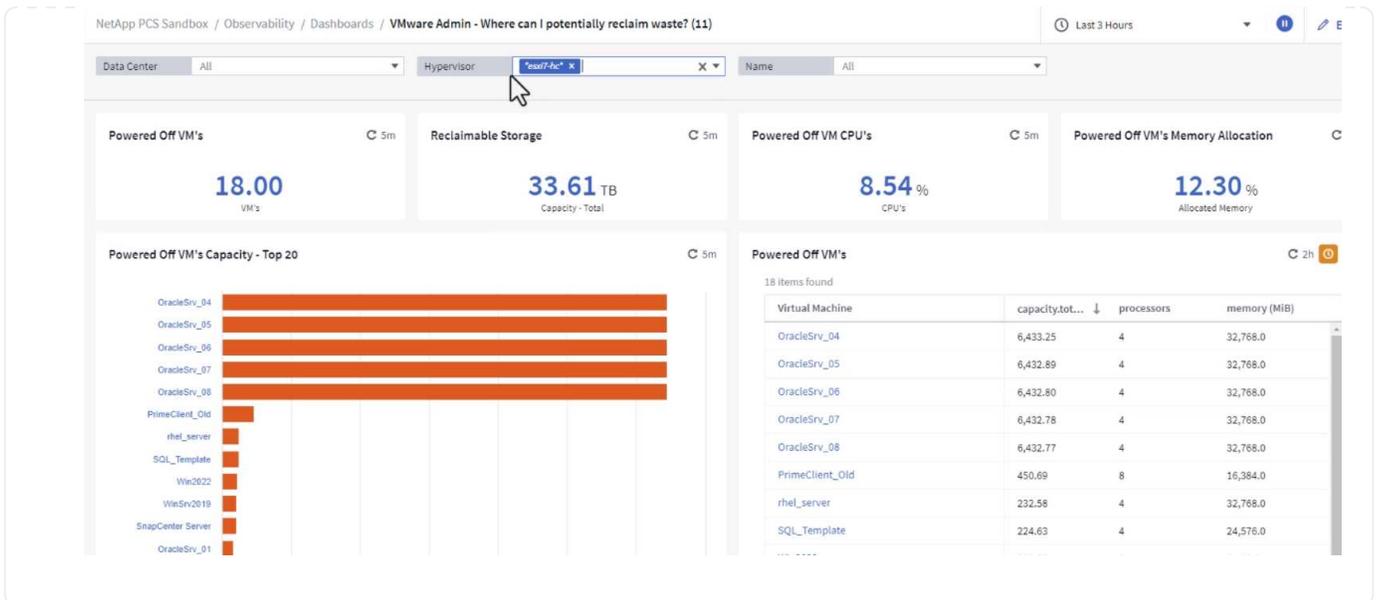
CPU Utilization

5m

121 items found

Virtual Machine	name
hammerdb-01	hammerdb-01
DS3DB0	DS3DB0
wc02-md-0-xwdgb-8cf48c96-qgn...	wc02-md-0-xwdgb-8cf48c96-qg...
ElasticLB0	ElasticLB0

4. Otro panel llamado **VMware Admin** - ¿Dónde puedo recuperar residuos? muestra VM apagadas ordenadas por su uso de capacidad.

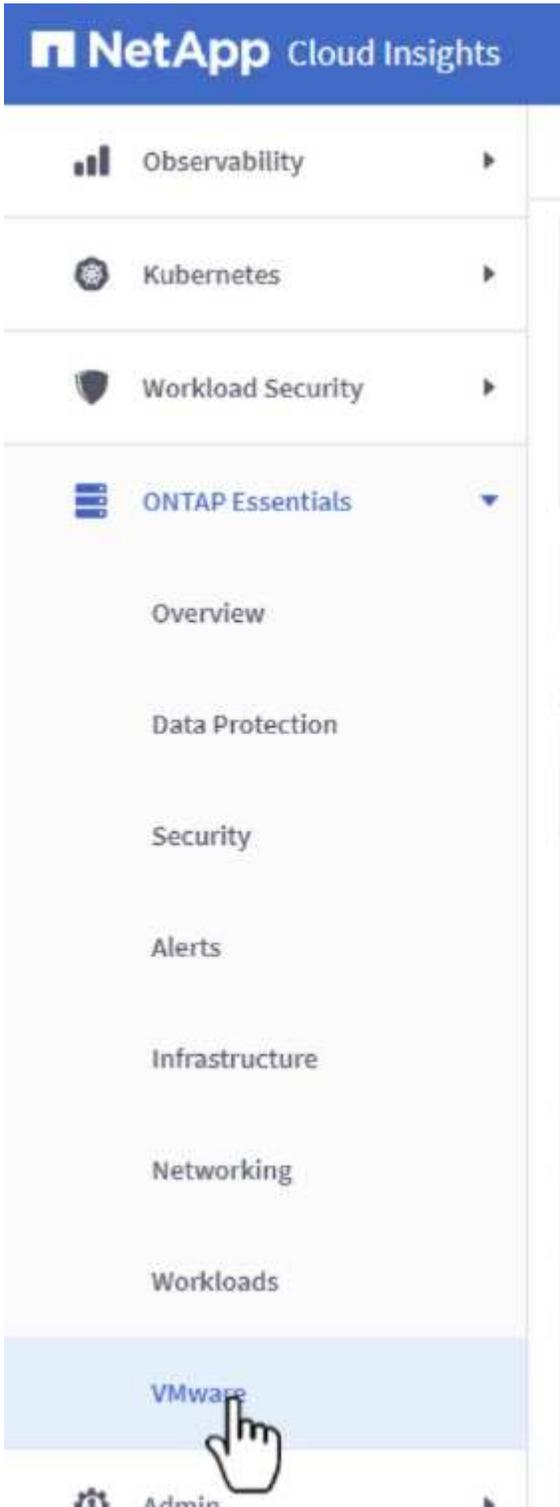


Utilice consultas para aislar y ordenar métricas

La cantidad de datos capturados por Cloud Insights es bastante completa. Las consultas de métricas proporcionan una forma eficaz de ordenar y organizar grandes cantidades de datos de formas útiles.

Consulte una consulta detallada de VMware en ONTAP Essentials

1. Navegue hasta **ONTAP Essentials > VMware** para acceder a una consulta de métricas de VMware completa.



2. En esta vista se le presentan varias 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.

VirtualMachine | All Virtual Machines

Filter by Attribute: storageResources.storage.vendor: NetApp | host.Los: VMware

Filter by Metric: +

Group By: Virtual Machine

Formatting: Show Expanded Details | Conditional Formatting | Background Color | Show In Range as green

281 Items found

Virtual Machine	name	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (I/O/s)	diskLatency.total...	diskThroughput...
01rfk8prodclient	01rfk8prodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8prodserver	02rfk8prodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8prodmaster01	03rfk8prodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8prodmaster02	04rfk8prodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8prodmaster03	05rfk8prodmaster03	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 se diseñó como un manual básico para aprender a comenzar a usar NetApp Cloud Insights y mostrar algunas de las potentes capacidades que puede ofrecer esta solución de observabilidad. Hay cientos de paneles de control y consultas métricas integradas en el producto, lo que facilita la puesta en marcha inmediata. 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 obtener más información sobre las tecnologías presentadas en esta solución, consulte la siguiente información adicional.

- ["Página de inicio de BlueXP y Cloud Insights de NetApp"](#)
- ["Documentación de NetApp Cloud Insights"](#)

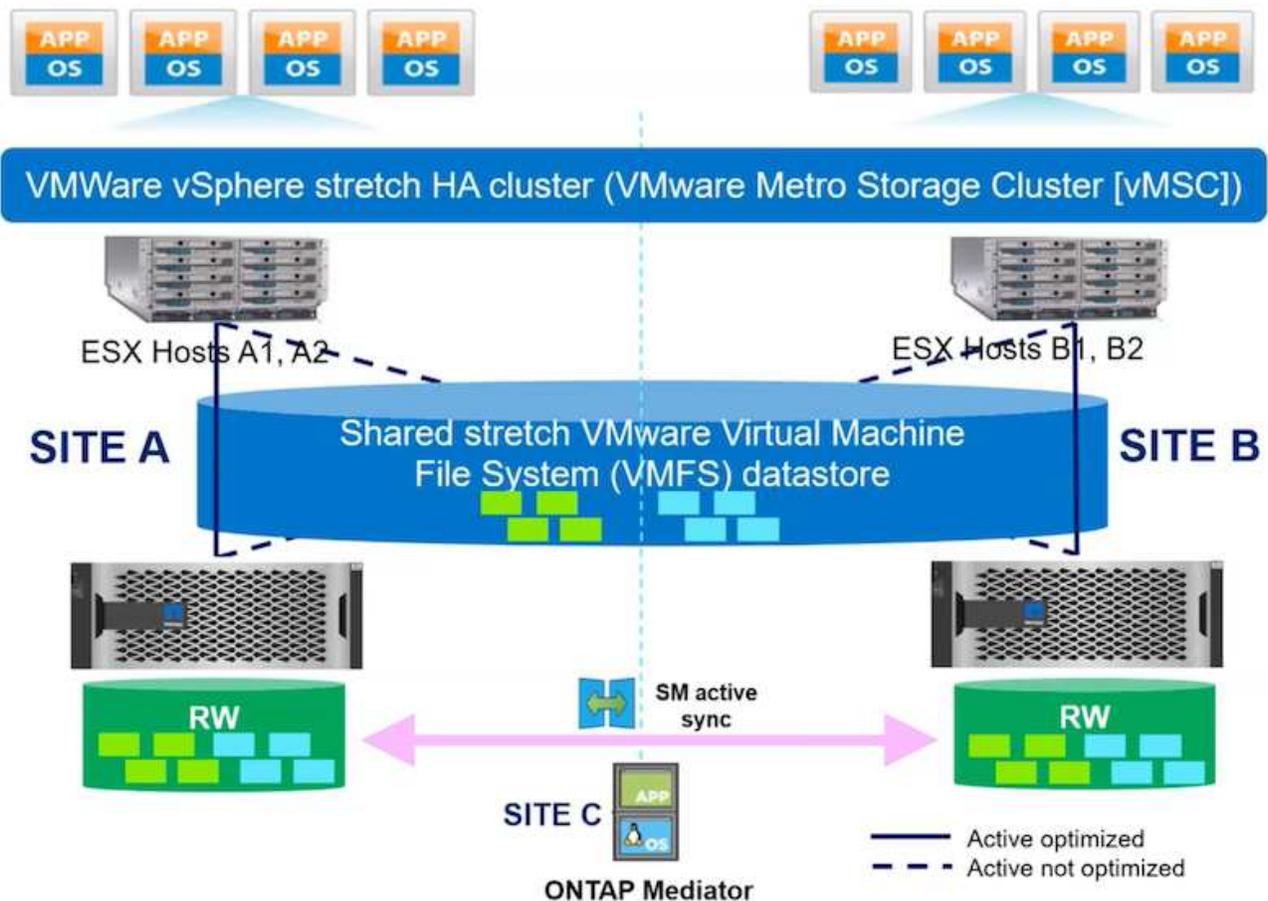
VMware vSphere Metro Storage Cluster con sincronización activa SnapMirror

"[VMware vSphere Metro Storage Cluster \(VMSC\)](#)" Es una solución de clúster ampliada en diferentes dominios de fallo para proporcionar movilidad * de carga de trabajo en zonas o sitios de disponibilidad. * evitación del tiempo de inactividad * prevención de desastres * recuperación rápida

Este documento proporciona detalles sobre la implementación de VMSC con ["Sincronización activa de SnapMirror \(SM-AS\)"](#) el uso de System Manager y las herramientas de ONTAP. Además, muestra cómo se puede proteger la VM replicando en un tercer sitio y gestionando con el complemento de SnapCenter para VMware vSphere.

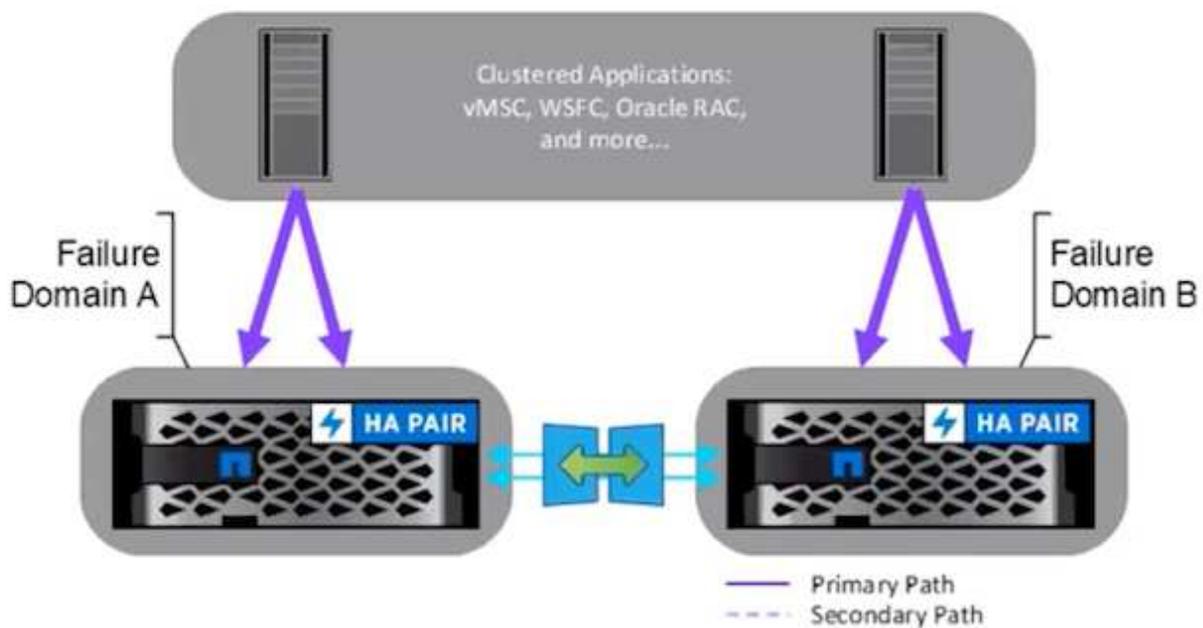
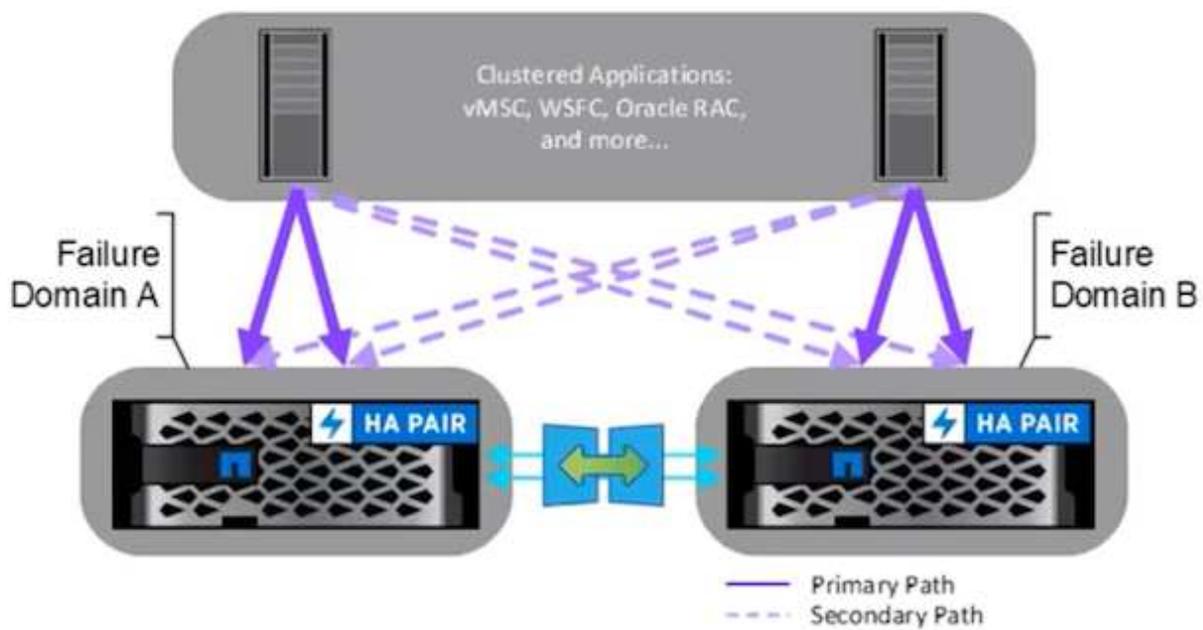
SnapMirror active sync

General availability release 9.15.1 for symmetric configuration



La sincronización activa de SnapMirror admite cabinas de almacenamiento ASA, AFF y FAS. Se recomienda utilizar el mismo tipo (modelos de rendimiento/capacidad) en ambos dominios de fallo. Actualmente, solo se admiten protocolos de bloque como FC e iSCSI. Para obtener más directrices de soporte, consulte ["Herramienta de matriz de interoperabilidad"](#) y ["Hardware Universe"](#)

VMSC admite dos modelos de implementación diferentes denominados Acceso de host uniforme y Acceso de host no uniforme. En una configuración de acceso de host uniforme, todos los hosts del clúster tienen acceso a la LUN en ambos dominios de fallos. Por lo general, se utiliza en diferentes zonas de disponibilidad en un mismo centro de datos.



En la configuración de acceso a host no uniforme, el host solo tiene acceso al dominio de fallo local. Normalmente se utiliza en diferentes sitios donde la ejecución de varios cables en los dominios de fallo es una opción restrictiva.



En el modo de acceso de host no uniforme, vSphere HA reiniciará las máquinas virtuales en otro dominio de fallo. La disponibilidad de las aplicaciones se verá afectada por su diseño. El modo de acceso al host no uniforme sólo se admite con ONTAP 9,15 en adelante.

Requisitos previos

- "Hosts VMware vSphere puestos en marcha con estructura de almacenamiento doble (dos HBA o VLAN doble para iSCSI) por host".
- "Las cabinas de almacenamiento se ponen en marcha con agregación de enlaces para puertos de datos (para iSCSI)".
- "Las máquinas virtuales de almacenamiento y las LIF están disponibles"
- "El tiempo de ida y vuelta de la latencia entre clústeres debe ser inferior a 10 milisegundos".
- "ONTAP Mediator VM se pone en marcha en un dominio de fallo diferente"
- "Se ha establecido la relación de paridad del clúster"
- "Se ha establecido una relación entre iguales de SVM"
- "Mediador de ONTAP registrado en el clúster de ONTAP"



Si utiliza un certificado autofirmado, el certificado de CA puede recuperarse de <installation path>/ontap_mediator/server_config/ca.crt en la máquina virtual de mediator.

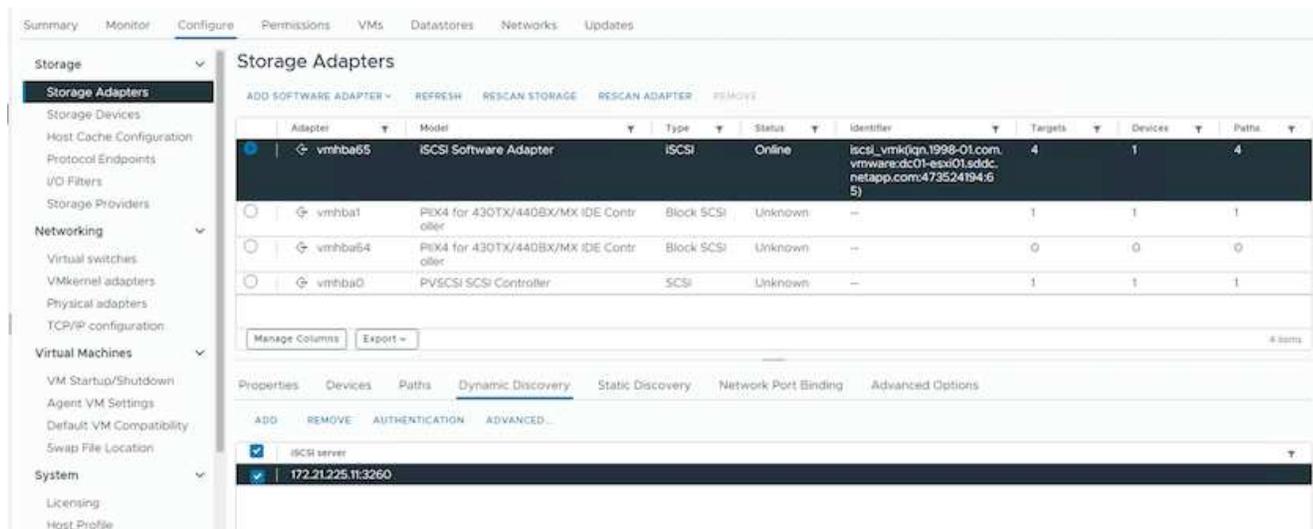
Acceso de host no uniforme del VMSC con la interfaz de usuario de System Manager de ONTAP.

Nota: Se pueden utilizar las herramientas de ONTAP 10,2 o superior para aprovisionar un almacén de datos ampliado con un modo de acceso de host no uniforme sin necesidad de cambiar las múltiples interfaces de usuario. Esta sección es solo para referencia si no se utilizan las herramientas de ONTAP.

1. Anote una de las direcciones IP de LIF de datos iSCSI de la cabina de almacenamiento de dominio de fallos local.

Name	Status	Storage VM	IPspace	Address	Current node	Current p...	Portset	Protocols	Ty...	Throughput
iscsi02	🟢	zonea	Default	172.21.226.11	E13A300_1	a0a-3482		iSCSI	D...	0
iscsi03	🟢	zonea	Default	172.21.225.12	E13A300_2	a0a-3481		iSCSI	D...	0.33
iscsi04	🟢	zonea	Default	172.21.226.12	E13A300_2	a0a-3482		iSCSI	D...	0.01
iscsi01	🟢	zonea	Default	172.21.225.11	E13A300_1	a0a-3481		iSCSI	D...	0

2. En vSphere host iSCSI Storage Adapter, agregue esa IP de iSCSI en la pestaña Dynamic Discovery.



Para el modo de acceso uniforme, debe proporcionar la dirección lif de datos iSCSI del dominio de fallo de origen y de destino.

3. Repita el paso anterior en los hosts de vSphere para el otro dominio de fallos agregando su IP de lif de datos iSCSI local en la pestaña de detección dinámica.
4. Con la conectividad de red correcta, deben existir cuatro conexiones iSCSI por host vSphere que tenga dos nic de VMkernel iSCSI y dos LIF de datos iSCSI por controladora de almacenamiento.

```
E13A300::> iscsi connection show -vserver zona -remote-address 172.21.225.71
-----
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zona        iscsi01      23    0 172.21.225.11  172.21.225.71  0
zona        iscsi03      17    0 172.21.225.12  172.21.225.71  0
2 entries were displayed.

E13A300::> iscsi connection show -vserver zona -remote-address 172.21.226.71
-----
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zona        iscsi02      24    0 172.21.226.11  172.21.226.71  0
zona        iscsi04      16    0 172.21.226.12  172.21.226.71  0
2 entries were displayed.
```

5. Crear LUN mediante ONTAP System Manager, configurar SnapMirror con la política de replicación AutomatedFailOverDuplex, seleccionar los iniciadores del host y establecer la proximidad del host.

Add LUNs ✕

Host ID:

Default HA:

Group with related LUNs ⓘ

Storage and optimization

NUMBER OF LUNS: CAPACITY PER LUN: GB

PERFORMANCE SERVICE LEVEL:

Not sure? [Get help selecting type](#)

Apply the performance limits enforcement to each LUN. If unchecked, these limits will be applied to the entire set of LUNs.

Protection

Enable Snapshot copies (Docker)

Enable SnapMirror (local or remote)

RESTRICTION ADJUST: Show legacy policies ⓘ

Source

CLUSTER:

STORAGE VIA:

COMPONENT GROUP:

Destination

CLUSTER: Refresh

STORAGE VIA:

Destination settings

ⓘ You should manually create an iGroup by adding replicated hosts in the destination cluster and map the group to the newly created LUNs.

Host information

HOST OPERATING SYSTEM: CVM POWER:

HOST SOURCES:

Existing initiator group

New initiator group using existing initiator groups

Host initiators

REFRESH GROUP NAME:

iSCSI Initiators (2)

Name	Description	In proximity to
<input type="checkbox"/> ipn.1954-01.com.redhat.51c1788998b	-	None
<input type="checkbox"/> ipn.1954-01.com.redhat.a3435046678	-	None
<input checked="" type="checkbox"/> ipn.1958-01.com.vmware.s01-aaa01.s0...	-	Source
<input checked="" type="checkbox"/> ipn.1958-01.com.vmware.s01-aaa02.s12...	-	Source
<input type="checkbox"/> ipn.1958-01.com.vmware.s02-aaa01.s0...	-	Destination

[+ Add initiator](#)

6. En otra cabina de almacenamiento del dominio de fallos, cree el iGroup SAN con sus iniciadores de host de vSphere y establezca la proximidad del host.

Overview Mapped LUNs

STORAGE VM
zonebTYPE
VMwarePROTOCOL
Mixed (iSCSI & FC)COMMENT
-PORTSET
-CONNECTION STATUS  OK

^ Initiators

Name	De...	Connection status 	In proximity to
iqn.1998-01.com.vmware:dc02-esxi01.sddc.netap...	-	 OK	zoneb
iqn.1998-01.com.vmware:dc02-esxi02.sddc.netap...	-	 OK	zoneb



Para el modo de acceso uniforme, el igroup se puede replicar desde el dominio de fallo de origen.

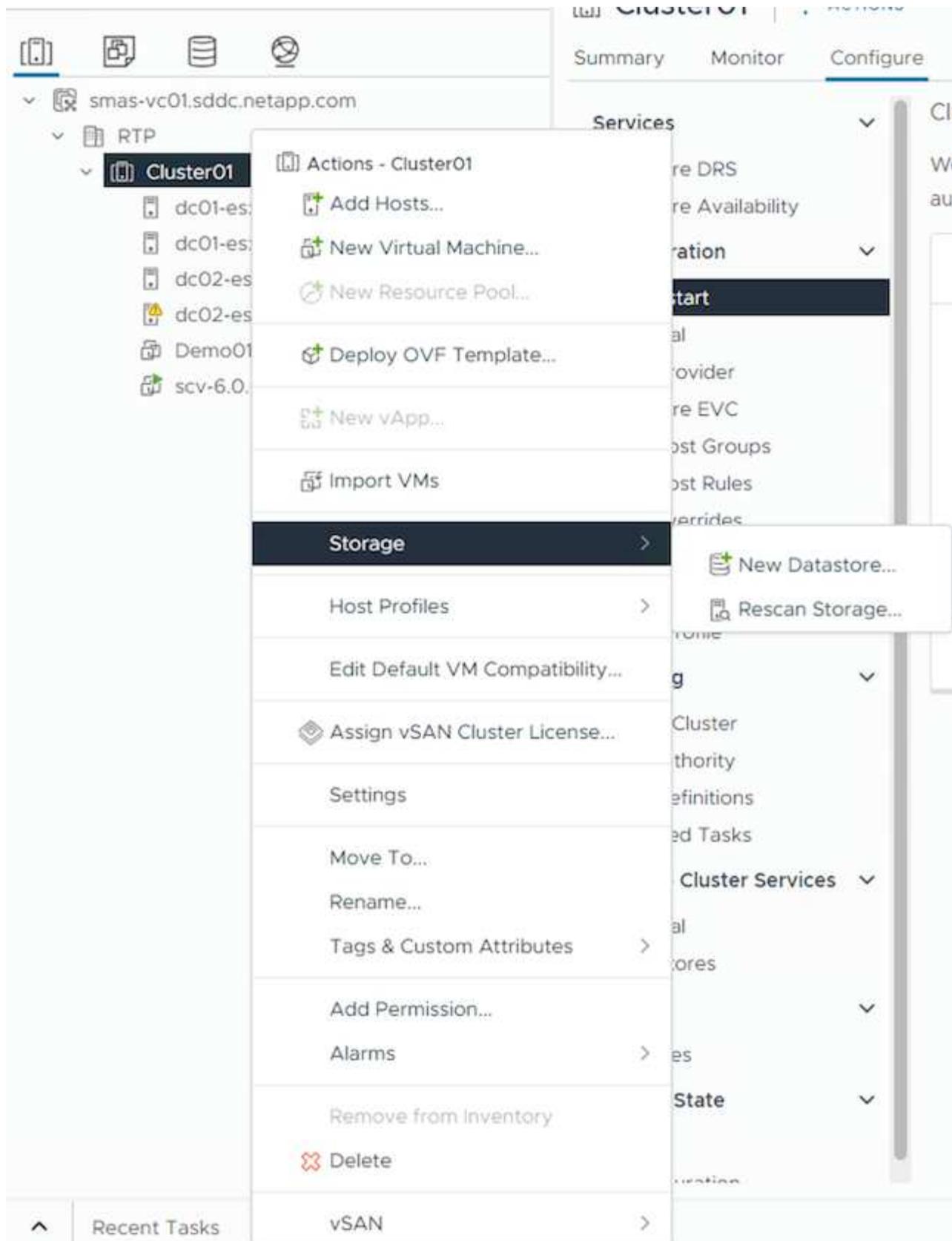
7. Asigne la LUN replicada con el mismo ID de asignación que en el dominio de fallo de origen.

Overview Mapped LUNs

[+ Add](#) [Map LUNs](#)[Filter](#)

<input type="checkbox"/>	Name	ID
<input type="checkbox"/>	ds02	1
<input type="checkbox"/>	ds01	0

8. En vCenter, haga clic con el botón derecho en vSphere Cluster y seleccione Rescan Storage Option.



9. En uno de los host de vSphere del clúster, compruebe que el dispositivo recién creado aparezca en el almacén de datos que muestra no consumido.

dc01-esxi01.sddc.netapp.com | ACTIONS

Summary Monitor **Configure** Permissions VMs Datastores Networks Updates

Storage

- Storage Adapters**
 - Storage Devices
 - Host Cache Configuration
 - Protocol Endpoints
 - I/O Filters
 - Storage Providers
- Networking**
 - Virtual switches
 - VMkernel adapters
 - Physical adapters
 - TCP/IP configuration
- Virtual Machines**
 - VM Startup/Shutdown
 - Agent VM Settings
 - Default VM Compatibility
 - Swap File Location
- System**
 - Licensing
 - Host Profile
 - Time Configuration
 - Authentication Services

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	ISCSI Software Adapter	ISCSI	Online	iscsi_vmk1(qn.1998-01.com,vmware:dc01-esxi01.sddc.netapp.com:473524194.65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Contr other	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Contr other	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	1	1	1

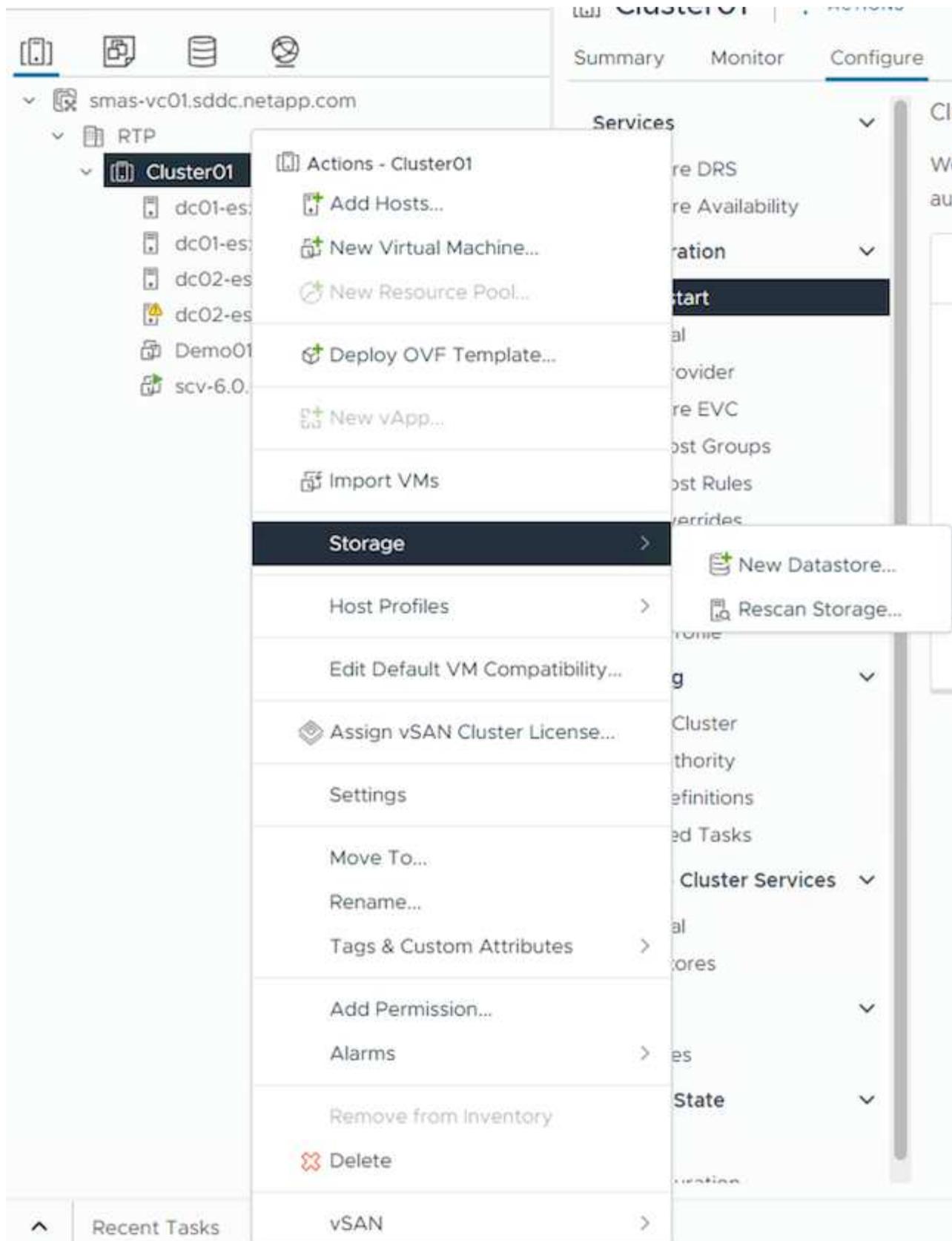
Manage Columns Export ▾ 4 items

Properties **Devices** Paths Dynamic Discovery Static Discovery Network Port Binding Advanced Options

REFRESH ATTACH DETACH RENAME

Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
NETAPP iSCSI Disk (naa.600a0980383038467724524975577931)	0	disk	250.00 GB	DS01	Attached	Supported	Flash	iSCSI
NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	1	disk	300.00 GB	Not Consumed	Attached	Supported	Flash	iSCSI

10. En vCenter, haga clic con el botón derecho en vSphere Cluster y seleccione New Datastore Option.



11. En el Asistente, recuerde proporcionar el nombre del almacén de datos y seleccionar el dispositivo con la capacidad y el identificador de dispositivo adecuados.

New Datastore

- Type
- Name and device selection**
- VMFS version
- Partition configuration
- Ready to complete

Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name:

Info: The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

Select a host:

Select a host to view its accessible disks/LUNs:

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Ch...
<input checked="" type="radio"/>	NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	1	300.00 G B	Supported	Flash	512e	Nc
<input type="radio"/>	Local VMware Disk (mpx.vmhba0:CO:T0:L0)	0	100.00 G B	Not support ed	HDD	512n	Nc

Manage Columns | Export v | 2 items

CANCEL | BACK | NEXT

12. Compruebe que el almacén de datos se haya montado en todos los hosts del clúster de ambos dominios con fallos.

DS02

Summary | Monitor | **Configure** | Permissions | Files | Hosts | VMs

Alarm Definitions
Scheduled Tasks
General
Device Backing
Connectivity and Multipathing
Hardware Acceleration
Capability sets
SnapCenter Plug-in for VMware
Resource Groups
Backups

Connectivity and Multipathing

Mount | Unmount

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
<input checked="" type="radio"/>	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

Manage Columns | 4 items

Device NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)

Multipathing Policies ACTIONS v

- Path Selection Policy: Round Robin (VMware)
- Storage Array Type Policy: VMW_SATP_ALUA
- Owner Plugin: NMP

Paths REFRESH | ENABLE | DISABLE

	Runtime Name	Status	Target	LUN	Preferred
<input type="radio"/>	vmhba65:CO:T0:L1	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56.vs.28.172.21.226.12.3260	1	No
<input type="radio"/>	vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56.vs.28.172.21.226.12.3260	1	No
<input type="radio"/>	vmhba65:C3:T0:L1	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56.vs.28.172.21.226.12.3260	1	No
<input type="radio"/>	vmhba65:C1:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56.vs.28.172.21.226.12.3260	1	No

DS02 ACTIONS

Summary Monitor **Configure** Permissions Files Hosts VMs

Alarm Definitions
Scheduled Tasks
General
Device Backing
Connectivity and Multipathing
Hardware Acceleration
Capability sets
SnapCenter Plug-in for VMware
Resource Groups
Backups

Connectivity and Multipathing

Mount UNMOUNT

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
<input type="radio"/>	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input checked="" type="radio"/>	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

Manage Columns 4 items

Device: NETAPP iSCSI Disk (naa.600a0980383038467724524975577933) ↗

Multipathing Policies ACTIONS

- Path Selection Policy: Round Robin (VMware)
- Storage Array Type: VMW_SATP_ALUA
- Policy
- Owner Plugin: NMP

Paths

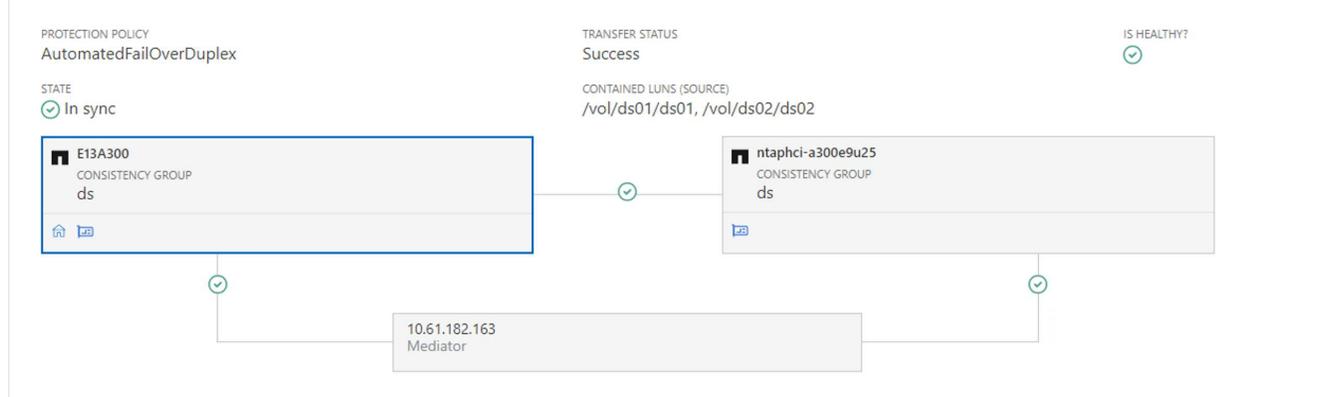
REFRESH ENABLE DISABLE

	Runtime Name	Status	Target	LLN	Preferred
<input type="radio"/>	vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.225.22.3260	1	No
<input type="radio"/>	vmhba65:C0:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.225.22.3260	1	No
<input type="radio"/>	vmhba65:C3:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.226.21.3260	1	No
<input type="radio"/>	vmhba65:C1:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.226.22.3260	1	No



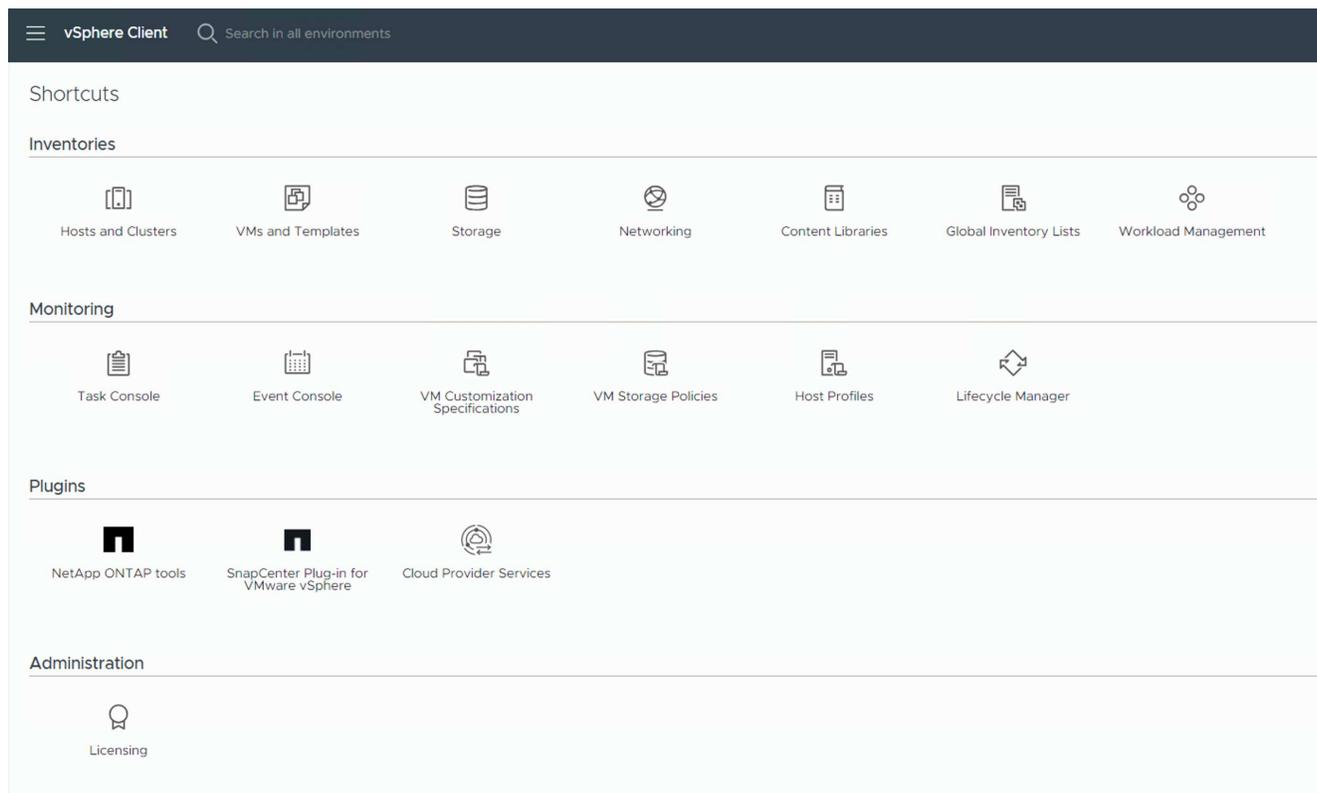
Las capturas de pantalla anteriores muestran E/S activas en un solo controlador, ya que utilizamos AFF. Para ASA, tendrá Active IO en todas las rutas.

13. Cuando se añaden almacenes de datos adicionales, es necesario recordar la expansión del grupo de consistencia existente para que sea coherente en todo el clúster de vSphere.



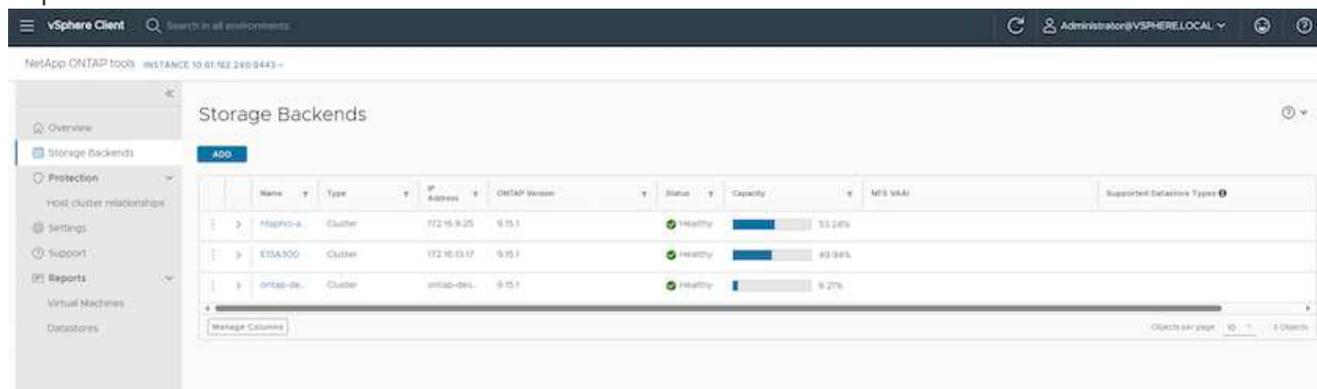
Modo de acceso de host uniforme VMSC con herramientas de ONTAP.

1. Compruebe que las herramientas de NetApp ONTAP se implementen y se registren en vCenter.



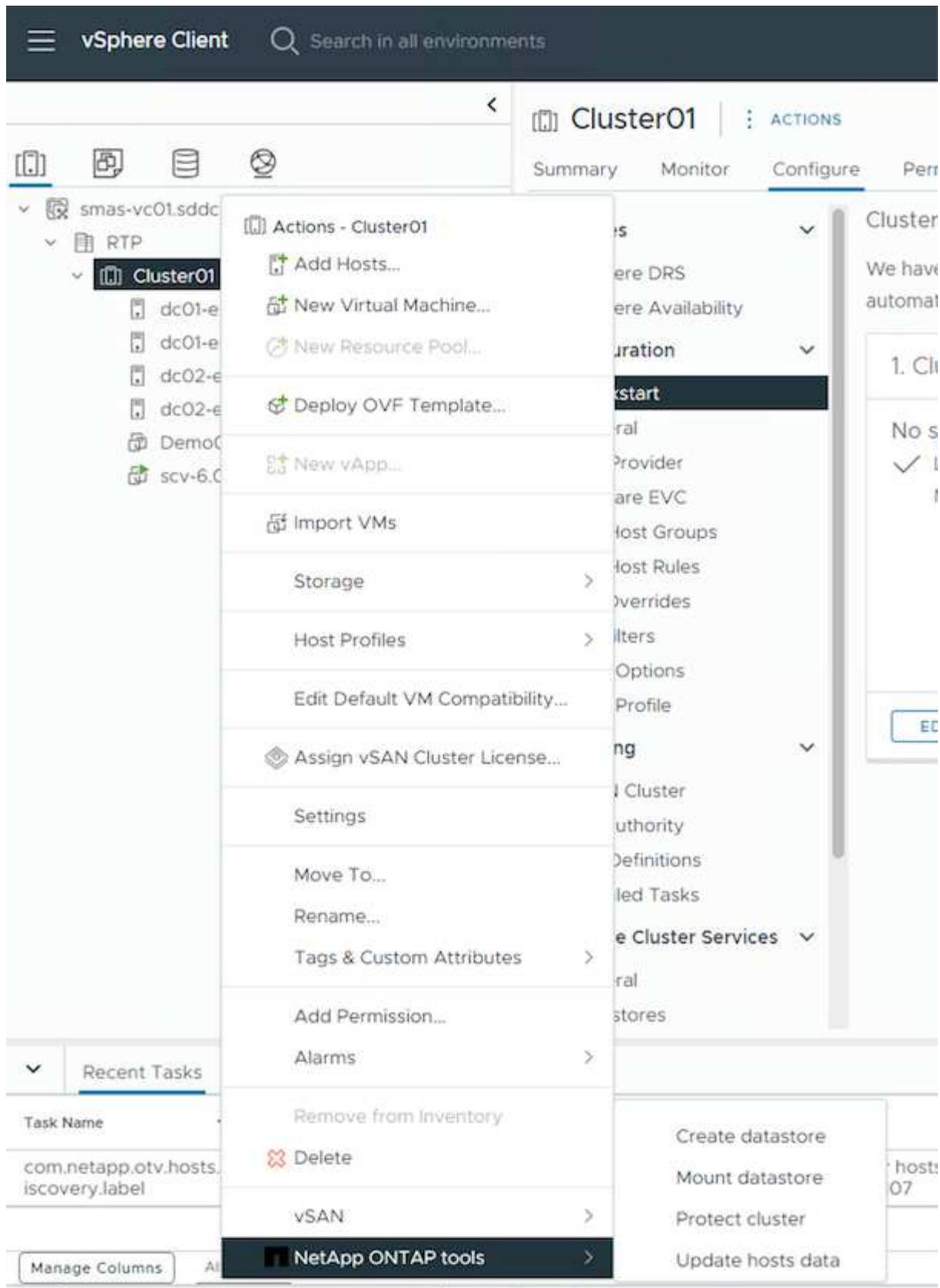
Si no es así, siga ["Puesta en marcha de Herramientas de ONTAP"](#) y ["Añada una instancia de vCenter Server"](#)

- Comprobar que los sistemas de almacenamiento de ONTAP están registrados en las herramientas de ONTAP. Esto incluye los sistemas de almacenamiento de dominio de fallo y el tercero para replicación remota asíncrona para su uso para protección de VM con el complemento SnapCenter para VMware vSphere.



De lo contrario, siga ["Añadir el back-end de almacenamiento mediante la interfaz de usuario del cliente de vSphere"](#)

- Actualice los datos del host para sincronizarlos con las herramientas de ONTAP y, a continuación, [" Cree un almacén de datos"](#).



4. Para habilitar SM-As, haga clic con el botón derecho en el clúster de vSphere y elija Protect Cluster en herramientas de NetApp ONTAP (consulte la captura de pantalla anterior)
5. Mostrará los almacenes de datos existentes para el clúster junto con los detalles de SVM. El nombre predeterminado del CG es <vSphere Cluster name>_<SVM name>. Haga clic en el botón Agregar relación.

Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. [Learn more](#)

Datastore type: * VMFS

Source storage VM: *
zonea
Cluster: E13A300
[2 datastores](#)

Consistency group name: * Cluster01_zonea

SnapMirror settings

[ADD RELATIONSHIP](#)

Target storage VM	Policy	Uniform Host Configuration	Host proximity
 No SnapMirror relationship found. You can protect datastores using one or more SnapMirror relationships.			
			Objects per page 5 0 Object

[CANCEL](#)

[PROTECT](#)

6. Seleccione la SVM de destino y establezca la política en AutomatedFailOverDuplex para SM-AS. Hay un conmutador para la configuración de host uniforme. Establezca la proximidad para cada host.

Add SnapMirror Relationship

Source storage VM: * E13A300 / zonaa

Target storage VM: * zoneb
Cluster: ntaphci-a300e9u25

Policy: * AutomatedFailOverDuplex

Uniform host configuration:

Host proximity settings

 As part of protection, all datastores will be mounted on all hosts.

SET PROXIMAL TO ▾

<input type="checkbox"/>	Hosts	Proximal to
<input type="checkbox"/>		
<input type="checkbox"/>	dc01-esxi02.sddc.netapp.com	Source ▾
<input type="checkbox"/>	dc02-esxi01.sddc.netapp.com	Target ▾

4 Objects

CANCEL

ADD

7. Compruebe la información de proximidad del host y otros detalles. Añada otra relación a un tercer sitio con una política de replicación de Asynchronous si es necesario. A continuación, haga clic en Proteger.

Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. [Learn more](#)

Datastore type: * VMFS

Source storage VM: * zonea
Cluster: E13A300
[2 datastores](#)

Consistency group name: * Cluster01_zonea

SnapMirror settings

[ADD RELATIONSHIP](#)

Target storage VM	Policy	Uniform Host Configuration	Host proximity
⋮ ntaphci-a300e9u25 / zoneb	AutomatedFailOverDuplex	Yes	Source (2), Target (2)

Objects per page 1 Object

[CANCEL](#) [PROTECT](#)

NOTA: Si planea usar el plugin de SnapCenter para VMware vSphere 6,0, la replicación debe configurarse a nivel de volumen en lugar de a nivel de grupo de consistencia.

- Con acceso de host uniforme, el host tiene conexión iSCSI a las dos cabinas de almacenamiento de dominio de fallo.

Connectivity and Multipathing

Host	Datastore Mounted	Datastore Connectivity	Mount Point
dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e

Device: NETAPP iSCSI Disk (naa.600a0980383038467724524975577931) -

Multipathing Policies: ACTIONS -

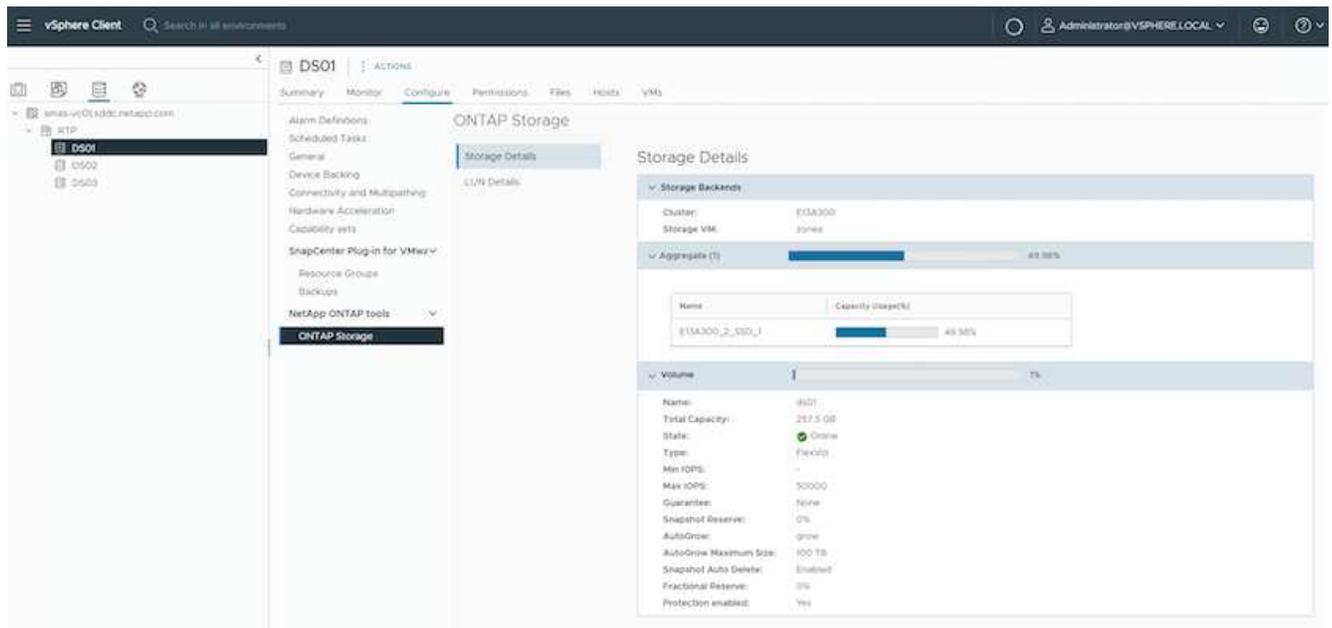
- Path Selection Policy: Round Robin (VMware)
- Storage Array Type: VMW_SATP_ALUA
- Policy: (empty)
- Owner Plugin: NMP

Paths:

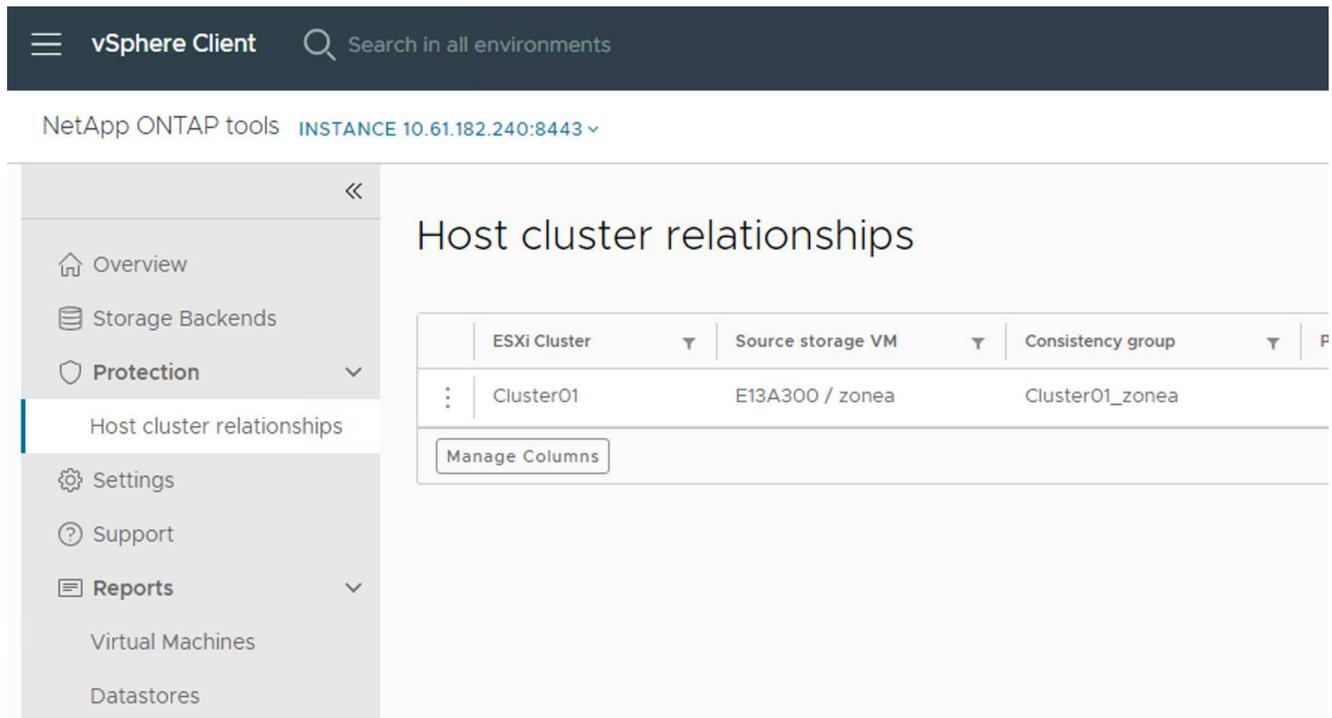
Runtime Name	Status	Target	LUN
vmhba65:C3:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.225.12.3260	0
vmhba65:C2:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.226.12.3260	0
vmhba65:C1:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.225.11.3260	0
vmhba65:C3:T0:L0	Active (VO)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.226.21.3260	0
vmhba65:C0:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.226.11.3260	0
vmhba65:C2:T0:L0	Active (VO)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.225.21.3260	0
vmhba65:C1:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.226.22.3260	0
vmhba65:C0:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.225.22.3260	0

NOTA: La captura de pantalla anterior es de AFF. Si la ASA, las operaciones de I/O ACTIVAS deben estar en todas las rutas con las conexiones de red adecuadas.

- El complemento Herramientas de ONTAP también indica que el volumen está protegido o no.

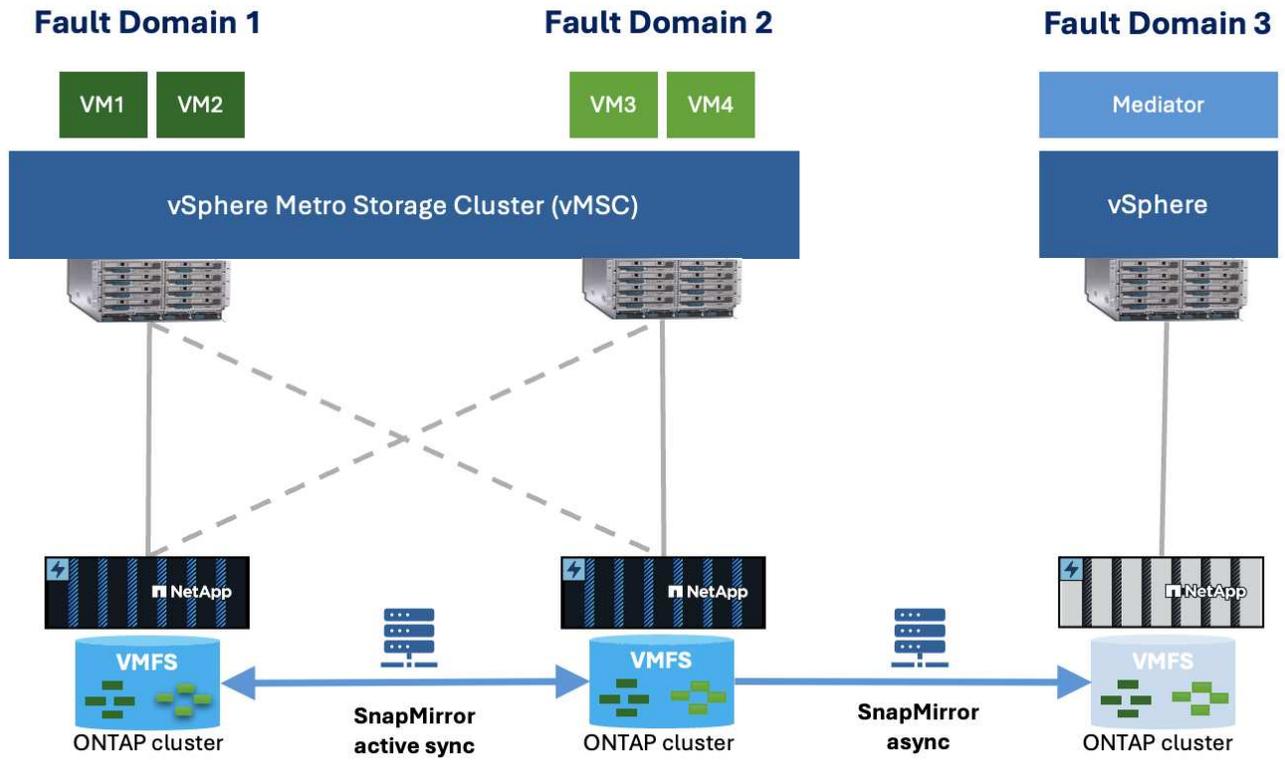


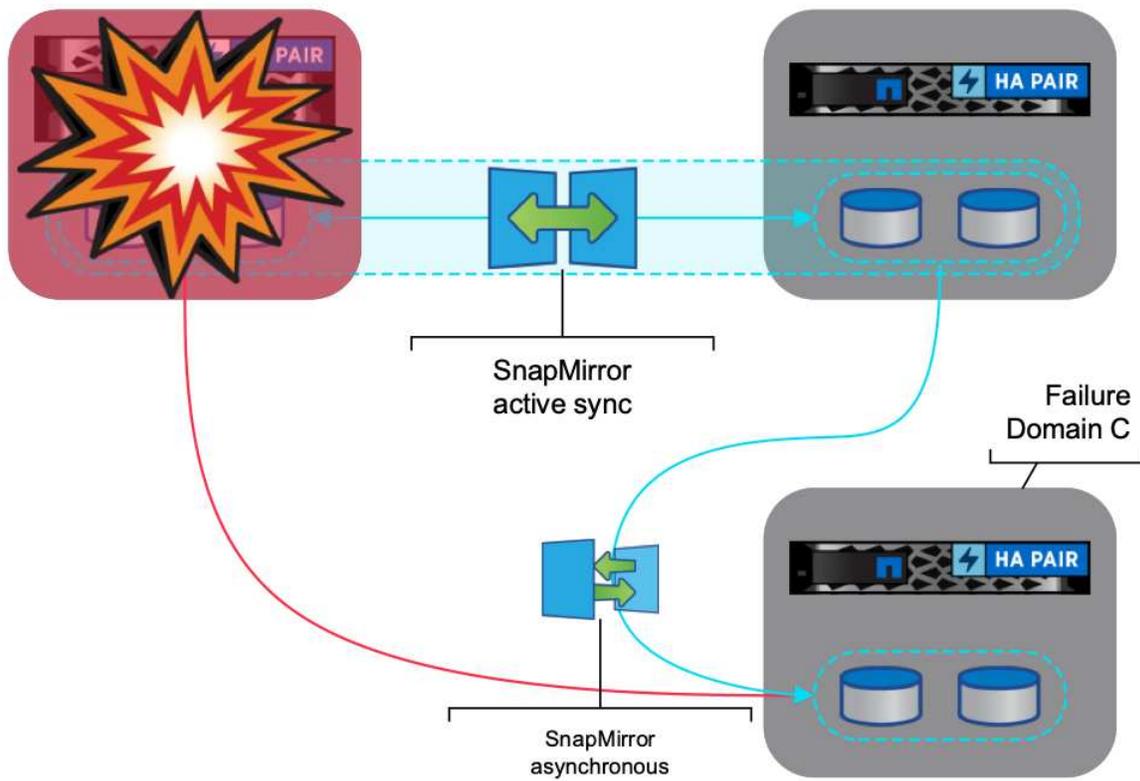
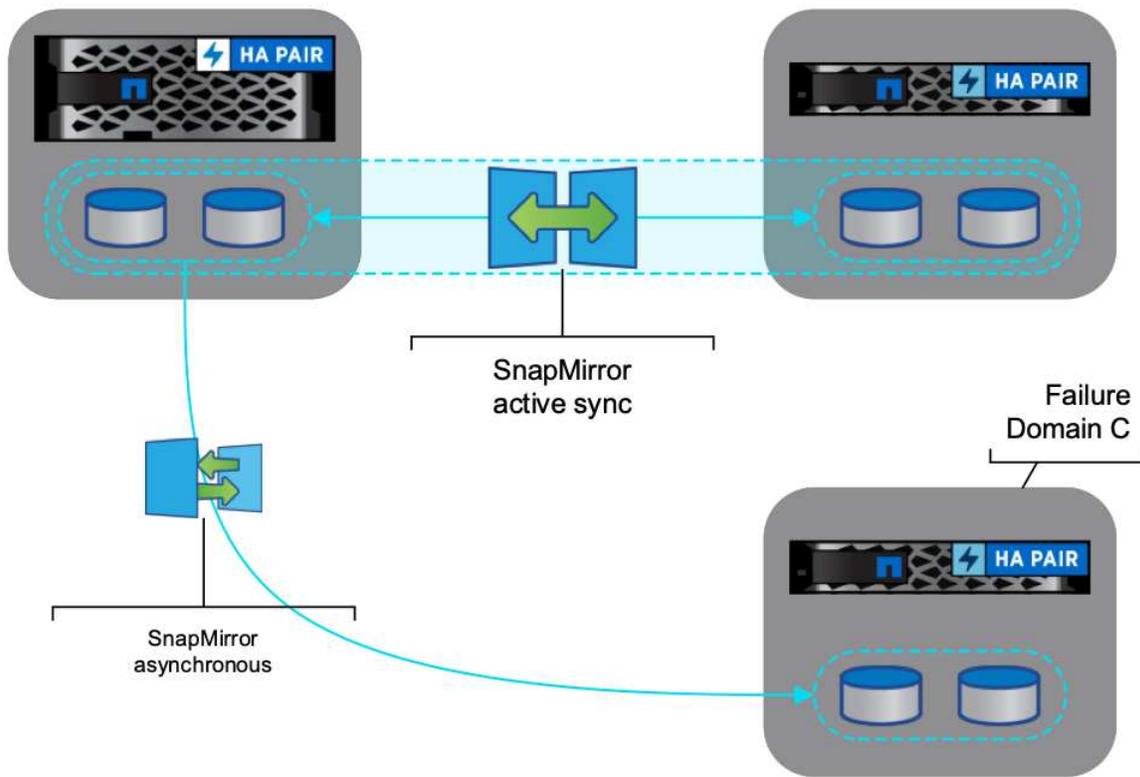
10. Para obtener más detalles y actualizar la información de proximidad del host, se puede utilizar la opción de relaciones del clúster de host en Herramientas de ONTAP.



Protección de máquina virtual con el plugin de SnapCenter para VMware vSphere.

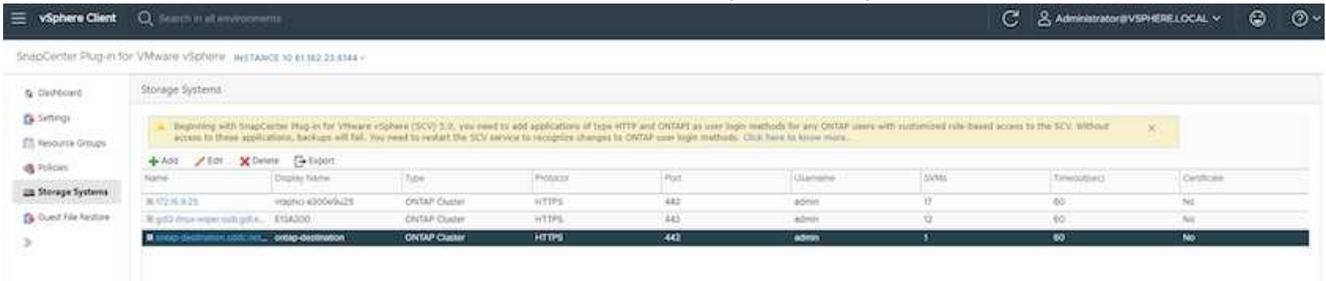
El plugin de SnapCenter para VMware vSphere (SCV) 6,0 o posterior admite la sincronización activa de SnapMirror y también en combinación con SnapMirror Async para replicar a un tercer dominio de fallos.



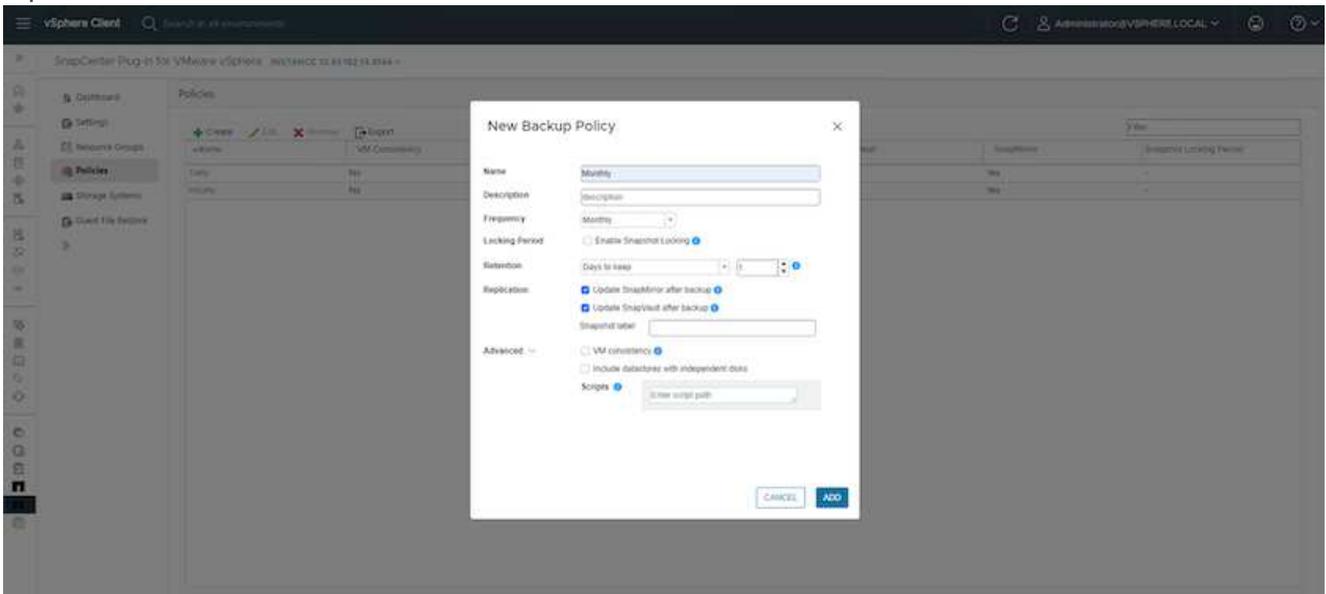


Los casos de uso admitidos incluyen: * Copia de seguridad y restauración de la máquina virtual o el almacén de datos desde cualquiera de los dominios de fallo con sincronización activa de SnapMirror. * Restaurar recursos desde el tercer dominio de falla.

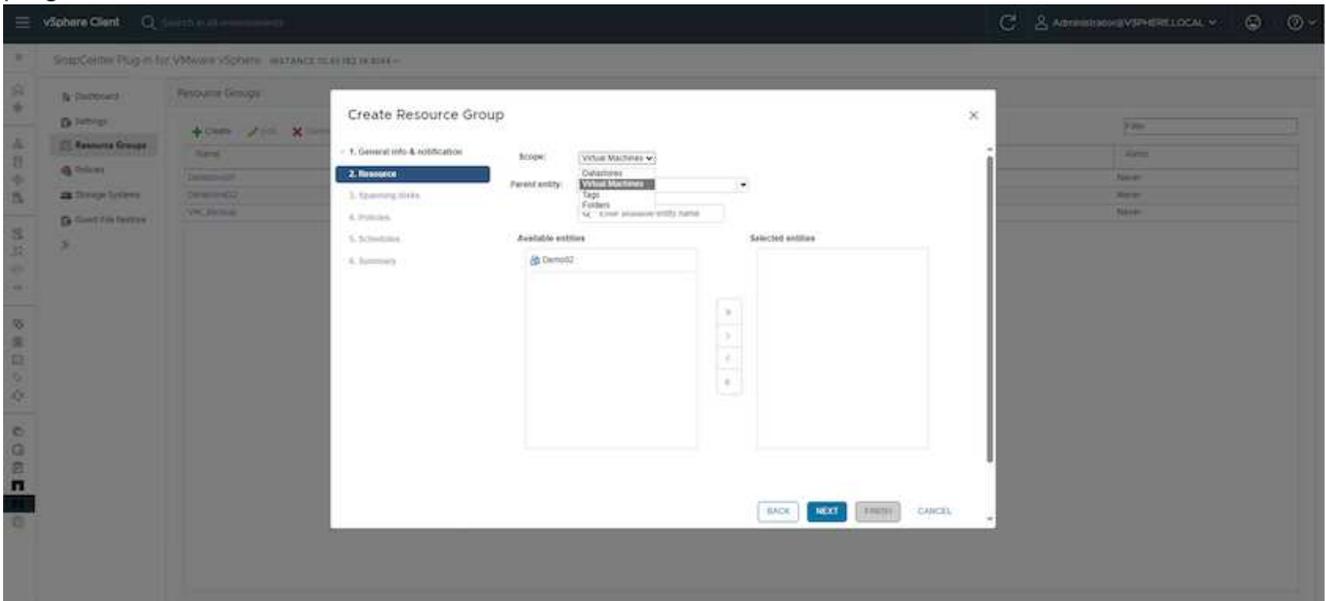
1. Añada todos los sistemas de almacenamiento de ONTAP que se han planificado utilizar en SCV.



2. Crear una política. Asegúrese de que Actualizar SnapMirror después de la copia de seguridad está comprobado para SM-AS y también Actualizar SnapVault después de la copia de seguridad para la replicación asíncrona en el tercer dominio de falla.



3. Cree un grupo de recursos con elementos deseados que deban protegerse y asociarse a la política y la programación.



NOTA: El nombre de la instantánea que termina en _recent no es compatible con SM-AS.

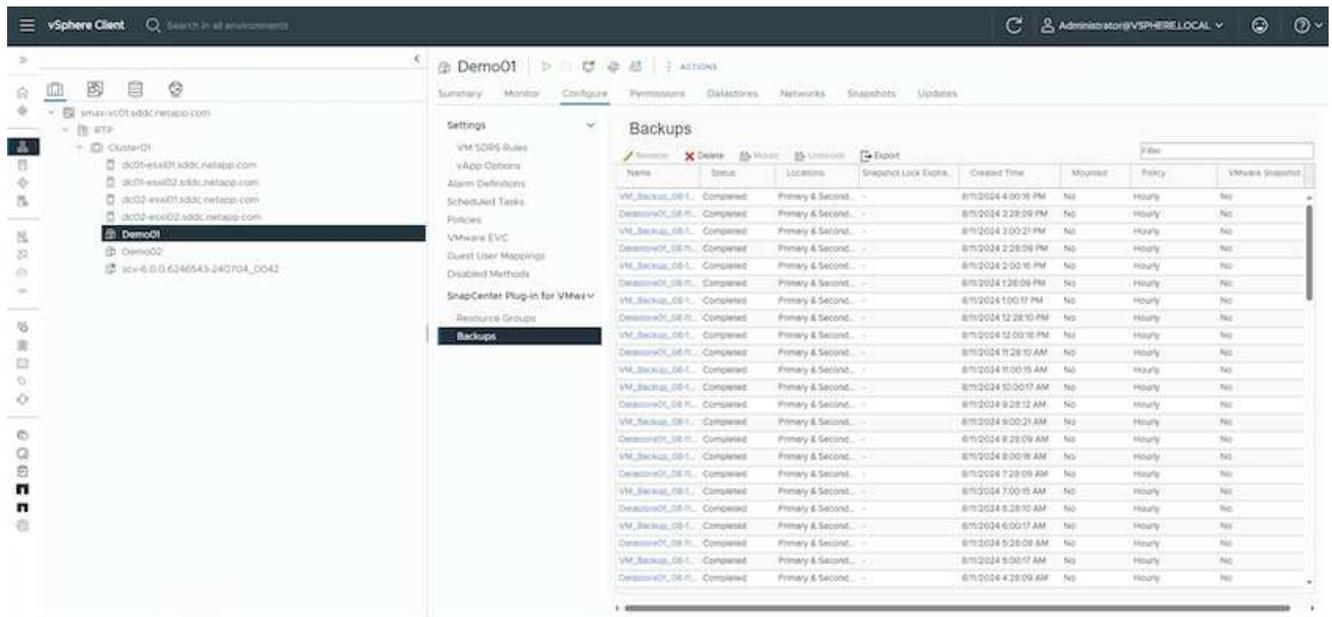
- Los backups se realizan en el tiempo programado según la política asociada al grupo de recursos. Los trabajos se pueden supervisar desde el supervisor de trabajos de la consola o desde la información de backup de esos recursos.

The screenshot shows the SnapCenter dashboard in vSphere Client. At the top, there's a navigation bar with 'vSphere Client' and a search bar. Below it, the dashboard is divided into several sections:

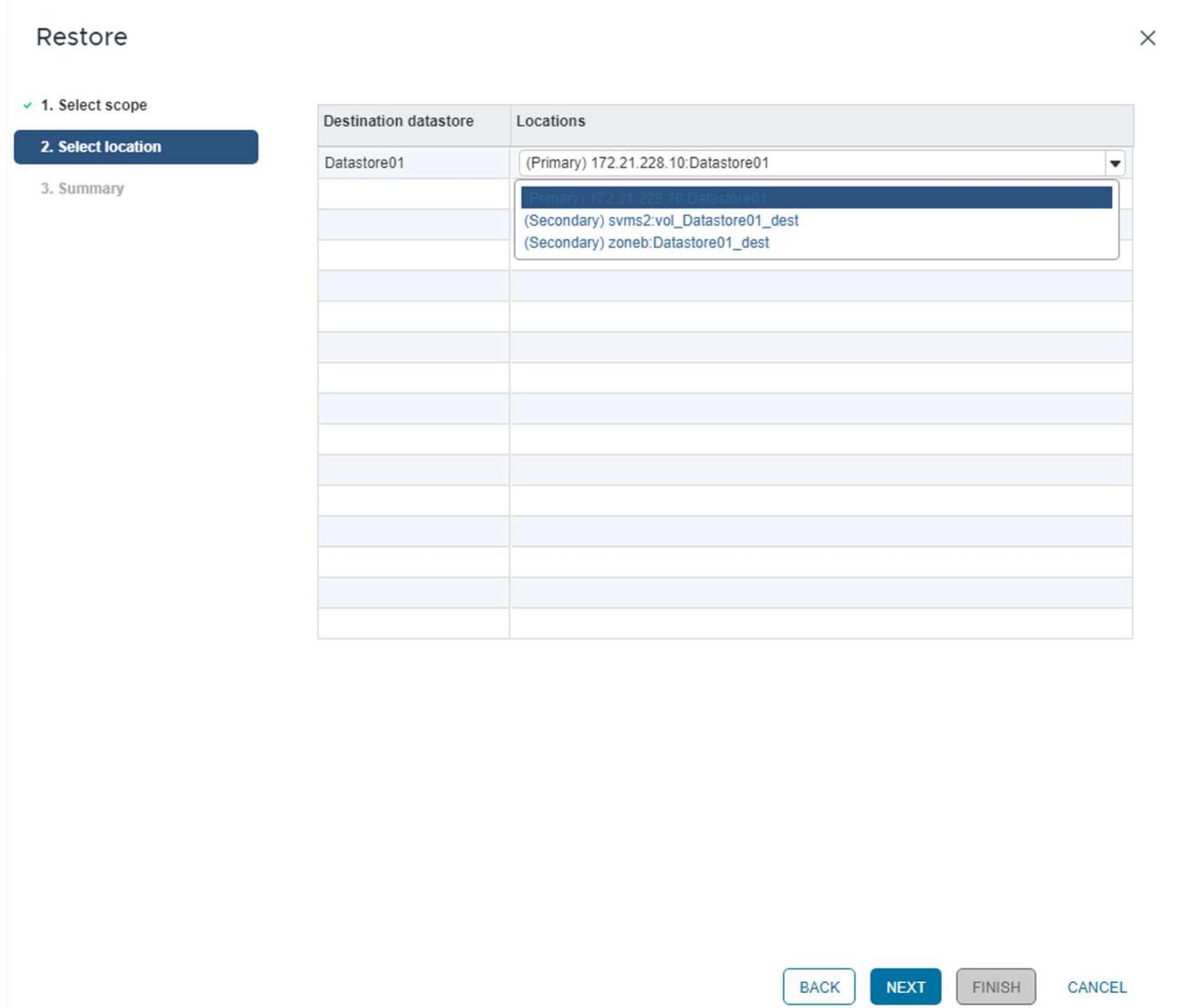
- RECENT JOB ACTIVITIES:** A list of backup jobs with columns for Name, Job ID, Status, and Time. Recent jobs include 'Backup Warning VM_Backup', 'Backup Successful Datastore1', 'Backup Successful VM_Backup', 'Backup Warning VM_Backup', and 'Backup Successful Datastore1'.
- JOB STATUS:** A donut chart showing overall job status: 52% Successful, 11 Failed, 71 Warning, and 1 Running.
- LATEST PROTECTION SUMMARY:** Three donut charts for Primary, Secondary, and Snapshot protection. Primary is 60% Protected (4 VMs not backed up, 2 Failed, 3 Successful). Secondary is 20% Replicated (2 VMs not replicated, 2 Failed, 1 Successful).
- STORAGE:** A bar chart showing storage usage for Snapshots: 4.64 GB (82 Snapshots), 5.12 GB (99 Snapshots), and 4.11 GB (42 Snapshots). It also highlights 66.46x Storage Savings, with 303.43 GB Saved and 4.64 GB Consumed.

The screenshot shows the configuration page for 'Datastore01' in SnapCenter. The left sidebar contains navigation options like 'Alarm Definitions', 'Scheduled Tasks', 'General', 'Device Backing', 'Connectivity and Multipathing', 'Hardware Acceleration', 'Cachability sets', 'NetApp ONTAP tools', 'SnapCenter Plug-in for VMware', 'Resource Groups', and 'Backups'. The main area displays a 'Backups' table with columns for Name, Status, Locations, Snapshot Lock Expi., Created Time, Mounted, Policy, and VMware Snapshot.

Name	Status	Locations	Snapshot Lock Expi.	Created Time	Mounted	Policy	VMware Snapshot
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 4:00:16 PM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 3:28:09 PM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 3:00:21 PM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 2:28:09 PM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 2:00:16 PM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 1:28:09 PM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 1:00:17 PM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 12:28:10 PM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 12:00:18 PM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 11:28:10 AM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 11:00:18 AM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 10:28:10 AM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 9:50:21 AM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 9:28:09 AM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 9:00:16 AM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 8:28:09 AM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 8:00:16 AM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 7:28:09 AM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 7:00:15 AM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 6:28:10 AM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 6:00:16 AM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 5:28:09 AM	No	Hourly	No
VM_Backup_DB-IT	Completed	Primary & Second	-	8/11/2024 5:00:17 AM	No	Hourly	No
Datastore01_DB-IT	Completed	Primary & Second	-	8/11/2024 4:28:09 AM	No	Hourly	No



5. Las máquinas virtuales se pueden restaurar a la misma instancia de vCenter o a una alternativa desde la SVM en el dominio de fallo primario o desde una de las ubicaciones secundarias.



6. También hay disponible una opción similar para la operación de montaje del almacén de datos.

Mount Backup ×

ESXi host name

Selected backup VM_Backup_08-11-2024_16.00.02.0270

Select datastore

<input type="checkbox"/>	Name	Location
<input type="checkbox"/>	Datastore01	Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270
<input type="checkbox"/>	Datastore02	Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270 Secondary:svms2:vol_Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270 Secondary:zoneb:Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270
<input type="checkbox"/>		
<input type="checkbox"/>		

⚠ Warning for ONTAP 9.12.1 and below version x

Para obtener ayuda con las operaciones adicionales con SCV, consulte ["Documentación del plugin de SnapCenter para VMware vSphere"](#)

Base de cloud de VMware

Base de cloud de VMware

VMware Cloud Foundation (VCF) es un conjunto de tecnologías que ofrece una ruta directa para acceder a una experiencia de nube híbrida. La solución VCF ofrece soporte para cargas de trabajo nativas de Kubernetes y basadas en máquinas virtuales. Los servicios esenciales como VMware vSphere, VMware vSAN, VMware NSX-T Data Center y VMware vRealize Cloud Management son componentes integrales del paquete VCF. Al combinarse, estos servicios establecen una infraestructura definida por software capaz de gestionar la informática, el almacenamiento, las redes, la seguridad y la gestión del cloud. Esta infraestructura colectiva proporciona una experiencia híbrida, en la que el marco VCF amplía el entorno desde el centro de datos in situ a Amazon Web Services (AWS), Azure y Google Cloud.

Recursos de documentación

Para obtener información detallada sobre las ofertas de NetApp para VMware Cloud Foundation, consulte la serie de blogs de cuatro (4) partes:

- ["NetApp y VMware Cloud Foundation se simplificaron. Parte 1: Introducción"](#)

- ["NetApp y VMware Cloud Foundation simplificaron la parte 2: VCF y almacenamiento principal de ONTAP"](#)
- ["NetApp y VMware Cloud Foundation simplificaron la parte 3: VCF y almacenamiento principal de Element"](#)
- ["NetApp y VMware Cloud Foundation simplificados: Parte 4: Herramientas de ONTAP para VMware y almacenamiento complementario"](#)
- [VMware Cloud Foundation con cabinas SAN All-Flash de NetApp*](#)
- ["VCF con matrices NetApp ASA, introducción y descripción general de la tecnología"](#)
- ["Utilice las herramientas de ONTAP para poner en marcha almacenes de datos iSCSI en un dominio de gestión de VCF"](#)
- ["Utilice las herramientas de ONTAP para implementar almacenes de datos vVols \(iSCSI\) en un dominio de carga de trabajo de VI"](#)
- ["Configure almacenes de datos NVMe over TCP para utilizarlos en un dominio de cargas de trabajo de VI"](#)
- ["Ponga en marcha y utilice el plugin de SnapCenter para VMware vSphere a fin de proteger y restaurar máquinas virtuales en un dominio de carga de trabajo de VI"](#)
- [VMware Cloud Foundation con cabinas AFF All-Flash de NetApp*](#)
- ["VCF con matrices NetApp AFF, introducción y descripción general de la tecnología"](#)
- ["Utilice ONTAP con NFS como almacenamiento principal para dominios de cargas de trabajo de VI"](#)
- ["Utilice las herramientas de ONTAP para implementar almacenes de datos NFS en un dominio de cargas de trabajo de VI"](#)

Soluciones NetApp FlexPod para VMware Cloud Foundation

- ["Expande el cloud híbrido de 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"](#)

VCF con cabinas NetApp ASA

VMware Cloud Foundation con cabinas SAN all-flash NetApp

VMware Cloud Foundation (VCF) es una plataforma integrada de centro de datos definido por software (SDDC) que proporciona una pila completa de infraestructura definida por software para ejecutar aplicaciones empresariales en un entorno de cloud híbrido. Combina funcionalidades de computación, almacenamiento, redes y gestión en una plataforma unificada que ofrece una experiencia operativa consistente en clouds privados y públicos.

Autor: Josh Powell

Este documento proporciona información sobre las opciones de almacenamiento disponibles para VMware Cloud Foundation mediante la cabina SAN all-flash de NetApp. Las opciones de almacenamiento admitidas se cubren con instrucciones específicas para poner en marcha almacenes de datos iSCSI como almacenamiento complementario para dominios de gestión y tanto almacenes de datos vVol (iSCSI) como NVMe/TCP como almacenes de datos complementarios para dominios de carga de trabajo. También se cubre la protección de datos de máquinas virtuales y almacenes de datos mediante SnapCenter para VMware vSphere.

Casos de uso

Casos de uso cubiertos en esta documentación:

- Opciones de almacenamiento para los clientes que buscan entornos uniformes tanto en clouds públicos como privados.
- Solución automatizada para poner en marcha infraestructura virtual para dominios de cargas de trabajo.
- Solución de almacenamiento escalable adaptada para satisfacer las necesidades en constante evolución, incluso cuando no se alinea directamente con los requisitos de recursos informáticos.
- Ponga en marcha el almacenamiento complementario en la gestión y en los dominios de cargas de trabajo de VI mediante ONTAP Tools para VMware vSphere.
- Proteger máquinas virtuales y almacenes de datos con el plugin de SnapCenter para VMware vSphere.

Destinatarios

Esta solución está dirigida a las siguientes personas:

- Arquitectos de soluciones que buscan opciones de almacenamiento más flexibles para entornos VMware diseñadas para maximizar el TCO.
- Arquitectos de soluciones que buscan opciones de almacenamiento VCF que ofrezcan opciones de protección de datos y recuperación ante desastres con los principales proveedores de cloud.
- Los administradores de almacenamiento que desean recibir instrucciones específicas sobre cómo configurar VCF con almacenamiento principal y complementario.
- Administradores de almacenamiento que desean instrucciones específicas sobre cómo proteger máquinas virtuales y almacenes de datos que residen en el almacenamiento de ONTAP.

Visión general de la tecnología

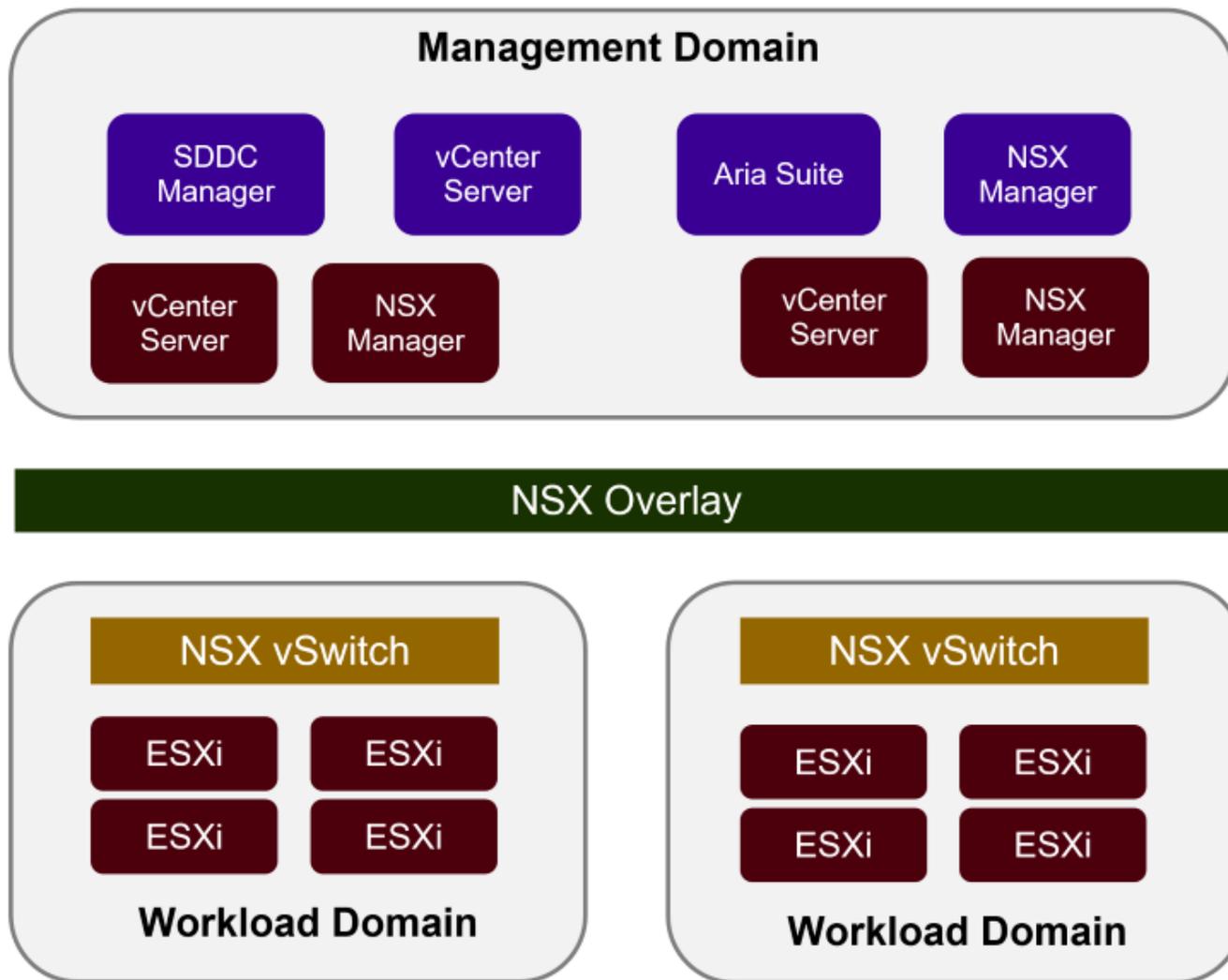
La solución VCF con NetApp ASA consta de los siguientes componentes principales:

Base de cloud de VMware

VMware Cloud Foundation amplía las ofertas de hipervisores vSphere de VMware combinando componentes clave como SDDC Manager, vSphere, vSAN, NSX y VMware Aria Suite para crear un centro de datos definido por software.

La solución VCF es compatible tanto con cargas de trabajo nativas de Kubernetes como con máquinas virtuales. Los servicios clave como VMware vSphere, VMware vSAN, VMware NSX-T Data Center y VMware Aria Cloud Management son componentes integrales del paquete VCF. Al combinarse, estos servicios establecen una infraestructura definida por software capaz de gestionar con eficiencia la informática, el almacenamiento, las redes, la seguridad y la gestión del cloud.

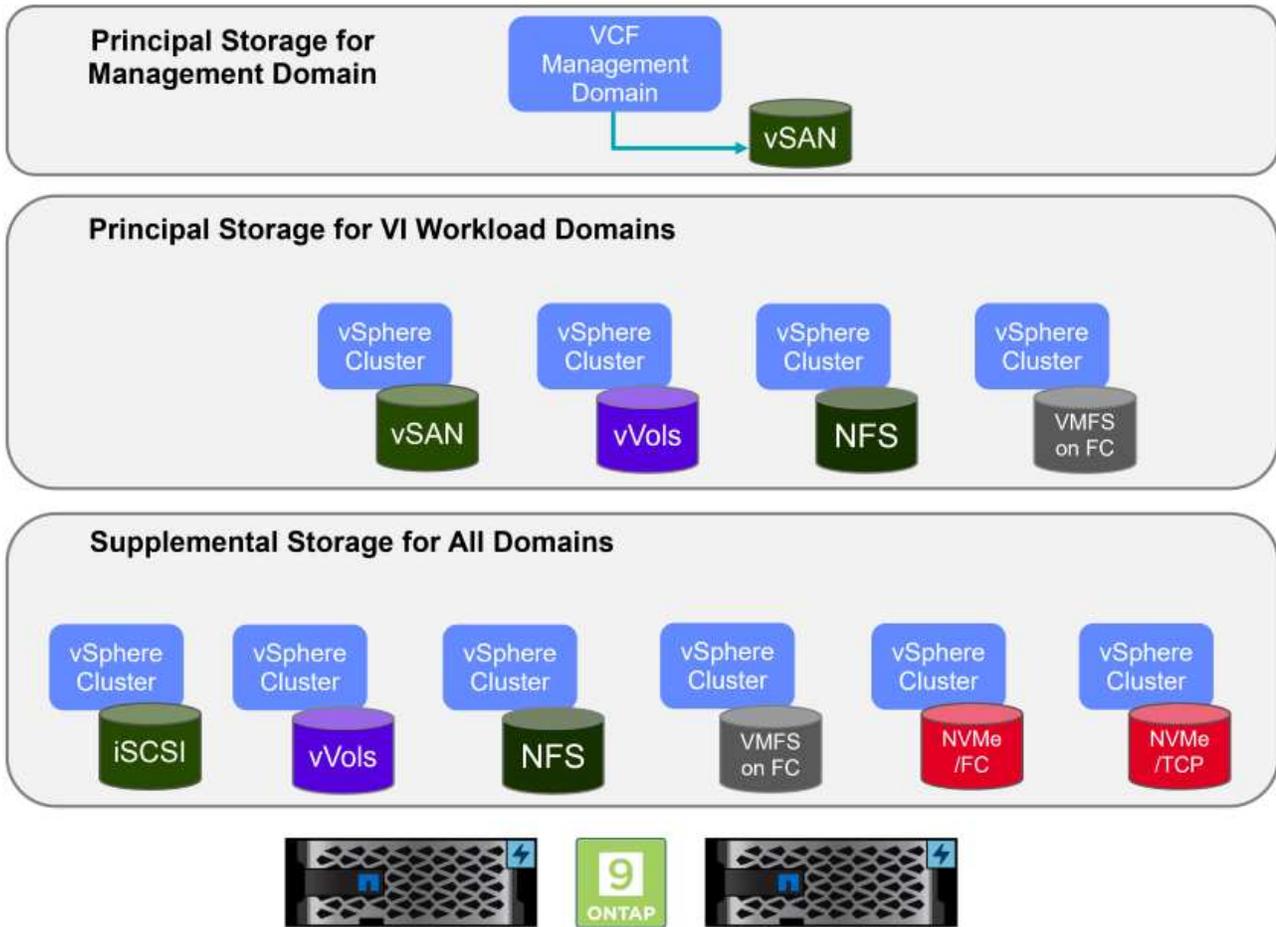
VCF se compone de un único dominio de gestión y hasta 24 dominios de carga de trabajo VI que cada uno representa una unidad de infraestructura lista para aplicaciones. Un dominio de carga de trabajo se compone de uno o más clústeres de vSphere que gestiona una única instancia de vCenter.



Para obtener más información sobre la arquitectura y planificación de VCF, consulte "[Modelos de arquitectura y tipos de dominio de carga de trabajo en VMware Cloud Foundation](#)".

Opciones de almacenamiento de VCF

VMware divide las opciones de almacenamiento para VCF en almacenamiento **principal** y **suplementario**. El dominio de gestión de VCF debe utilizar vSAN como su almacenamiento principal. Sin embargo, existen muchas opciones de almacenamiento suplementarias para el dominio de gestión y las opciones de almacenamiento principal y suplementario disponibles para los dominios de carga de trabajo VI.



Almacenamiento principal para dominios de carga de trabajo

El almacenamiento principal se refiere a cualquier tipo de almacenamiento que se puede conectar directamente a un dominio de carga de trabajo de VI durante el proceso de configuración dentro de SDDC Manager. El almacenamiento principal se pone en marcha con el administrador SDDC como parte de la orquestación de la creación de un clúster y es el primer almacén de datos configurado para un dominio de carga de trabajo. Incluye vSAN, vVols (VMFS), NFS y VMFS en Fibre Channel.

Almacenamiento suplementario para dominios de gestión y carga de trabajo

El almacenamiento complementario es el tipo de almacenamiento que se puede añadir a los dominios de las cargas de trabajo o gestión en cualquier momento una vez que se ha creado el clúster. El almacenamiento complementario representa la gama más amplia de opciones de almacenamiento compatibles, que son compatibles con las cabinas de NetApp ASA. El almacenamiento complementario se puede poner en marcha usando herramientas de ONTAP para VMware vSphere para la mayoría de los tipos de protocolo de almacenamiento.

Recursos de documentación adicionales para VMware Cloud Foundation:

- * ["Documentación de VMware Cloud Foundation"](#)
- * ["Tipos de almacenamiento compatibles para VMware Cloud Foundation"](#)
- * ["Gestión del almacenamiento en VMware Cloud Foundation"](#)

Cabinas All-Flash SAN NetApp

La cabina all-flash SAN (ASA) de NetApp es una solución de almacenamiento de alto rendimiento diseñada para satisfacer los requisitos más exigentes de los centros de datos modernos. Combina la velocidad y la

fiabilidad del almacenamiento flash con las funciones avanzadas de gestión de datos de NetApp para ofrecer un rendimiento, una escalabilidad y una protección de datos excepcionales.

La gama ASA está compuesta por los modelos A-Series y C-Series.

Las cabinas flash all-NVMe NetApp A-Series están diseñadas para cargas de trabajo de alto rendimiento, con una latencia ultrabaja y una alta resiliencia, lo que las convierte en adecuadas para aplicaciones de misión crítica.



Las cabinas flash QLC de C-Series se dirigen a casos de uso de mayor capacidad, y ofrecen la velocidad de la tecnología flash con la economía del flash híbrido.



Para obtener información detallada, consulte ["Página de destino de NetApp ASA"](#).

Compatibilidad con protocolos de almacenamiento

ASA admite todos los protocolos SAN estándar, incluidos iSCSI, Fibre Channel (FC), Fibre Channel sobre Ethernet (FCoE) y NVME over Fabrics.

iSCSI - NetApp ASA proporciona una sólida compatibilidad con iSCSI, lo que permite el acceso a nivel de bloque a dispositivos de almacenamiento a través de redes IP. Ofrece una integración perfecta con iniciadores iSCSI, lo que permite aprovisionar y gestionar LUN iSCSI de manera eficaz. Funciones avanzadas de ONTAP, como rutas múltiples, autenticación CHAP y compatibilidad con ALUA.

Para obtener directrices de diseño sobre configuraciones de iSCSI, consulte la ["Documentación de referencia de configuración de SAN"](#).

Canal de fibra - NetApp ASA ofrece soporte integral para el canal de fibra (FC), una tecnología de red de alta velocidad comúnmente utilizada en redes de área de almacenamiento (SAN). ONTAP se integra sin

problemas con la infraestructura de FC y proporciona un acceso por bloques fiable y eficiente a los dispositivos de almacenamiento. Ofrece funciones como la división en zonas, las rutas múltiples y el inicio de sesión estructural (FLOGI) para optimizar el rendimiento, mejorar la seguridad y garantizar una conectividad perfecta en entornos FC.

Para obtener directrices de diseño sobre configuraciones de Fibre Channel, consulte ["Documentación de referencia de configuración de SAN"](#).

NVMe over Fabrics - NetApp ONTAP y ASA admiten NVMe over Fabrics. NVMe/FC permite utilizar dispositivos de almacenamiento NVMe sobre infraestructura Fibre Channel y NVMe/TCP sobre redes IP de almacenamiento.

Para obtener directrices de diseño en NVMe, consulte ["Configuración, compatibilidad y limitaciones de NVMe"](#)

Tecnología activo-activo

Las cabinas NetApp All-Flash SAN permiten rutas activo-activo que pasan por ambas controladoras, por lo que no es necesario que el sistema operativo host espere a que se produzca un error en una ruta activa antes de activar la ruta alternativa. Esto significa que el host puede utilizar todas las rutas disponibles en todas las controladoras, asegurando que las rutas activas siempre estén presentes sin importar si el sistema está en estado constante o si se debe someter a una operación de conmutación por error de la controladora.

Además, NetApp ASA ofrece una función distintiva que mejora significativamente la velocidad de la conmutación por error de SAN. Cada controladora replica continuamente los metadatos LUN esenciales con su asociado. Como resultado, cada controladora está preparada para asumir las responsabilidades del servicio de datos en caso de un fallo repentino de su compañero. Esta preparación es posible debido a que la controladora ya posee la información necesaria para comenzar a utilizar las unidades que se gestionaron previamente por la controladora con el error.

Con rutas activo-activo, las tomas de control planificadas y sin planificar tienen tiempos de reanudación de I/O de 2-3 segundos.

Para obtener más información, consulte ["TR-4968, cabina All-SAS NetApp: Disponibilidad e integridad de los datos con NetApp ASA"](#).

Garantías de almacenamiento

NetApp ofrece un conjunto único de garantías de almacenamiento con cabinas SAN All-Flash NetApp. Sus ventajas únicas incluyen:

- **Garantía de eficiencia de almacenamiento:** * Consiga un alto rendimiento al tiempo que minimiza el costo de almacenamiento con la Garantía de Eficiencia de Almacenamiento. 4:1 para cargas de trabajo SAN.

Garantía de disponibilidad de datos de 6 Nines (99,9999%): garantiza la corrección de los tiempos de inactividad no planificados en más de 31,56 segundos al año.

Garantía de recuperación de ransomware: Recuperación de datos garantizada en caso de un ataque de ransomware.

Consulte ["Portal de productos de NetApp ASA"](#) si quiere más información.

Herramientas de ONTAP de NetApp para VMware vSphere

Las herramientas de ONTAP para VMware vSphere permiten a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Las herramientas de ONTAP también incluyen un proveedor de API de VMware vSphere para el conocimiento del almacenamiento (VASA)* para sistemas de almacenamiento de ONTAP, que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidades de almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

Para obtener más información sobre las herramientas de NetApp ONTAP, consulte la ["Herramientas de ONTAP para documentación de VMware vSphere"](#) página.

Plugin de SnapCenter para VMware vSphere

El plugin de SnapCenter para VMware vSphere (SCV) es una solución de software de NetApp que ofrece una protección de datos completa para entornos VMware vSphere. Está diseñado para simplificar y agilizar el proceso de protección y gestión de máquinas virtuales y almacenes de datos. SCV utiliza almacenamiento Snapshot y replicación a cabinas secundarias para cumplir objetivos de tiempo de recuperación reducidos.

El plugin de SnapCenter para VMware vSphere ofrece las siguientes funcionalidades en una interfaz unificada, integrada con el cliente de vSphere:

Instantáneas basadas en políticas - SnapCenter le permite definir políticas para crear y administrar instantáneas consistentes con aplicaciones de máquinas virtuales (VM) en VMware vSphere.

- Automatización * - La creación y gestión automatizada de instantáneas basadas en políticas definidas ayudan a garantizar una protección de datos consistente y eficiente.

VM-Level Protection - La protección granular a nivel de VM permite una gestión y recuperación eficientes de máquinas virtuales individuales.

- Características de eficiencia del almacenamiento * - La integración con las tecnologías de almacenamiento de NetApp proporciona funciones de eficiencia del almacenamiento como deduplicación y compresión para instantáneas, minimizando los requisitos de almacenamiento.

El complemento de SnapCenter orquesta el modo inactivo de máquinas virtuales junto con los snapshots basados en hardware en las cabinas de almacenamiento de NetApp. La tecnología SnapMirror se utiliza para replicar copias de backups en sistemas de almacenamiento secundarios, incluso en el cloud.

Para obtener más información, consulte ["Documentación del plugin de SnapCenter para VMware vSphere"](#).

La integración de BlueXP habilita estrategias de backup de 3-2-1 que amplían las copias de datos en el almacenamiento de objetos en el cloud.

Para obtener más información sobre estrategias de backup 3-2-1 con BlueXP, visita ["3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales"](#).

Descripción general de la solución

Los escenarios presentados en esta documentación mostrarán cómo usar sistemas de almacenamiento de ONTAP como almacenamiento complementario para dominios de cargas de trabajo y gestión. Además, el plugin de SnapCenter para VMware vSphere se utiliza para proteger máquinas virtuales y almacenes de datos.

Escenarios cubiertos en esta documentación:

- **Utilice las herramientas de ONTAP para implementar almacenes de datos iSCSI en un dominio de administración de VCF.** Haga clic en "[aquí](#)" para pasos de despliegue.
- **Utilice las herramientas de ONTAP para implementar almacenes de datos vVols (iSCSI) en un dominio de carga de trabajo VI.** Haga clic en "[aquí](#)" para pasos de despliegue.
- **Configurar almacenes de datos NVMe sobre TCP para su uso en un dominio de carga de trabajo VI.** Haga clic en "[aquí](#)" para pasos de despliegue.
- * Implementar y utilizar el complemento de SnapCenter para VMware vSphere para proteger y restaurar máquinas virtuales en un dominio de carga de trabajo VI*. Haga clic en "[aquí](#)" para pasos de despliegue.

Utilice las herramientas de ONTAP para configurar el almacenamiento complementario para los dominios de gestión de VCF

En esta situación, mostraremos cómo poner en funcionamiento y utilizar las herramientas de ONTAP para VMware vSphere (OTV) a fin de configurar un almacén de datos iSCSI para un dominio de gestión de VCF.

Autor: Josh Powell

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

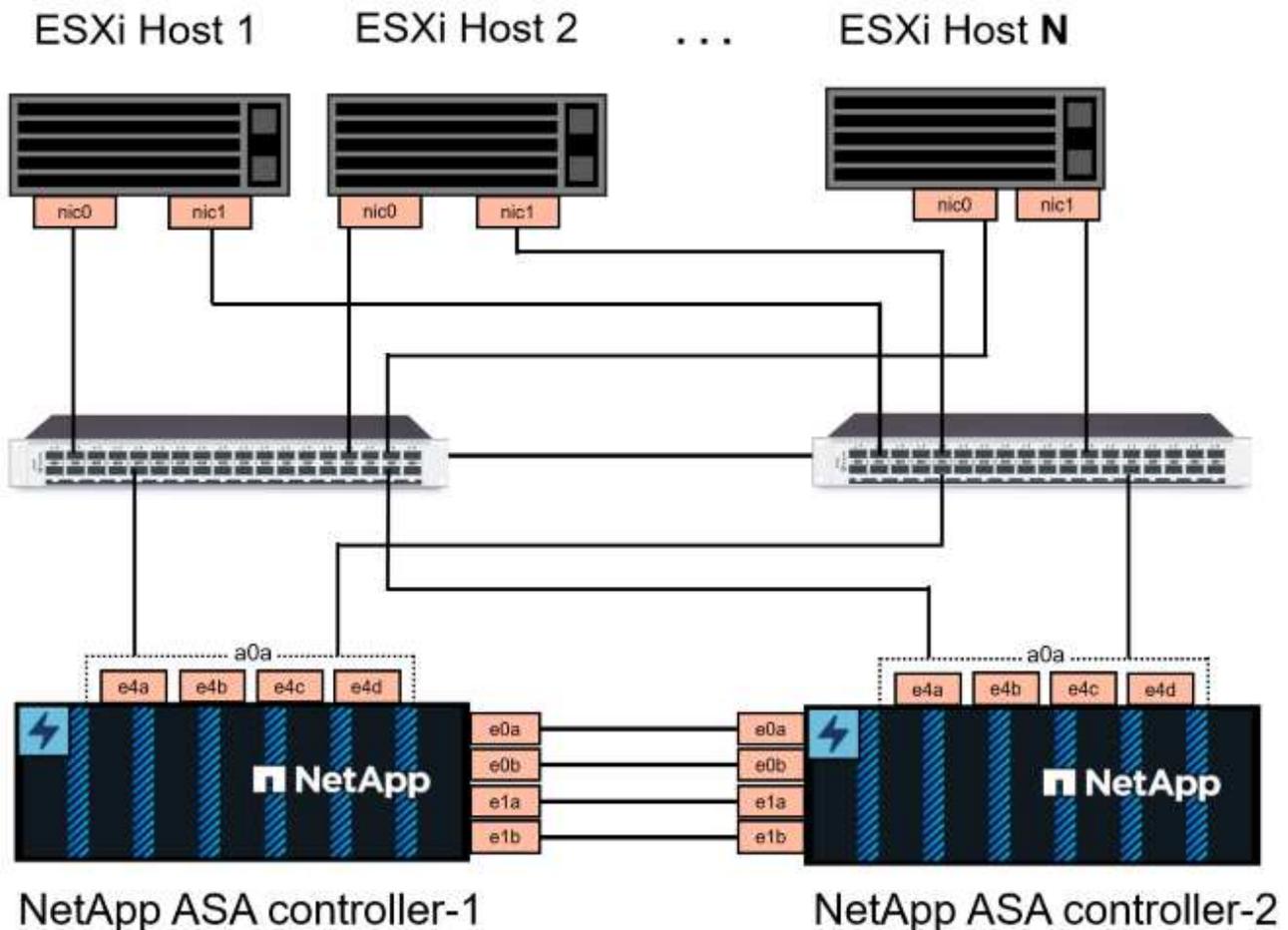
- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico de iSCSI.
- Cree grupos de puertos distribuidos para las redes iSCSI en el dominio de gestión de VCF.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de gestión de VCF.
- Implemente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

Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP ASA con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.
- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.

NetApp recomienda diseños de red completamente redundantes para iSCSI. En el siguiente diagrama se muestra un ejemplo de una configuración redundante, que proporciona tolerancia a fallos para los sistemas de almacenamiento, los switches, los adaptadores de red y los sistemas host. Consulte NetApp "[Referencia para la configuración DE SAN](#)" para obtener más información.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes ethernet independientes para todas las SVM en configuraciones de iSCSI.

Esta documentación muestra el proceso de crear una SVM nueva y especificar la información de dirección IP para crear varias LIF para el tráfico de iSCSI. Para agregar LIF nuevos a una SVM existente, consulte "[Crear una LIF \(interfaz de red\)](#)".

Para obtener información adicional sobre el uso de almacenes de datos VMFS iSCSI con VMware, consulte "[Almacén de datos VMFS de vSphere: Entorno de administración del almacenamiento iSCSI con ONTAP](#)".



En situaciones en las que se configuran varios adaptadores VMkernel en la misma red IP, se recomienda utilizar el enlace de puerto iSCSI de software en los hosts ESXi para garantizar el equilibrio de carga entre los adaptadores. Consulte el artículo de la base de conocimientos "[Consideraciones sobre el uso de la vinculación de puertos iSCSI de software en ESX/ESXi \(2038869\)](#)".

Pasos de despliegue

Para implementar las herramientas de ONTAP y utilizarlo para crear un almacén de datos VMFS en el dominio de gestión de VCF, lleve a cabo los siguientes pasos:

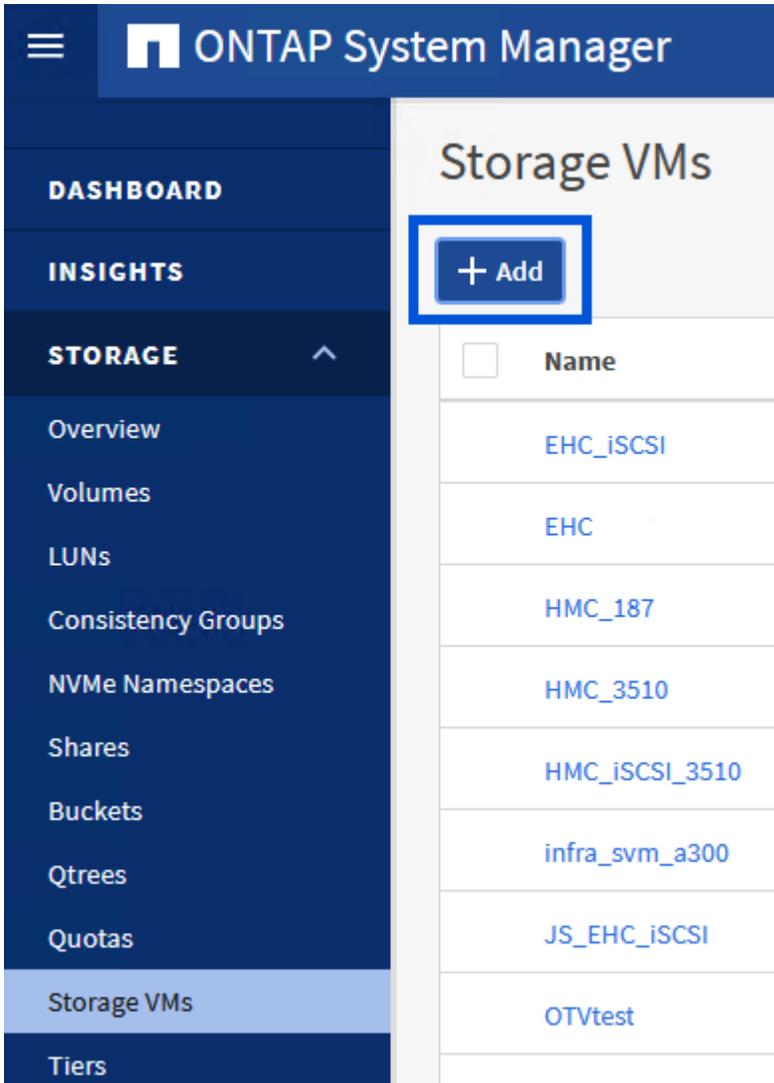
Crear SVM y LIF en el sistema de almacenamiento ONTAP

El siguiente paso se lleva a cabo en ONTAP System Manager.

Crear la máquina virtual de almacenamiento y las LIF

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

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



2. En el asistente de **Add Storage VM**, proporcione un **Name** para la SVM, seleccione **IP Space** y, a continuación, en **Access Protocol**, haga clic en la pestaña ***iSCSI** y marque la casilla **Enable iSCSI**.

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes o utilizar una configuración independiente.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet independientes para todas las SVM en configuraciones de iSCSI.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

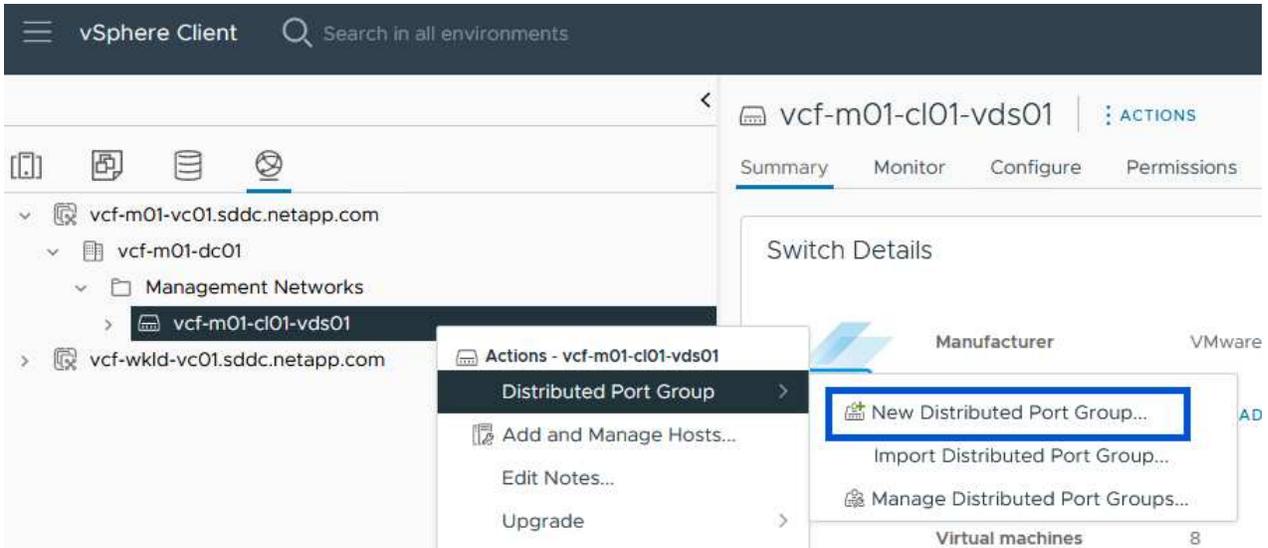
Configure las redes para iSCSI en hosts ESXi

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

Crear grupos de puertos distribuidos para el tráfico de iSCSI

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

1. Desde el cliente vSphere para el clúster de dominio de gestión, vaya a **Inventory > Networking**. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos...**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding Static binding

Port allocation Elastic ⓘ

Number of ports 8

Network resource pool (default)

VLAN

VLAN type VLAN

VLAN ID 3374

Advanced

Customize default policies configuration

CANCEL

BACK

NEXT

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 que ha introducido el **VLAN ID** correcto.
6. Una vez que ambos grupos de puertos han sido creados, navegue al primer grupo de puertos y seleccione la acción para **Editar configuración**....

The screenshot shows the vSphere Client interface. The top navigation bar includes the vSphere Client logo and a search bar. The main content area is divided into a left-hand navigation pane and a right-hand details pane. The left pane shows a tree view of the environment, with the path **vcf-m01-cl01-vds01** expanded to show several port groups. The port group **vcf-m01-cl01-vds01-pg-iscsi-a** is selected, and a context menu is open over it, with the **Edit Settings...** option highlighted. The right-hand pane displays the **Distributed Port Group Details** for the selected port group. The details include:

Property	Value
Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-m01-cl01-vds01
Network protocol profile	--
Network resource pool	--
Hosts	4

7. En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda y haz clic en **uplink2** para moverlo hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a ×

General	Load balancing	Route based on originating virtual por ▾
Advanced	Network failure detection	Link status only ▾
VLAN	Notify switches	Yes ▾
Security	Failback	Yes ▾
Traffic shaping		
Teaming and failover		
Monitoring		
Miscellaneous		

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL OK

8. Repita este paso para el segundo grupo de puertos iSCSI. Sin embargo, esta vez mueva **uplink1** hacia abajo a **Uplinks sin usar**.

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

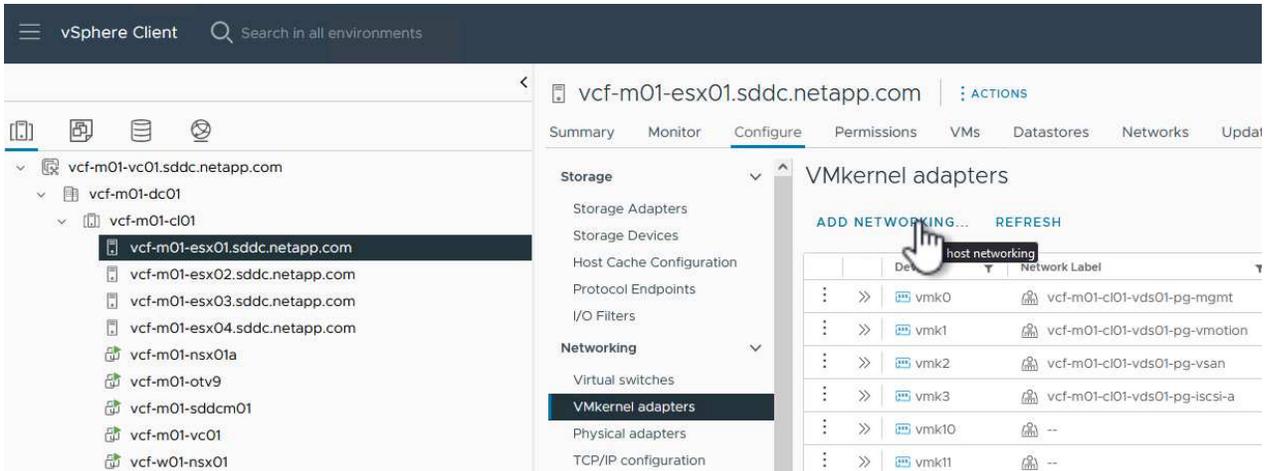
 uplink1



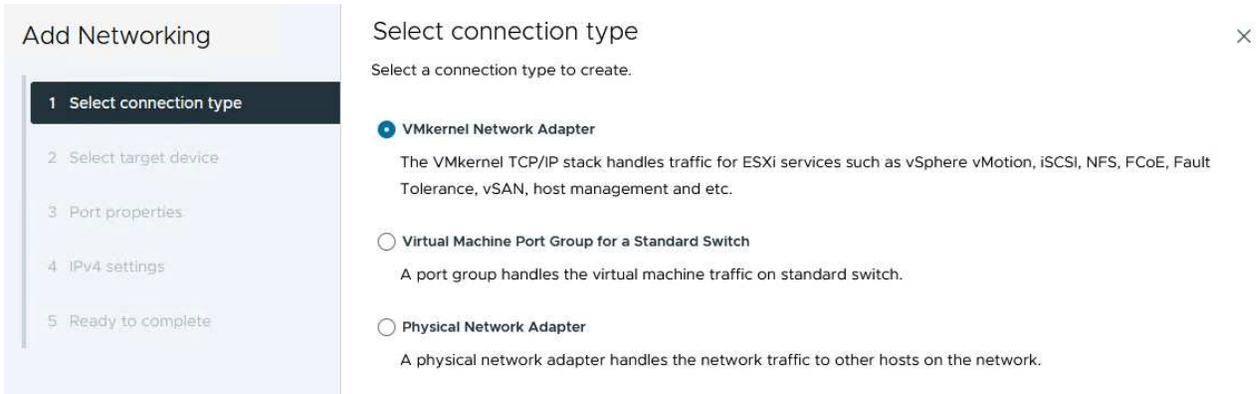
Crear adaptadores de VMkernel en cada host ESXi

Repita este proceso en cada host ESXi del dominio de gestión.

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de gestión. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** 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.

Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-ci01-vds01
<input checked="" type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-a	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-b	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-mgmt	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vmotion	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vsan	--	vcf-m01-ci01-vds01

Manage Columns 6 items

CANCEL

BACK

NEXT

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

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties**
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label vcf-m01-ci01-vds01-pg-iscsi-a (vcf-m01-ci01-vds01)

MTU Get MTU from switch 9000

TCP/IP stack Default

Available services

- Enabled services
- vMotion
 - Provisioning
 - Fault Tolerance logging
 - Management
 - vSphere Replication
 - vSphere Replication NFC
 - vSAN
 - vSAN Witness
 - vSphere Backup NFC
 - NVMe over TCP
 - NVMe over RDMA

5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

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

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

Distributed port group vcf-m01-cl01-vds01-pg-iscsi-a

Distributed switch vcf-m01-cl01-vds01
- ▼ Port properties

New port group vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.114 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

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

Pon en marcha y utiliza herramientas de ONTAP para configurar el almacenamiento

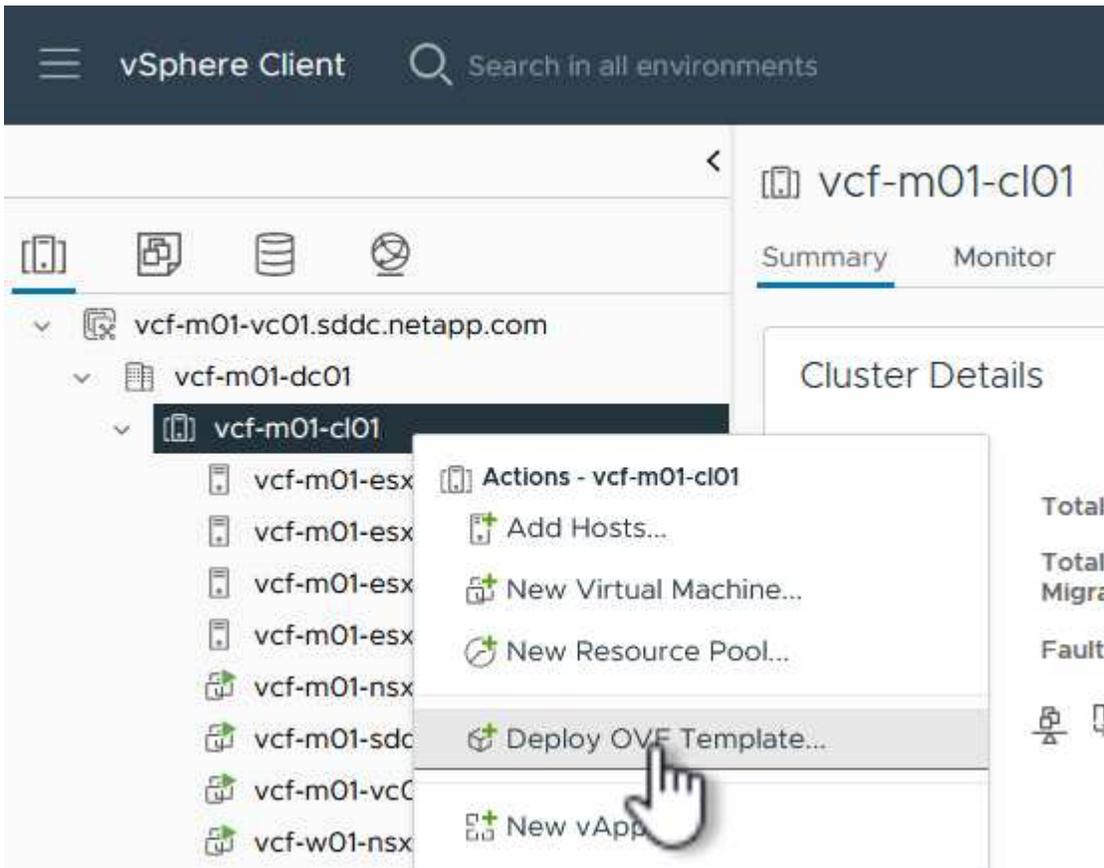
Los siguientes pasos se realizan en el clúster de dominio de gestión de VCF mediante el cliente vSphere e implican la puesta en marcha de OTV, la creación de un almacén de datos iSCSI de VMFS y la migración de equipos virtuales de gestión al nuevo almacén de datos.

Ponga en marcha herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware vSphere (OTV) se ponen en marcha como dispositivo de máquina virtual y proporcionan una interfaz de usuario integrada de vCenter para gestionar el almacenamiento de ONTAP.

Complete lo siguiente para poner en marcha herramientas de ONTAP para VMware vSphere:

1. Obtenga la imagen OVA de las herramientas de ONTAP de la "[Sitio de soporte de NetApp](#)" y descárguelo a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de gestión 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 de **Desplegar plantilla OVF** haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de herramientas ONTAP descargado en el paso anterior.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vmware-9.13-9554.ova

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

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

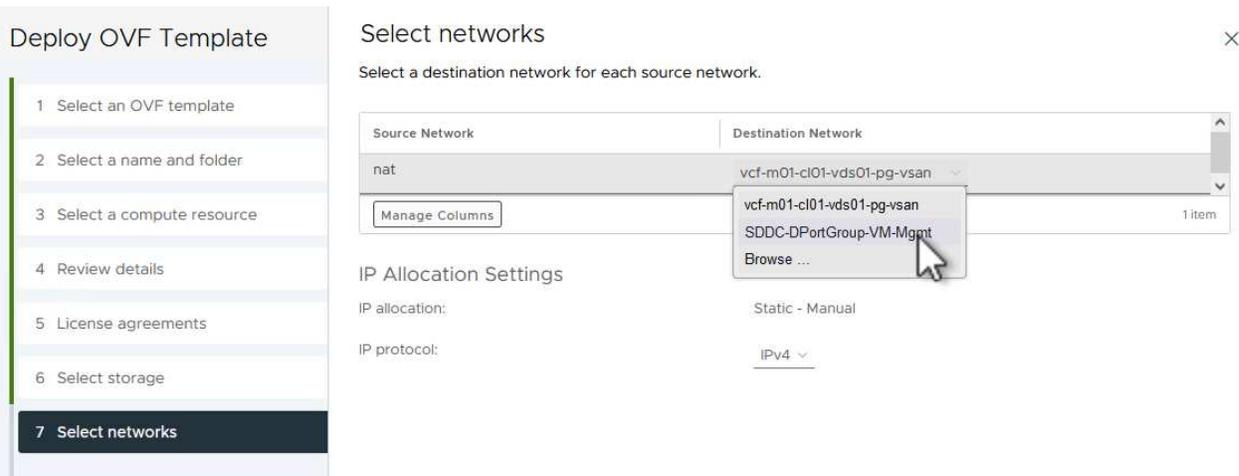
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns Items per page 10 5 items

7. En la página Seleccionar red, seleccione la red que se utiliza para el tráfico de gestión.



8. En la página Personalizar plantilla, rellene toda la información necesaria:

- 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 **Enable VMware Cloud Foundation (VCF)**. El modo VCF no es necesario para implementar almacenamiento complementario.
- El FQDN o la dirección IP del dispositivo de vCenter y proporciona credenciales para vCenter.
- Proporcione los campos de propiedades de red necesarios.

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.

! 2 properties have invalid values X

System Configuration	4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. <input type="text" value="172.21.166.1"/>
Maintenance User Password (*)	Password to assign to maint user account.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>

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

Configure vCenter or Enable VCF	5 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="172.21.166.140"/>
Port (*)	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
Username (*)	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
Password (*)	Specify the password of an existing vCenter to register to.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>

Network Properties	8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-m01-otv9"/>
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is

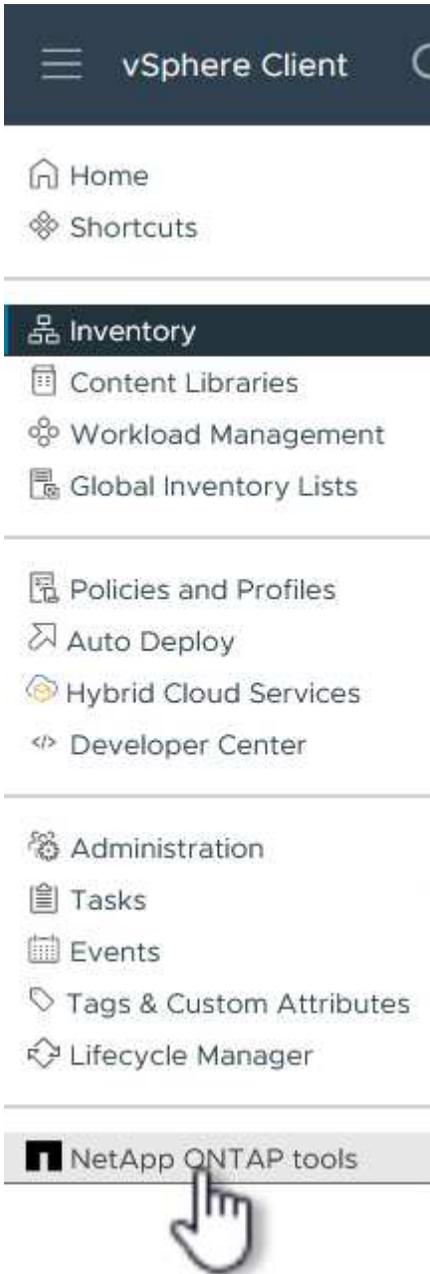
CANCEL BACK NEXT

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

Configure un almacén de datos iSCSI de VMFS en el dominio de gestión mediante OTV

Realice lo siguiente para utilizar OTV para configurar un almacén de datos iSCSI de VMFS como almacenamiento complementario en el dominio de gestión:

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



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

vSphere Client Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings

Reports

- Datastore Report
- Virtual Machine Report
- vVols Datastore Report
- vVols Virtual Machine Report
- Log Integrity Report

ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

Add Storage System

Add storage systems to ONTAP tools for VMware vSphere.



Provision Datastore

Create traditional or vVols datastores.



Next Steps

 [View Dashboard](#)

View and monitor the datastores in ONTAP tools for VMware vSphere.

 [Settings](#)

Configure administrative settings such as credentials, alarm thresholds.

[What's new?](#)
September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

Resources

- [ONTAP tools for VMware vSphere Documentation Resources](#)
- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)

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

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	

CANCEL

SAVE & ADD MORE

ADD



4. Haga clic en **Sí** para autorizar el certificado de 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

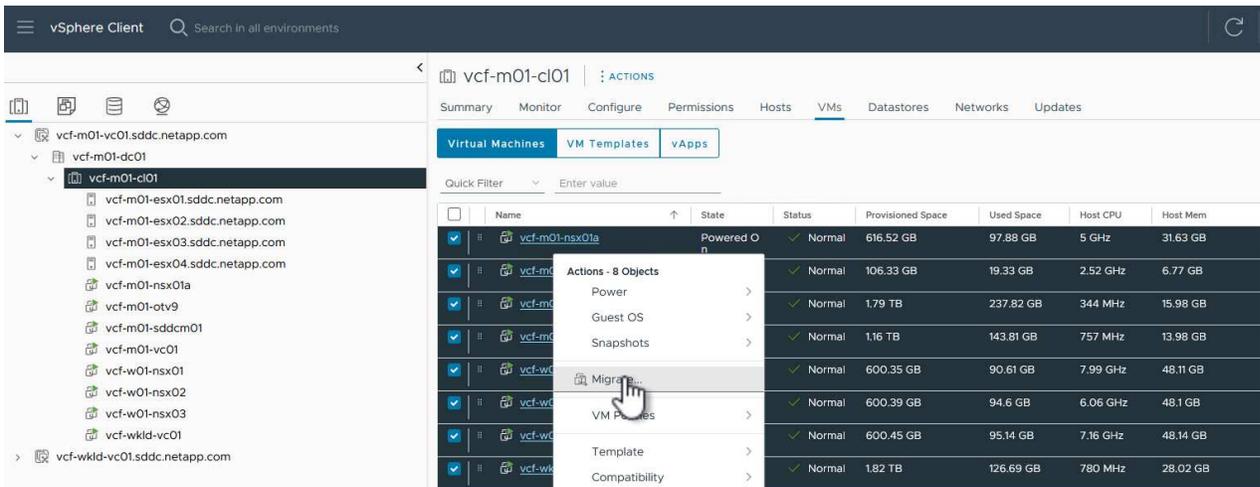
ADD

Migrar VM de gestión's a almacén de datos iSCSI

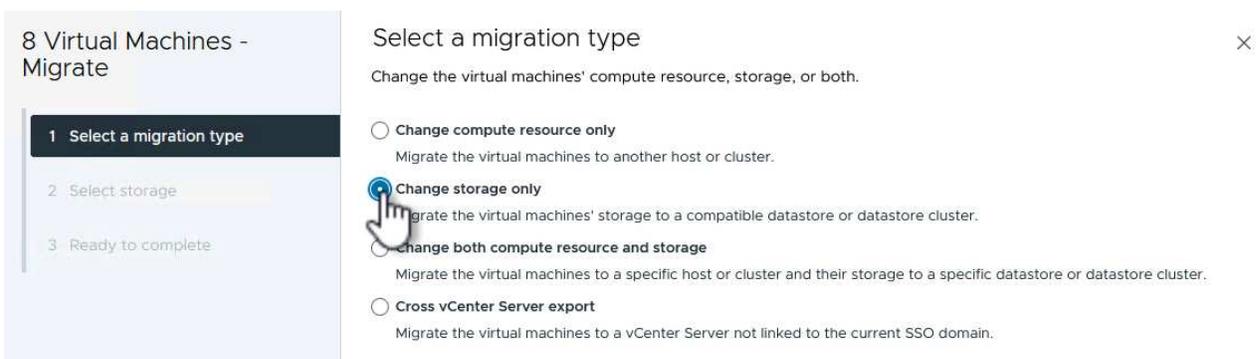
En los casos en los que se prefiera utilizar almacenamiento ONTAP para proteger vMotion del equipo virtual de gestión VCF se puede utilizar para migrar los equipos virtuales al almacén de datos iSCSI recién creado.

Complete los siguientes pasos para migrar los equipos virtuales de gestión de VCF al almacén de datos iSCSI.

1. Desde vSphere Client, navegue hasta el clúster de 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 **Migrate...**



3. En el asistente de **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.

8 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage**
- 3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Same format as source

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB
vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB

Manage Columns Items per page 10 2 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK **NEXT**

5. Revise las selecciones y haga clic en **Finish** para iniciar la migración.

6. El estado de reubicación se puede ver desde el panel **Tareas recientes**.

Task Name	Target	Status	Details
Relocate virtual machine	vcf-w01-nsx03	38%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-wkld-vc01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-otv9	36%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-nsx01a	49%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx02	47%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-sddcm01	39%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-vc01	44%	Migrating Virtual Machine active state

Información adicional

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["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 gestión de VCF](#)

Utilice las herramientas de ONTAP para configurar el almacenamiento complementario (vVols) para los dominios de carga de trabajo de VCF

En esta situación, mostraremos cómo implementar y utilizar las herramientas de ONTAP para VMware vSphere para configurar un **vVols datastore** para un dominio de carga de trabajo VCF.

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

Autor: Josh Powell

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

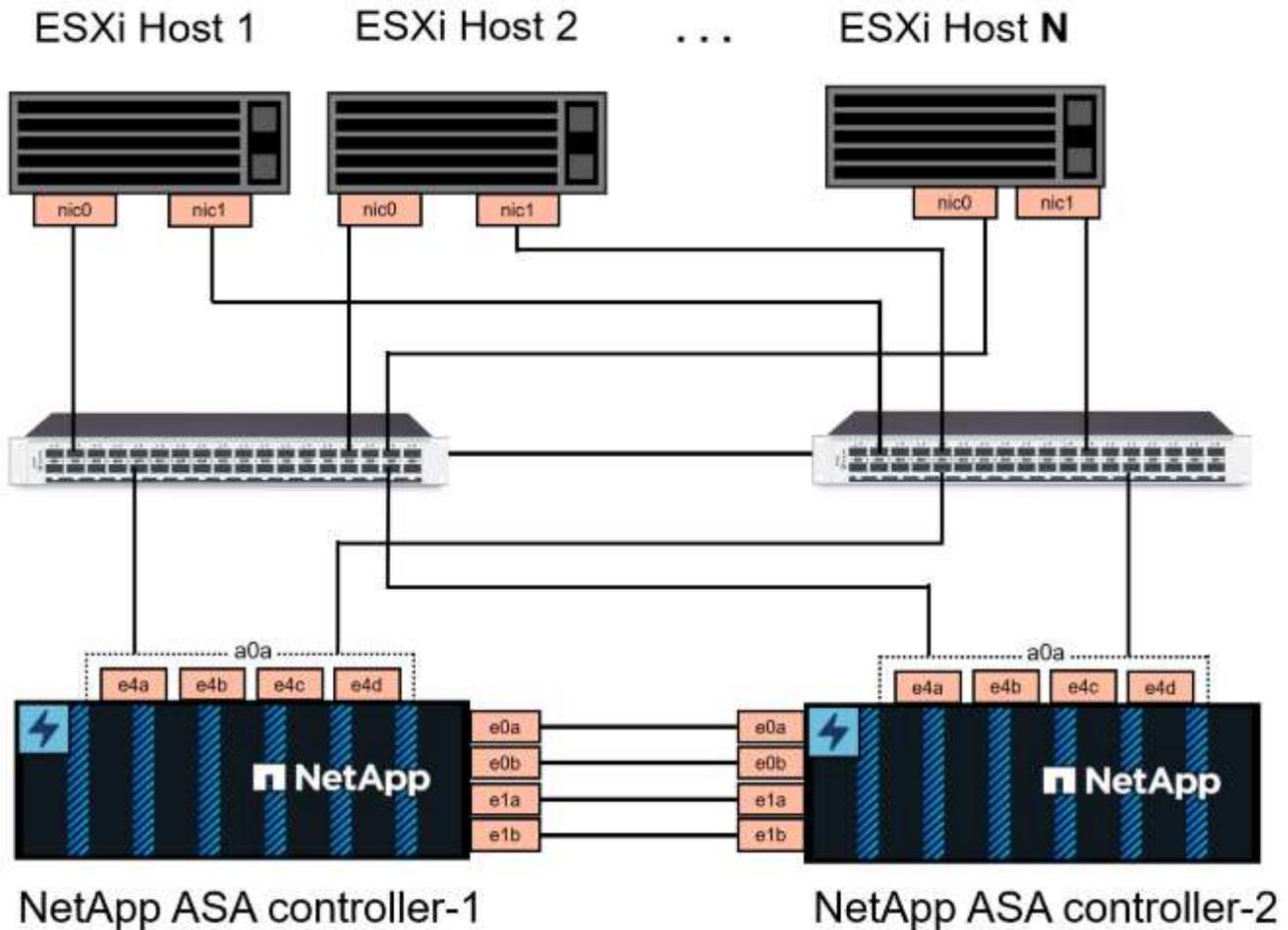
- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico de iSCSI.
- Cree grupos de puertos distribuidos para redes iSCSI en el dominio de carga de trabajo de VI.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de carga de trabajo VI.
-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

Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP ASA con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.
- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.
- Se ha desplegado anteriormente un dominio de carga de trabajo de VI.

NetApp recomienda diseños de red completamente redundantes para iSCSI. En el siguiente diagrama se muestra un ejemplo de una configuración redundante, que proporciona tolerancia a fallos para los sistemas de almacenamiento, los switches, los adaptadores de red y los sistemas host. Consulte NetApp ["Referencia para la configuración DE SAN"](#) para obtener más información.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes ethernet independientes para todas las SVM en configuraciones de iSCSI.

Esta documentación muestra el proceso de crear una SVM nueva y especificar la información de dirección IP para crear varias LIF para el tráfico de iSCSI. Para agregar LIF nuevos a una SVM existente, consulte "[Crear una LIF \(interfaz de red\)](#)".



En situaciones en las que se configuran varios adaptadores VMkernel en la misma red IP, se recomienda utilizar el enlace de puerto iSCSI de software en los hosts ESXi para garantizar el equilibrio de carga entre los adaptadores. Consulte el artículo de la base de conocimientos "[Consideraciones sobre 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 VMFS iSCSI con VMware, consulte "[Almacén de datos VMFS de vSphere: Entorno de administración del almacenamiento iSCSI con ONTAP](#)".

Pasos de despliegue

Para desplegar las herramientas de ONTAP y utilizarlo para crear un almacén de datos vVols en el dominio de administración de VCF, lleve a cabo los siguientes pasos:

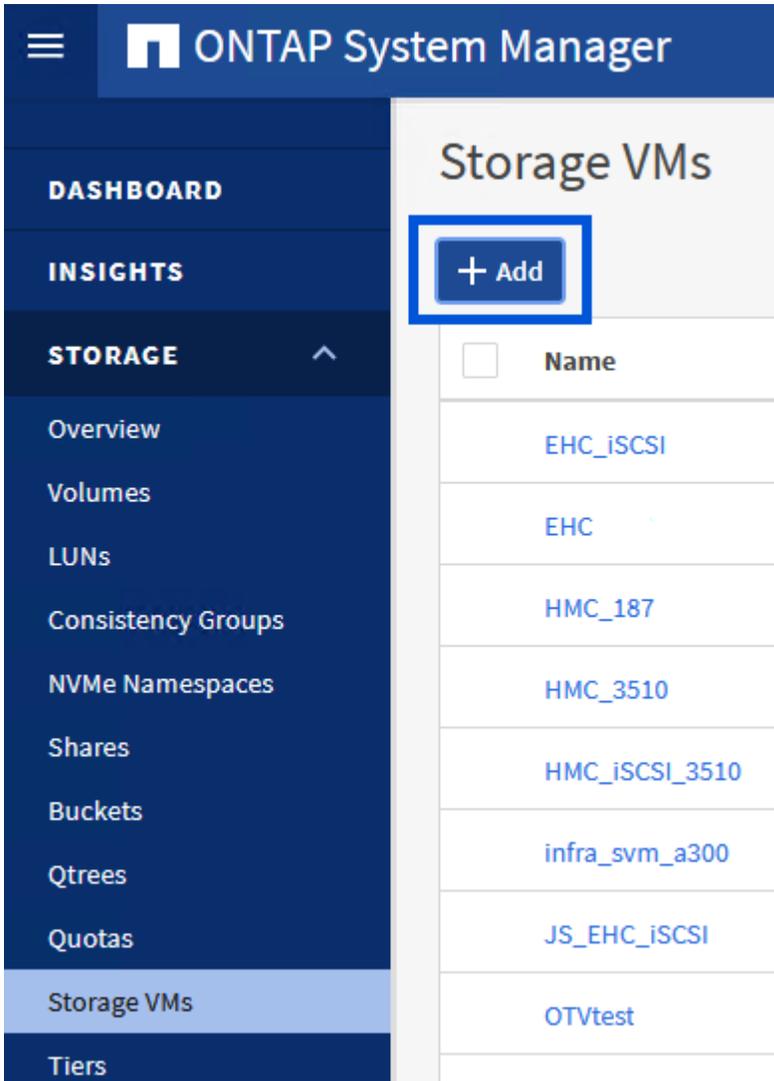
Crear SVM y LIF en el sistema de almacenamiento ONTAP

El siguiente paso se lleva a cabo en ONTAP System Manager.

Crear la máquina virtual de almacenamiento y las LIF

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

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



2. En el asistente de **Add Storage VM**, proporcione un **Name** para la SVM, seleccione **IP Space** y, a continuación, en **Access Protocol**, haga clic en la pestaña **iSCSI** y marque la casilla **Enable iSCSI**.

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes o utilizar una configuración independiente.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet independientes para todas las SVM en configuraciones de iSCSI.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

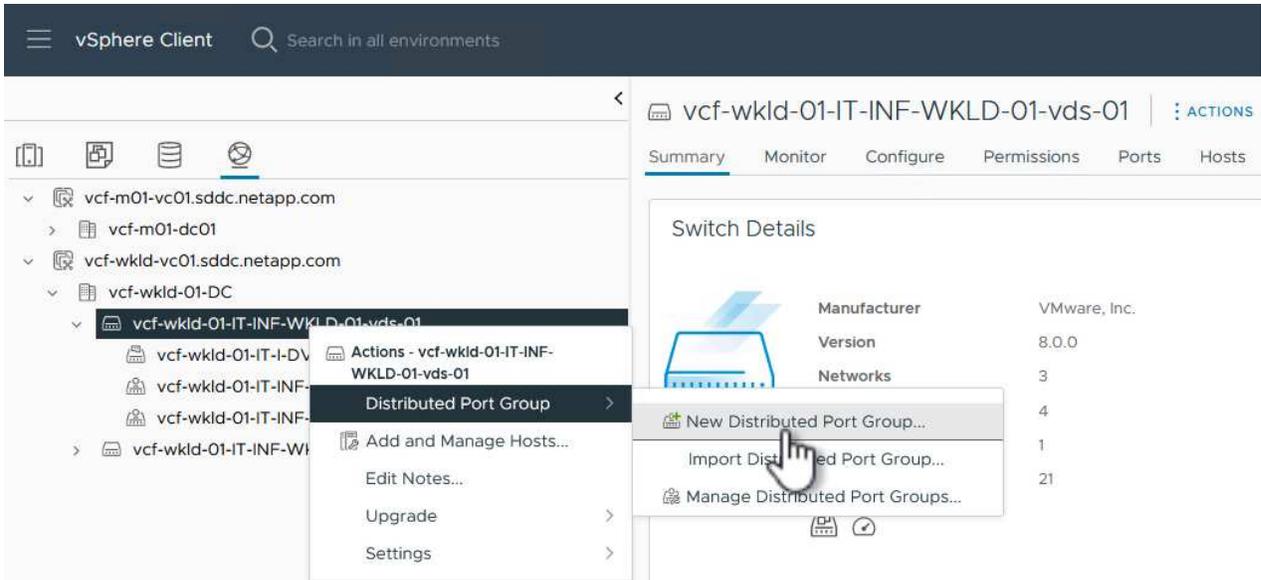
Configure las redes para iSCSI en hosts ESXi

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

Crear grupos de puertos distribuidos para el tráfico de iSCSI

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

1. En el cliente vSphere , desplácese hasta **Inventory > Networking** para el dominio de la carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos....**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

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 que ha introducido el **VLAN ID** correcto.
6. Una vez que ambos grupos de puertos han sido creados, navegue al primer grupo de puertos y seleccione la acción para **Editar configuración...**

The screenshot shows the vSphere Client interface. On the left, a tree view displays the hierarchy of environments, with the selected path being: vcf-wkld-01-IT-INF-WKLD-01-vds-01 > vcf-wkld-01-iscsi-a. A context menu is open over the selected item, showing options like 'Actions - vcf-wkld-01-iscsi-a', 'Edit Settings...', and 'Customize Configuration...'. On the right, the 'Distributed Port Group Details' panel is visible, showing the following configuration:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01
Network protocol profile	--

7. En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda y haz clic en **uplink2** para moverlo hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a

General | Load balancing | Route based on originating virtual por

Advanced | Network failure detection | Link status only

VLAN | Notify switches | Yes

Security | Failback | Yes

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL OK

8. Repita este paso para el segundo grupo de puertos iSCSI. Sin embargo, esta vez mueva **uplink1** hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General | Load balancing | Route based on originating virtual por

Advanced | Network failure detection | Link status only

VLAN | Notify switches | Yes

Security | Failback | Yes

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

Standby uplinks

uplink2

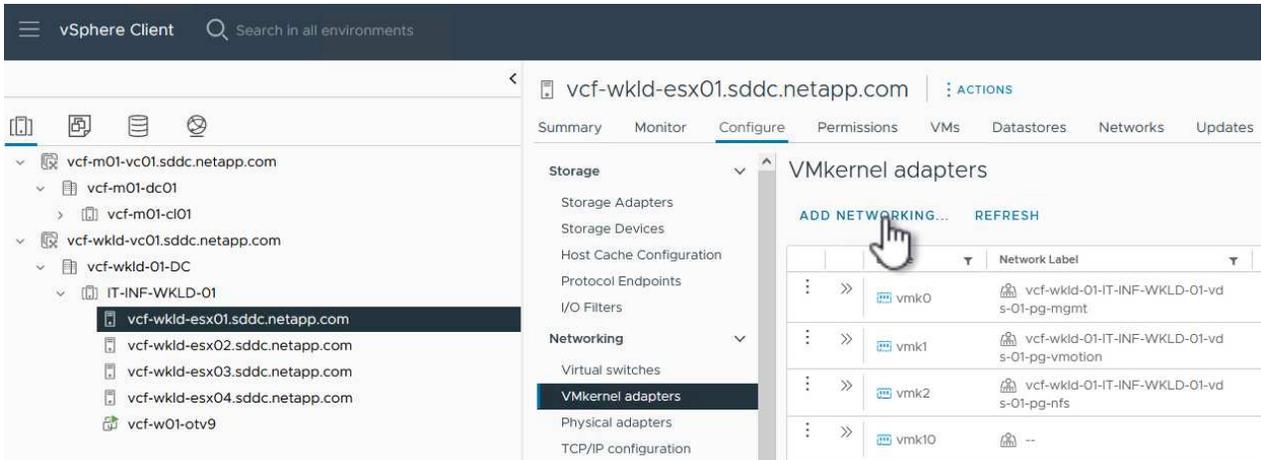
Unused uplinks

uplink1

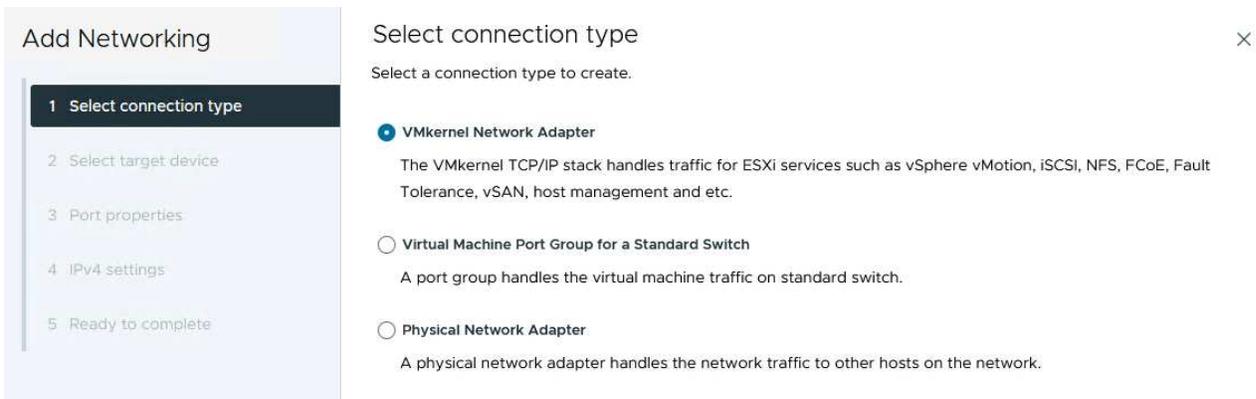
Crear adaptadores de VMkernel en cada host ESXi

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

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de la carga de trabajo. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** 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.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device

Select a target device for the new connection.

Select an existing network
 Select an existing standard switch
 New standard switch

Quick Filter

	Name	NSX Port Group ID	Distributed Switch
<input checked="" type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

5 items

CANCEL BACK NEXT

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

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

vMotion

vSphere Replication NFC

NVMe over RDMA

Provisioning

vSAN

Fault Tolerance logging

vSAN Witness

Management

vSphere Backup NFC

vSphere Replication

NVMe over TCP

5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

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

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

- ▼ **Select target device**

Distributed port group vcf-wkld-01-iscsi-a

Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
- ▼ **Port properties**

New port group vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ **IPv4 settings**

IPv4 address 172.21.118.127 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

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

Pon en marcha y utiliza herramientas de ONTAP para configurar el almacenamiento

Los siguientes pasos se realizan en el clúster de dominio de gestión de VCF mediante el cliente vSphere e implican la puesta en marcha de herramientas de ONTAP, la creación de un almacén de datos iSCSI vVols y la migración de equipos virtuales de gestión al nuevo almacén de datos.

Para dominios de carga de trabajo de VI, Herramientas de ONTAP se instala en el clúster de gestión de VCF, pero se registra en el vCenter asociado al dominio de carga de trabajo de VI.

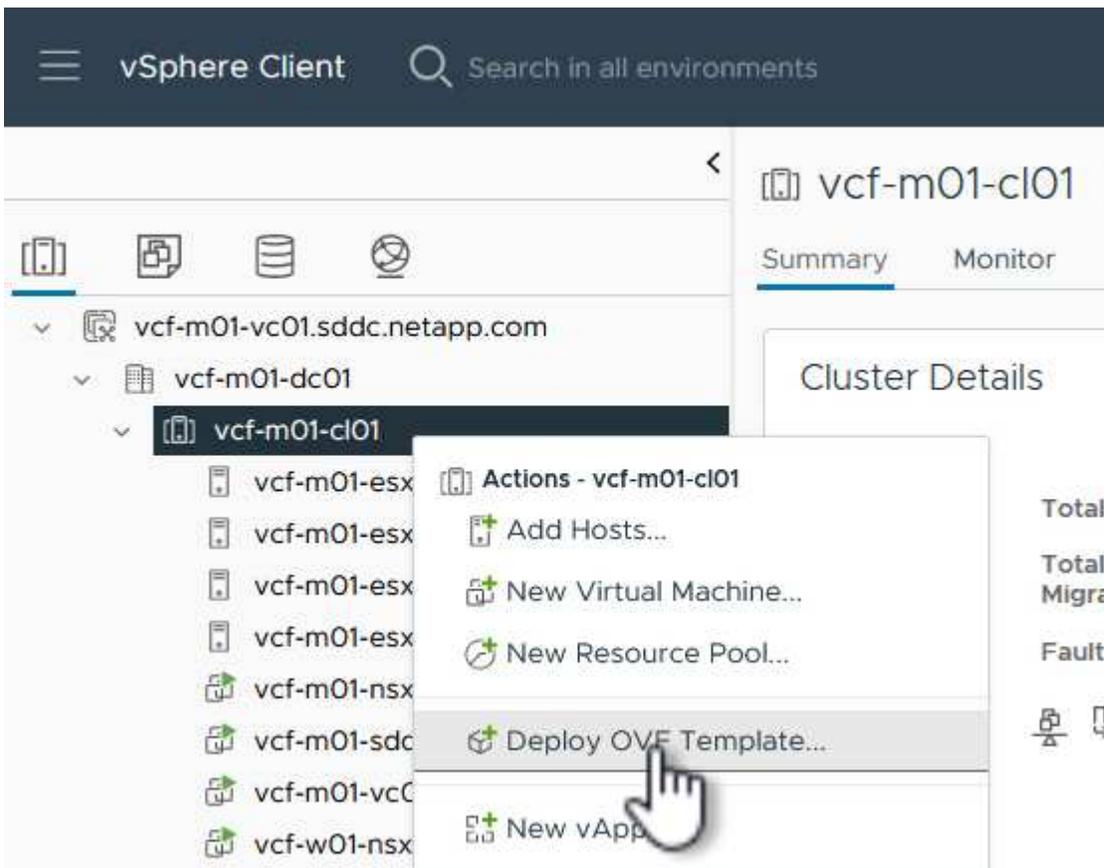
Para obtener información adicional sobre la puesta en marcha y el uso de las herramientas de ONTAP en un entorno múltiple de vCenter, consulte ["Requisitos para registrar herramientas de ONTAP en varios entornos de vCenter Server"](#).

Ponga en marcha herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware vSphere se ponen en marcha como dispositivo de máquina virtual y proporcionan una interfaz de usuario integrada de vCenter para gestionar el almacenamiento de ONTAP.

Complete lo siguiente para poner en marcha herramientas de ONTAP para VMware vSphere:

1. Obtenga la imagen OVA de las herramientas de ONTAP de la "[Sitio de soporte de NetApp](#)" y descárguelo a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de gestión 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 de **Desplegar plantilla OVF** haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de herramientas ONTAP descargado en el paso anterior.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

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

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

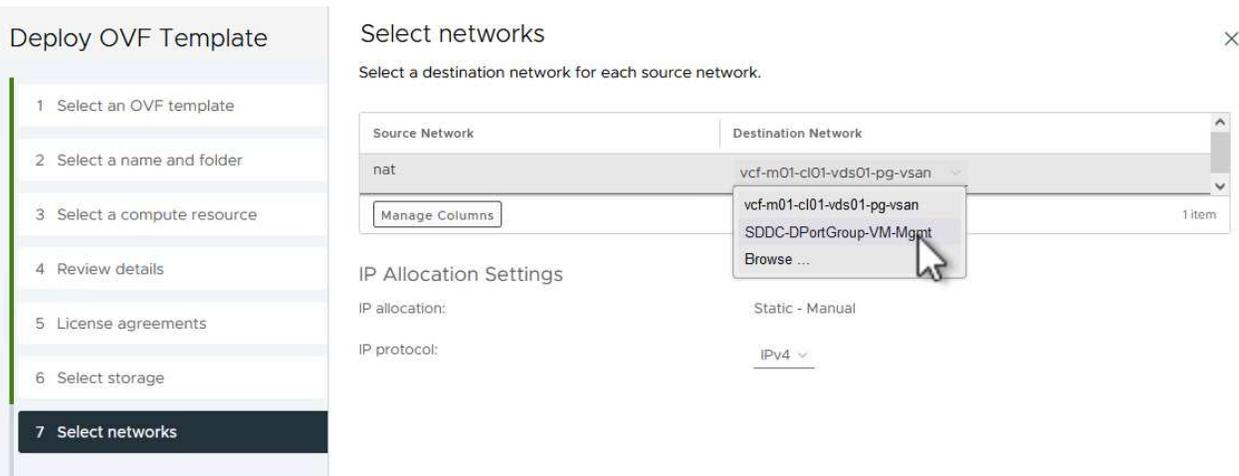
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsant01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns Items per page 10 5 items

7. En la página Seleccionar red, seleccione la red que se utiliza para el tráfico de gestión.



8. En la página Personalizar plantilla, rellene toda la información necesaria:

- Contraseña que se utilizará para el acceso administrativo a las herramientas de ONTAP.
- Dirección IP del servidor NTP.
- Contraseña de la cuenta de mantenimiento de ONTAP Tools.
- ONTAP Herramientas Derby contraseña de la base de datos.
- No marque la casilla para **Enable 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 necesarios.

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.

! 2 properties have invalid values X

System Configuration		4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.	
	Password 👁
	Confirm Password 👁
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1	
Maintenance User Password (*)	Password to assign to maint user account.	
	Password 👁
	Confirm Password 👁

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

! 2 properties have invalid values X

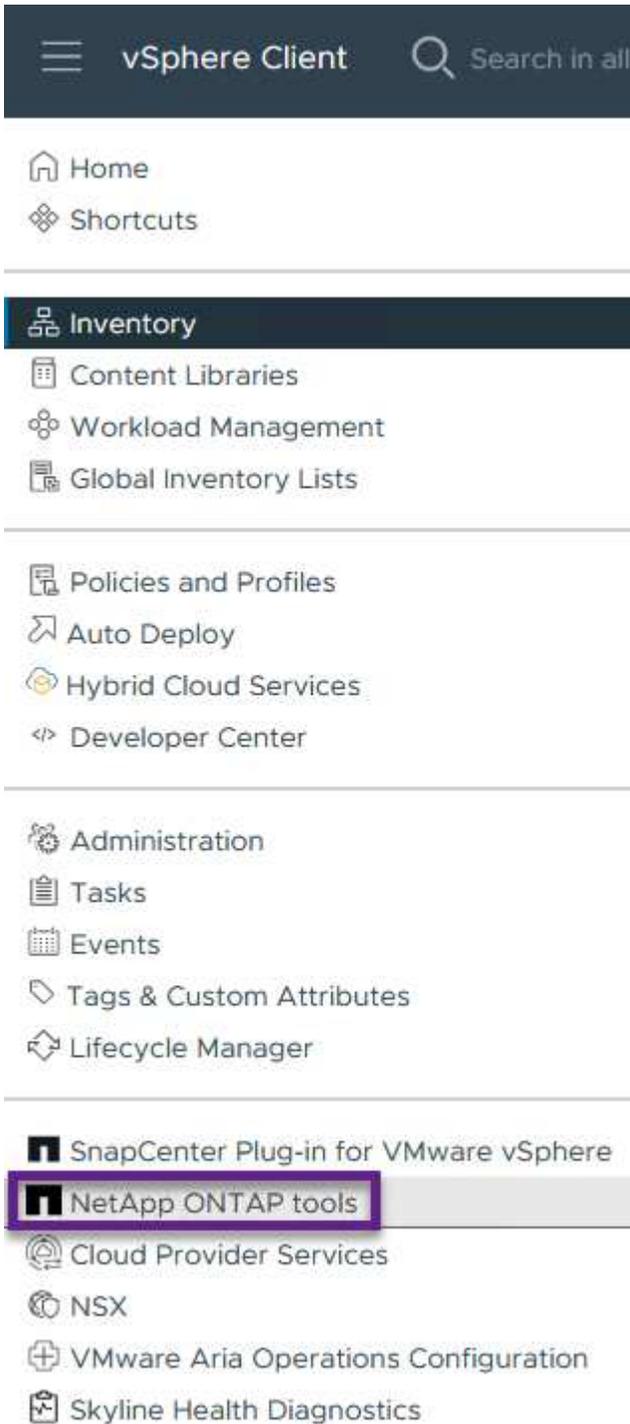
Configure vCenter or Enable vCenter		3 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>	
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com	
Port (*)	Specify the HTTPS port of an existing vCenter to register to. 443	
Username (*)	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
Password (*)	Specify the password of an existing vCenter to register to.	
	Password 👁
	Confirm Password 👁
Network Properties		8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9	
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

CANCEL BACK NEXT

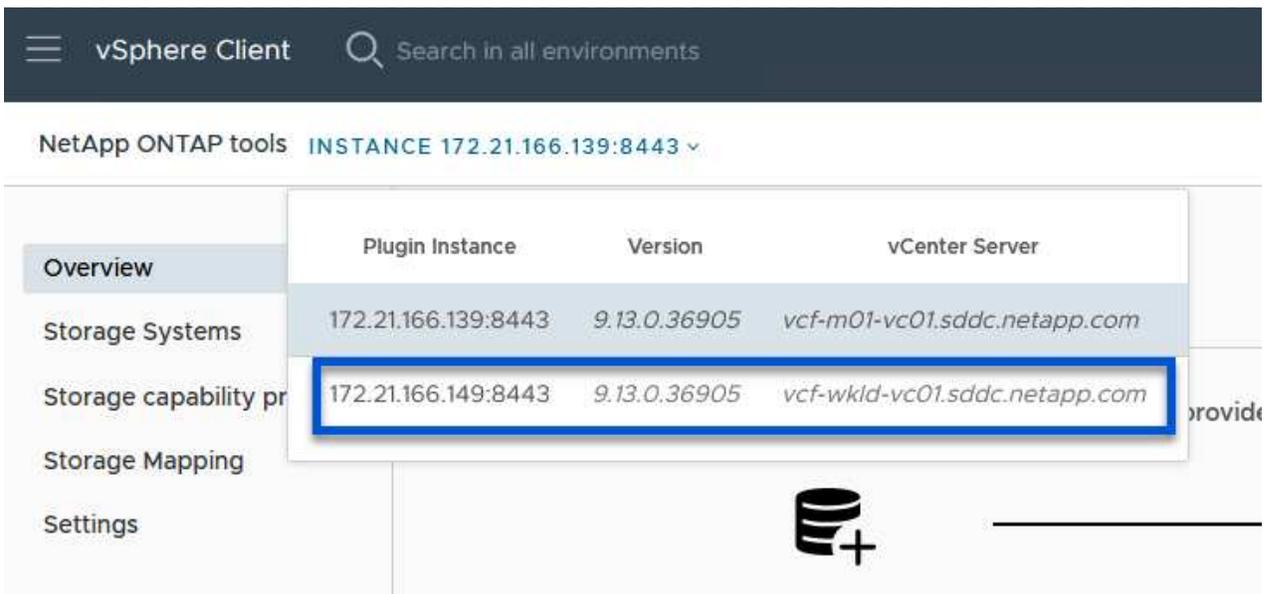
9. Revise toda la información en la página Listo para completar y haga clic en Finalizar para comenzar a implementar el dispositivo Herramientas de ONTAP.

Agregar un sistema de almacenamiento a las herramientas de ONTAP.

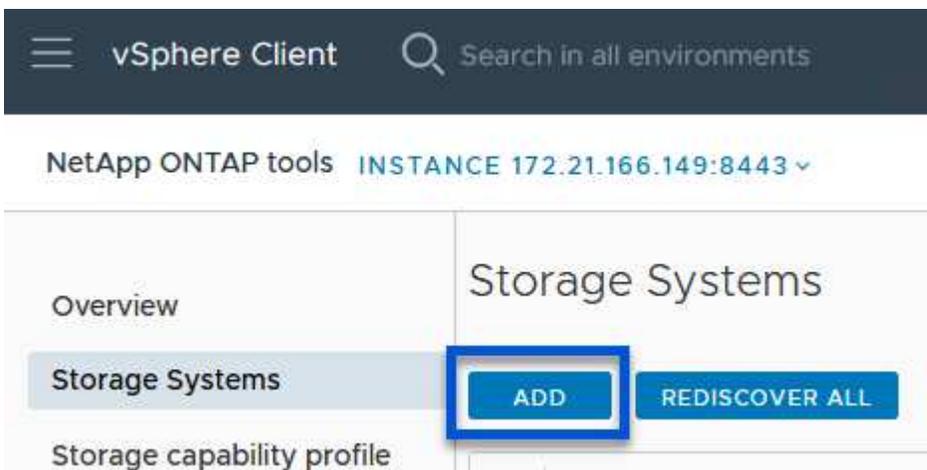
1. Acceda a herramientas de NetApp ONTAP seleccionándolo en el menú principal del vSphere Client.



2. En el menú desplegable **INSTANCIA** de la interfaz de la herramienta ONTAP, seleccione la instancia de herramientas ONTAP asociada al dominio de carga de trabajo que se va a gestionar.



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



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



VVol requiere credenciales del clúster de ONTAP en lugar de credenciales de 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	<input type="text" value="vcf-m01-vc01.sddc.netapp.com"/> ▾
Name or IP address:	<input type="text" value="172.16.9.25"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="••••••••"/>
Port:	<input type="text" value="443"/>

Advanced options 

ONTAP Cluster Certificate: Automatically fetch Manually upload

CANCEL

SAVE & ADD MORE

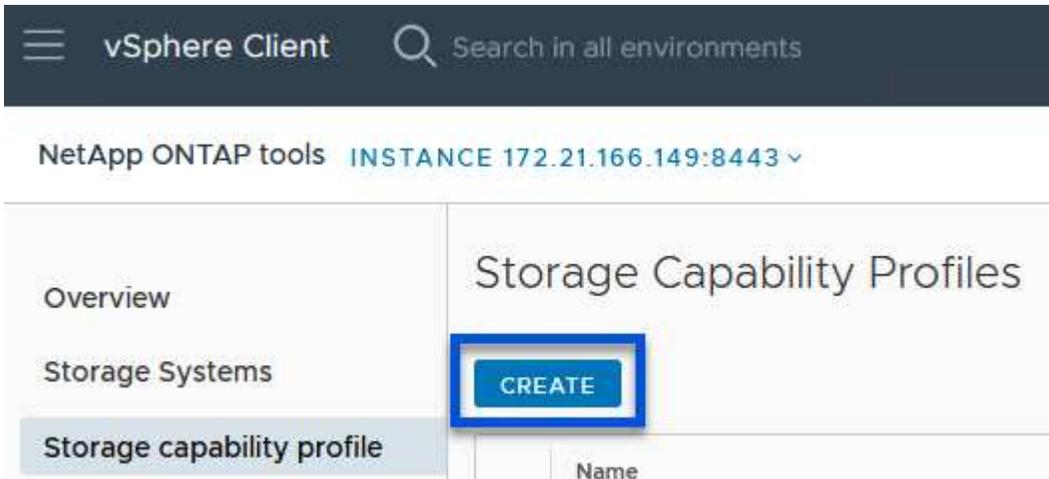
ADD

Crear un perfil de capacidad de almacenamiento en las herramientas de ONTAP

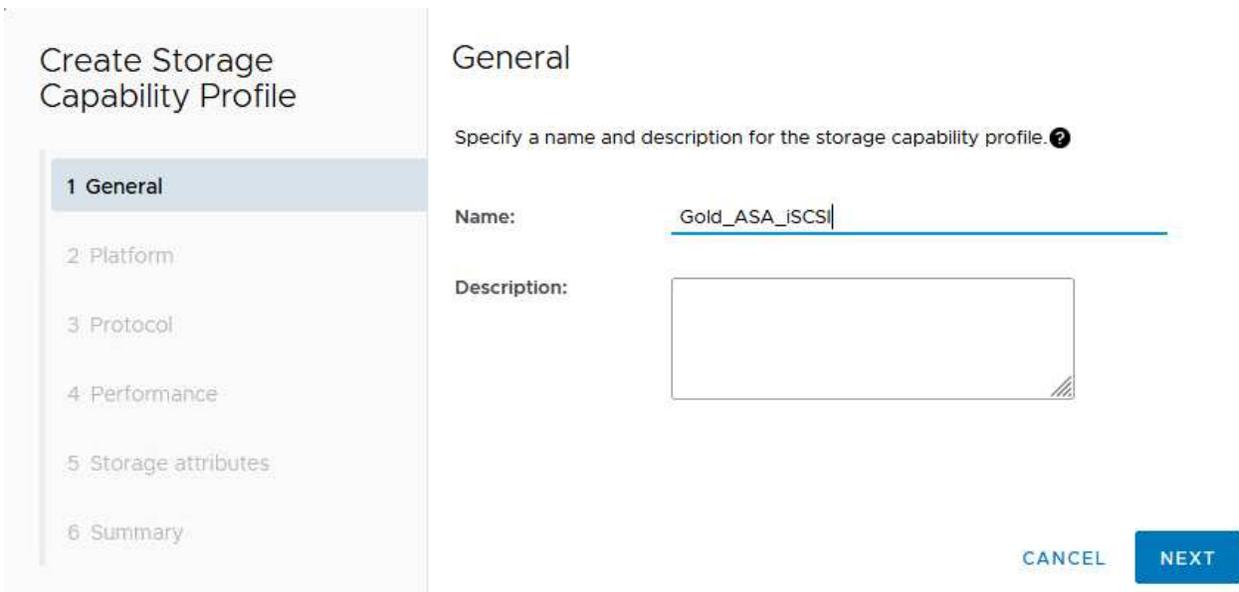
Los perfiles de funcionalidad de almacenamiento describen las funciones de una cabina de almacenamiento o un sistema de almacenamiento. Incluyen definiciones de calidad de servicio y se utilizan para seleccionar sistemas de almacenamiento que cumplan con los parámetros definidos en el perfil. Se puede utilizar uno de los perfiles proporcionados o se pueden crear otros nuevos.

Para crear un perfil de funcionalidad del almacenamiento en las herramientas de ONTAP, 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 de **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 debe ser una cabina SAN All-Flash establecida en **asimétrica** en false.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Platform

Platform: Performance

Asymmetric:



CANCEL

BACK

NEXT

4. A continuación, seleccione la opción de protocolo o * cualquiera * para permitir todos los protocolos posibles. Haga clic en **Siguiente** para continuar.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Protocol

Protocol:

Any

Any

FCP

iSCSI

NVMe/FC

CANCEL

BACK

NEXT

5. La página **PERFORMANCE** permite establecer la calidad del servicio en forma de IOPS mínima y máxima permitida.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Storage attributes

Deduplication:

Yes



Compression:

Yes



Space reserve:

Thin



Encryption:

No



Tiering policy (FabricPool):

None



CANCEL

BACK

NEXT

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

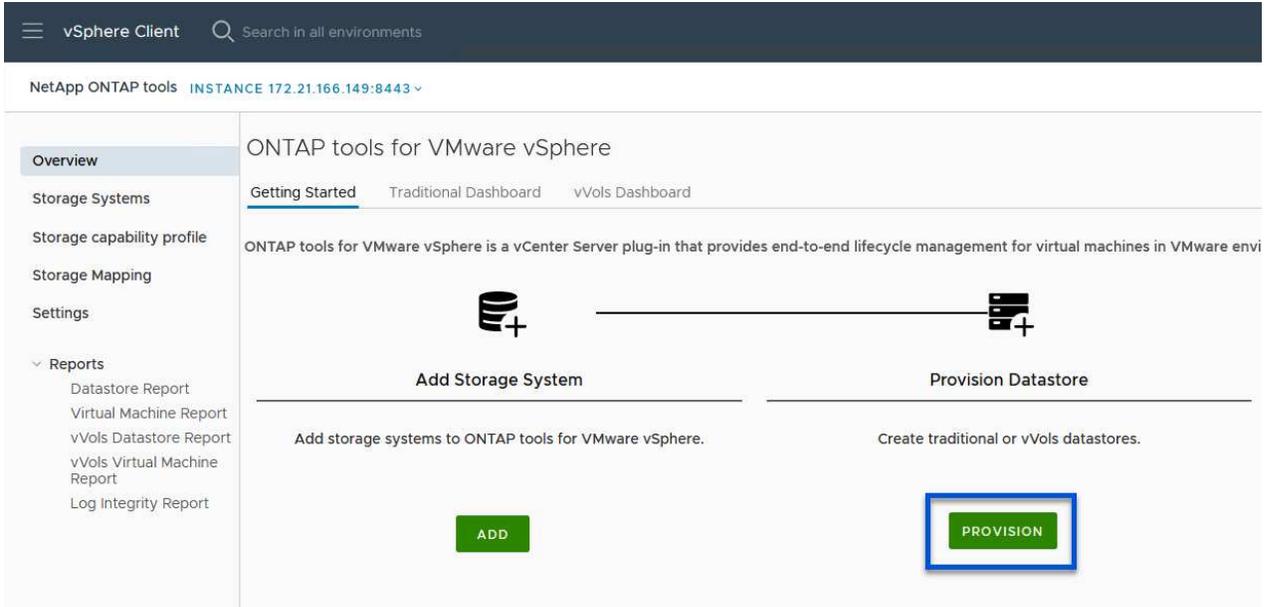
FINISH



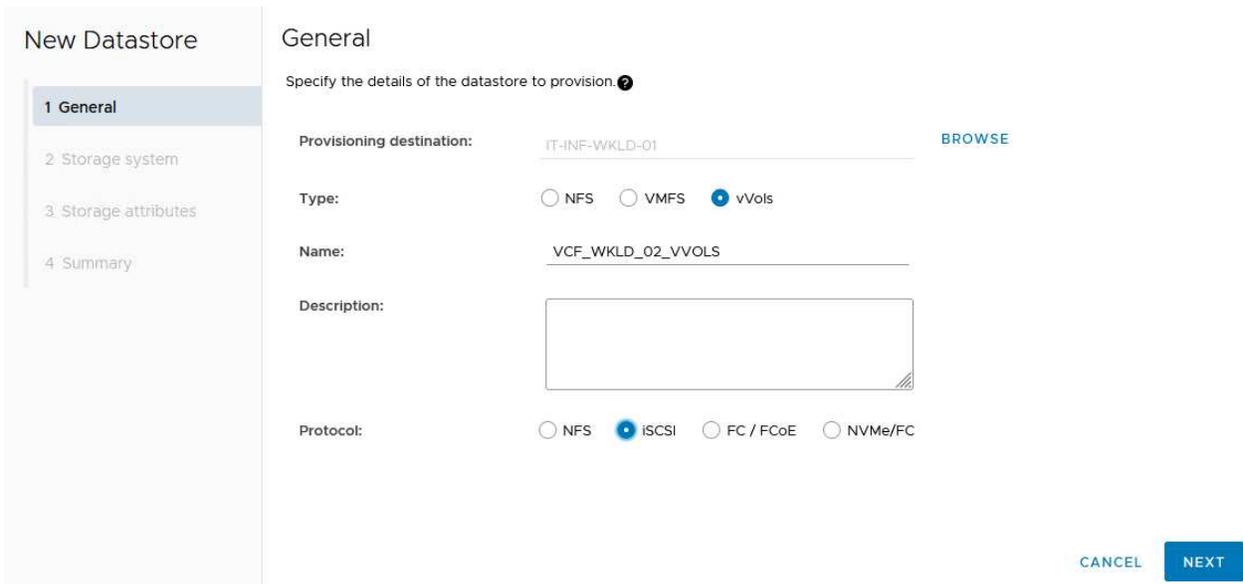
Cree un almacén de datos vVols en Herramientas de ONTAP

Para crear un almacén de datos vVols en Herramientas de ONTAP, lleve a cabo los siguientes pasos:

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



2. En la página **General** del asistente New Datasstore, seleccione el centro de datos de vSphere o el destino del clúster. Seleccione **vVols** como tipo de almacén de datos, rellene 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 el perfil de capacidad de almacenamiento, el sistema de almacenamiento y SVM. Haga clic en **Siguiente** para continuar.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

- AFF_Encrypted_Min50_ASA_A
- FAS_Default
- FAS_Max20
- Custom profiles
- ASA_Gold_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_iSCSI

CANCEL BACK NEXT

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

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCaggr02 - (27053.3 GE	Thin

ADD
CANCEL BACK NEXT

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

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

Datastore type: vVols
Protocol: iSCSI
Storage capability profile: ASA_Gold_iSCSI

Storage system details

Storage system: ntaphcl-a300e9u25
SVM: VCF_iSCSI

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
vcf_wkld_02_vvols	3000 GB	EHCAGgr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

CANCEL
BACK
FINISH

Información adicional

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

Configurar el almacenamiento complementario NVMe/TCP para dominios de carga de trabajo de VCF

En esta situación, mostraremos cómo configurar el almacenamiento complementario NVMe/TCP para un dominio de carga de trabajo de VCF.

Autor: Josh Powell

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 de VI.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de carga de trabajo VI.
- Añada adaptadores NVMe/TCP en los hosts ESXi.
- Implemente un almacén de datos NVMe/TCP.

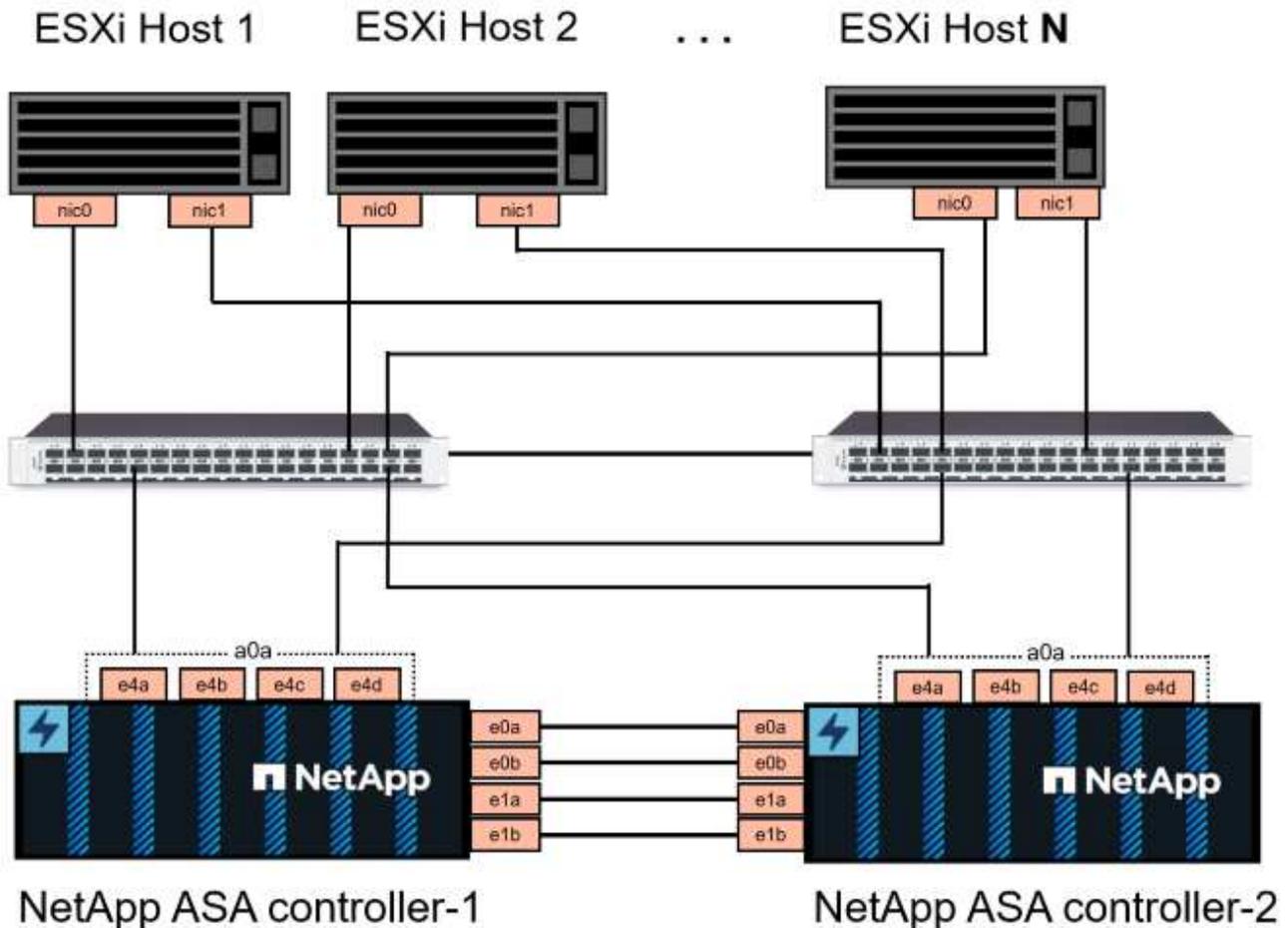
Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP ASA con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.
- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.

- Se ha desplegado anteriormente un dominio de carga de trabajo de VI.

NetApp recomienda diseños de red totalmente redundantes para NVMe/TCP. En el siguiente diagrama se muestra un ejemplo de una configuración redundante, que proporciona tolerancia a fallos para los sistemas de almacenamiento, los switches, los adaptadores de red y los sistemas host. Consulte NetApp ["Referencia para la configuración DE SAN"](#) para obtener más información.



Para la multivía y la conmutación al nodo de respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes ethernet independientes para todas las SVM en las configuraciones de NVMe/TCP.

Esta documentación muestra el proceso de crear una SVM nueva y especificar la información de dirección IP para crear varias LIF para el tráfico NVMe/TCP. Para agregar LIF nuevos a una SVM existente, consulte ["Crear una LIF \(interfaz de red\)"](#).

Si quiere más información sobre las consideraciones de diseño de NVMe para sistemas de almacenamiento ONTAP, consulte ["Configuración, compatibilidad y limitaciones de NVMe"](#).

Pasos de despliegue

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

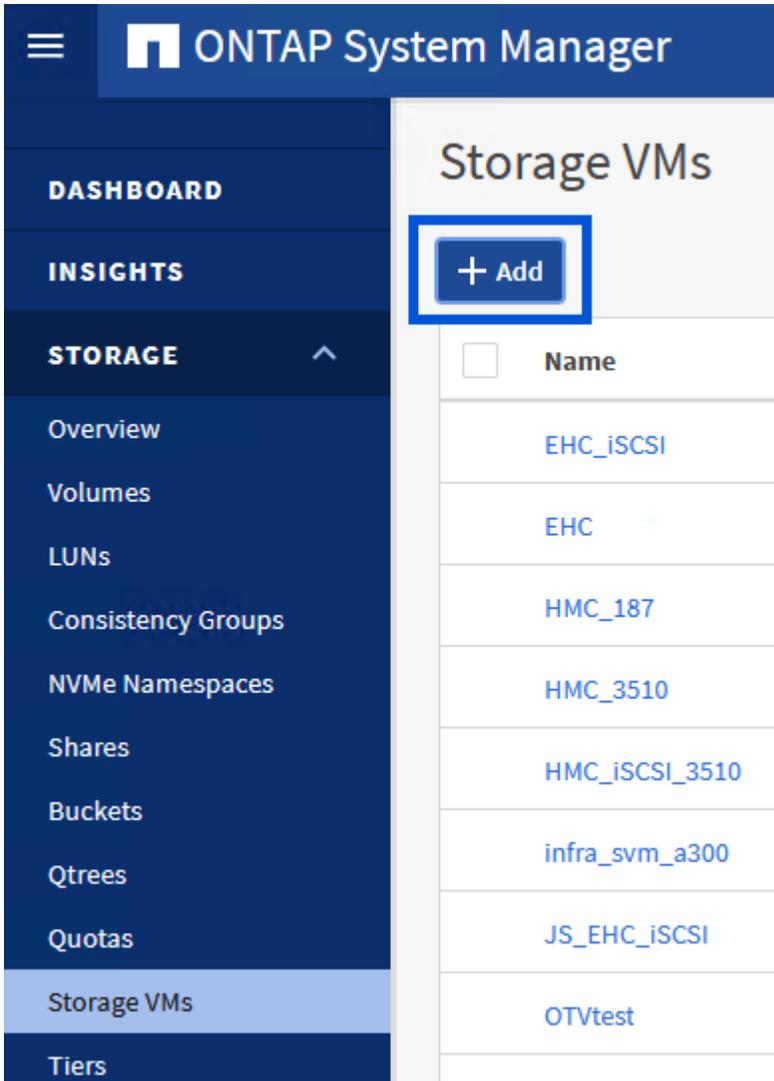
Crear SVM, LIF y espacio de nombres de NVMe en el sistema de almacenamiento ONTAP

El siguiente paso se lleva a cabo en ONTAP System Manager.

Crear la máquina virtual de almacenamiento y las LIF

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

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



2. En el asistente de **Add Storage VM**, proporcione un **Name** para la SVM, seleccione **IP Space** y, a continuación, en **Access Protocol**, haga clic en la pestaña **NVMe** y marque la casilla **Enable NVMe/TCP**.

Add Storage VM



STORAGE VM NAME

VCF_NVMe

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable NVMe/FC

Enable NVMe/TCP

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de las LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes, o utilizar una configuración independiente.



Para la multivía y la conmutación al nodo de respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet independientes para todas las SVM en las configuraciones de NVMe/TCP.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.189

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT 

NFS_iSCSI 

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.189

PORT

a0a-3375 

ntaphci-a300-02

IP ADDRESS

172.21.118.190

PORT

a0a-3374 

IP ADDRESS

172.21.119.190

PORT

a0a-3375 

Storage VM Administration

Manage administrator account

Save

Cancel

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

Cree el espacio de nombres de NVMe

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

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

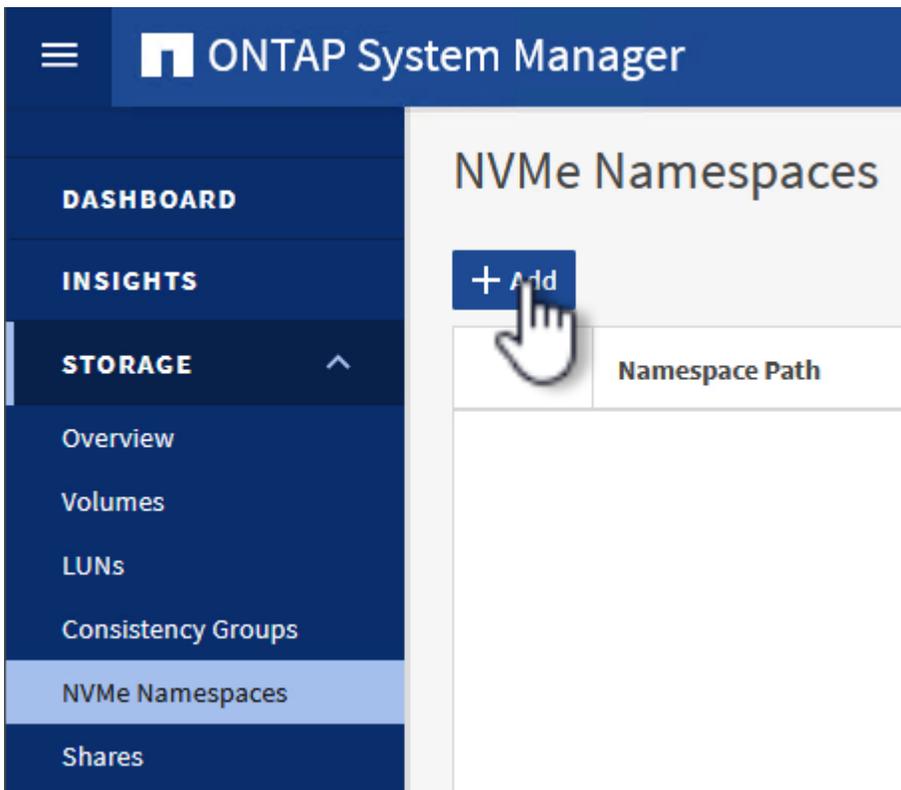
1. Abra una sesión SSH con un host ESXi del clúster para obtener el NQN. Utilice el siguiente comando de la CLI:

```
esxcli nvme info get
```

Debería aparecer una salida similar a la siguiente:

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

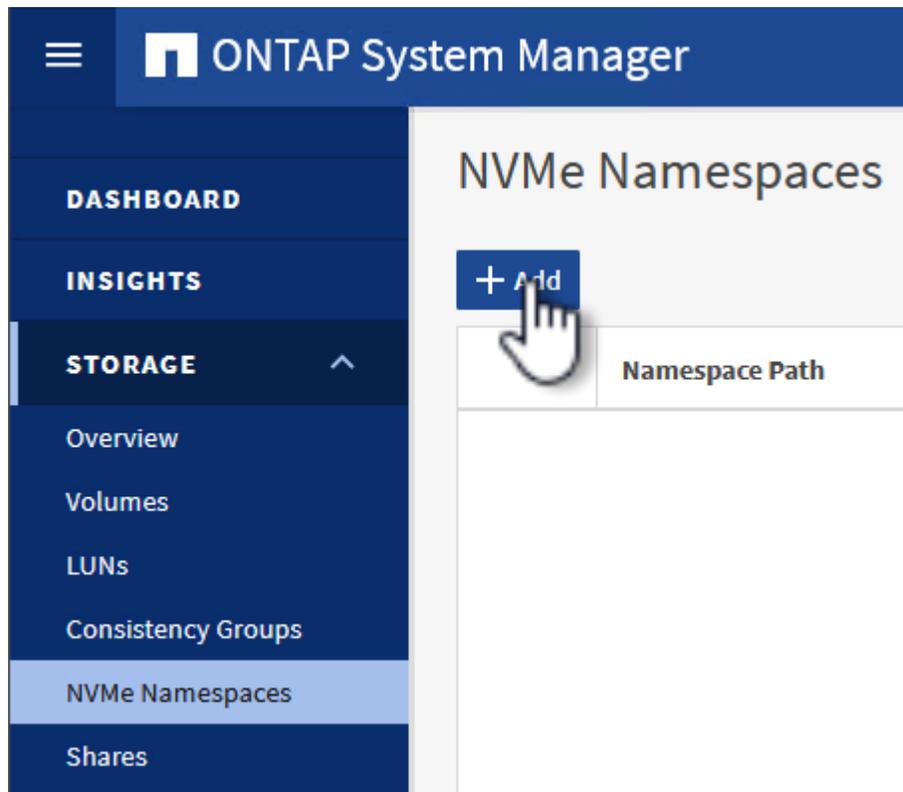
2. Registre el NQN de cada host ESXi del clúster
3. Desde el Administrador del sistema de ONTAP, navegue hasta **Espacios de nombres de NVMe** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.



4. En la página **Add NVMe Namespace**, rellene un prefijo de nombre, el número de espacios de

nombres que se van 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 previamente recopilados 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 **Save** para crear el espacio de nombres NVMe.



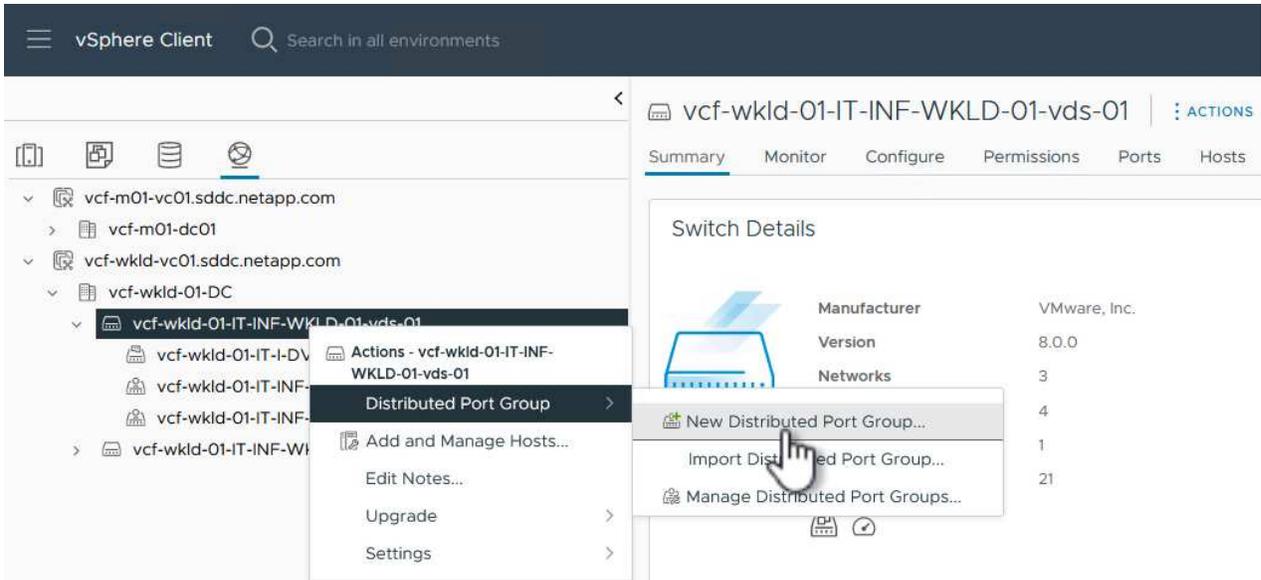
Configure los adaptadores de red y de software NVMe en hosts ESXi

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

Cree grupos de puertos distribuidos para el tráfico de NVMe/TCP

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

1. En el cliente vSphere , desplácese hasta **Inventory > Networking** para el dominio de la carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos...**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

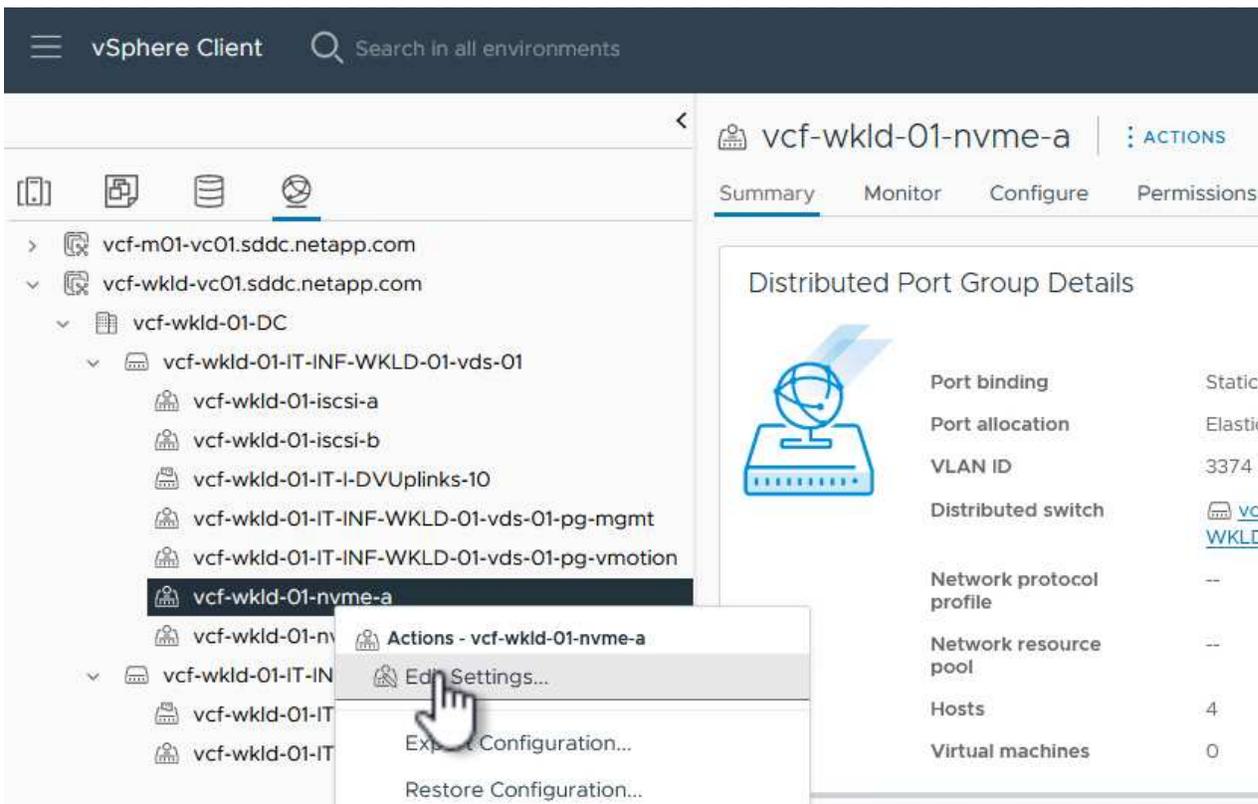
Port binding	Static binding
Port allocation	Elastic ?
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

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 que ha introducido el **VLAN ID** correcto.
6. Una vez que ambos grupos de puertos han sido creados, navegue al primer grupo de puertos y seleccione la acción para **Editar configuración....**



7. En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda y haz clic en **uplink2** para moverlo hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing Route based on originating virtual port

Network failure detection Link status only

Notify switches Yes

Failback Yes

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

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

uplink1 hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and fallover

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

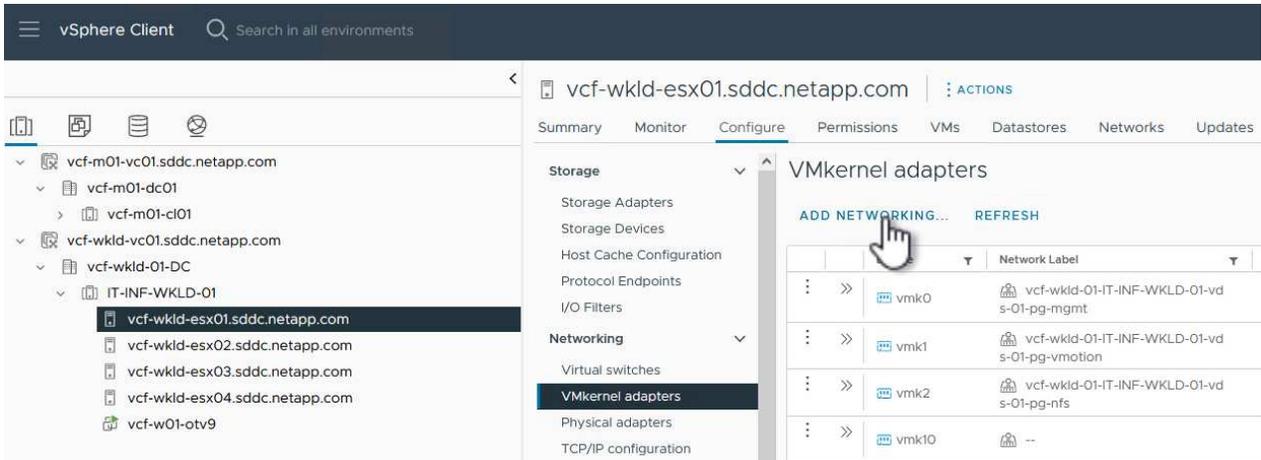
Unused uplinks

uplink1

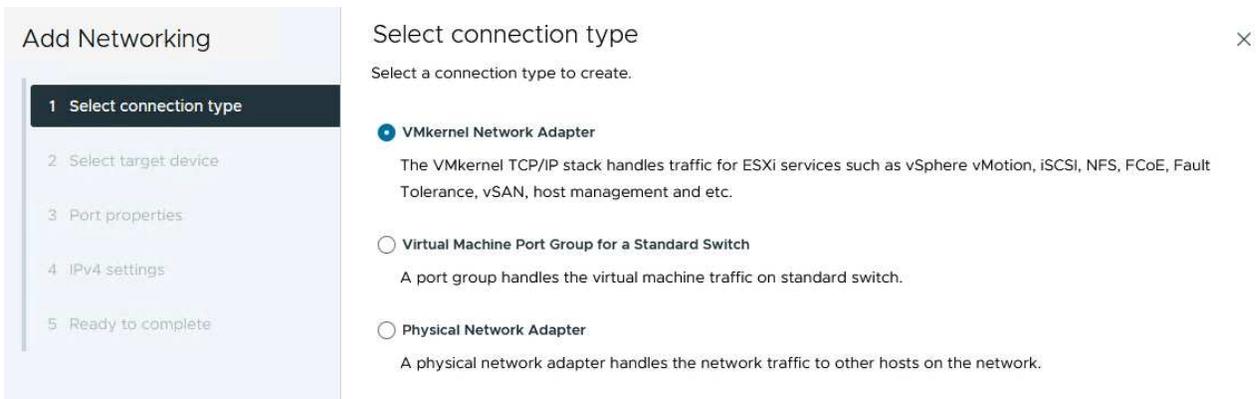
Crear adaptadores de VMkernel en cada host ESXi

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

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de la carga de trabajo. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** 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.

Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 7 Items

CANCEL

BACK

NEXT

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

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

<input checked="" type="checkbox"/> vMotion	<input type="checkbox"/> vSphere Replication NFC	<input type="checkbox"/> NVMe over RDMA
<input type="checkbox"/> Provisioning	<input type="checkbox"/> vSAN	
<input type="checkbox"/> Fault Tolerance logging	<input type="checkbox"/> vSAN Witness	
<input type="checkbox"/> Management	<input type="checkbox"/> vSphere Backup NFC	
<input type="checkbox"/> vSphere Replication	<input checked="" type="checkbox"/> NVMe over TCP	

CANCEL
BACK
NEXT

5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically

Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

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

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ Port properties

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

▼ IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

CANCEL

BACK

FINISH

Packages

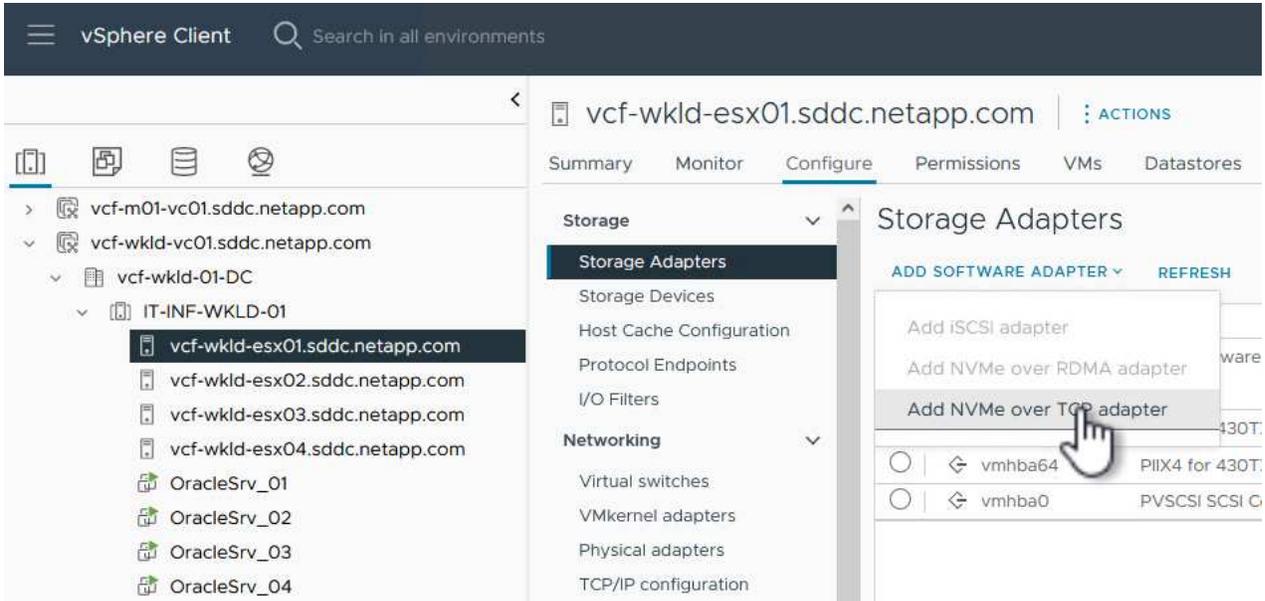
7. Repita este proceso para crear un adaptador de VMkernel para la segunda red iSCSI.

Añada el adaptador NVMe over TCP

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

Para instalar los adaptadores NVMe over TCP y detectar las controladoras NVMe, complete los pasos siguientes:

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



2. En la ventana **Add Software NVMe over TCP adapter**, accede al menú desplegable **Physical Network Adapter** y selecciona el adaptador de red físico correcto en el que habilitar el adaptador NVMe.

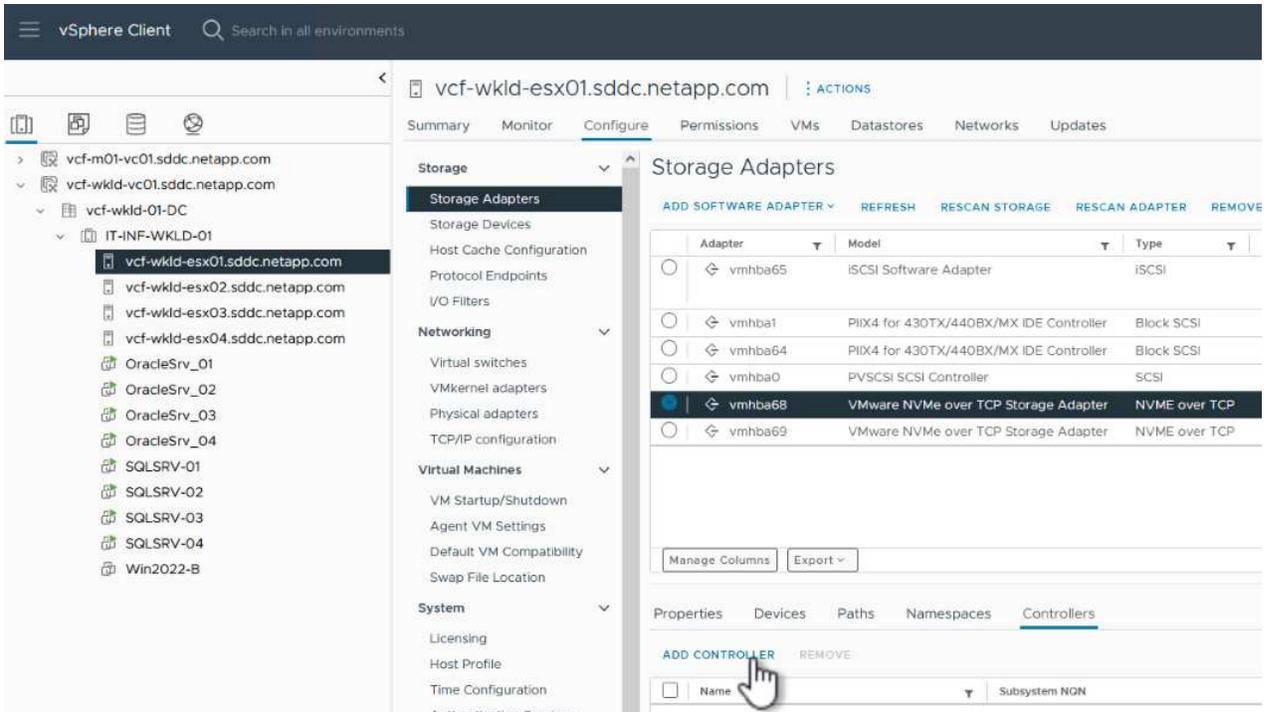
Add Software NVMe over TCP adapter | vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter



3. Repita este proceso para la segunda red asignada al tráfico NVMe over TCP, asignando el adaptador físico correcto.
4. Seleccione uno de los adaptadores NVMe over 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.
 - Rellene direcciones IP para una de las interfaces lógicas de SVM en la misma red que el adaptador físico asignado a este adaptador de NVMe over TCP.
 - Haga clic en el botón **Discover Controllers**.
 - En la lista de controladoras detectadas, haga clic en la casilla de comprobación de las dos controladoras con direcciones de red alineadas con este adaptador NVMe over TCP.
 - Haga clic en el botón **OK** para agregar los controladores seleccionados.

Add controller | vmhba68



Automatically

Manually

Host NQN

nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-...

COPY

IP

1

172.21.118.189

Enter IPv4 / IPv6 address

Central discovery controller

Port Number

Range more from 0

Digest parameter

Header digest

Data digest

DISCOVER CONTROLLERS

2

Select which controller to connect

<input type="checkbox"/>	Id	Subsystem NQN	Transport Type	IP	Port Number
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.189	4420
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF	nvm	172.21.118.190	4420

Manage Columns 4 items

3

4

OK

6. Después de unos segundos, es recomendable que aparezca el espacio de nombres de NVMe en la pestaña Devices.

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.net app.com:794177624:65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

Manage Columns Export ▾ 6 items

Properties **Devices** Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

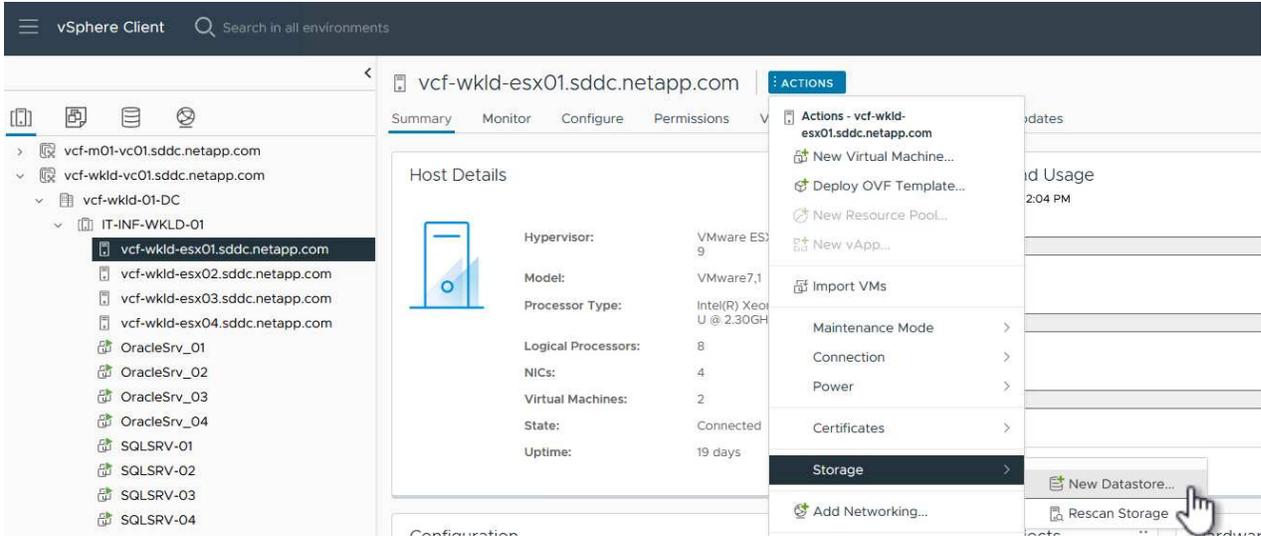
Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
NVMe TCP Disk (uuid.929a6a9045764784 9146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTRAN: RT

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

Ponga en marcha un almacén de datos de NVMe sobre TCP

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

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi del clúster de dominio de la carga de trabajo. En el menú **Acciones**, selecciona **Almacenamiento > Nuevo Datastore...**



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

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name VCF_WKLD_04_NVMe

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl
<input checked="" type="radio"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n	N
<input type="radio"/>	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

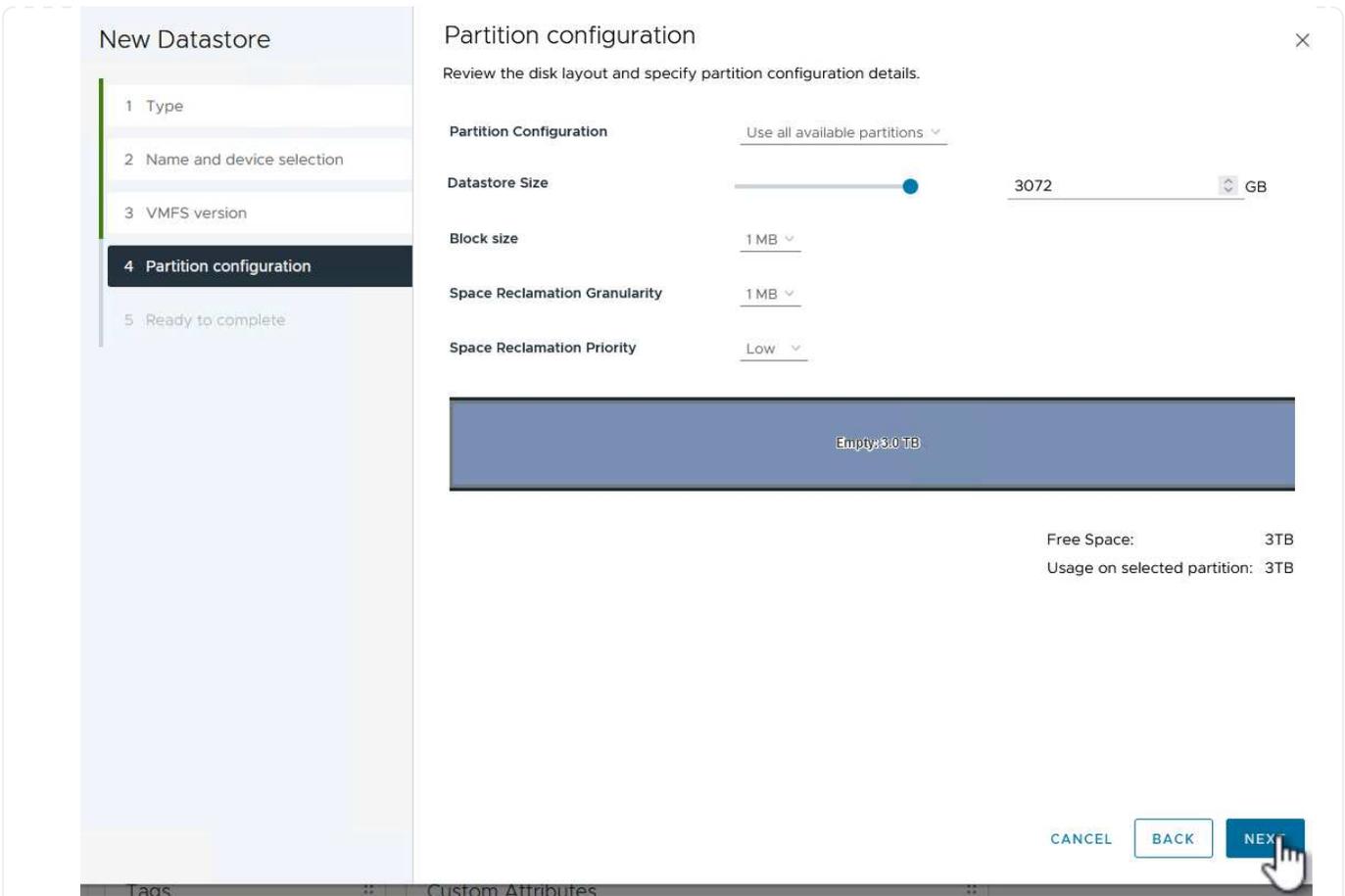
Manage Columns Export 3 items

CANCEL

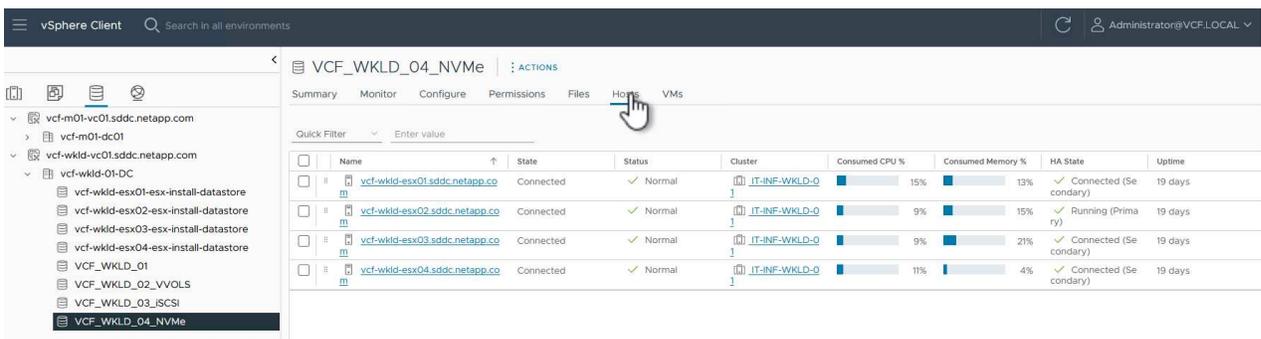
BACK

NEXT

4. En la página **VMFS version** seleccione la versión de VMFS para el almacén de datos.
5. En la página **Configuración de partición**, realice los cambios deseados 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 configuró correctamente, todos los hosts ESXi del clúster deben aparecer en la lista y tener acceso al nuevo almacén de datos.



Información adicional

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

Utilice el complemento de SnapCenter para VMware vSphere para proteger las máquinas virtuales en los dominios de carga de trabajo de VCF

En este escenario, mostraremos cómo poner en marcha y utilizar el complemento de SnapCenter para VMware vSphere (SCV) para realizar backups y restaurar máquinas virtuales y almacenes de datos en un dominio de carga de trabajo de VCF. SCV utiliza la tecnología Snapshot de ONTAP para realizar copias de backup rápidas y eficientes de los volúmenes de almacenamiento de ONTAP que alojan almacenes de datos de vSphere. La tecnología SnapMirror y SnapVault se usa para crear backups secundarios en un sistema de almacenamiento independiente y con políticas de retención que imiten el volumen original o pueden ser independientes del volumen original para su retención a largo plazo.

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

Autor: Josh Powell

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Ponga en marcha el plugin de SnapCenter para VMware vSphere (SCV) en el dominio de la carga de trabajo de VI.
- Añada sistemas de almacenamiento a SCV.
- Cree políticas de backup en SCV.
- Cree grupos de recursos en SCV.
- Utilice SCV para realizar backup de almacenes de datos o máquinas virtuales específicas.
- Utilice SCV para restaurar las máquinas virtuales a una ubicación alternativa del clúster.
- Utilice SCV para restaurar archivos en un sistema de archivos Windows.

Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

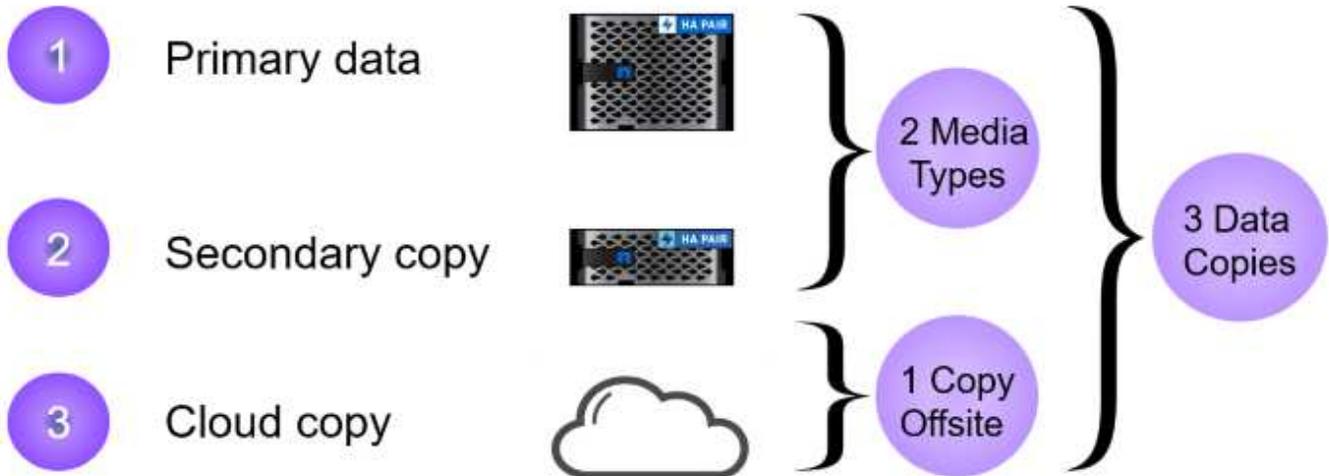
- Un sistema de almacenamiento de ONTAP ASA con almacenes de datos VMFS iSCSI asignados al clúster de dominio de cargas de trabajo.
- Un sistema de almacenamiento secundario de ONTAP configurado para recibir backups secundarios mediante SnapMirror.
- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.
- Se ha desplegado anteriormente un dominio de carga de trabajo de VI.
- Hay máquinas virtuales en la SCV del clúster designada para proteger.

Para obtener información sobre la configuración de almacenes de datos VMFS iSCSI como almacenamiento complementario, consulte ["ISCSI como almacenamiento complementario para Dominios de Gestión"](#) en esta documentación. El proceso para utilizar OTV para desplegar almacenes de datos es idéntico para los

dominios de gestión y carga de trabajo.



Además de replicar los backups realizados con SCV en el almacenamiento secundario, se pueden hacer copias de los datos externos en el almacenamiento de objetos en uno de los tres (3) proveedores de cloud líderes que utilicen el backup y recuperación de datos de NetApp BlueXP para máquinas virtuales. Para obtener más información, consulte la solución ["3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales"](#).



Pasos de despliegue

Para implementar el plugin de SnapCenter y utilizarlo para crear backups, y restaurar máquinas virtuales y almacenes de datos, complete los siguientes pasos:

Implemente y utilice SCV para proteger los datos en un dominio de carga de trabajo de VI

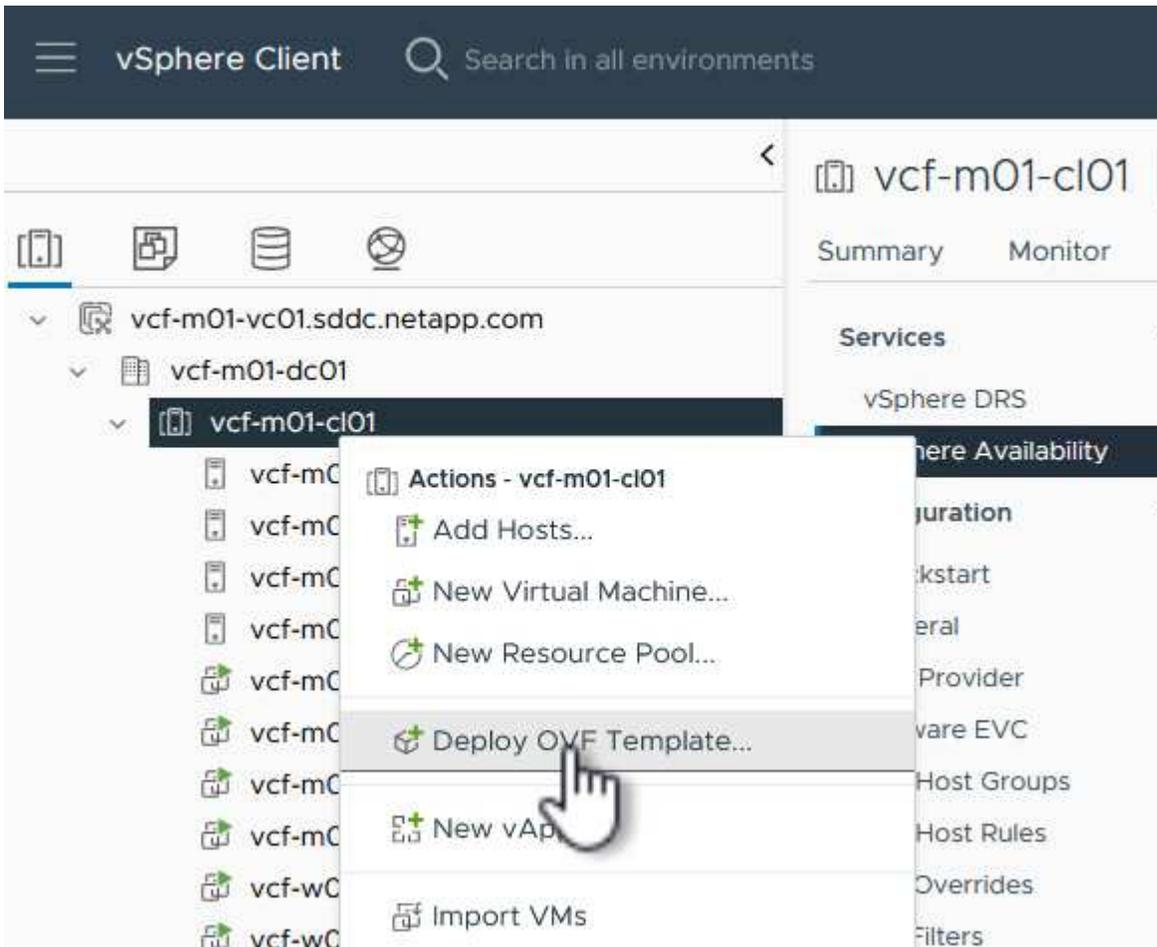
Complete los siguientes pasos para poner en marcha, configurar y utilizar SCV para proteger los datos en un dominio de carga de trabajo de VI:

Ponga en marcha el complemento SnapCenter para VMware vSphere

El plugin de SnapCenter se aloja en el dominio de gestión de VCF, pero se registra en el para el dominio de carga de trabajo de VI para vCenter. 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 gestionados por una única instancia de vCenter.

Complete los siguientes pasos desde el cliente de vCenter para poner en marcha SCV en el dominio de cargas de trabajo de VI:

1. Descargue el archivo OVA para la implementación de SCV desde el área de descarga del sitio de soporte de NetApp "[AQUÍ](#)".
2. Desde el dominio de gestión vCenter Client, seleccione **Desplegar plantilla OVF...**



3. En el asistente **Implementar plantilla OVF**, haga clic en el botón de opción **Archivo local** y, a continuación, seleccione cargar la plantilla OVF descargada anteriormente. 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 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

UPLOAD FILES

scv-5.OP2-240310_1514.ova

4. En la página **Seleccionar nombre y carpeta**, proporcione un nombre para la VM del broker de datos SCV y una carpeta en el dominio de administración. Haga clic en **Siguiente** para continuar.
5. En la página **Select a compute resource**, seleccione el cluster de dominio de administración o el host ESXi específico dentro del cluster para instalar la VM.
6. Revise la información relativa a la plantilla OVF en la página **Detalles de revisión** 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 VM y seleccione el **formato de disco virtual** y **Política de almacenamiento de VM**. En esta solución, la máquina virtual se instalará en un almacén de datos VMFS iSCSI ubicado en un sistema de almacenamiento de ONTAP, como se ha puesto en marcha previamente en una sección separada de este documento. 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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format

VM Storage Policy

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/> mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB	
<input type="radio"/> vcf-m01-cl01-ds-vsant01	--	999.97 GB	49.16 GB	957.54 GB	
<input type="radio"/> vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	

Compatibility

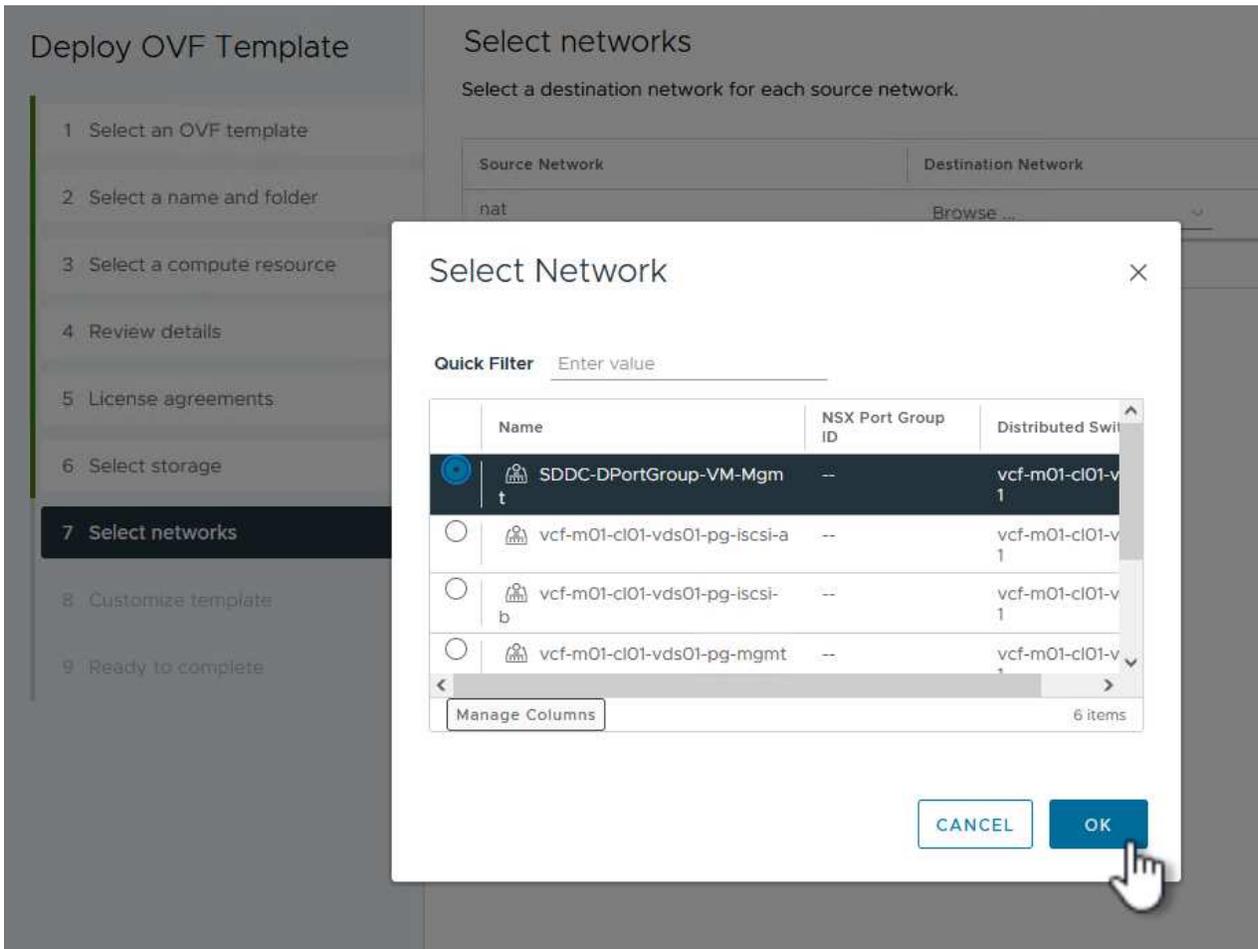
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. En la página **Seleccionar red**, seleccione la red de administración que pueda 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 necesaria para la implementación:

- El FQDN o la IP, y credenciales para la carga de trabajo el dispositivo vCenter de dominio.
- Credenciales para la cuenta administrativa de SCV.
- Credenciales para la cuenta de mantenimiento de SCV.
- IPv4 Detalles de las propiedades de red (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.

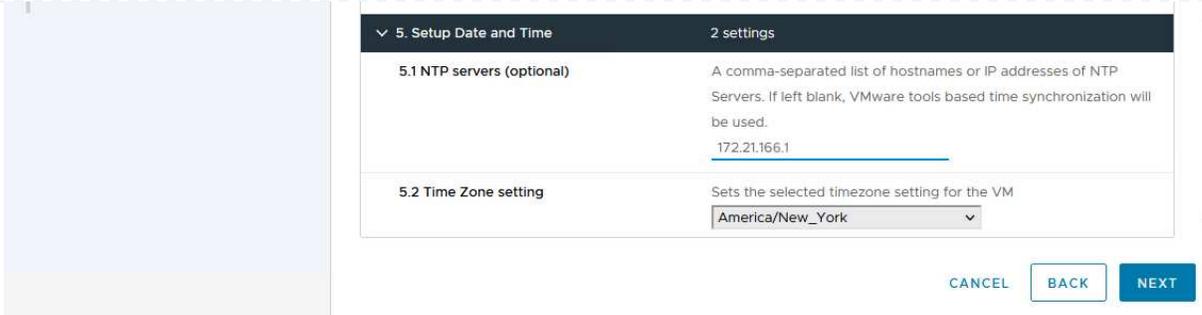
1. Register to existing vCenter		4 settings
1.1 vCenter Name(FQDN) or IP Address	<input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>	
1.2 vCenter username	<input type="text" value="administrator@vcf.local"/>	
1.3 vCenter password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
1.4 vCenter port	<input type="text" value="443"/>	
2. Create SCV Credentials		2 settings
2.1 Username	<input type="text" value="admin"/>	
2.2 Password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
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) <input type="text" value="172.21.166.148"/>	
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="255.255.255.0"/>	
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.1"/>	
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) <input type="text" value="10.61.185.231"/>	
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) <input type="text" value="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) <input type="text" value="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) <input type="text"/>	
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired) <input type="text"/>	

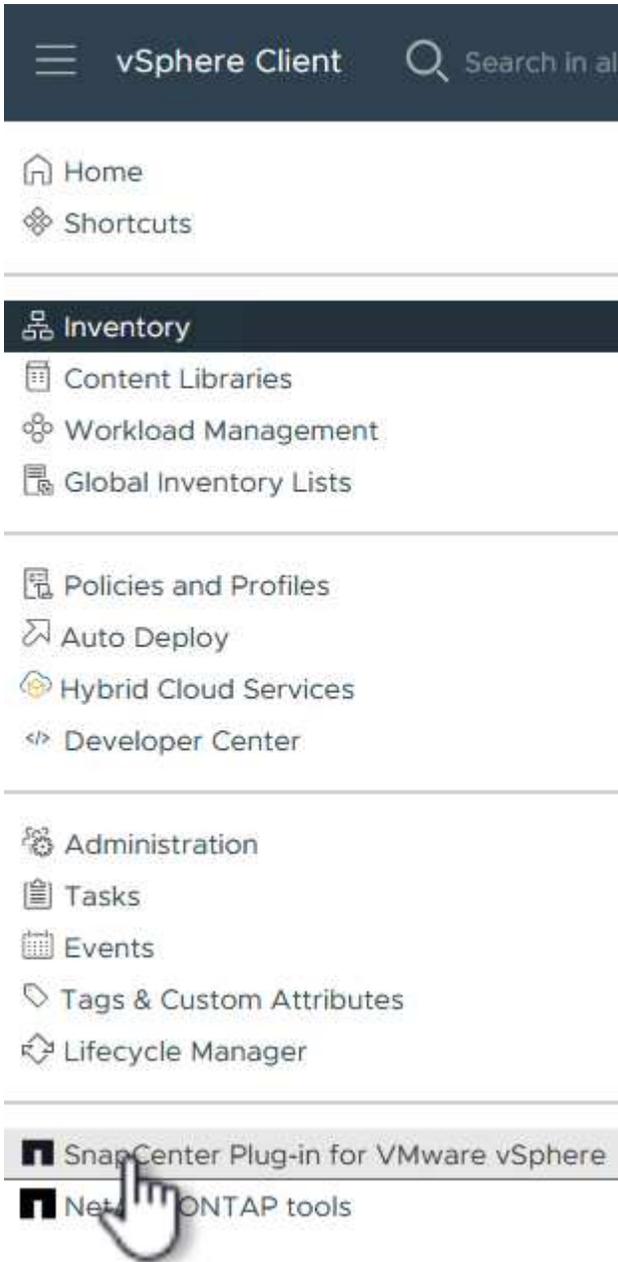


10. Por último, en la página **Listo para completar**, revise todos los ajustes y haga clic en Finalizar para iniciar la implementación.

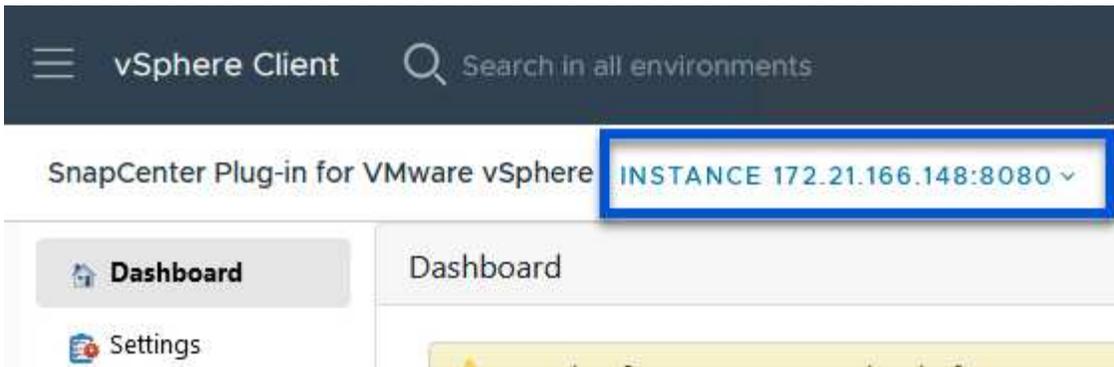
Añada sistemas de almacenamiento a SCV

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

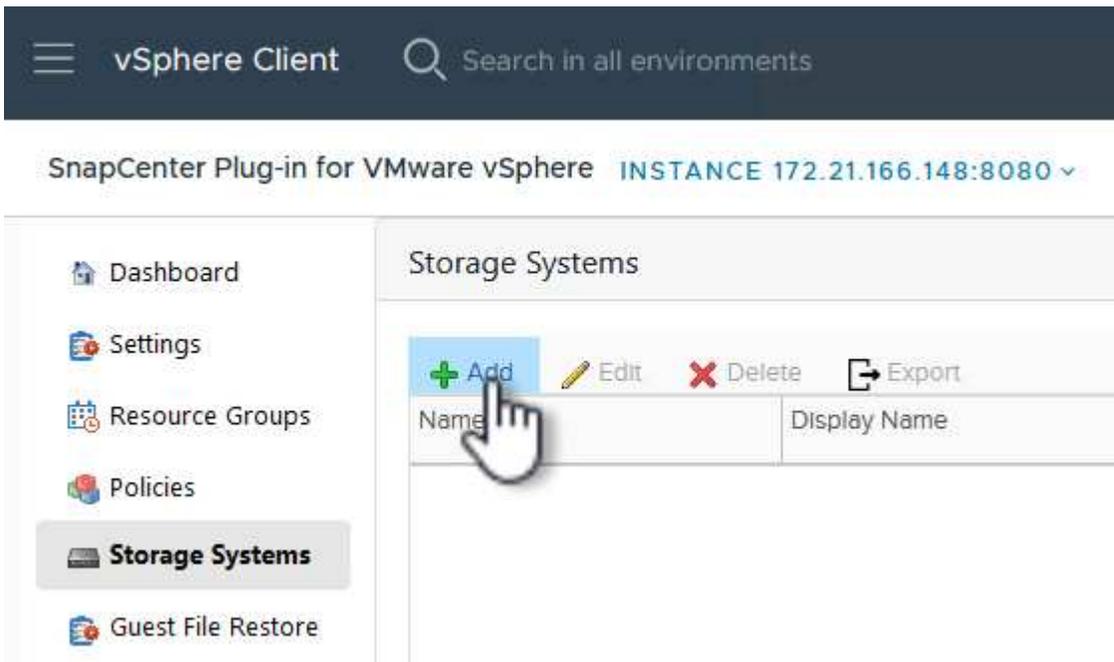
1. Es posible acceder a SCV desde el menú principal de vSphere Client.



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 va a proteger.



3. Navegue a **Storage Systems** en el menú de la izquierda y haga clic en **Add** para comenzar.



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

Add Storage System



Storage System	<input type="text" value="172.16.9.25"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> Seconds
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>

Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system

CANCEL

ADD



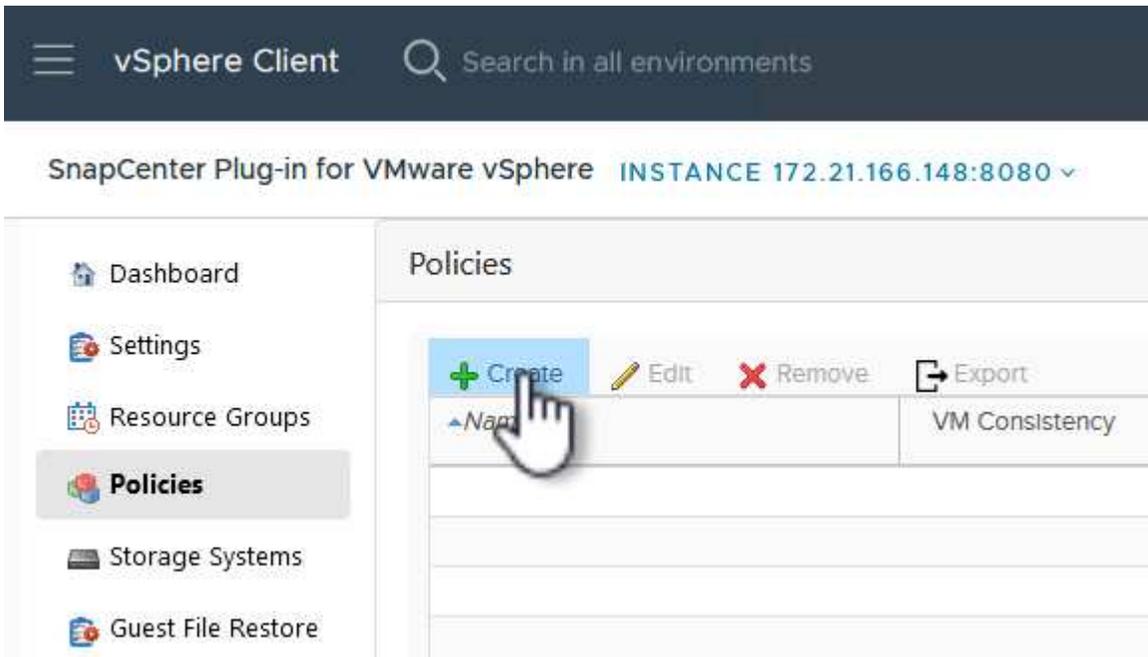
5. Repita este procedimiento para gestionar cualquier sistema de almacenamiento adicional, incluidos los sistemas que se van a utilizar como destino de backup secundario.

Configure políticas de backup en SCV

Para obtener más información sobre la creación de políticas de backup de SCV, consulte "[Crear políticas de backup para máquinas virtuales y almacenes de datos](#)".

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

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



2. En el formulario **Nueva política de copia de seguridad**, proporcione un **Nombre** y **Descripción** para la política, la **Frecuencia** en la que se realizarán las copias de seguridad y el período **Retención** que especifica cuánto tiempo se mantendrá la copia de seguridad.

El período de bloqueo permite que la función ONTAP SnapLock cree instantáneas a prueba de manipulaciones y permite la configuración del período de bloqueo.

Para **Replicación** Seleccione si desea actualizar las relaciones subyacentes de SnapMirror o SnapVault para el volumen de almacenamiento de ONTAP.



La replicación de SnapMirror y de SnapVault es similar ya que ambos utilizan la tecnología SnapMirror de ONTAP para replicar de forma asíncrona los volúmenes de almacenamiento en un sistema de almacenamiento secundario para mejorar la protección y la seguridad. Para las relaciones de SnapMirror, la programación de retención especificada en la política de backup de SCV gobernará la retención tanto del volumen primario como secundario. Con las relaciones de SnapVault, es posible establecer un programa de retención separado en el sistema de almacenamiento secundario para programas de retención a largo plazo o distintos. En este caso, la etiqueta de Snapshot se especifica en la política de backup de SCV y en la política asociada con el volumen secundario, para identificar a qué volúmenes va a aplicar la programación de retención independiente a.

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

New Backup Policy



Name

Description

Frequency

Locking Period Enable Snapshot Locking ⓘ

Retention ⓘ

Replication Update SnapMirror after backup ⓘ
 Update SnapVault after backup ⓘ

Snapshot label

Advanced ▾ VM consistency ⓘ
 Include datastores with independent disks

Scripts ⓘ

CANCEL

ADD

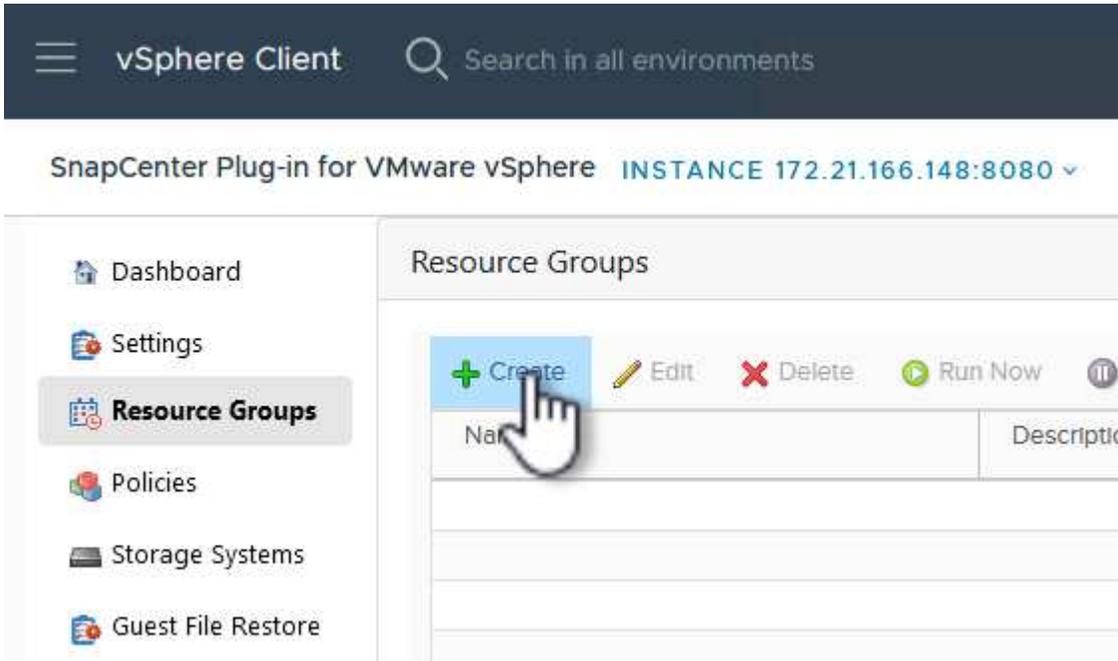


Cree grupos de recursos en SCV

Para obtener más información sobre la creación de SCV Resource Groups, consulte "[Crear grupos de recursos](#)".

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

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 notificación**, proporcione un nombre para el grupo de recursos, la configuración de notificación y cualquier otra opción adicional para el nombre de las instantáneas.
3. En la página **Recurso**, seleccione los almacenes de datos y las máquinas virtuales que se van a proteger en el grupo de recursos. Haga clic en **Siguiente** para continuar.



Incluso cuando solo se seleccionan máquinas virtuales específicas, siempre se realiza un backup 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 la selección únicamente de máquinas virtuales específicas para backup limita la posibilidad de restaurar únicamente a dichas máquinas virtuales.

Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Enter available entity name

Available entities

OracleSrv_01
OracleSrv_02
OracleSrv_03
OracleSrv_04

Selected entities

SQLSRV-01
SQLSRV-02
SQLSRV-03
SQLSRV-04

BACK

NEXT

FINISH

CANCEL

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

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

Manually select the spanning datastores to be included ⓘ

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

BACK

NEXT

FINISH

CANCEL

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

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

6. Summary

Daily_Snapmi... ▼

Type

Daily

Every

1 Day(s)

Starting

04/04/2024

At

04 45 PM

BACK

NEXT

FINISH

CANCEL

7. Finalmente revise el **Summary** y haga clic en **Finish** para crear el grupo de recursos.

Create Resource Group

- 1. General info & notification
- 2. Resource
- 3. Spanning disks
- 4. Policies
- 5. Schedules
- 6. Summary**

Name	SQL_Servers						
Description							
Send email	Never						
Latest Snapshot name	None ⓘ						
Custom snapshot format	None ⓘ						
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04						
Spanning	False						
Policies	<table><thead><tr><th>Name</th><th>Frequency</th><th>Snapshot Locking Period</th></tr></thead><tbody><tr><td>Daily_Snapmir...</td><td>Daily</td><td>-</td></tr></tbody></table>	Name	Frequency	Snapshot Locking Period	Daily_Snapmir...	Daily	-
Name	Frequency	Snapshot Locking Period					
Daily_Snapmir...	Daily	-					

BACK

NEXT

FINISH

CANCEL

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

vSphere Client

SnapCenter Plug-in for VMware vSphere [INSTANCE 172.21.166.148:8080](#) ▾

Dashboard

Settings

Resource Groups

Policies

Storage Systems

Guest File Restore

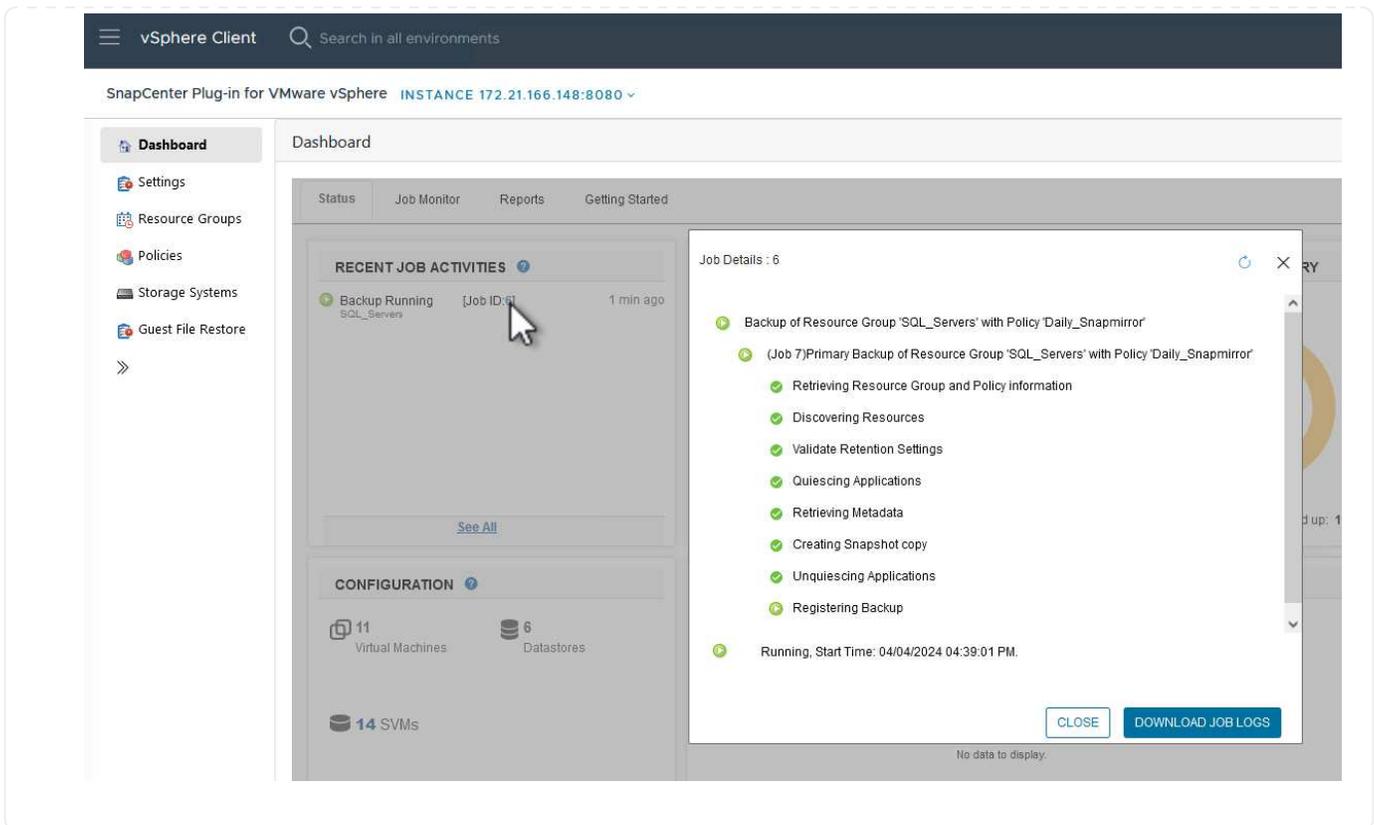
»

Resource Groups

[+](#) Create [✎](#) Edit [✖](#) Delete [▶](#) Run Now [⏸](#) Suspend [▶](#) Resume [📄](#) Export

Name	Description	Policy
SQL_Servers		Daily_

9. Navegue hasta el **Panel** y, en **Actividades recientes** haga clic en el número que aparece junto a **ID de trabajo** para abrir el monitor de trabajos y ver el progreso del trabajo en ejecución.



Utilice SCV para restaurar máquinas virtuales, VMDK y archivos

El plugin de SnapCenter permite restaurar máquinas virtuales, VMDK, archivos y carpetas a partir de backups principales o secundarios.

Las máquinas virtuales pueden restaurarse al host original, o bien a un host alternativo de la misma instancia de vCenter Server, o bien a un host ESXi alternativo gestionado por la misma instancia de vCenter o cualquier instancia de vCenter en modo vinculado.

Las máquinas virtuales VVol pueden restaurarse en el host original.

Los VMDK de máquinas virtuales tradicionales pueden restaurarse tanto a un almacén de datos original como a uno alternativo.

Los VMDK de las máquinas virtuales VVol pueden restaurarse en el almacén de datos original.

Pueden restaurarse archivos y carpetas individuales en una sesión de restauración de archivos invitados, lo que conecta una copia de backup de un disco virtual y luego restaura los archivos y las carpetas que se seleccionan.

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

Restaurar máquinas virtuales mediante el plugin de 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 desplácese hasta **SnapCenter Plug-in for VMware vSphere**. Seleccione **Restaurar** en el submenú.

OracleSrv_04 | Summary | Monitor | Configure | Permissions

Guest OS | Virtual Mac

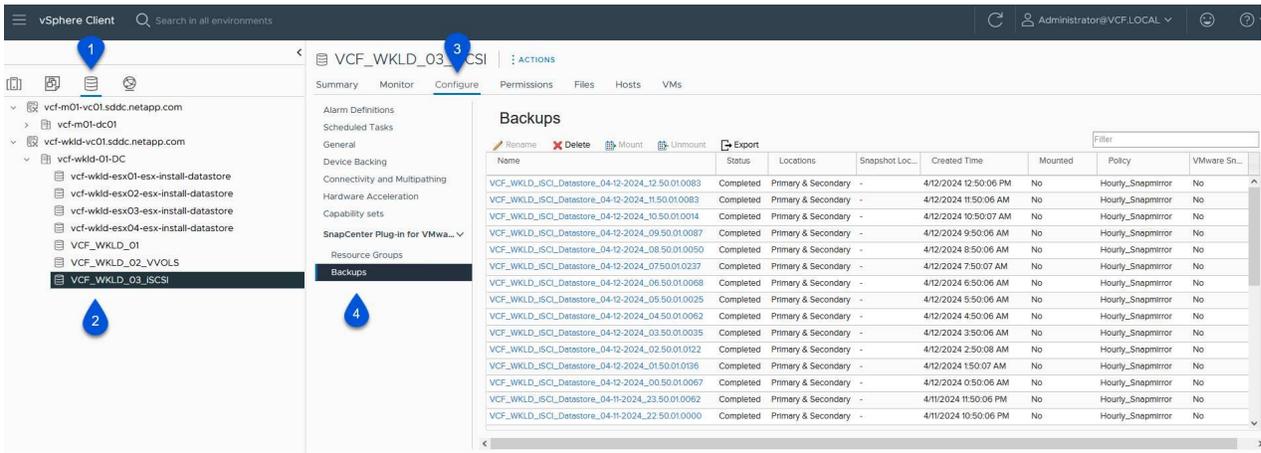
Actions - OracleSrv_04

- 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
 - Create Resource Group
 - Add to Resource Group
 - Attach Virtual Disk(s)
 - Detach Virtual Disk(s)
 - Restore
 - File Restore

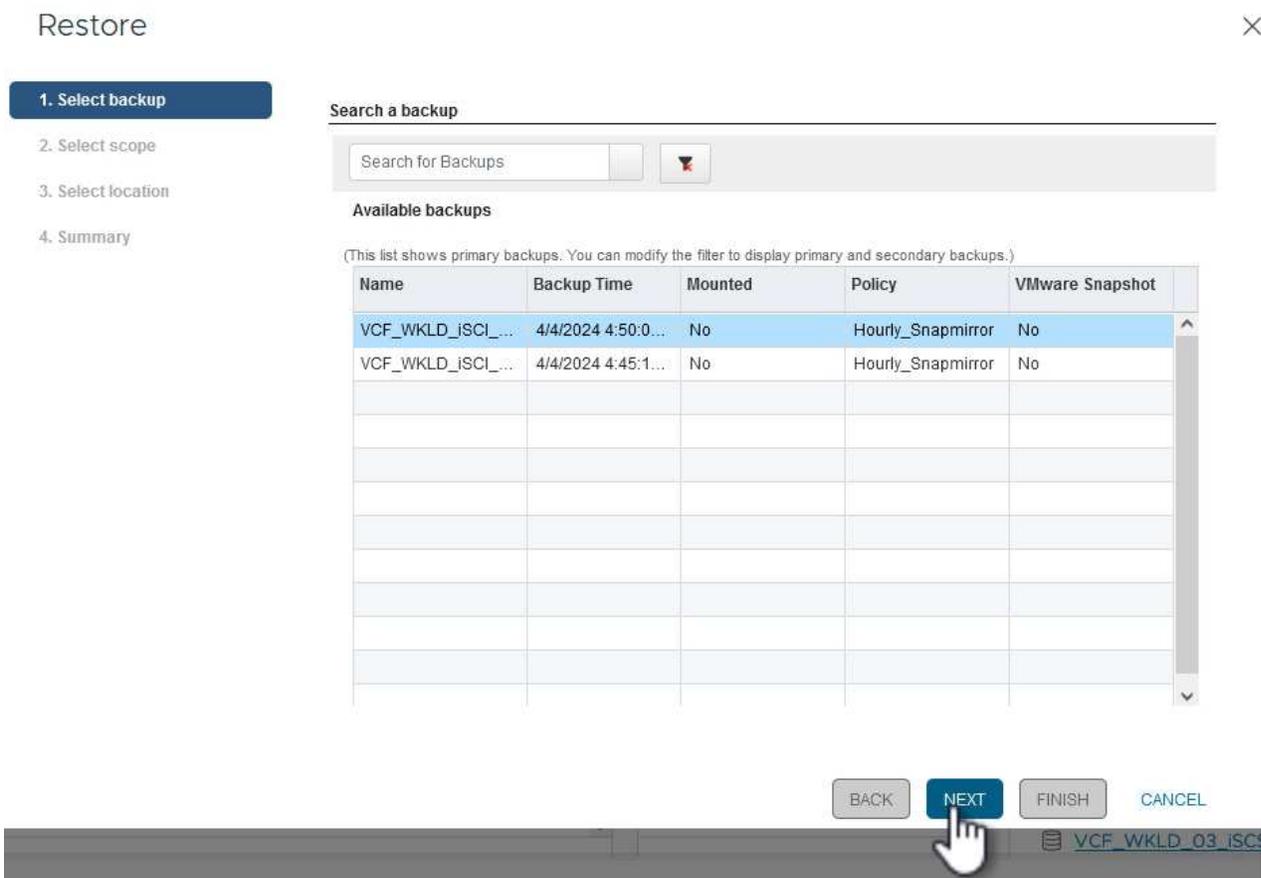
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision | VCF_WKLD_03_ISCSI
vcf-wkld-01-IT-INF-WKLD-01-vc (connected) | 00:50:56:83:02:f
Disconnected
ESXI 7.0 U2 and later (VM vers



Una alternativa es navegar al almacén de datos en inventario y, a continuación, en la pestaña **Configurar**, ir a **SnapCenter Plug-in for VMware vSphere > Backups**. Desde el backup elegido, seleccione las máquinas virtuales que se van a restaurar.



2. En el asistente **Restore**, seleccione la copia de seguridad que se va a utilizar. Haga clic en **Siguiente** para continuar.



3. En la página **Select Scope**, rellene todos los campos requeridos:

- **Restore Scope** - Seleccione esta opción para restaurar toda la máquina virtual.
- **Restart VM** - Elija si desea iniciar la VM después de la restauración.
- **Restaurar ubicación** - Elija restaurar a la ubicación original o a una ubicación alternativa. Al elegir una ubicación alternativa, seleccione las opciones de cada uno de los campos:
 - **Destination vCenter Server:** VCenter local o vCenter alternativo en modo vinculado
 - **Destino ESXi host**
 - **Red**
 - **Nombre de VM después de restaurar**
 - **Seleccione el almacén de datos:**

Restore
✕

✓ 1. Select backup

2. Select scope

3. Select location

4. Summary

Restore scope Entire virtual machine ▾

Restart VM

Restore Location

Original Location
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)

Alternate Location
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server 172.21.166.143 ▾

Destination ESXi host vcf-wkld-esx04.sddc.netapp.com ▾

Network vcf-wkld-01-HT-INF-WKLD-01-vds-01-pg- ▾

VM name after restore OracleSrv_04_restored

Select Datastore: VCF_WKLD_03_iSCSI ▾

BACK
NEXT
FINISH
CANCEL

VCF_WKLD_03_iSCSI

Haga clic en **Siguiente** para continuar.

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

Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- 3. Select location**
- 4. Summary

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest
	< >

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

Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- ✓ 3. Select location
- 4. Summary**

Virtual machine to be restored	OracleSrv_04
Backup name	VCF_WKLD_iSCSI_Datastore_04-04-2024_16.50.00.0940
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.143
ESXi host to be used to mount the backup	vcf-wkld-esx04.sddc.netapp.com
VM Network	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
Destination datastore	VCF_WKLD_03_iSCSI
VM name after restore	OracleSrv_04_restored



Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

FINISH

CANCEL

6. El progreso de los trabajos de restauración puede supervisarse desde el panel **Recent Tasks** de vSphere Client y desde el monitor de trabajos de SCV.

- 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
VCF_WKLD_ISCI_Datastore_04-04-2024...
- Backup Successful [Job ID:15] 8 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:12] 13 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:9] 13 min ago
SQL_Servers
- Backup Successful [Job ID:6] 19 min ago
SQL_Servers

[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.sdd c.netapp.com	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 P M
NetApp Restore	vcf-wkld-esx04.sdd c.netapp.com	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 P M

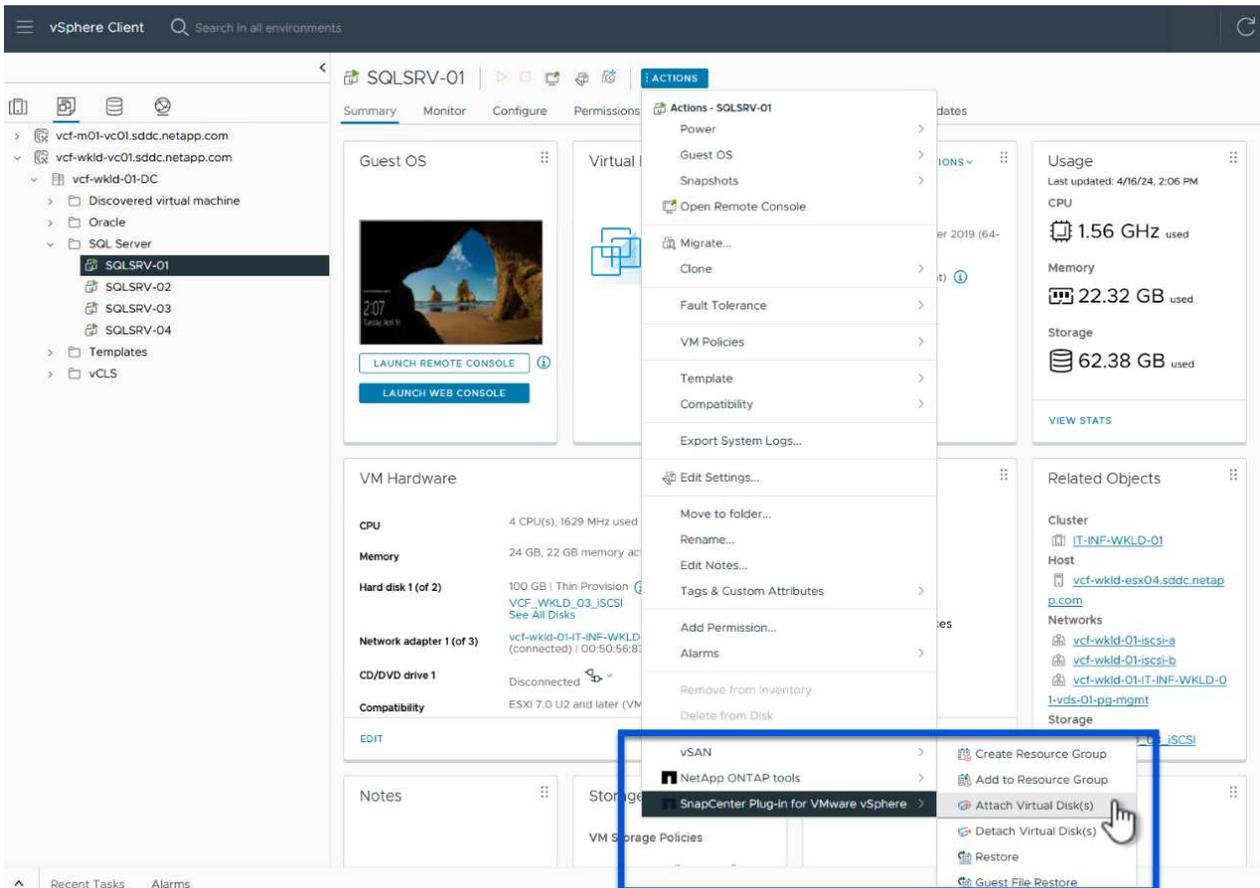
Manage Columns Running More Tasks

Restaurar VMDK mediante el plugin de SnapCenter

ONTAP Tools permite restaurar por completo los VMDK a su ubicación original o conectar un VMDK como disco nuevo a un sistema host. En este caso, se conectará un VMDK a un host Windows para acceder al sistema de archivos.

Para asociar un VMDK a partir de un backup, complete los siguientes pasos:

1. En vSphere Client, desplácese a una máquina virtual y, en el menú **Acciones**, seleccione **SnapCenter Plug-in for VMware vSphere > Attach Virtual Disk(s)**.



2. En el asistente **Attach Virtual Disk(s)**, seleccione la instancia de copia de seguridad que se va a utilizar y el VMDK que se va a asociar.

Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

Backup

(This list shows primary backups. **1** modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Las opciones de filtro pueden utilizarse para localizar backups y mostrar backups de sistemas de almacenamiento primarios y secundarios.

Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

Backup

(This list shows primary backups)

Name
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231

Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Time range

From

Hour Minute Second

To

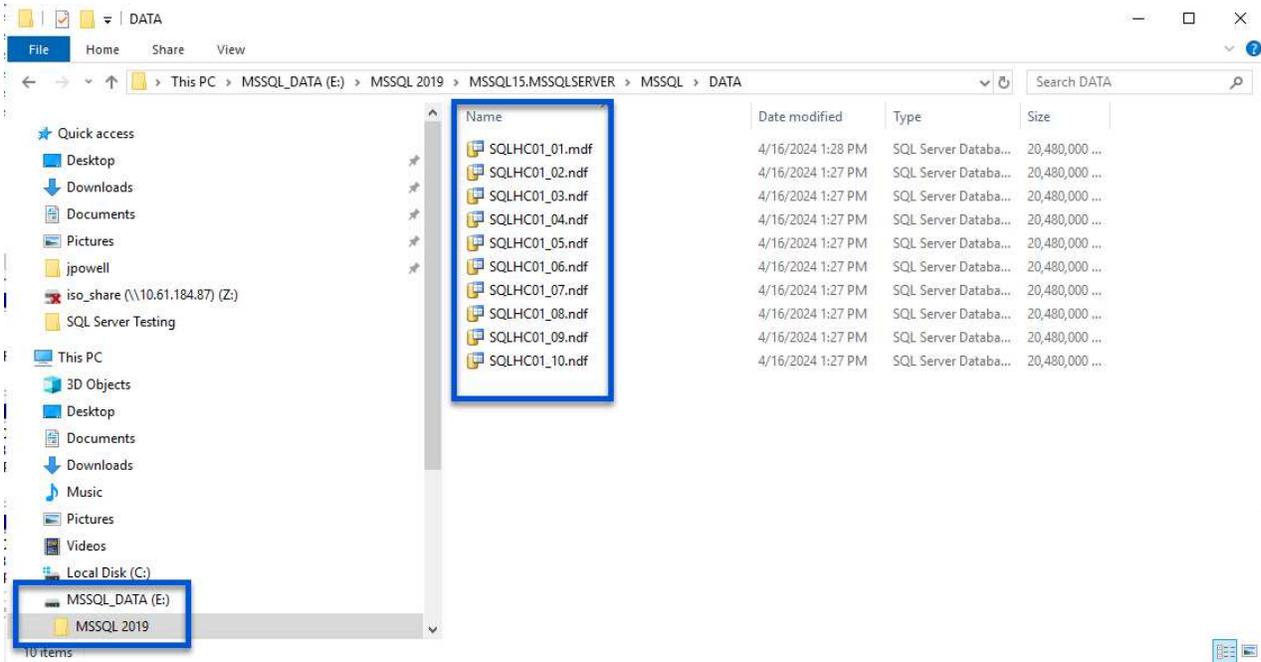
Hour Minute Second

VMware snapshot

Mounted

Location

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



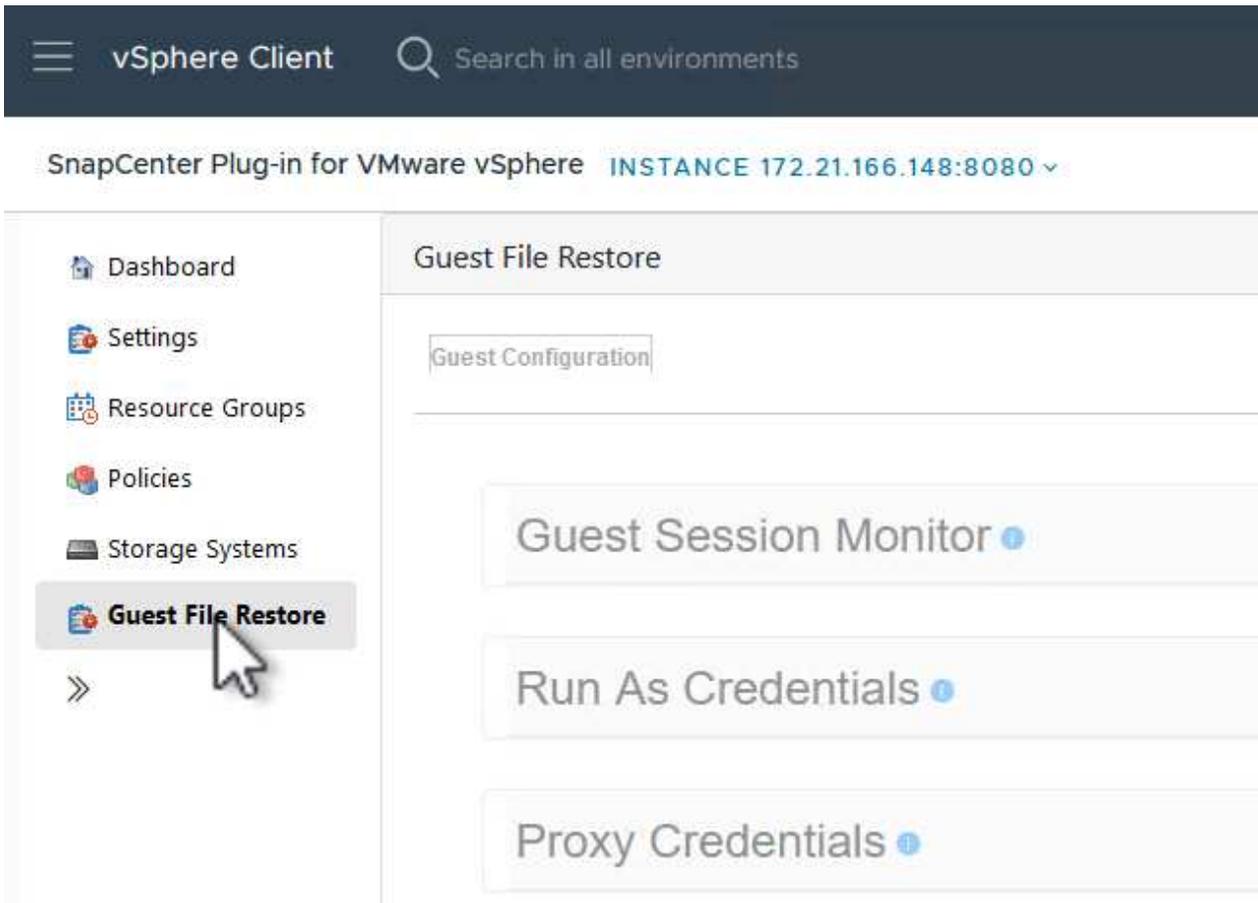
Restauración de sistemas de archivos invitados mediante el plugin de SnapCenter

ONTAP Tools cuenta con restauraciones de sistemas de archivos invitados desde un VMDK en sistemas operativos Windows Server. Este proceso está preformado de forma centralizada a partir de la interfaz del plugin de SnapCenter.

Para obtener información detallada, consulte "[Restaurar archivos y carpetas invitados](#)" En el sitio de documentación de SCV.

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

1. El primer paso es crear credenciales Run As para facilitar el acceso al sistema host de Windows. En vSphere Client, vaya a la interfaz del plugin CSV y haga clic en **Guest File Restore** en el menú principal.



2. En **Ejecutar como Credenciales** haz clic en el icono + para abrir la ventana **Ejecutar como Credenciales**.
3. Introduzca un nombre para el registro de credenciales, un nombre de usuario de administrador y una contraseña para el sistema Windows y, a continuación, haga clic en el botón **Select VM** para seleccionar una VM proxy opcional que se utilizará para la restauración.

Run As Credentials



Run As Name	<input type="text" value="Administrator"/>	
Username	<input type="text" value="administrator"/>	
Password	<input type="password" value="••••••••"/>	
Authentication Mode	<input type="text" value="Windows"/>	
VM Name	<input type="text"/>	



CANCEL

SAVE

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

Proxy VM



VM Name

SQLSRV-01

Search by ESXi Host

ESXi Host

vcf-wkld-esx04.sddc.netapp.com

Virtual Machine

SQLSRV-01

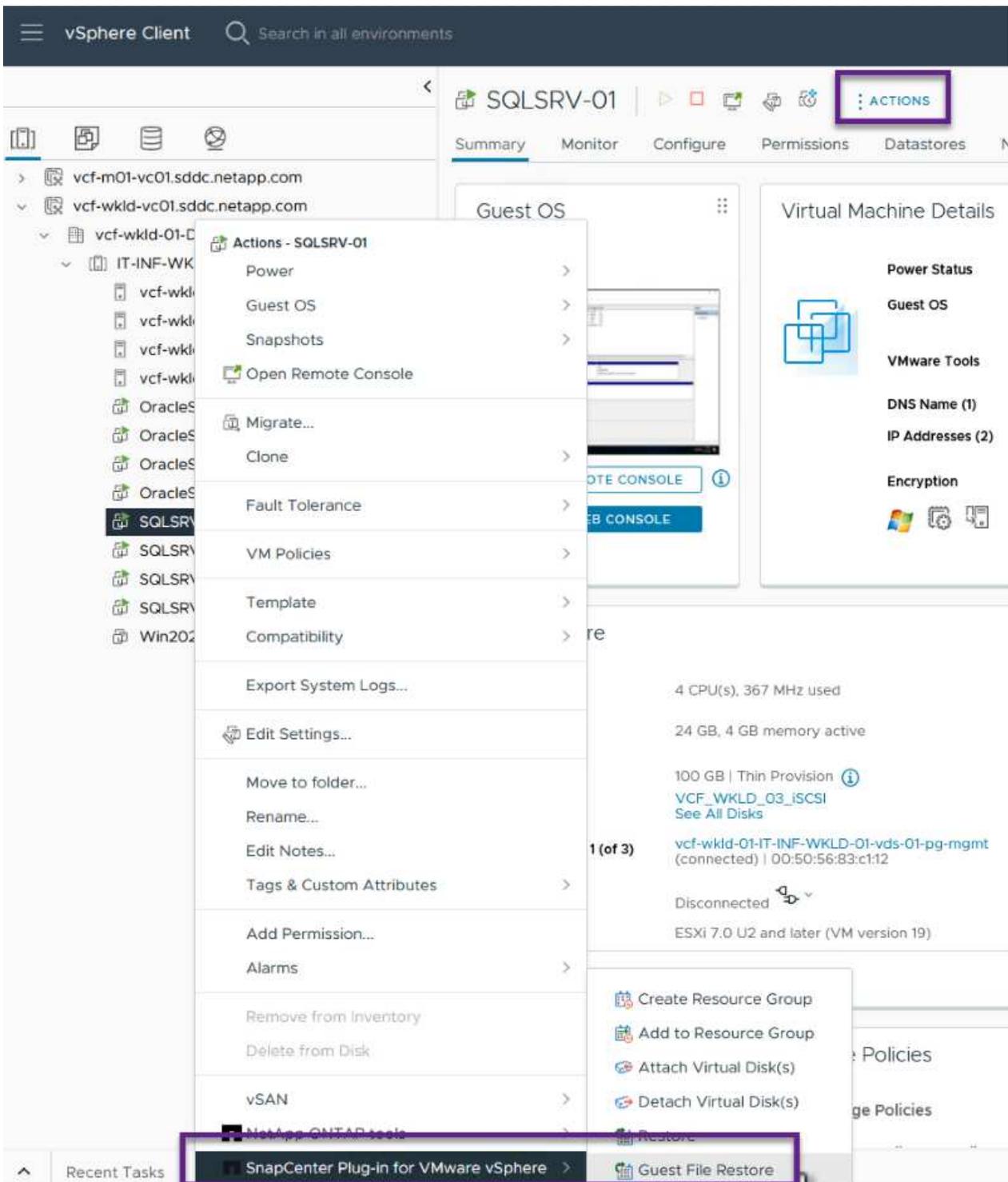
Search by Virtual Machine name

CANCEL

SAVE



5. Haga clic en **Guardar** de nuevo en la ventana **Ejecutar como Credenciales** para completar el guardado del registro.
6. A continuación, desplácese a una máquina virtual del inventario. En el menú **Acciones**, o haciendo clic derecho en la máquina virtual, seleccione **SnapCenter Plug-in for VMware vSphere > Guest File Restore**.



7. En la página **Restore Scope** del asistente **Guest File Restore**, seleccione la copia de seguridad desde la que desea restaurar, el VMDK en particular y la ubicación (primaria o secundaria) desde la que desea restaurar el VMDK. Haga clic en **Siguiente** para continuar.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iscsi_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iscsi:VCF_WKLD_03_iscsi:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iscsi_dest:SQL_Servers_04-16-2024_13.52.34.0329

BACK NEXT FINISH CANCEL



8. En la página **Detalles del invitado**, seleccione usar **VM invitado** o **Usar gues File Restore proxy VM** para la restauración. Además, rellene aquí la configuración de notificaciones por correo electrónico si lo desea. Haga clic en **Siguiente** para continuar.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

Use Guest File Restore proxy VM

Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

9. Por último, revise la página **Summary** y haga clic en **Finish** para comenzar la sesión de Restauración del sistema de archivos invitados.
10. De nuevo en la interfaz del plugin de SnapCenter, navegue a **Restauración de archivos invitados** de nuevo y vea la sesión en ejecución en **Monitor de sesión de invitado**. Haga clic en el icono en **Examinar archivos** para continuar.

The screenshot shows the vSphere Client interface with the SnapCenter Plug-in for VMware vSphere. The main content area displays the "Guest File Restore" configuration page. Below the configuration, there is a "Guest Session Monitor" table with the following data:

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13.52.34.0329	SQLSRV-01	[VCF_WKLD_03_JSCSI]sc-202404161419...	E:\	23h:58m	

Below the table, there are sections for "Run As Credentials" and "Proxy Credentials", both with expandable dropdown menus.

11. En el asistente de **Guest File Browse**, seleccione la carpeta o los archivos que desea restaurar y la ubicación del sistema de archivos en la que desea restaurarlos. Finalmente, haga clic en **Restaurar** para iniciar el proceso **Restaurar**.

Guest File Browse



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



E:\MSSQL 2019

	Name	Size	
<input type="checkbox"/>	MSSQL15.MSSQLSERVER		^
			v

Selected 0 Files / 1 Directory

Name	Path	Size	Delete	
MSSQL 2019	E:\MSSQL 2019			^
				v

Select Restore Location



Select address family for UNC path:

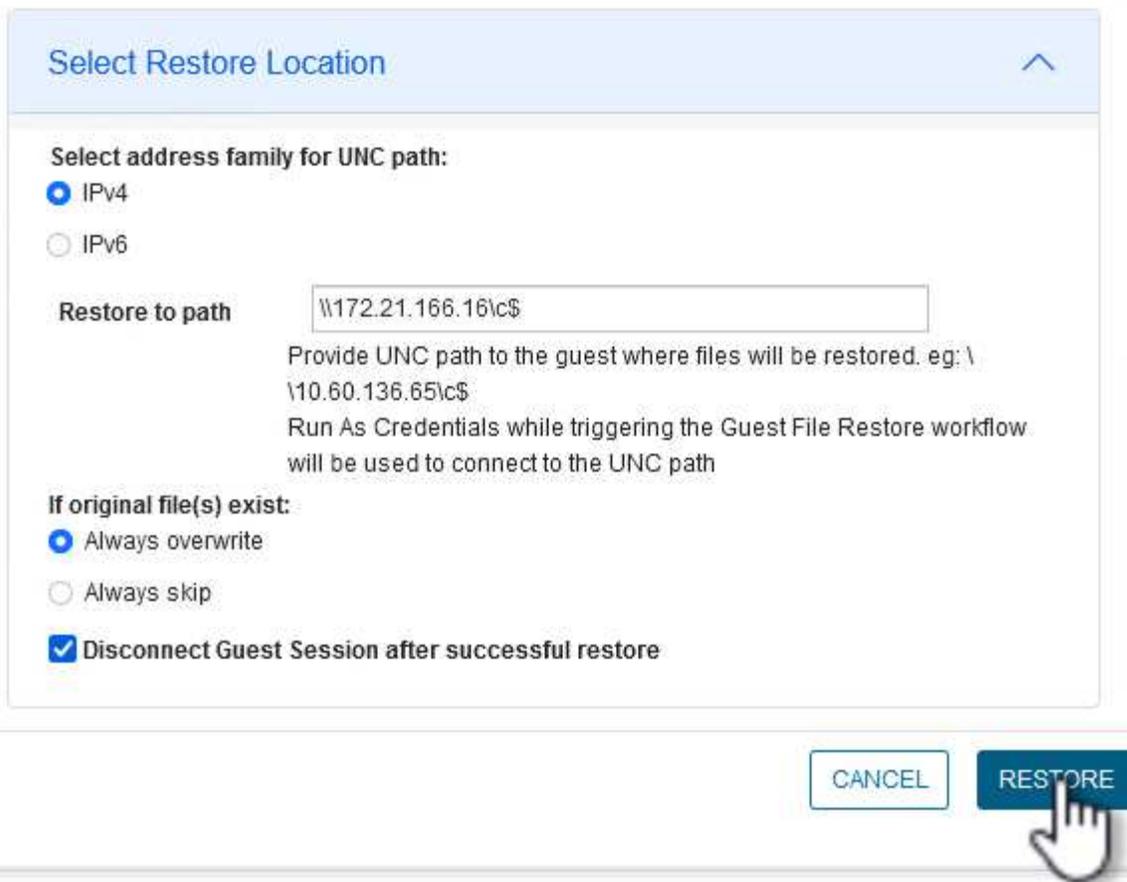
IPv4

IPv6

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 acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre el uso del plugin de SnapCenter para VMware vSphere, consulte el ["Documentación del plugin de SnapCenter para VMware vSphere"](#).

VCF con cabinas NetApp AFF

VMware Cloud Foundation con cabinas NetApp AFF

VMware Cloud Foundation (VCF) es una plataforma integrada de centro de datos definido por software (SDDC) que proporciona una pila completa de infraestructura definida por software para ejecutar aplicaciones empresariales en un entorno de cloud híbrido. Combina funcionalidades de computación, almacenamiento, redes y gestión en una plataforma unificada que ofrece una experiencia operativa consistente en clouds privados y públicos.

Autor: Josh Powell, Ravi BCB

Este documento proporciona información sobre las opciones de almacenamiento disponibles para VMware Cloud Foundation mediante el sistema de almacenamiento AFF All-Flash de NetApp. Las opciones de almacenamiento compatibles se tratan con instrucciones específicas para la creación de dominios de carga de trabajo con almacenes de datos NFS y VVOL como almacenamiento principal, así como una serie de opciones de almacenamiento complementarias.

Casos de uso

Casos de uso cubiertos en esta documentación:

- Opciones de almacenamiento para los clientes que buscan entornos uniformes tanto en clouds públicos como privados.
- Solución automatizada para poner en marcha infraestructura virtual para dominios de cargas de trabajo.
- Solución de almacenamiento escalable adaptada para satisfacer las necesidades en constante evolución, incluso cuando no se alinea directamente con los requisitos de recursos informáticos.
- Implemente dominios de carga de trabajo VCF VI usando ONTAP como almacenamiento principal.
- Ponga en marcha almacenamiento complementario en dominios de cargas de trabajo de infraestructuras virtuales mediante ONTAP Tools para VMware vSphere.

Destinatarios

Esta solución está dirigida a las siguientes personas:

- Arquitectos de soluciones que buscan opciones de almacenamiento más flexibles para entornos VMware diseñadas para maximizar el TCO.
- Arquitectos de soluciones que buscan opciones de almacenamiento VCF que ofrezcan opciones de protección de datos y recuperación ante desastres con los principales proveedores de cloud.
- Los administradores de almacenamiento que desean comprender cómo configurar VCF con almacenamiento principal y complementario.

Visión general de la tecnología

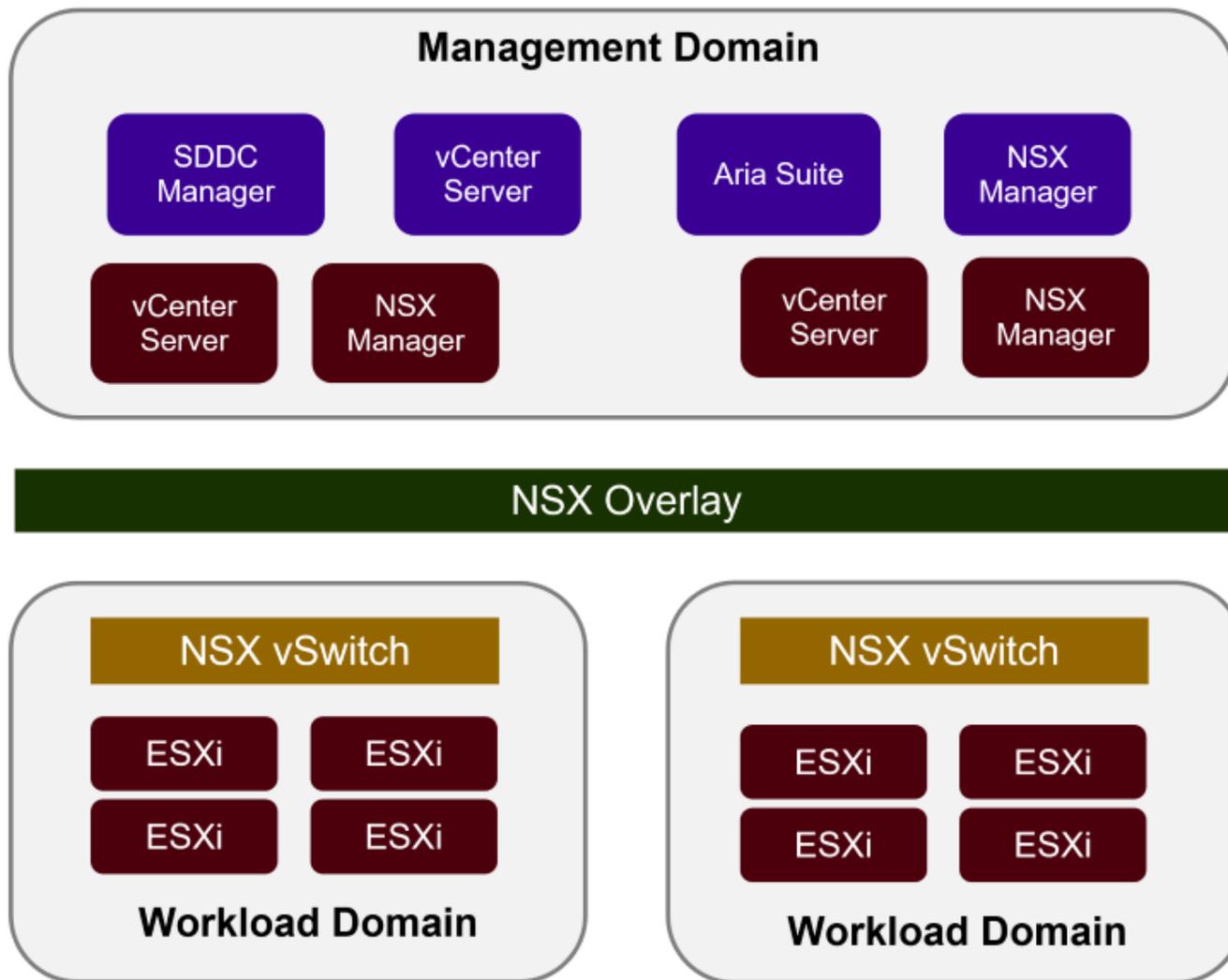
La solución VCF con NetApp AFF consta de los siguientes componentes principales:

Base de cloud de VMware

VMware Cloud Foundation amplía las ofertas de hipervisores vSphere de VMware combinando componentes clave como SDDC Manager, vSphere, vSAN, NSX y VMware Aria Suite para crear un centro de datos virtualizado.

La solución VCF es compatible tanto con cargas de trabajo nativas de Kubernetes como con máquinas virtuales. Los servicios clave, como VMware vSphere, VMware vSAN, VMware NSX-T Data Center y VMware vRealize Cloud Management, son componentes integrales del paquete VCF. Al combinarse, estos servicios establecen una infraestructura definida por software capaz de gestionar con eficiencia la informática, el almacenamiento, las redes, la seguridad y la gestión del cloud.

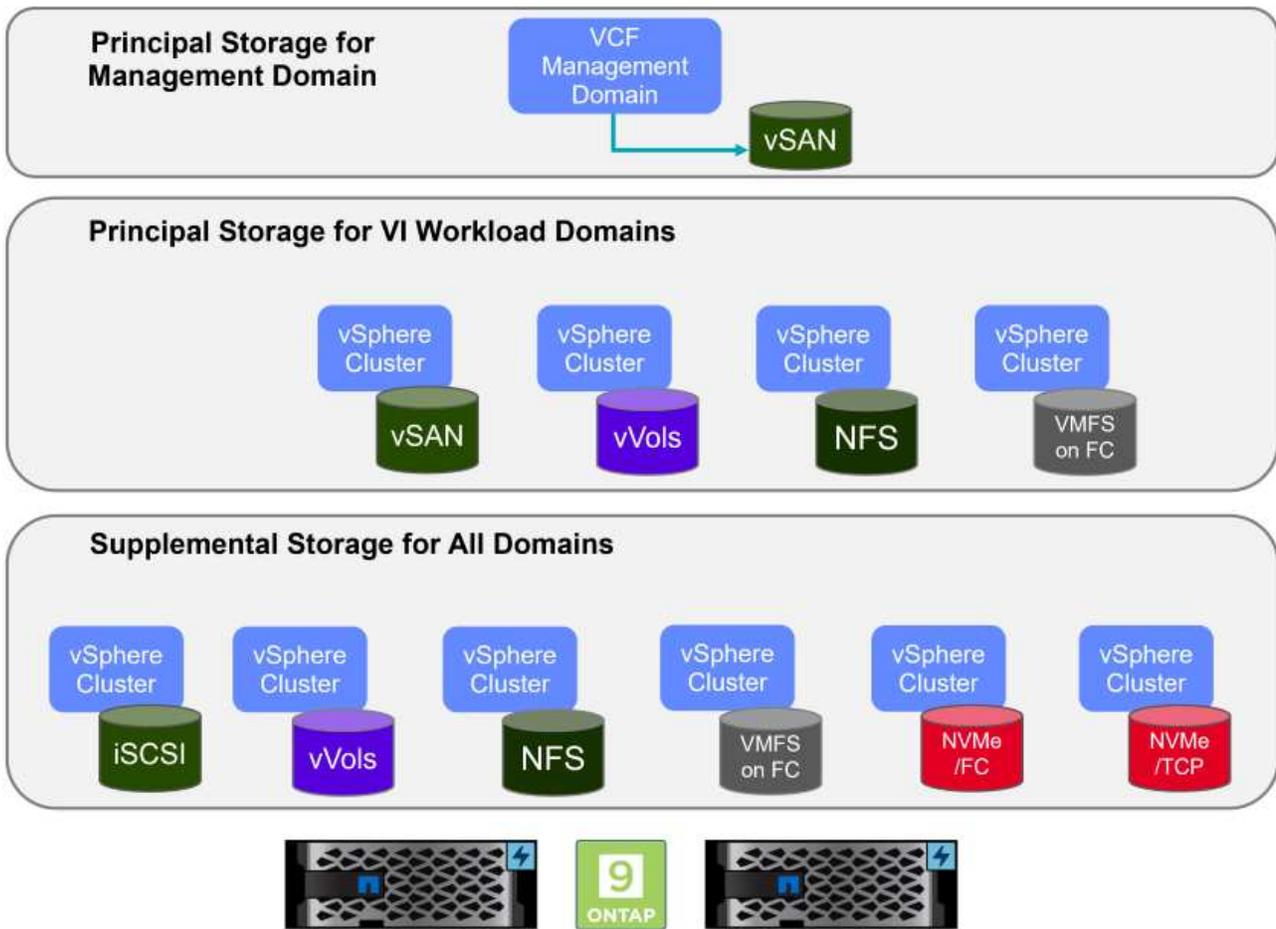
VCF se compone de un único dominio de gestión y hasta 24 dominios de carga de trabajo VI que representan una unidad de infraestructura lista para aplicaciones. Un dominio de carga de trabajo se compone de uno o más clústeres de vSphere que gestiona una única instancia de vCenter.



Para obtener más información sobre la arquitectura y planificación de VCF, consulte "[Modelos de arquitectura y tipos de dominio de carga de trabajo en VMware Cloud Foundation](#)".

Opciones de almacenamiento de VCF

VMware divide las opciones de almacenamiento para VCF en almacenamiento **principal** y **suplementario**. El dominio de gestión VCF debe utilizar vSAN como su almacenamiento principal. Sin embargo, hay muchas opciones de almacenamiento suplementarias para el dominio de gestión y las opciones de almacenamiento principal y suplementario disponibles para los dominios de carga de trabajo VI.



Almacenamiento principal para dominios de carga de trabajo

Almacenamiento principal se refiere a cualquier tipo de almacenamiento que se puede conectar directamente a un dominio de carga de trabajo VI durante el proceso de configuración dentro de SDDC Manager. El almacenamiento principal es el primer almacén de datos configurado para un dominio de carga de trabajo e incluye vSAN, vVols (VMFS), NFS y VMFS en Fibre Channel.

Almacenamiento suplementario para dominios de gestión y carga de trabajo

El almacenamiento complementario es el tipo de almacenamiento que se puede añadir a los dominios de las cargas de trabajo o gestión en cualquier momento una vez que se ha creado el clúster. El almacenamiento complementario representa la gama más amplia de opciones de almacenamiento compatibles, que son compatibles con las cabinas de NetApp AFF.

Recursos de documentación adicionales para VMware Cloud Foundation:

- * ["Documentación de VMware Cloud Foundation"](#)
- * ["Tipos de almacenamiento compatibles para VMware Cloud Foundation"](#)
- * ["Gestión del almacenamiento en VMware Cloud Foundation"](#)

Cabinas de almacenamiento all-flash de NetApp

Las cabinas de NetApp AFF (All Flash FAS) son soluciones de almacenamiento de alto rendimiento diseñadas para aprovechar la velocidad y la eficiencia de la tecnología flash. Las cabinas de AFF incorporan funciones de gestión de datos integradas, como backups basados en Snapshot, replicación, thin provisioning y funcionalidades de protección de datos.

Las cabinas NetApp AFF utilizan el sistema operativo de almacenamiento ONTAP y ofrecen compatibilidad integral con protocolos de almacenamiento para todas las opciones de almacenamiento compatibles con VCF, todo ello en una arquitectura unificada.

Las cabinas de almacenamiento NetApp AFF están disponibles en los Sistemas C-Series basados en flash de mayor rendimiento, A-Series y QLC. Ambas series usan unidades flash NVMe.

Para obtener más información sobre las cabinas de almacenamiento NetApp AFF A-Series, consulte la "[AFF A-Series de NetApp](#)" página de destino.

Para obtener más información sobre las cabinas de almacenamiento C-Series de NetApp, consulte la "[NetApp AFF C-Series](#)" página de destino.

Herramientas de ONTAP de NetApp para VMware vSphere

ONTAP Tools para VMware vSphere (OTV) permite a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Las herramientas de ONTAP también incluyen un proveedor de API de VMware vSphere para el conocimiento del almacenamiento (VASA)* para sistemas de almacenamiento de ONTAP que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidades de almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

Para obtener más información sobre las herramientas de NetApp ONTAP, consulte la "[Herramientas de ONTAP para documentación de VMware vSphere](#)" página.

Descripción general de la solución

En los escenarios presentados en esta documentación, demostraremos cómo utilizar los sistemas de almacenamiento de ONTAP como almacenamiento principal para las implementaciones de dominio de carga de trabajo VCF VI. Además, instalaremos y utilizaremos ONTAP Tools para VMware vSphere para configurar almacenes de datos complementarios para Dominios de carga de trabajo de VI.

Escenarios cubiertos en esta documentación:

- **Configure y use un almacén de datos NFS como almacenamiento principal durante la implementación del dominio de carga de trabajo VI.** Haga clic "[aquí](#)" para pasos de despliegue.
- **Instale y demuestre el uso de las herramientas de ONTAP para configurar y montar almacenes de datos NFS como almacenamiento complementario en dominios de carga de trabajo VI.** Haga clic "[aquí](#)" para pasos de despliegue.

NFS como almacenamiento principal para dominios de cargas de trabajo VI

En este escenario, demostraremos cómo configurar un almacén de datos NFS como almacenamiento principal para la implementación de un dominio de carga de trabajo VI

en VCF. Cuando sea necesario, consultaremos la documentación externa para conocer los pasos que deben realizarse en el SDDC Manager de VCF y cubriremos los pasos específicos de la parte de configuración del almacenamiento.

Autor: Josh Powell, Ravi BCB

Descripción general del escenario

Este escenario cubre los siguientes pasos de alto nivel:

- Verifique las redes de la máquina virtual de almacenamiento (SVM) de ONTAP y de que haya una interfaz lógica (LIF) presente para transportar el tráfico de 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 de ONTAP.
- Cree un pool de redes para el tráfico NFS y vMotion en SDDC Manager.
- Hosts de comisión en VCF para su uso en un dominio de carga de trabajo de VI.
- Implemente un dominio de carga de trabajo de VI en VCF utilizando un almacén de datos NFS como almacenamiento principal.
- Instale el plugin de NetApp NFS para VMware VAAI

Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Sistema de almacenamiento de NetApp AFF con una máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico de NFS.
- La interfaz lógica (LIF) se ha creado en la red IP que es para transportar el tráfico NFS y está asociada con la SVM.
- La puesta en marcha del dominio de gestión de VCF ha finalizado y se puede acceder a la interfaz del administrador de SDDC.
- 4 hosts ESXi configurados para la comunicación en la red de gestión de VCF.
- Direcciones IP reservadas para el tráfico de almacenamiento vMotion y NFS en la VLAN o el segmento de red establecido para este fin.



Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario asegurarse de que 1) la red de gestión se pueda enrutar al servidor NFS o 2) se haya añadido una LIF para la red de gestión a la SVM que aloja el volumen de almacenes de datos NFS, para garantizar que se pueda continuar con la validación.

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

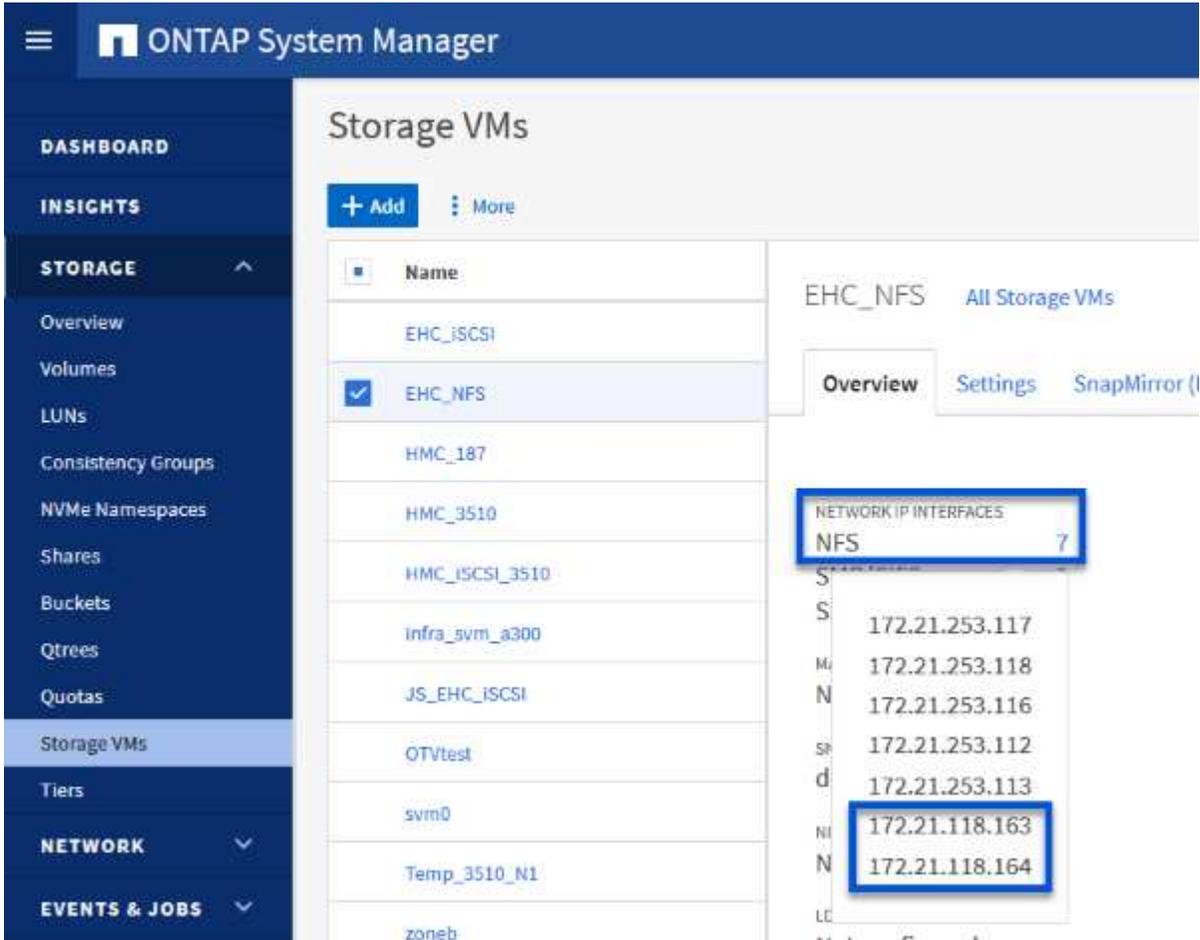
Pasos de despliegue

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

Verifique la conexión a redes de la SVM de ONTAP

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

1. Desde el Administrador del sistema de ONTAP navegue a **VM de almacenamiento** en el menú de la izquierda y haga clic en la SVM que se utilizará para el tráfico NFS. En la pestaña **Overview**, en **NETWORK ip INTERFACES**, haz clic en el valor numérico a la derecha de **nfs**. En la lista, compruebe que aparecen las direcciones IP de LIF necesarias.



The screenshot shows the ONTAP System Manager interface. The left sidebar contains navigation menus for DASHBOARD, INSIGHTS, STORAGE, and NETWORK. The main content area is titled 'Storage VMs' and shows a list of storage virtual machines. The 'EHC_NFS' SVM is selected. The 'Overview' tab is active, and the 'NETWORK IP INTERFACES' section is expanded, showing a list of interfaces with IP addresses. The 'nfs' interface is highlighted, and its associated IP addresses (172.21.118.163 and 172.21.118.164) are circled in blue.

Como alternativa, compruebe las LIF asociadas a una SVM desde la CLI de ONTAP con el siguiente comando:

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

1. Compruebe que los hosts ESXi se puedan comunicar con el servidor NFS de ONTAP. Inicie sesión en el host ESXi mediante SSH y haga ping en el LIF de la SVM:

```
vmkping <IP Address>
```

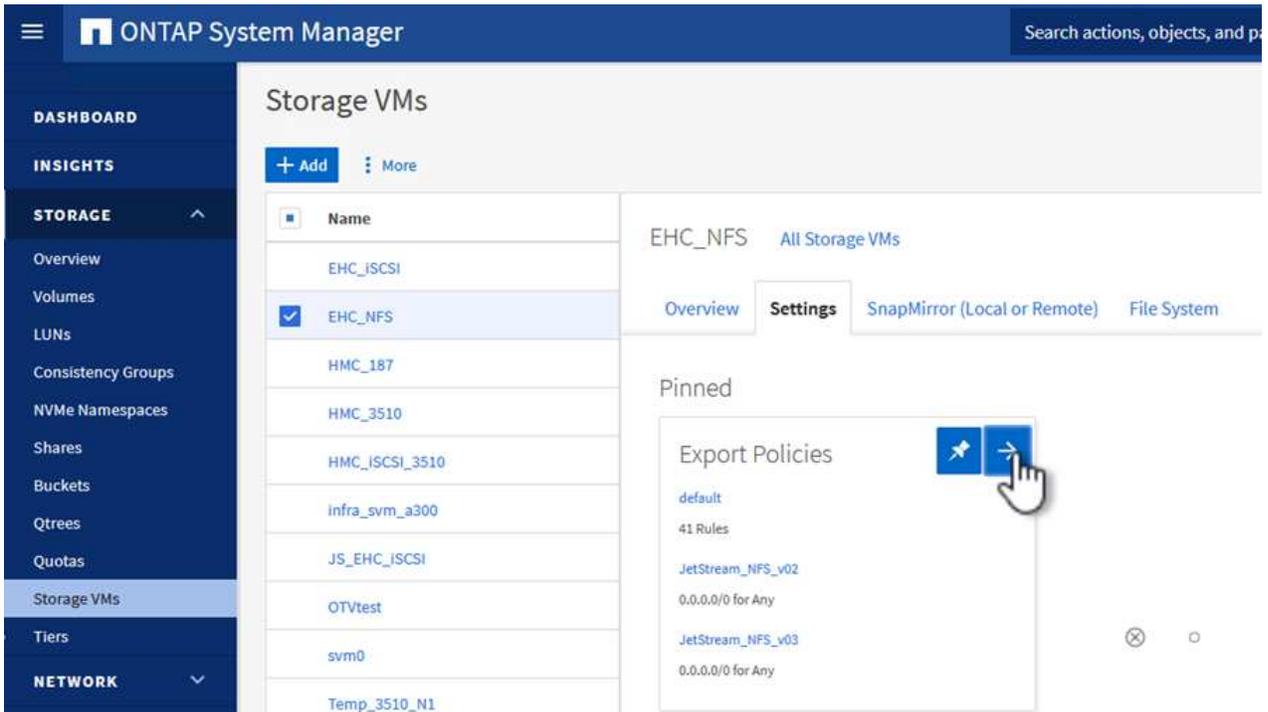


Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario asegurarse de que 1) la red de gestión se pueda enrutar al servidor NFS o 2) se haya añadido una LIF para la red de gestión a la SVM que aloja el volumen de almacenes de datos NFS, para garantizar que se pueda continuar con la validación.

Crear una política de exportación para compartir el volumen NFS

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

1. En el Administrador del sistema de ONTAP, haga clic en **VM 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.

New export policy

NAME

WKLD_DM01

Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

4. Rellene las direcciones IP, el rango de direcciones IP o la red que desee incluir en la regla. Desmarque las casillas **SMB/CIFS** y **FlexCache** y realice selecciones para los detalles de acceso a continuación. Seleccionar los cuadros UNIX es suficiente para el acceso a los hosts ESXi.

New Rule



CLIENT SPECIFICATION

172.21.166.0/24

ACCESS PROTOCOLS

SMB/CIFS

FlexCache

NFS NFSv3 NFSv4

ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All (As anonymous user)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save



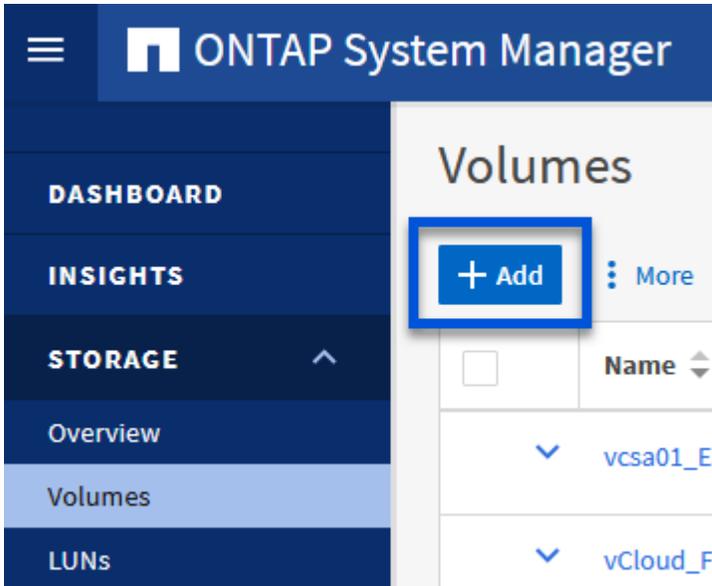
Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario garantizar que la política de exportación incluya la red de gestión de VCF para permitir que la validación continúe.

- Una vez introducidas todas las reglas, haz clic en el botón **Guardar** para guardar la nueva Política de exportación.
- Como alternativa, puede crear políticas y reglas de exportación en la CLI de ONTAP. Consulte los pasos para crear una política de exportación y añadir reglas en la documentación de ONTAP.
 - Utilice la interfaz de línea de comandos de ONTAP para "[Cree una política de exportación](#)".
 - Utilice la interfaz de línea de comandos de ONTAP para "[Añada una regla a una política de exportación](#)".

Crear volumen NFS

Cree un volumen NFS en el sistema de almacenamiento de ONTAP que se utilizará como almacén de datos en la puesta en marcha del dominio de carga de trabajo.

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



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

Add Volume



NAME

VCF_WKLD_01

CAPACITY

5



TiB



STORAGE VM

EHC_NFS



Export via NFS

[More Options](#)

Cancel

Save

3. En Permisos de acceso, seleccione la política de exportación, que incluye la red de gestión VCF o la dirección IP y las direcciones IP de red NFS que se utilizarán para la validación del tráfico NFS Server y NFS.

Access Permissions

Export via NFS

GRANT ACCESS TO HOST

default 

- JetStream_NFS_v04
Clients : 0.0.0.0/0 | Access protocols : Any
- NFSmountTest01
3 rules
- NFSmountTestReno01
Clients : 0.0.0.0/0 | Access protocols : Any
- PerfTestVols
Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS
- TestEnv_VPN
Clients : 172.21.254.0/24 | Access protocols : Any
- VCF_WKLD
2 rules
- WKLD_DM01
2 rules
- Wkld01_NFS
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.252.208

+



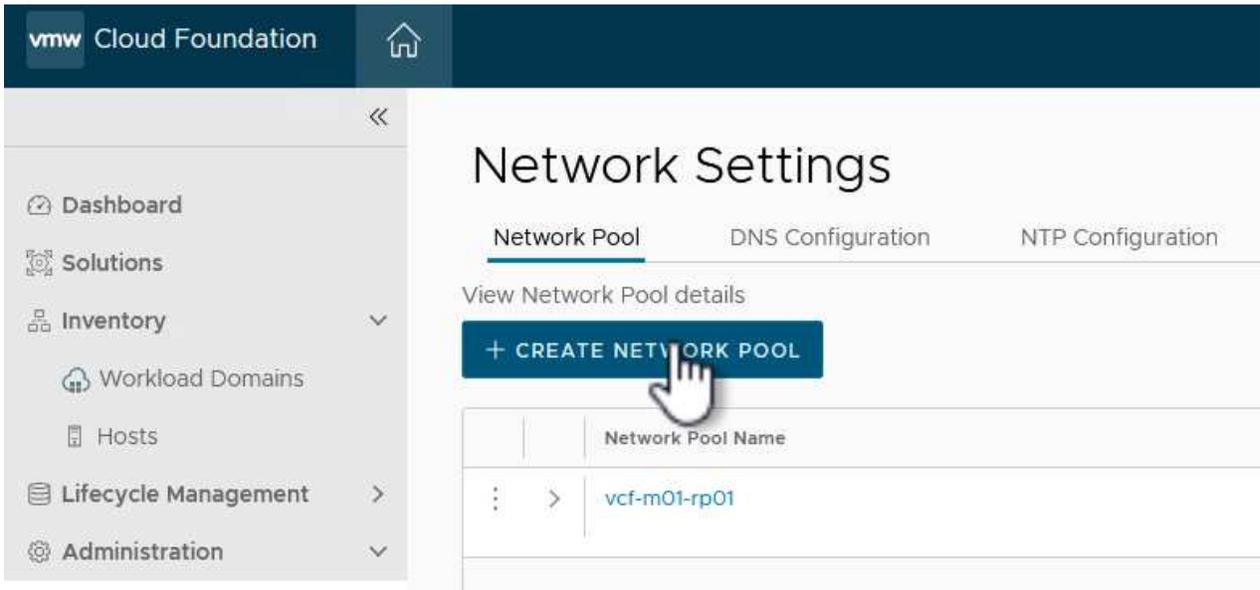
Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario asegurarse de que 1) la red de gestión se pueda enrutar al servidor NFS o 2) se haya añadido una LIF para la red de gestión a la SVM que aloja el volumen de almacenes de datos NFS, para garantizar que se pueda continuar con la validación.

1. Como alternativa, los volúmenes ONTAP se pueden crear en la interfaz de línea de comandos de ONTAP. Para obtener más información, consulte "[lun create](#)" Comando del en la documentación de los comandos de la ONTAP.

Cree un pool de redes en SDDC Manager

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

1. Desde la interfaz web de SDDC Manager, navegue hasta **Network Settings** en el menú de la izquierda y haga clic en el botón **+ Create Network Pool**.



2. Rellene un nombre para el pool de redes, seleccione la casilla de verificación para NFS y rellene todos los detalles de redes. Repita esto para la información de red de vMotion.

vmw Cloud Foundation

Network Settings

Network Pool DNS Configuration NTP Configuration

Create Network Pool

Ensure that all required networks are selected based on their usage for workload domains.

Network Pool Name NFS_NPOOL

Network Type vSAN NFS iSCSI vMotion

NFS Network Information

VLAN ID	<u>3374</u>
MTU	<u>9000</u>
Network	<u>172.21.118.0</u>
Subnet Mask	<u>255.255.255.0</u>
Default Gateway	<u>172.21.118.1</u>

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

<u>172.21.118.145</u>	To	<u>172.21.118.148</u>	REMOVE
<u>xxx.xxx.xxx.xxx</u>	To	<u>xxx.xxx.xxx.xxx</u>	ADD

vMotion Network Information

VLAN ID	<u>3423</u>
MTU	<u>9000</u>
Network	<u>172.21.167.0</u>
Subnet Mask	<u>255.255.255.0</u>
Default Gateway	<u>172.21.167.1</u>

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

<u>172.21.167.121</u>	To	<u>172.21.167.124</u>	REMOVE
<u>xxx.xxx.xxx.xxx</u>	To	<u>xxx.xxx.xxx.xxx</u>	ADD

[CANCEL](#) [SAVE](#)

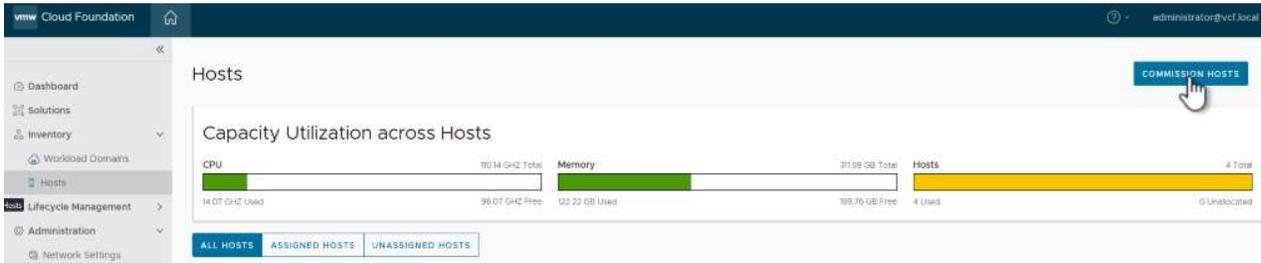
3. Haga clic en el botón **Guardar** para completar la creación del grupo de redes.

Anfitriones de comisión

Para que los hosts ESXi puedan implementarse como dominio de carga de trabajo, deben agregarse al inventario de SDDC Manager. Esto implica proporcionar la información requerida, pasar la validación e iniciar el proceso de puesta en marcha.

Para obtener más información, consulte "[Anfitriones de comisión](#)" En la Guía de administración de VCF.

1. Desde la interfaz del Administrador de SDDC navega a **HOSTS** en el menú de la izquierda y haz clic en el botón **COMISION HOSTS**.



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

Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

- Select All**
- Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- Host is configured with DNS server for forward and reverse lookup and FQDN.
- Hostname should be same as the FQDN.
- Management IP is configured to first NIC port.
- Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- Host hardware health status is healthy without any errors.
- All disk partitions on HDD / SSD are deleted.
- Ensure required network pool is created and available before host commissioning.
- Ensure hosts to be used for VSAN workload domain are associated with VSAN enabled network pool.
- Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

CANCEL

PROCEED

3. En la ventana **Host Addition and Validation**, rellene el **Host FQDN**, **Storage Type**, el nombre **Network Pool** que incluye las direcciones IP de almacenamiento vMotion y NFS que se utilizarán para el dominio de carga de trabajo y las credenciales para acceder al host ESXi. Haga clic en **Add** para agregar el host al grupo de hosts que se van a validar.

Host Addition and Validation

▼ Add Hosts

You can either choose to add host one at a time or download [JSON](#) template and perform bulk commission.

Add new Import

Host FQDN

Storage Type vSAN NFS VMFS on FC vVol

Network Pool Name ⓘ

User Name

Password ⓘ



Hosts Added

✓ Hosts added successfully. Add more or confirm fingerprint and validate host

REMOVE

Confirm all Finger Prints ⓘ

VALIDATE ALL

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status ⓘ
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 ⓘ	172.21.166.135	✗ SHA256:CKbsinf EOG+Hz/ lpFUoFDI2tLuY FZ47WicVdp6v EGM	⊖ Not Validated

1 hosts

CANCEL

NEXT

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

Hosts Added

✔ Host Validated Successfully. ✕

REMOVE Confirm all Finger Prints (i) VALIDATE ALL

<input checked="" type="checkbox"/>	FGDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01 (i)	172.21.166.138	✔ SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	✔ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01 (i)	172.21.166.137	✔ SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2IOWZDPFH+z0	✔ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01 (i)	172.21.166.136	✔ SHA256:AMhyR60OpTQ1YYq0DJhqVbj/M/GvrQaqUy7Ce+M4IWY	✔ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 (i)	172.21.166.135	✔ SHA256:CKbsinfEOG+ +z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	✔ Valid

CANCEL NEXT

6. Revise la lista de hosts a los que se va a poner en servicio y haga clic en el botón **Comisión** para iniciar el proceso. Supervise el proceso de puesta en marcha desde el panel Tarea del gestor 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

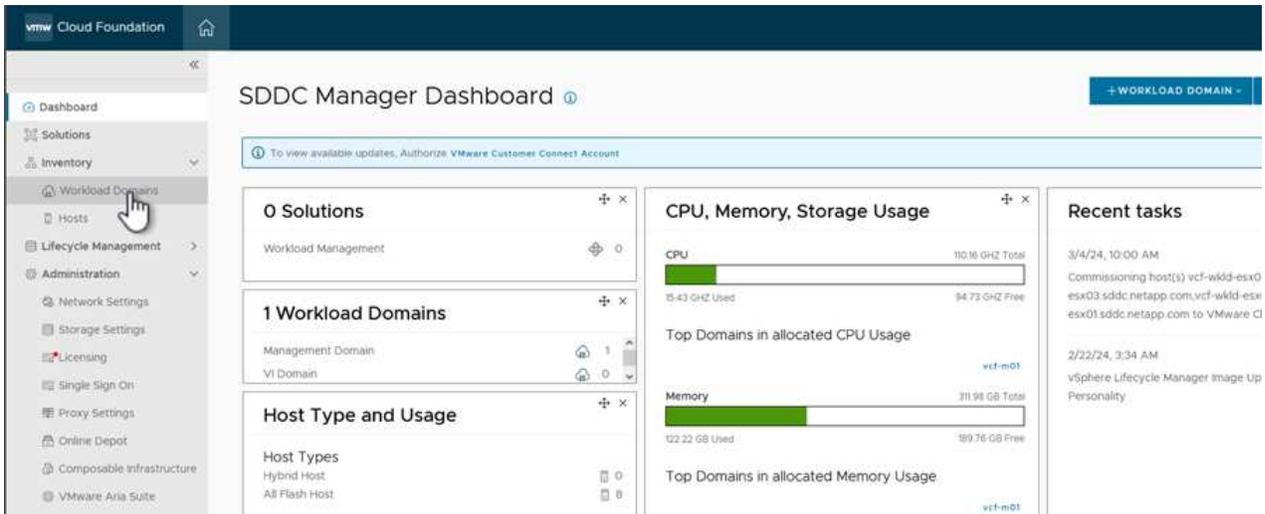
COMMISSION

Desplegar dominio de carga de trabajo VI

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

Para obtener instrucciones detalladas sobre la implementación de un dominio de carga de trabajo de VI, consulte ["Despliegue un dominio de carga de trabajo de VI mediante la interfaz de usuario de SDDC Manager"](#).

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



2. En el asistente de configuración VI, rellene las secciones de **Información general**, **Cluster**, **Compute**, **Networking** y **Selección de host** según sea necesario.

Para obtener información sobre cómo rellenar la información necesaria en el Asistente de configuración de VI, consulte ["Despliegue un dominio de carga de trabajo de VI mediante la interfaz de usuario de SDDC Manager"](#).

VI Configuration

1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

7 Switch Configuration

8 License

9 Review

+

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

The screenshot shows the 'VI Configuration' interface with a sidebar on the left containing a list of steps: 1 General Info, 2 Cluster, 3 Compute, 4 Networking, 5 Host Selection, 6 NFS Storage (highlighted), 7 Switch Configuration, 8 License, and 9 Review. The main content area is titled 'NFS Storage' and contains the 'NFS Share Details' section. This section has three input fields: 'Datastore Name' with the value 'VCF_WKLD_01', 'Folder' with the value '/VCF_WKLD_01', and 'NFS Server IP Address' with the value '172.21.118.163'. Each field has an information icon (i) to its right.

2. En el asistente de configuración de VI, complete los pasos de configuración y licencia del switch y, a continuación, haga clic en * Finalizar * para iniciar el proceso de creación del dominio de carga de trabajo.

VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage
- 7 Switch Configuration
- 8 License
- 9 Review**

Review

General

Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain

Cluster

Cluster Name	IT-INF-WKLD-01
--------------	----------------

Compute

vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1

Networking

NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxc101.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

CANCEL BACK **FINISH**

3. Supervise el proceso y resuelva los problemas de validación que surjan durante el proceso.

Instale el plugin de NetApp NFS para VMware VAAI

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

Para obtener instrucciones paso a paso sobre la puesta en marcha del plugin de NFS de NetApp para VMware VAAI siga las instrucciones en "[Instale el plugin de NetApp NFS para VMware VAAI](#)".

Demostración en vídeo de esta solución

[Almacenes de datos NFS como almacenamiento principal para dominios de carga de trabajo de VCF](#)

Utilice las herramientas de ONTAP para configurar almacenamiento complementario (NFS y vVols) para los dominios de carga de trabajo de VCF

En este escenario, mostraremos cómo implementar y usar las herramientas de ONTAP para VMware vSphere para configurar un **almacén de datos NFS** y un **vVols datastore** para un dominio de carga de trabajo VCF.

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

Autor: Josh Powell, Ravi BCB

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 de NFS.
- Cree un grupo de puertos distribuidos para la red NFS en el dominio de carga de trabajo de VI.
- Cree un adaptador vmkernel para NFS en los hosts ESXi para el dominio de carga de trabajo VI.
- Implemente las herramientas de ONTAP en el dominio de la carga de trabajo de VI.
- Cree un nuevo almacén de datos NFS en el dominio de carga de trabajo de VI.
- Cree un nuevo almacén de datos vVols en el dominio de carga de trabajo de VI.

Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP AFF con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.
- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.
- Se ha desplegado anteriormente un dominio de carga de trabajo de VI.

NetApp recomienda diseños de red redundantes para NFS, lo que proporciona tolerancia a fallos para sistemas de almacenamiento, switches, adaptadores de red y sistemas host. Es común poner en marcha NFS con una única subred o varias subredes, en función de los requisitos de la arquitectura.

Consulte "[Prácticas recomendadas para ejecutar NFS con VMware vSphere](#)" Para obtener información detallada específica de VMware vSphere.

Para obtener orientación de red sobre el uso de ONTAP con VMware vSphere, consulte la "[Configuración de red: NFS](#)" De la documentación de aplicaciones empresariales de NetApp.

En esta documentación se muestra el proceso de crear una SVM nueva y especificar la información de la dirección IP para crear varias LIF para el tráfico de NFS. Para agregar LIF nuevos a una SVM existente, consulte "[Crear una LIF \(interfaz de red\)](#)".

Pasos de despliegue

Para implementar las herramientas de ONTAP y utilizarlas para crear un almacén de datos vVols y NFS en el dominio de gestión de VCF, lleve a cabo los siguientes pasos:

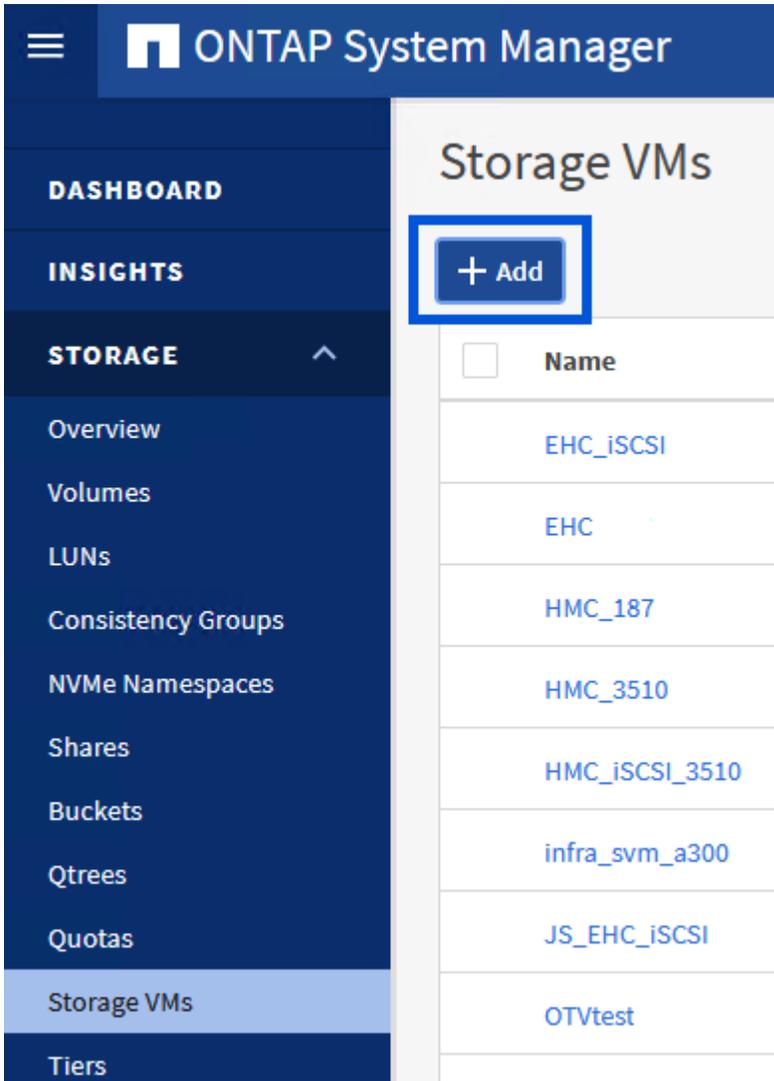
Crear SVM y LIF en el sistema de almacenamiento ONTAP

El siguiente paso se lleva a cabo en ONTAP System Manager.

Crear la máquina virtual de almacenamiento y las LIF

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

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



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

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



No es necesario marcar el botón **Permitir acceso al cliente NFS** aquí, ya que se utilizarán herramientas de ONTAP para VMware vSphere para automatizar el proceso de implementación del almacén de datos. Esto incluye proporcionar acceso de cliente para los hosts ESXi.

Y n.o 160;

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes o utilizar una configuración independiente.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

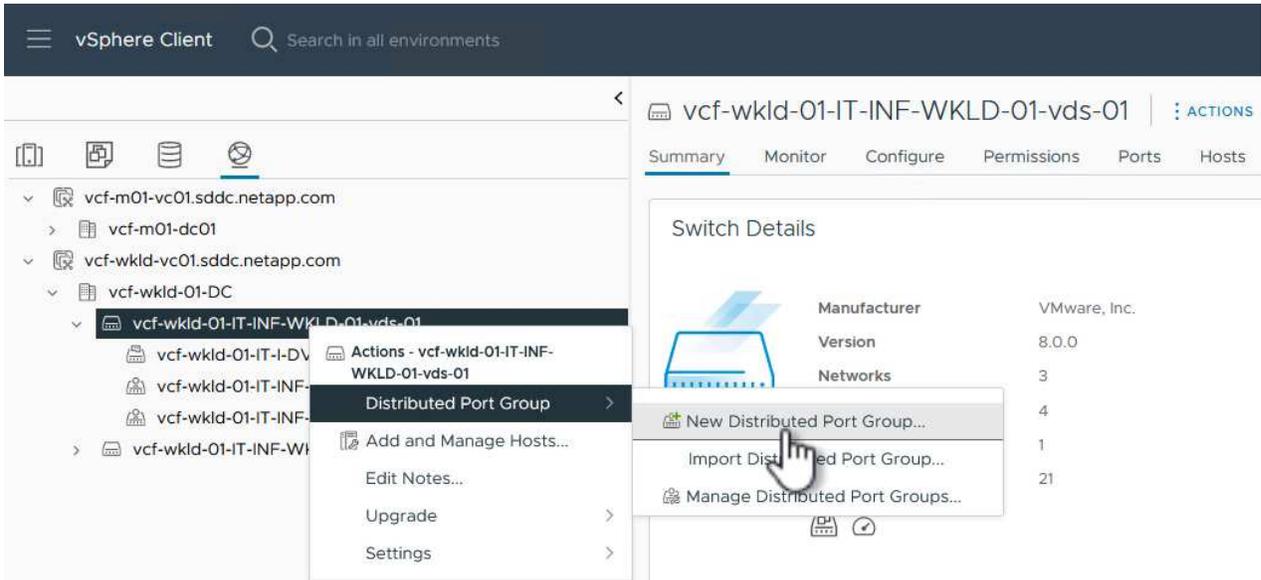
Configure las redes para NFS en los hosts ESXi

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

Cree 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 el tráfico NFS:

1. En el cliente vSphere , desplácese hasta **Inventory > Networking** para el dominio de la carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos....**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

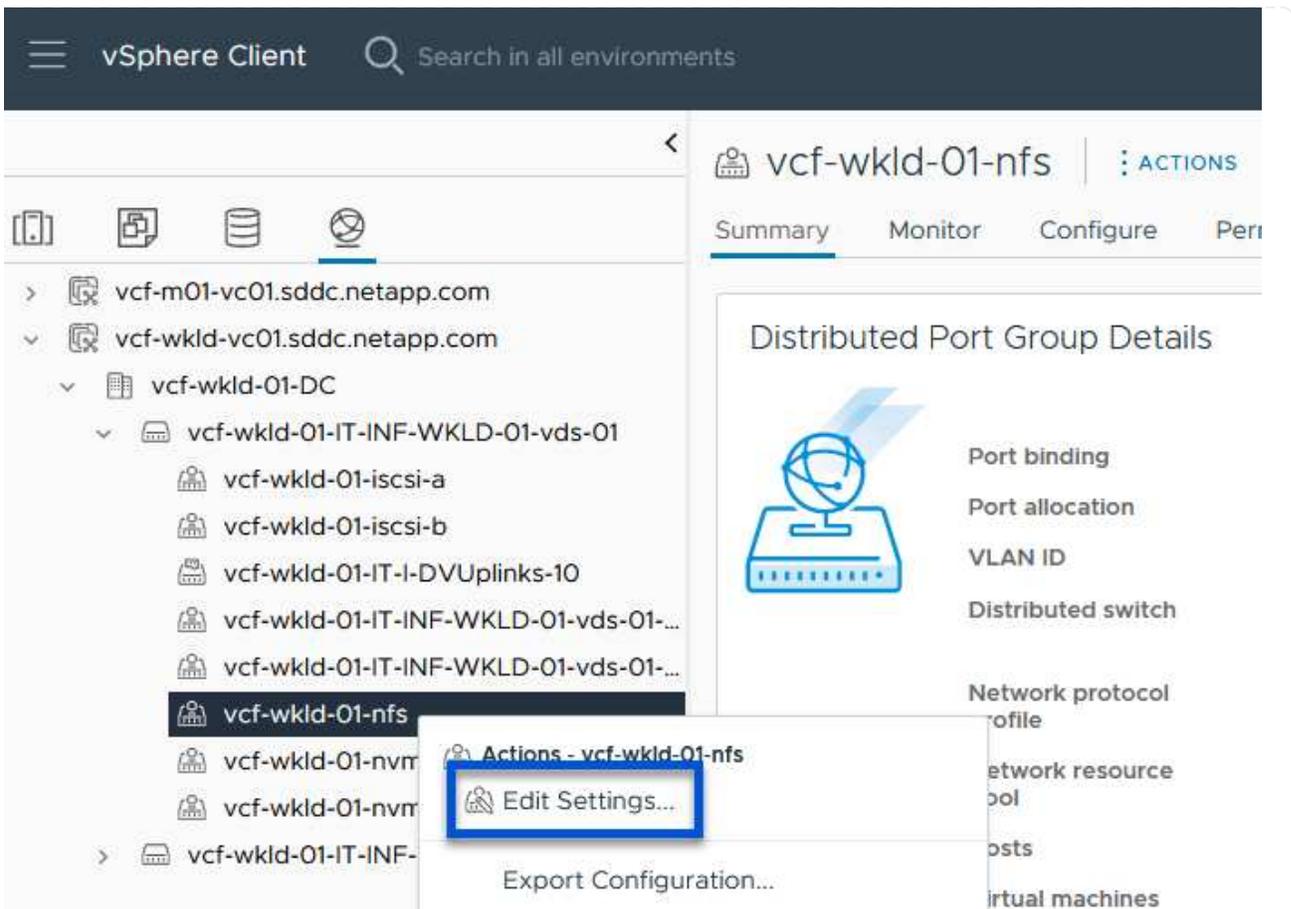
Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

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 en **Editar configuración....**



6. En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda. Habilite el trabajo en equipo 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 hacia abajo a **Uplinks no utilizados**.

Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port 

Network failure detection

Link status only 

Notify switches

Yes 

Failback

Yes 

Failover order 

MOVE UP MOVE DOWN

Active uplinks

 uplink2

 uplink1

Standby uplinks

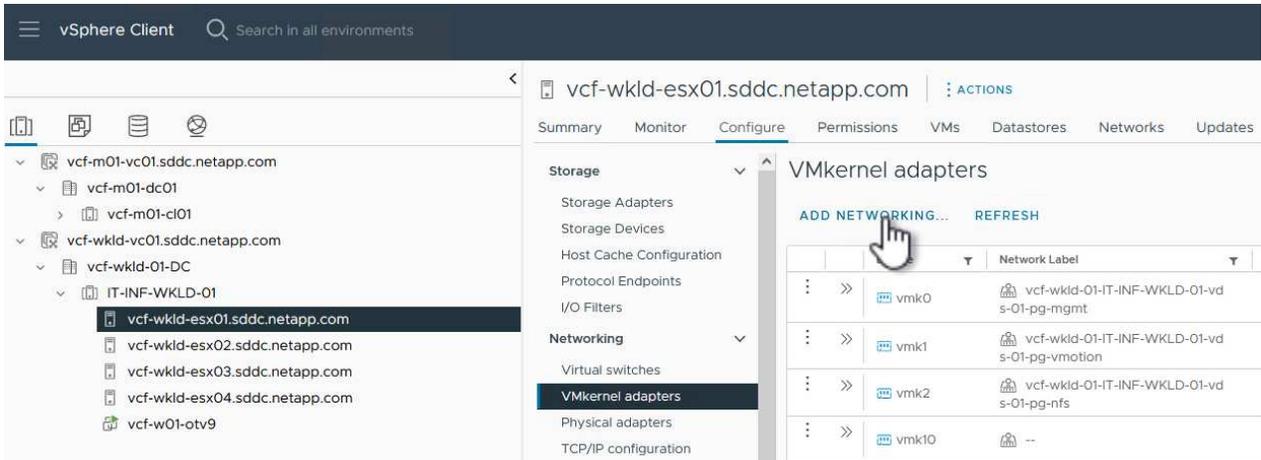
Unused uplinks

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

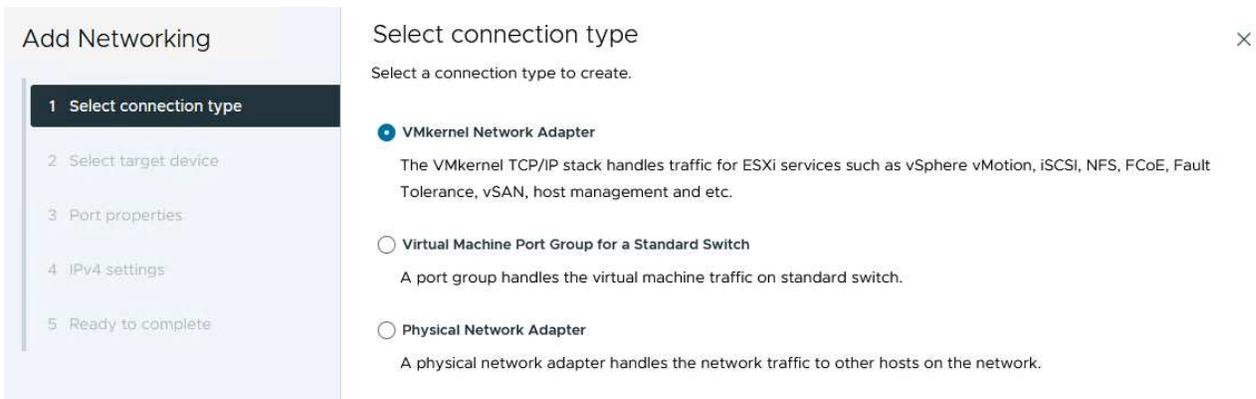
Crear un adaptador de VMkernel en cada host ESXi

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

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de la carga de trabajo. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** 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.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 8 items

CANCEL

BACK

NEXT

4. En la página **Propiedades del puerto**, mantenga los valores predeterminados (no hay servicios habilitados) y haga clic en **Siguiente** para continuar.
5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
- Use static IPv4 settings

IPv4 address 172.21.118.145

Subnet mask 255.255.255.0

Default gateway Override default gateway for this adapter

172.21.166.1

DNS server addresses 10.61.185.231

CANCEL

BACK

NEXT

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings
- Ready to complete**

Ready to complete ✕

Review your selections before finishing the wizard

▼ **Select target device**

Distributed port group	vcf-wkld-01-nfs
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ **Port properties**

New port group	vcf-wkld-01-nfs (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled

CANCEL **BACK** **FINISH**

Pon en marcha y utiliza herramientas de ONTAP para configurar el almacenamiento

Los siguientes pasos se realizan en el clúster de dominio de gestión de VCF mediante el cliente vSphere e implican la puesta en marcha de OTV, la creación de un almacén de datos NFS vVols y la migración de equipos virtuales de gestión al nuevo almacén de datos.

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

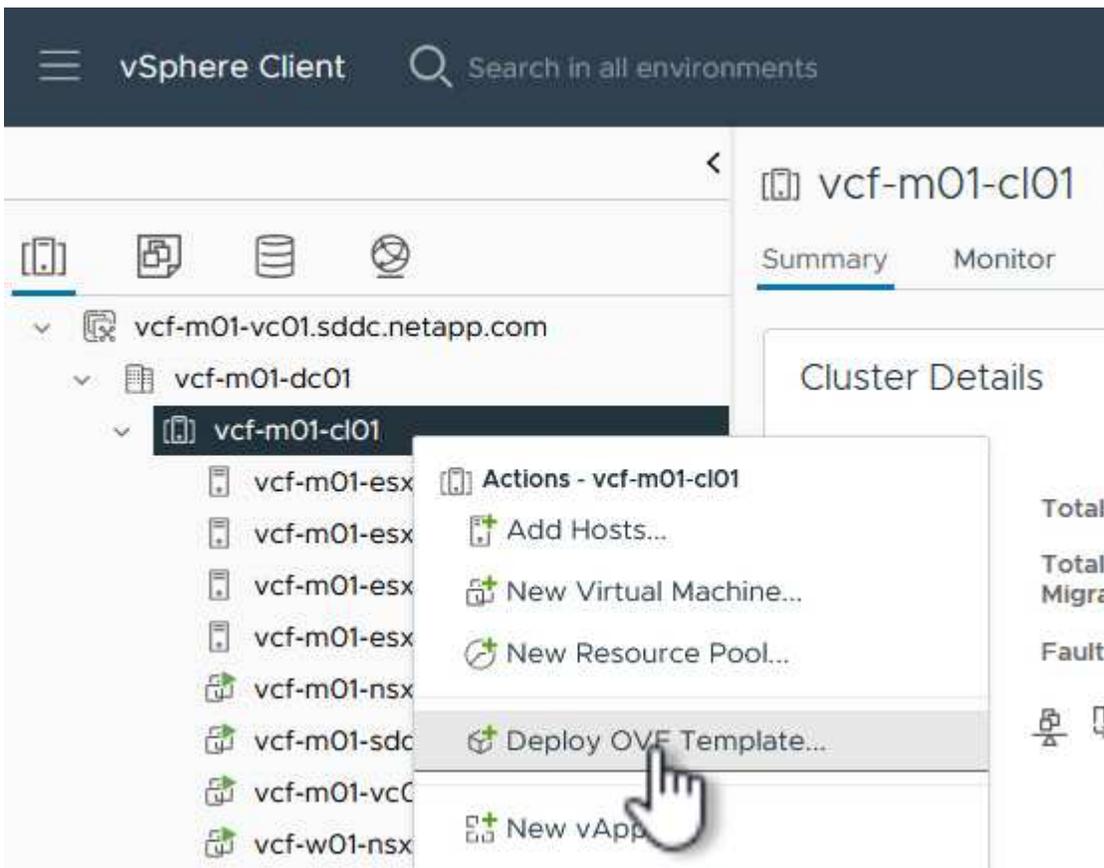
Para obtener información adicional sobre la puesta en marcha y el uso de las herramientas de ONTAP en un entorno múltiple de vCenter, consulte ["Requisitos para registrar herramientas de ONTAP en varios entornos de vCenter Server"](#).

Ponga en marcha herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware vSphere (OTV) se ponen en marcha como dispositivo de máquina virtual y proporcionan una interfaz de usuario integrada de vCenter para gestionar el almacenamiento de ONTAP.

Complete lo siguiente para poner en marcha herramientas de ONTAP para VMware vSphere:

1. Obtenga la imagen OVA de las herramientas de ONTAP de la "[Sitio de soporte de NetApp](#)" y descárguelo a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de gestión 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 de **Desplegar plantilla OVF** haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de herramientas ONTAP descargado en el paso anterior.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vmware-9.13-9554.ova

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

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

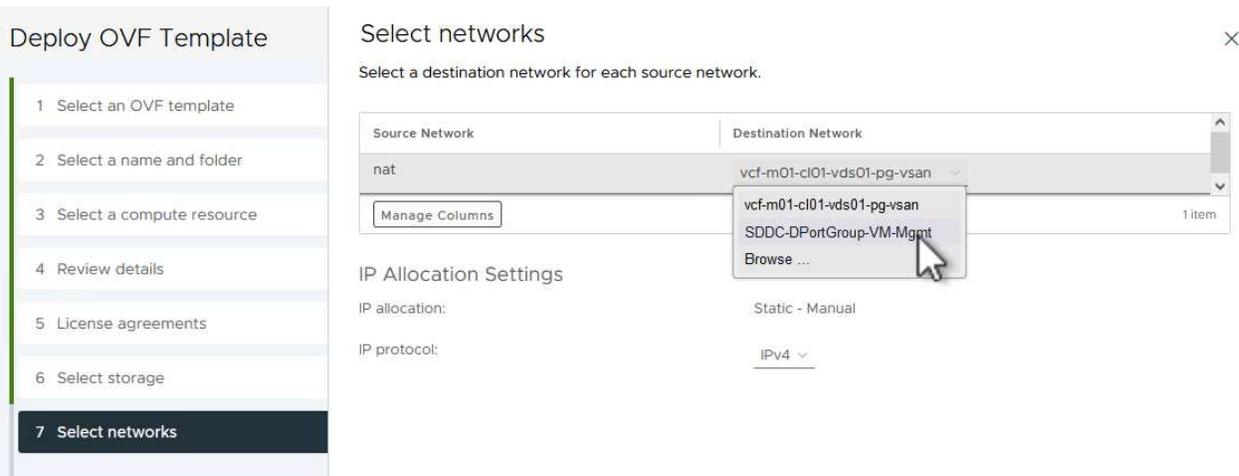
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns Items per page 10 5 items

7. En la página Seleccionar red, seleccione la red que se utiliza para el tráfico de gestión.



8. En la página Personalizar plantilla, rellene toda la información necesaria:

- 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 **Enable 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 necesarios.

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.

! 2 properties have invalid values X

System Configuration		4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.	
	Password 👁
	Confirm Password 👁
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1	
Maintenance User Password (*)	Password to assign to maint user account.	
	Password 👁
	Confirm Password 👁

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

! 2 properties have invalid values X

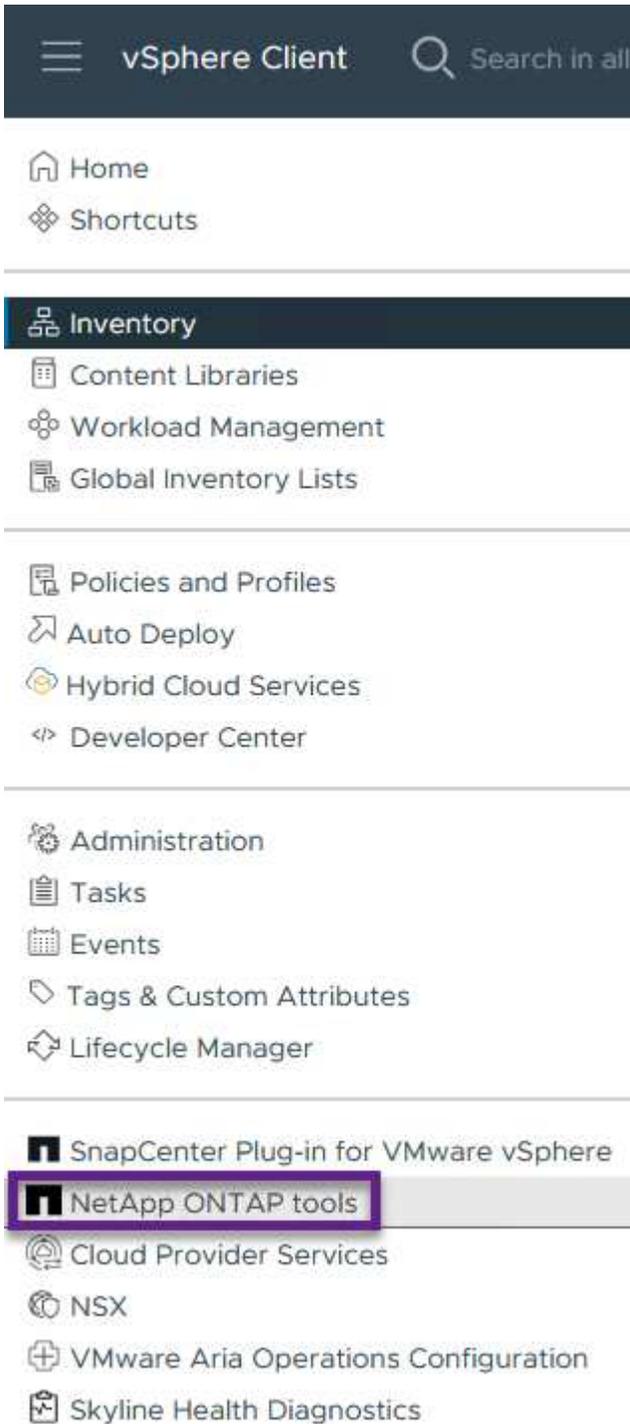
Configure vCenter or Enable vCenter		3 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>	
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com	
Port (*)	Specify the HTTPS port of an existing vCenter to register to. 443	
Username (*)	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
Password (*)	Specify the password of an existing vCenter to register to.	
	Password 👁
	Confirm Password 👁
Network Properties		8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9	
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

CANCEL BACK NEXT

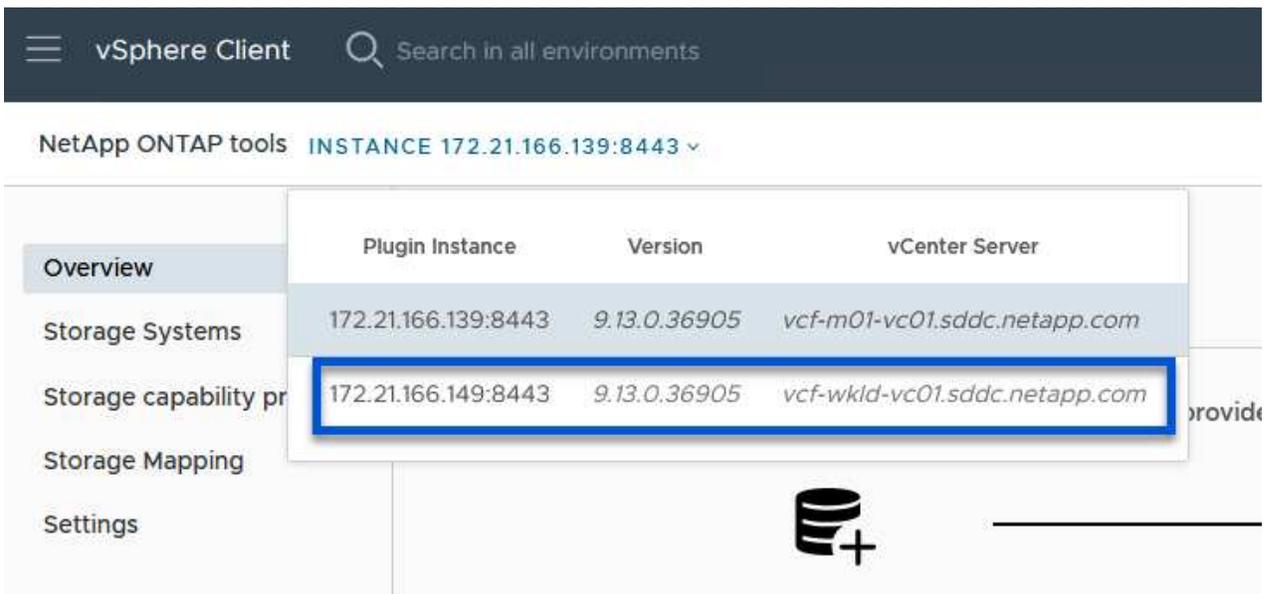
9. Revise toda la información en la página Listo para completar y haga clic en Finalizar para comenzar a desplegar el dispositivo OTV.

Agregar un sistema de almacenamiento a las herramientas de ONTAP.

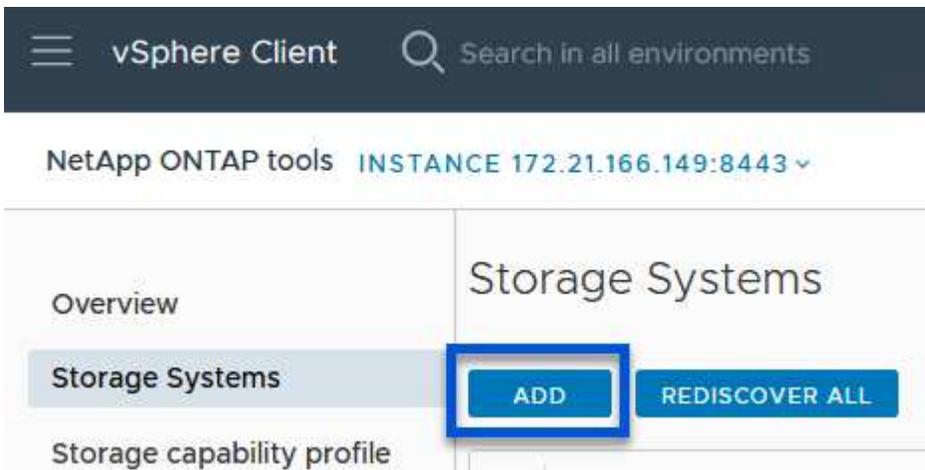
1. Acceda a herramientas de NetApp ONTAP seleccionándolo en el menú principal del vSphere Client.



2. En el menú desplegable **INSTANCE** de la interfaz de la herramienta ONTAP, seleccione la instancia OTV asociada al dominio de carga de trabajo que se va a gestionar.



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



4. Rellene la dirección IP, las credenciales del sistema de almacenamiento y el número de puerto. Haga clic en **Add** 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

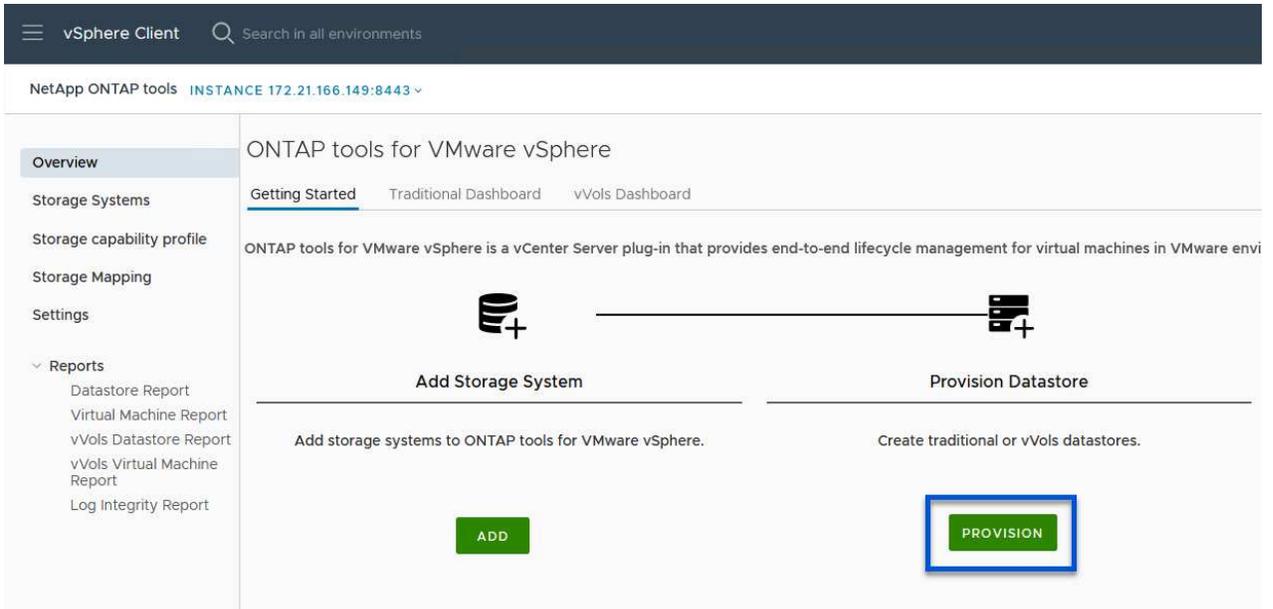
SAVE & ADD MORE

ADD

Cree un almacén de datos NFS en Herramientas de ONTAP

Complete los siguientes pasos para implementar un almacén de datos de ONTAP, en ejecución en NFS, mediante las herramientas de ONTAP.

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



2. En la página **General** del asistente New Datastore, seleccione el centro de datos de vSphere o el destino del clúster. Seleccione **nfs** como tipo de almacén de datos, rellene un nombre para el almacén de datos y seleccione el protocolo. Elija si desea usar volúmenes de FlexGroup y si desea usar un archivo de funcionalidad de almacenamiento para el aprovisionamiento. Haga clic en **Siguiente** para continuar.

Nota: Si selecciona **Distribuir datos de almacén de datos a través del clúster**, se creará el volumen subyacente como un volumen FlexGroup que impide el uso de perfiles de capacidad de almacenamiento. Consulte "[Configuraciones para volúmenes de FlexGroup admitidas y no compatibles](#)" Para obtener más información sobre el uso de FlexGroup Volumes.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

General

Specify the details of the datastore to provision. 

Provisioning destination: [BROWSE](#)

Type: NFS VMFS vVols

Name:

Size:

Protocol: NFS 3 NFS 4.1

Distribute datastore data across the ONTAP cluster.

Use storage capability profile for provisioning

[Advanced options >](#)

[CANCEL](#)

[NEXT](#)

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profile:

Storage system:

Storage VM:

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Aggregate:

Volumes:

[Advanced options >](#)

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

Aggregate:	FHCAsqr02
------------	-----------

CANCEL

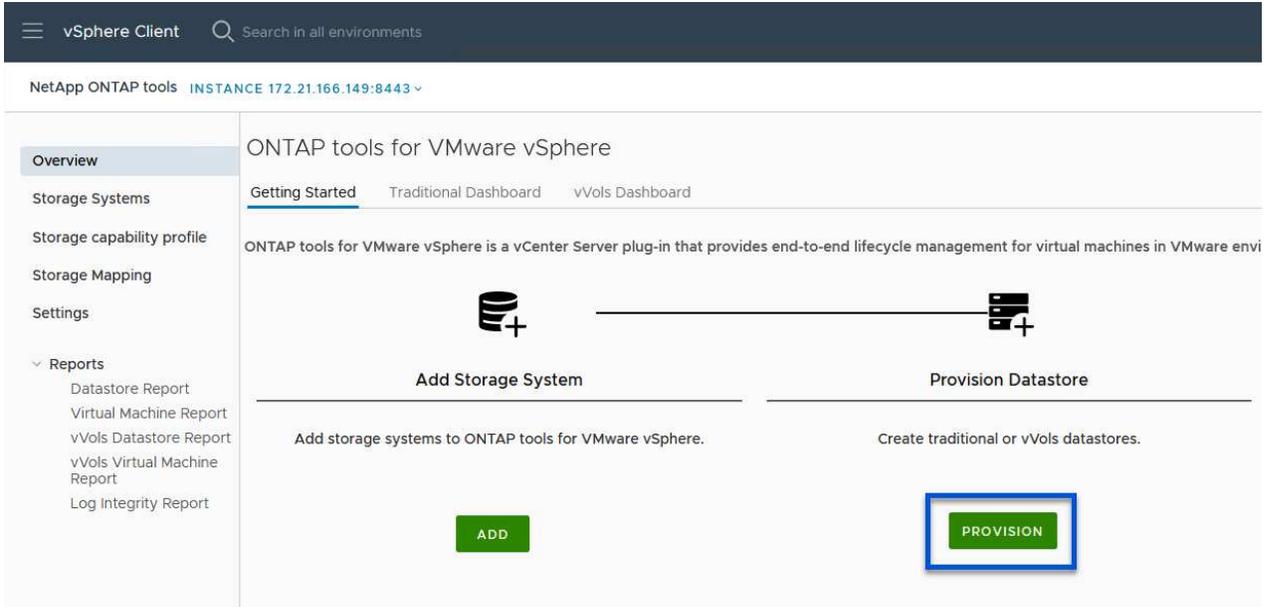
BACK

FINISH

Cree un almacén de datos vVols en Herramientas de ONTAP

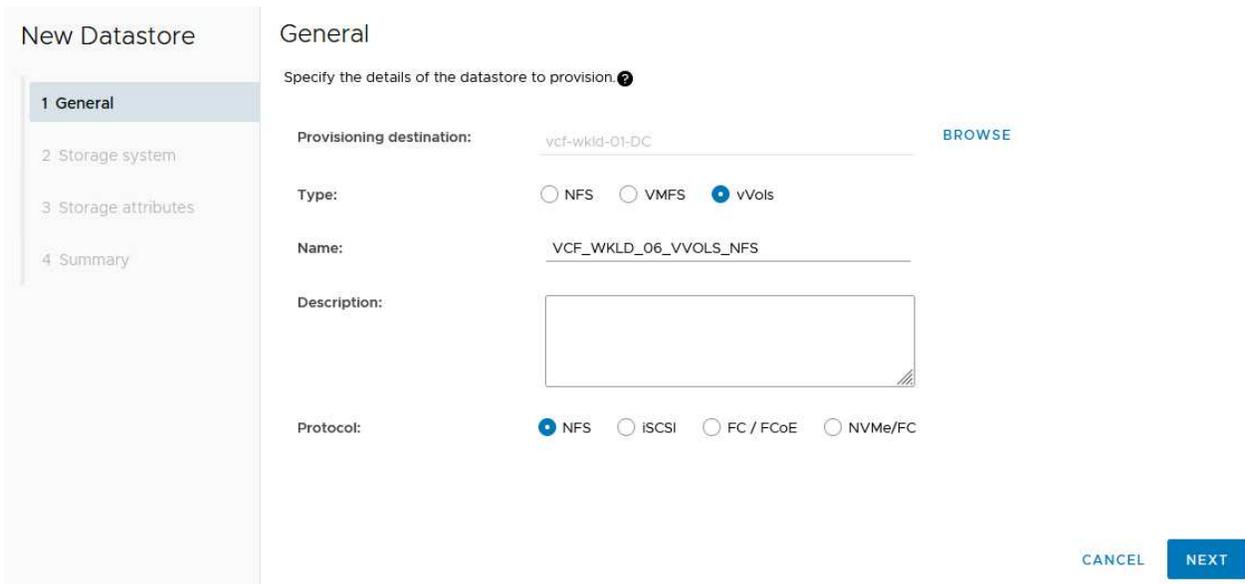
Para crear un almacén de datos vVols en Herramientas de ONTAP, lleve a cabo los siguientes pasos:

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



The screenshot shows the vSphere Client interface. At the top, there is a search bar and the text "vSphere Client". Below that, it says "NetApp ONTAP tools INSTANCE 172.21.166.149:8443". The main content area is titled "ONTAP tools for VMware vSphere" and has three tabs: "Getting Started", "Traditional Dashboard", and "vVols Dashboard". The "Getting Started" tab is active. Below the tabs, there is a description: "ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi". There are two main sections: "Add Storage System" with an "ADD" button, and "Provision Datastore" with a "PROVISION" button. The "PROVISION" button is highlighted with a blue box.

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



The screenshot shows the "New Datastore" wizard in the vSphere Client. The "General" tab is selected. The wizard is titled "Specify the details of the datastore to provision". The "Provisioning destination" is "vcf-wkld-01-DC" with a "BROWSE" button. The "Type" is "vVols" (selected with a radio button). The "Name" is "VCF_WKLD_06_VVOLS_NFS". The "Description" field is empty. The "Protocol" is "NFS" (selected with a radio button). At the bottom right, there are "CANCEL" and "NEXT" buttons.

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profile:	Platinum_AFF_A	▼
Storage system:	ntaphci-a300e9u25 (172.16.9.25)	▼
Storage VM:	VCF_NFS	▼

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

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
<u>vcf_wkld_06_vvc</u>	2000	Platinum_AFF_A	EHCaggr02 - (25404 GB I	Thin

ADD

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
vcf_wkld_06_vvols	2000 GB	Platinum_AFF_A	EHCaggr02

1 - 1 of 1 Item

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
		Platinum_AFF_A	EHCaggr02 - (25407.15 G	Thin

ADD

Default storage capability profile: Platinum_AFF_A

CANCEL

BACK

NEXT

5. Por último, revise el **Summary** y haga clic en **Finish** para iniciar el proceso de creación del almacén de datos de VVol.

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_06_VVOLS_NFS

Datastore type: vVols

Protocol: NFS

Storage capability profile: Platinum_AFF_A

Storage system details

Storage system: ntaphci-a300e9u25

SVM: EHC_NFS

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL
BACK
FINISH

Información adicional

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

Migración de equipos virtuales

Migrar máquinas virtuales a almacenes de datos de ONTAP

Autor: Suresh Thoppay

VMware vSphere de Broadcom es compatible con almacenes de datos VMFS, NFS y VVol para alojar máquinas virtuales. Los clientes tienen la opción de crear estos almacenes de datos con infraestructuras hiperconvergentes o con sistemas de almacenamiento compartido centralizados. Los clientes a menudo ven el valor de alojarse en sistemas de almacenamiento basados en ONTAP para proporcionar copias Snapshot y clones de máquinas virtuales con gestión eficiente del espacio, flexibilidad para elegir varios modelos de implementación en todos los centros de datos y clouds, eficiencia operativa con herramientas de supervisión y alerta, seguridad, gobernanza y herramientas de cumplimiento opcionales para inspeccionar los datos de máquinas virtuales. etc,

Las máquinas virtuales alojadas en almacenes de datos de ONTAP pueden protegerse usando el complemento de SnapCenter para VMware vSphere (SCV). SCV crea copias Snapshot basadas en el almacenamiento y también replica en el sistema de almacenamiento de ONTAP remoto. Las restauraciones se pueden realizar desde sistemas de almacenamiento principales o secundarios.

Los clientes tienen flexibilidad para elegir las operaciones de Cloud Insights o Aria o la combinación de ambas herramientas u otras herramientas de terceros que utilizan la api de ONTAP para solucionar problemas,

supervisar el rendimiento, informar y notificar alertas.

Los clientes pueden aprovisionar fácilmente un almacén de datos con el complemento de herramientas de ONTAP para vCenter o su API y máquinas virtuales se pueden migrar a almacenes de datos de ONTAP incluso aunque se encienda.



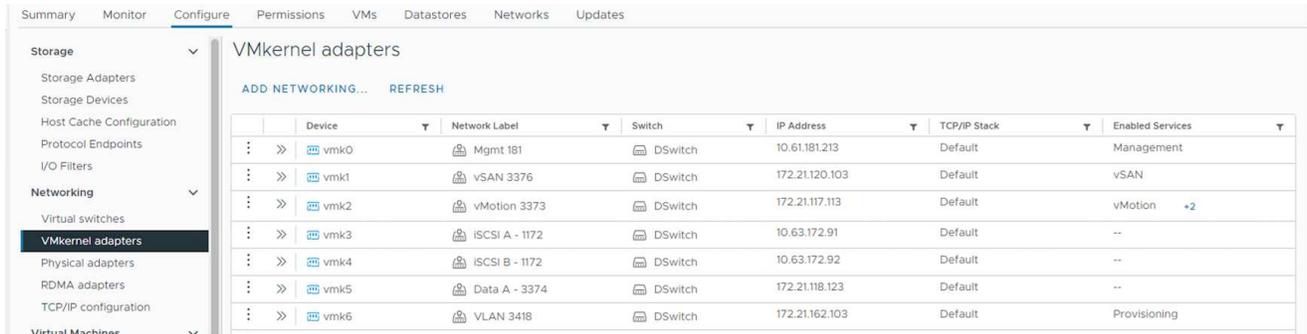
Algunas máquinas virtuales que se ponen en marcha con una herramienta de gestión externa, como Aria Automation, Tanzu (u otros tipos de Kubernetes) dependen normalmente de la política de almacenamiento de máquina virtual. Si se migra entre los almacenes de datos dentro de la misma política de almacenamiento de máquinas virtuales, tendría que reducir el impacto en las aplicaciones. Consulte con los propietarios de aplicaciones para migrar correctamente estas máquinas virtuales a un nuevo almacén de datos. Se ha introducido vSphere 8 ["Notificación de VMotion"](#) Preparar la aplicación para vMotion.

Requisitos de red

Migración de equipos virtuales con vMotion

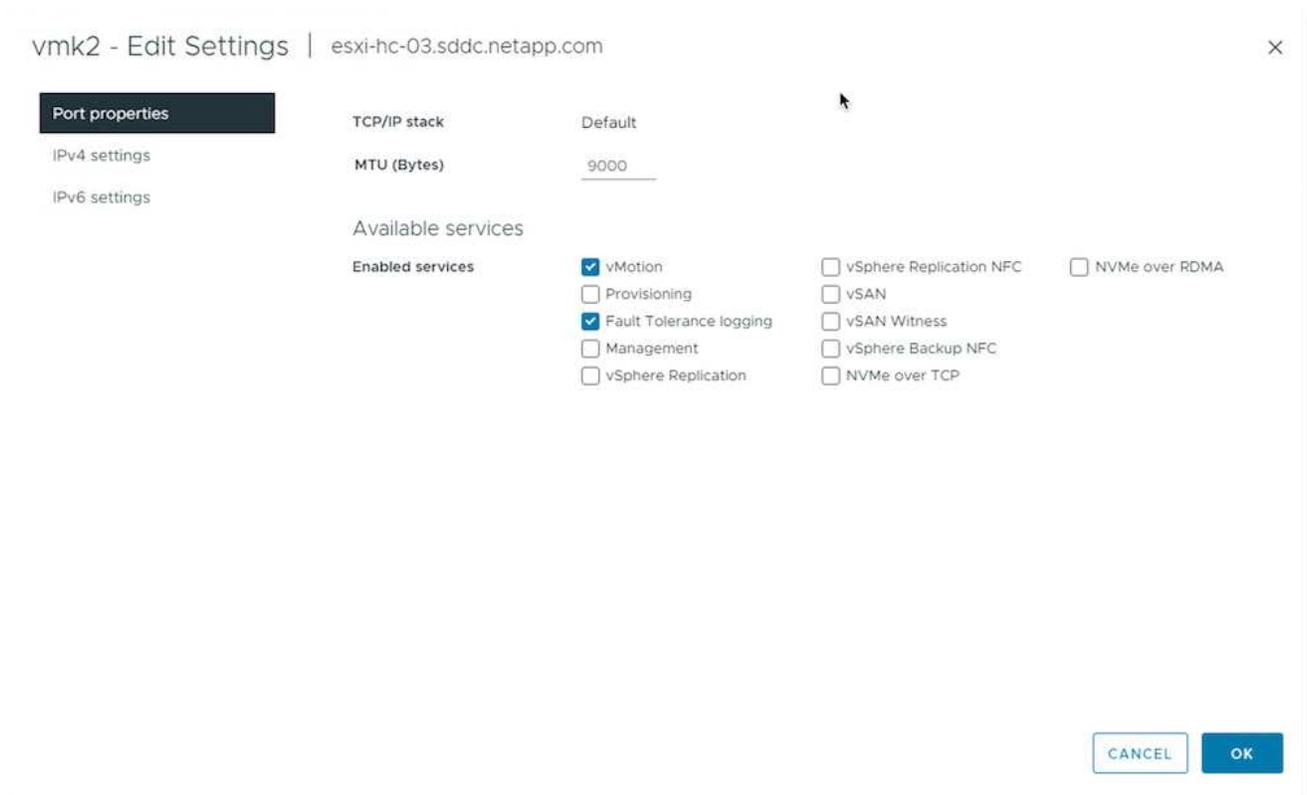
Se asume que ya hay una red de almacenamiento doble para que el almacén de datos de ONTAP proporcione conectividad, tolerancia a fallos y aumento del rendimiento.

La migración de equipos virtuales entre los hosts de vSphere también se realiza mediante la interfaz de VMkernel del host de vSphere. Para la migración en caliente (equipos virtuales con encendido), se utiliza la interfaz de VMkernel con el servicio vMotion y, para la migración en frío (equipos virtuales apagados), se consume la interfaz de VMkernel con el servicio de aprovisionamiento habilitado para trasladar los datos. Si no se encuentra una interfaz válida, utilizará la interfaz de gestión para mover los datos que puede que no sea deseable para ciertos casos prácticos.



Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
vmk0	Mgmt 181	DSwitch	10.61.181.213	Default	Management
vmk1	vSAN 3376	DSwitch	172.21.120.103	Default	vSAN
vmk2	vMotion 3373	DSwitch	172.21.117.113	Default	vMotion +2
vmk3	iSCSI A - 1172	DSwitch	10.63.172.91	Default	--
vmk4	iSCSI B - 1172	DSwitch	10.63.172.92	Default	--
vmk5	Data A - 3374	DSwitch	172.21.118.123	Default	--
vmk6	VLAN 3418	DSwitch	172.21.162.103	Default	Provisioning

Cuando edita la interfaz de VMkernel, aquí está la opción para habilitar los servicios requeridos.



vmk2 - Edit Settings | esxi-hc-03.sddc.netapp.com

Port properties

IPv4 settings

IPv6 settings

TCP/IP stack: Default

MTU (Bytes): 9000

Available services

Enabled services:

- vMotion
- Provisioning
- Fault Tolerance logging
- Management
- vSphere Replication
- vSphere Replication NFC
- vSAN
- vSAN Witness
- vSphere Backup NFC
- NVMe over TCP
- NVMe over RDMA

CANCEL OK



Asegúrese de que hay al menos dos nic de enlace ascendente activas de alta velocidad disponibles para el grupo de puertos utilizado por las interfaces de VMkernel de vMotion y Provisioning.

Escenarios de migración de equipos virtuales

VMotion se utiliza a menudo para migrar las máquinas virtuales independientemente de su estado de energía. A continuación, encontrará más consideraciones y procedimiento de migración para escenarios específicos.

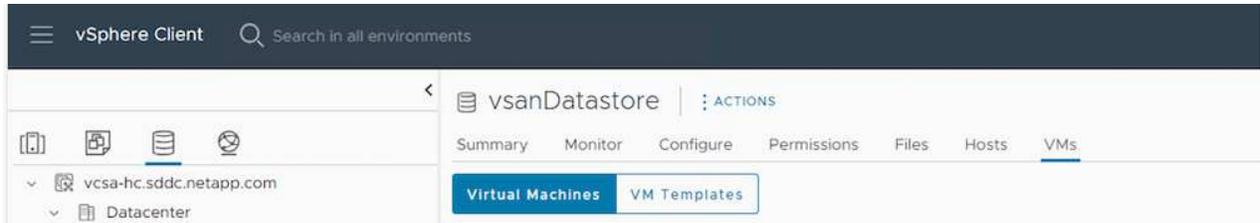


Comprender "[Condiciones de la máquina virtual y limitación de vSphere vMotion](#)" Antes de continuar con cualquier opción de migración de la máquina virtual.

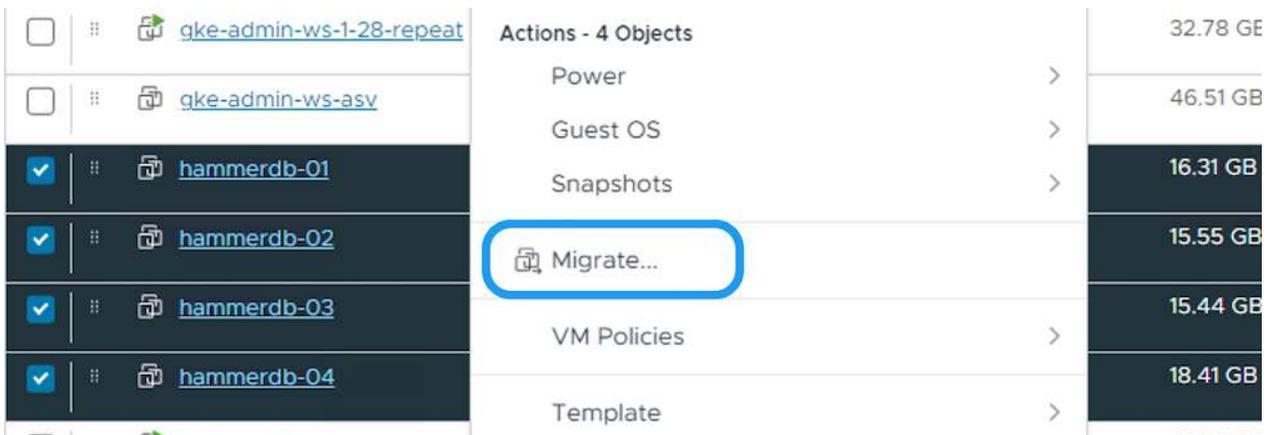
Migración de equipos virtuales desde un almacén de datos de vSphere específico

Siga el procedimiento que se indica a continuación para migrar equipos virtuales a un nuevo almacén de datos mediante la interfaz de usuario.

1. Con vSphere Web Client, seleccione el Datastore en el inventario de almacenamiento y haga clic en la pestaña VMs.



2. Seleccione las máquinas virtuales que se deben migrar y haga clic con el botón derecho del ratón para seleccionar la opción Migrate.



3. Elija la opción para cambiar solo el almacenamiento, haga clic en Siguiente

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Seleccione la política de almacenamiento de máquina virtual deseada y seleccione el almacén de datos compatible. Haga clic en Siguiente.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Thin Provision

VM Storage Policy NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/> ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
<input type="radio"/> DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
<input type="radio"/> destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
<input type="radio"/> DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
<input type="radio"/> E13A400_JCSI	Incompatible	2 TB	858.66 GB	1.85 TB	N

Manage Columns Items per page 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Revise y haga clic en Finalizar.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

×

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL

BACK

FINISH

Para migrar equipos virtuales mediante PowerCLI, aquí está el script de ejemplo.

```
#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
```

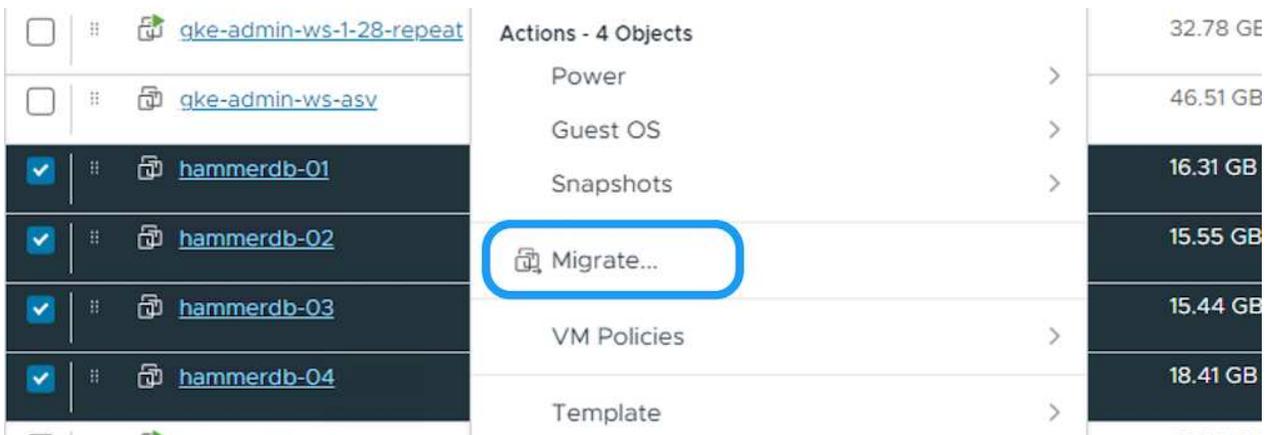
Migración de equipos virtuales en el mismo clúster de vSphere

Siga el procedimiento que se indica a continuación para migrar equipos virtuales a un nuevo almacén de datos mediante la interfaz de usuario.

1. Con vSphere Web Client, seleccione el Cluster en el inventario Host and Cluster y haga clic en la pestaña VMs.



2. Seleccione las máquinas virtuales que se deben migrar y haga clic con el botón derecho del ratón para seleccionar la opción Migrate.



3. Elija la opción para cambiar solo el almacenamiento, haga clic en Siguiente

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Seleccione la política de almacenamiento de máquina virtual deseada y seleccione el almacén de datos compatible. Haga clic en Siguiente.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Thin Provision

VM Storage Policy NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/> ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
<input type="radio"/> DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
<input type="radio"/> destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
<input type="radio"/> DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
<input type="radio"/> E13A400_JCSI	Incompatible	2 TB	858.66 GB	1.85 TB	\

Manage Columns Items per page 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Revise y haga clic en Finalizar.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

×

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL

BACK

FINISH

Para migrar equipos virtuales mediante PowerCLI, aquí está el script de ejemplo.

```

#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 Cluster de almacenes de datos está en uso con un DRS (programación dinámica de recursos) de almacenamiento totalmente automatizado y ambos almacenes de datos (de origen y destino) son del mismo tipo (VMFS/NFS/VVol), mantenga ambos almacenes de datos en el mismo clúster de almacenamiento y migre máquinas virtuales desde un almacén de datos de origen habilitando el modo de mantenimiento en el origen. La experiencia será parecida al modo en que se gestionan los hosts de computación para el mantenimiento.

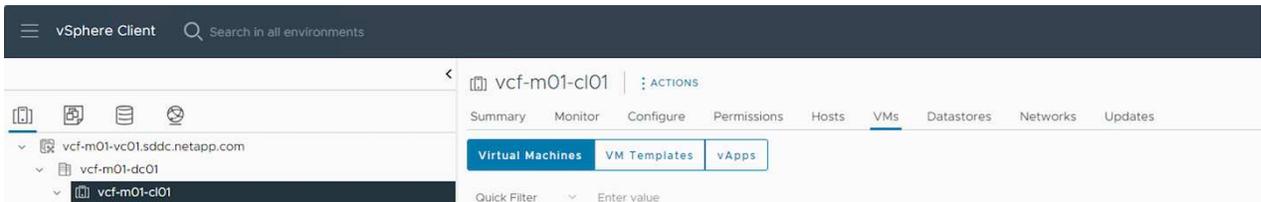
Migración de equipos virtuales entre varios clústeres de vSphere



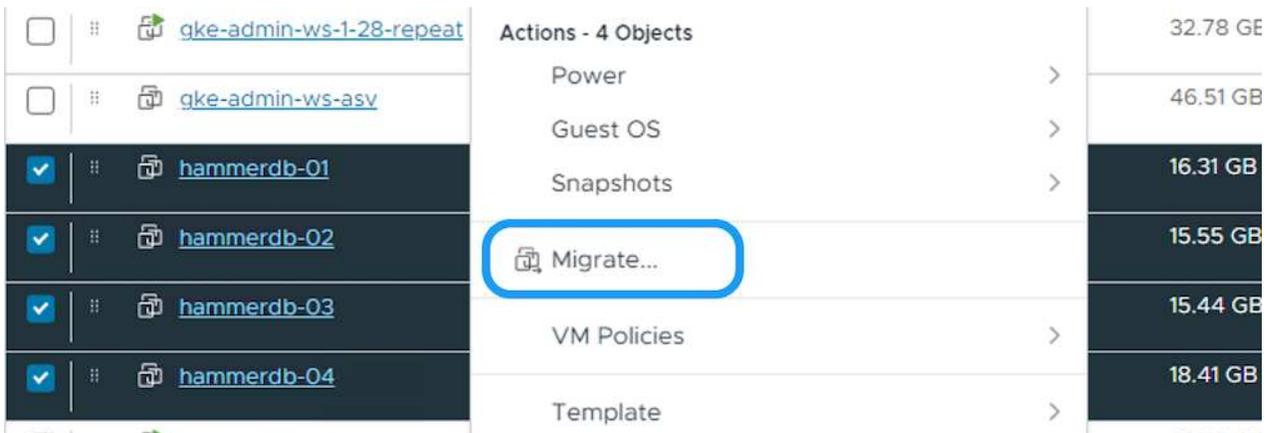
Consulte "[Compatibilidad con CPU y vSphere Enhanced vMotion Compatibility](#)" Cuando los hosts de origen y destino son de una familia o modelo de CPU diferente.

Siga el procedimiento que se indica a continuación para migrar equipos virtuales a un nuevo almacén de datos mediante la interfaz de usuario.

1. Con vSphere Web Client, seleccione el Cluster en el inventario Host and Cluster y haga clic en la pestaña VMs.



2. Seleccione las máquinas virtuales que se deben migrar y haga clic con el botón derecho del ratón para seleccionar la opción Migrate.



3. Elija la opción para cambiar el recurso de computación y el almacenamiento, haga clic en Siguiente

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Navegue y elija el clúster adecuado para migrar.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ▼ vcf-wkld-vc01.sddc.netapp.com
 - ▼ vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Seleccione la política de almacenamiento de máquina virtual deseada y seleccione el almacén de datos compatible. Haga clic en Siguiente.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

Select virtual disk format Thin Provision ▾

VM Storage Policy NFS ▾

Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/> VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	
<input type="radio"/> VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	
<input type="radio"/> VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB	
<input type="radio"/> vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/> vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/> vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	

Items per page 10 ▾ 7 items

Compatibility

✓ Compatibility checks succeeded.

6. Seleccione la carpeta de VM para colocar las VM de destino.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- ▾ vcf-wkld-01-DC
 - > Discovered virtual machine
 - > vCLS

Compatibility

✓ Compatibility checks succeeded.

7. Seleccione el grupo de puertos de destino.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
» SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Revise y haga clic en Finalizar.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

Para migrar equipos virtuales mediante PowerCLI, aquí está el script de ejemplo.

```

#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

```

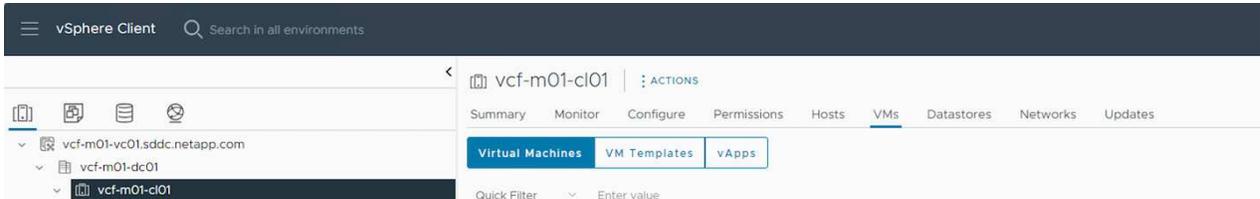
Migración de equipos virtuales entre servidores de vCenter en el mismo dominio de SSO

Siga el procedimiento a continuación para migrar máquinas virtuales a un nuevo servidor vCenter Server que se muestra en la misma interfaz de usuario del cliente de vSphere.

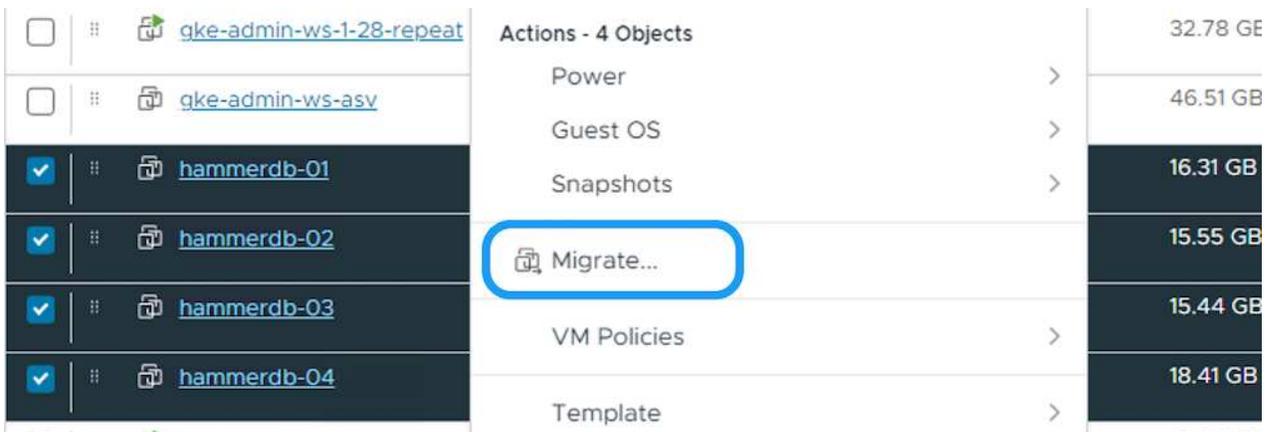


Para conocer requisitos adicionales, como versiones de vCenter de origen y destino, etc., compruebe "[Documentación de vSphere sobre requisitos para vMotion entre instancias de vCenter Server](#)"

1. Con vSphere Web Client, seleccione el Cluster en el inventario Host and Cluster y haga clic en la pestaña VMs.



2. Seleccione las máquinas virtuales que se deben migrar y haga clic con el botón derecho del ratón para seleccionar la opción Migrate.



3. Elija la opción para cambiar el recurso de computación y el almacenamiento, haga clic en Siguiente

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Seleccione el clúster de destino en la instancia de vCenter Server de destino.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ▼ vcf-wkld-vc01.sddc.netapp.com
 - ▼ vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Seleccione la política de almacenamiento de máquina virtual deseada y seleccione el almacén de datos compatible. Haga clic en Siguiente.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE
CONFIGURE PER DISK

Select virtual disk format Thin Provision ▾
 VM Storage Policy NFS ▾

	Name	Storage Compatibility	Capacity	Provisioned	Free
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB
<input type="radio"/>	VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
<input type="radio"/>	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Manage Columns
Items per page 10 ▾ 7 items

Compatibility
 ✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

6. Seleccione la carpeta de VM para colocar las VM de destino.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
 - > Discovered virtual machine
 - > vCLS

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

7. Seleccione el grupo de puertos de destino.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
» SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Revise las opciones de migración y haga clic en Finish.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

Para migrar equipos virtuales mediante PowerCLI, aquí está el script de ejemplo.

```

#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

```

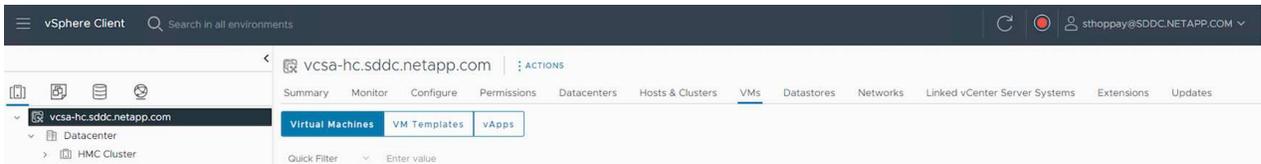
Migración de equipos virtuales entre servidores de vCenter en un dominio de SSO diferente



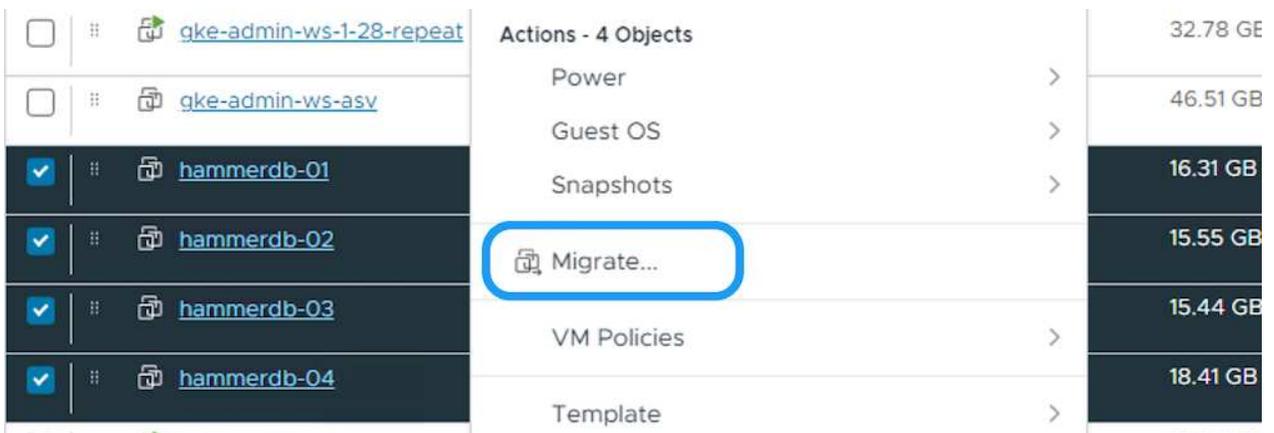
En este escenario se asume que existe la comunicación entre los servidores de vCenter. De lo contrario, compruebe el escenario de ubicación en todo el centro de datos indicado a continuación. Para conocer los requisitos previos, compruebe "[Documentación de vSphere en Advanced Cross vCenter vMotion](#)"

Siga el procedimiento a continuación para migrar máquinas virtuales a una instancia de vCenter Server distinta a través de la interfaz de usuario.

1. Con vSphere Web Client, seleccione la instancia de vCenter Server de origen y haga clic en la pestaña VMs.



2. Seleccione las máquinas virtuales que se deben migrar y haga clic con el botón derecho del ratón para seleccionar la opción Migrate.



3. Elija la opción Cross vCenter Server export y haga clic en Next

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only**
Migrate the virtual machines to another host or cluster.
- Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.
 - Keep VMs on the source vCenter Server (performs a VM clone operation).

CANCEL NEXT



La máquina virtual también puede importarse desde el servidor vCenter de destino. Para este procedimiento, compruebe "[Importe o clone una máquina virtual con Advanced Cross vCenter vMotion](#)"

4. Proporcione los detalles de las credenciales de vCenter y haga clic en Login.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

SAVED VCENTER SERVERS NEW VCENTER SERVER

vCenter Server address
vCenter Server FQDN or IP address

Username
example@domain.local

Password
Password

Save vCenter Server address

LOGIN

CANCEL BACK NEXT

5. Confirme y acepte la huella digital de certificados SSL de vCenter Server

Security Alert ✕

Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:
17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

 Connect anyway?

Click Yes if you trust the vCenter Server.
Click No to cancel connecting to the vCenter Server.

6. Expanda vCenter de destino y seleccione el clúster de computación de destino.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource**
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a compute resource ✕

Select a cluster, host, vApp or resource pool to run the virtual machines.

VM ORIGIN ⓘ

- vcf-wkld-vc01.sddc.netapp.com
 - vcf-wkld-01-DC
 - IT-INF-WKLD-01**

Compatibility

✓ Compatibility checks succeeded.

7. Seleccione el almacén de datos de destino según la política de almacenamiento de la máquina virtual.

Migrate | SQLSRV-05

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select folder
6 Select networks
7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration. VM ORIGIN ⓘ

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format Thin Provision
VM Storage Policy NFS

Name	Storage Compatibility	Capacity	Provisioned	Free
<input checked="" type="radio"/> VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB
<input type="radio"/> VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB
<input type="radio"/> VCF_WKLD_03_ISCSI	Incompatible	3 TB	1.35 TB	2.59 TB
<input type="radio"/> vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
<input type="radio"/> vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Manage Columns Items per page 10 7 items

Compatibility
✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

8. Seleccione la carpeta de VM de destino.

Migrate | SQLSRV-05

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select folder
6 Select networks
7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration. VM ORIGIN ⓘ

Select location for the virtual machine migration.

- vcf-wkld-01-DC
 - Discovered virtual machine
 - Oracle
 - SQL Server**
 - vCLS

Compatibility
✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

9. Seleccione el grupo de puertos de VM para cada asignación de tarjeta de interfaz de red.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration. VM ORIGIN ⓘ

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

	Source Network	Used By	Destination Network
>>	Mgmt 181	1 VMs / 1 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-01-p
>>	Data A - 3374	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-a
>>	Data B - 3375	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-b

3 items

[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

10. Revise y haga clic en Finish para iniciar vMotion en vCenter Server.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration. VM ORIGIN ⓘ

Migration Type	Change compute resource and storage
Virtual Machine	SQLSRV-05
vCenter	vcf-wkld-vc01.sddc.netapp.com
Folder	SQL Server
Cluster	IT-INF-WKLD-01
Networks	Virtual network adapters from 3 networks will be reassigned to new destination networks
Storage	VCF_WKLD_01
VM storage policy	NFS
Disk Format	Thin Provision

CANCEL BACK FINISH

Para migrar equipos virtuales mediante PowerCLI, aquí está el script de ejemplo.

```

#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 en distintas ubicaciones de centros de datos

- Cuando el tráfico de la capa 2 se extiende entre los centros de datos mediante la federación NSX u otras opciones, siga el procedimiento para migrar las máquinas virtuales a través de los servidores vCenter.
- HCX ofrece varios "tipos de migración" La inclusión de la replicación ayudó a vMotion en todos los centros de datos a mover equipos virtuales sin ningún tiempo de inactividad.
- "[Gestor de recuperación de sitios \(SRM\)](#)" Suele tener finalidad para la recuperación ante desastres y, con frecuencia, también se utiliza para la migración planificada con la replicación basada en cabinas de almacenamiento.
- Utiliza productos de protección de datos continua (CDP) "[API de vSphere para IO \(VAIO\)](#)" Para interceptar los datos y enviar una copia a una ubicación remota en una solución RPO prácticamente nula.
- También se pueden utilizar los productos de backup y recuperación. Pero a menudo resulta en un objetivo de tiempo de recuperación más largo.
- "[Recuperación ante desastres como servicio \(DRaaS\) de BlueXP](#)" Utiliza la replicación basada en cabinas de almacenamiento y automatiza ciertas tareas para recuperar las máquinas virtuales en el sitio de destino.

Migración de equipos virtuales en un entorno de cloud híbrido

- "[Configure el modo vinculado híbrido](#)" y siga el procedimiento de "[Migración de equipos virtuales entre servidores de vCenter en el mismo dominio de SSO](#)"
- HCX ofrece varios "tipos de migración" Incluido Replication Assisted vMotion en los centros de datos para mover el equipo virtual mientras está encendido.
 - Enlace: [./ehc/aws-migrate-vmware-hcx.html](https://ehc/aws-migrate-vmware-hcx.html) [TR 4942: Migrar las cargas de trabajo a un almacén de datos FSx ONTAP mediante VMware HCX]
 - Link: [./ehc/azure-migrate-vmware-hcx.html](https://ehc/azure-migrate-vmware-hcx.html) [TR-4940: Migre cargas de trabajo a un almacén de datos de Azure NetApp Files mediante VMware HCX: Guía de inicio rápido]
 - Link: [./esc/gcp-migrate-vmware-hcx.html](https://esc/gcp-migrate-vmware-hcx.html) [Migrar cargas de trabajo a almacén de datos de Google Cloud NetApp Volumes en Google Cloud VMware Engine con VMware HCX: Guía de inicio rápido]
- "[Recuperación ante desastres como servicio \(DRaaS\) de BlueXP](#)" Utiliza la replicación basada en cabinas de almacenamiento y automatiza ciertas tareas para recuperar las máquinas virtuales en el sitio de destino.
- Con productos de protección de datos continua (CDP) compatibles que utilizan "[API de vSphere para IO \(VAIO\)](#)" Para interceptar los datos y enviar una copia a una ubicación remota en una solución RPO prácticamente nula.



Cuando la máquina virtual de origen reside en un almacén de datos VVOL basado en bloques, puede replicarse con SnapMirror a Amazon FSx ONTAP o Cloud Volumes ONTAP (CVO) en otros proveedores de cloud admitidos y consumirse como volumen iSCSI con máquinas virtuales nativas de la nube.

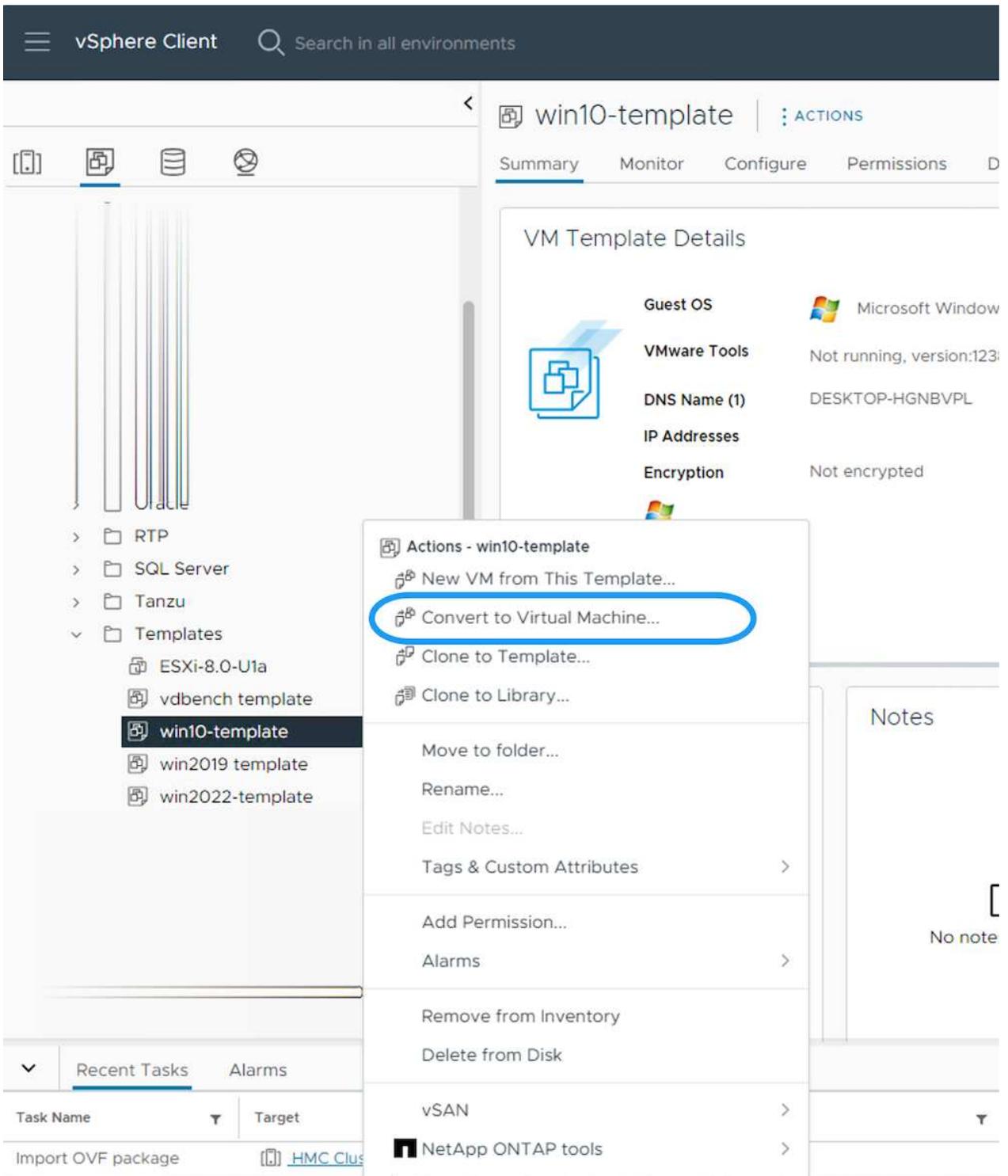
Escenarios de migración de plantillas de equipos virtuales

VCenter Server o una biblioteca de contenido pueden gestionar las plantillas de máquinas virtuales. La distribución de plantillas de VM, plantillas OVF y OVA, otros tipos de archivos se gestionan publicándolo en la biblioteca de contenido local y las bibliotecas de contenido remotas pueden suscribirse a ella.

- Las plantillas de máquinas virtuales almacenadas en el inventario de vCenter pueden convertirse en máquinas virtuales y utilizar las opciones de migración de máquinas virtuales.
- Las plantillas OVF y OVA, otros tipos de archivos almacenados en la biblioteca de contenido se pueden clonar en otras bibliotecas de contenido.
- Biblioteca de contenido Las plantillas de máquinas virtuales se pueden alojar en cualquier almacén de datos y es necesario agregarlas a la nueva biblioteca de contenido.

Migración de plantillas de equipos virtuales alojadas en almacenes de datos

1. En vSphere Web Client, haga clic con el botón derecho en la plantilla de máquina virtual en la vista de la carpeta VM and Templates y seleccione la opción de convertir a máquina virtual.



2. Cuando se convierta como equipo virtual, siga las opciones de migración de la máquina virtual.

Clonación de elementos de biblioteca de contenido

1. En vSphere Web Client, seleccione Bibliotecas de contenido



 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

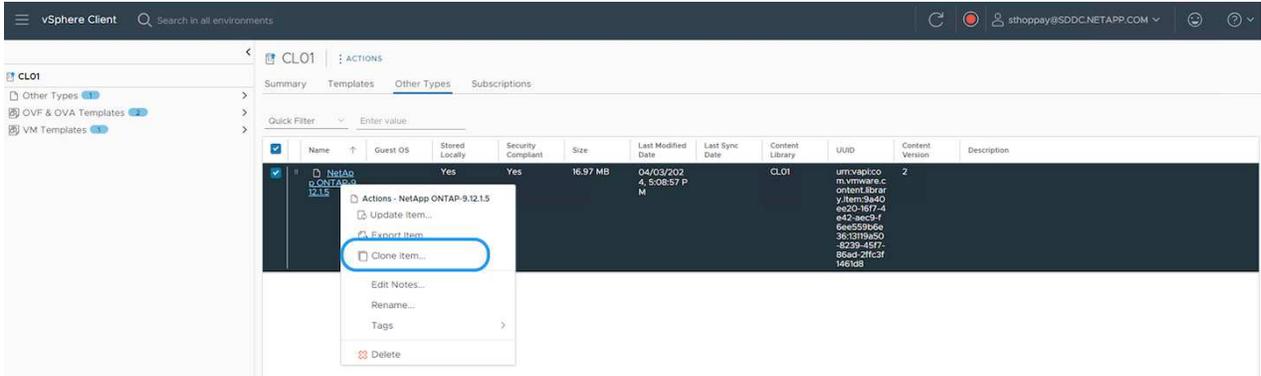
 Cloud Provider Services

 NSX

 VMware Aria Operations Configuration

 Skyline Health Diagnostics

2. Seleccione la biblioteca de contenido en la que desea clonar el elemento
3. Haga clic con el botón derecho del ratón en el elemento y haga clic en Clonar elemento ..



Si utiliza el menú de acción, asegúrese de que aparece el objeto de destino correcto para realizar la acción.

4. Seleccione la biblioteca de contenido de destino y haga clic en Aceptar.

Clone Library Item | NetApp ONTAP-9.12.15 ×

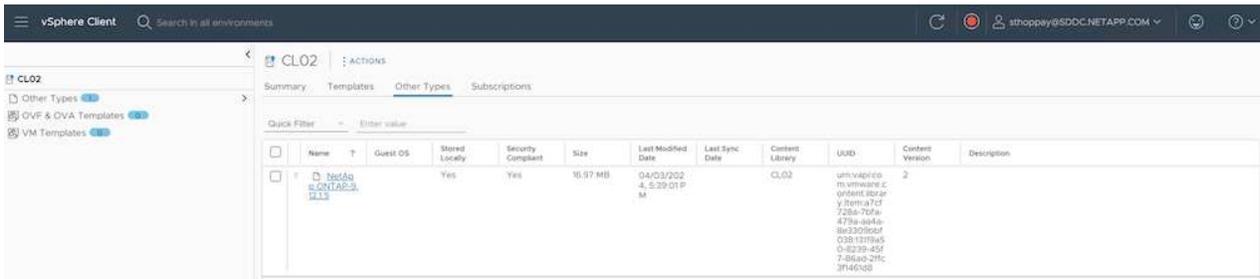
Name

Notes

Select a content library where to clone the library item.

	Name	Notes	Creation Date
<input type="radio"/>	CL01		9/26/2023, 5:02:03 PM
<input checked="" type="radio"/>	CL02		4/1/2024, 12:37:51 PM

5. Compruebe que el elemento está disponible en la biblioteca de contenido de destino.



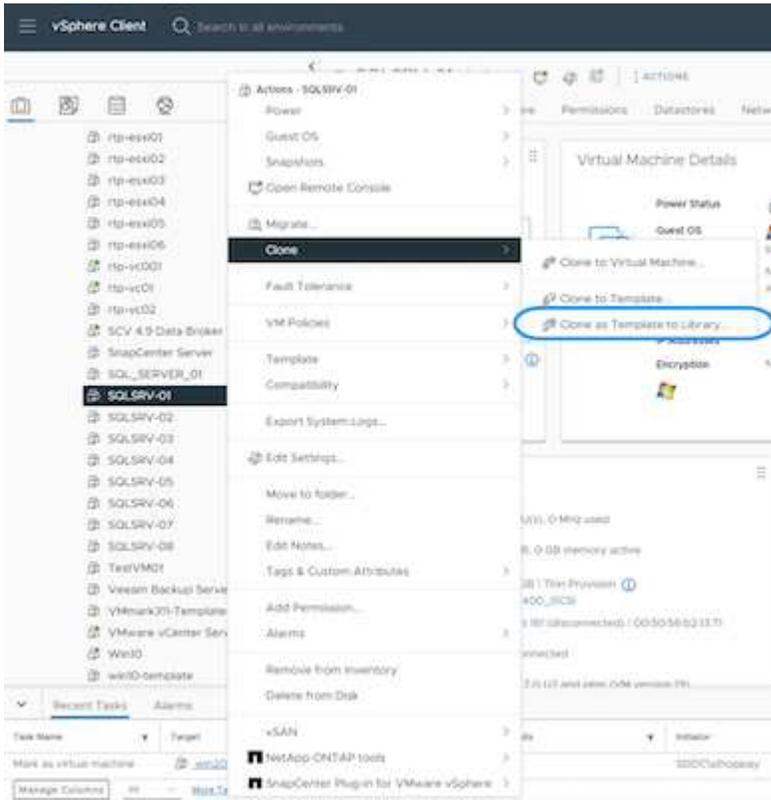
Aquí está el script PowerCLI de ejemplo para copiar los elementos de la biblioteca de contenido de la biblioteca de contenido CL01 a la CL02.

```
#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-ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL02' -Server
$targetvc)
```

Adición de VM 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 la plantilla VM para clonar en library, sólo puede almacenarla como plantilla OVF y OVA y no como plantilla VM.

2. Confirme que el tipo de plantilla está seleccionado como plantilla de VM y siga respondiendo al asistente para completar la operación.

SQLSRV-01 - Clone Virtual Machine To Template

Basic information

1 Basic information

2 Location

3 Select a compute resource

4 Select storage

5 Ready to complete

Template type: VM Template

Name: SQLSRV-01

Notes:

Select a folder for the template:

- vcsa-hc.sddc.netapp.com
 - Datacenter

CANCEL NEXT

 Para obtener más información sobre las plantillas de máquinas virtuales 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.

- En función de dónde se aprovisiona el almacén de datos de ONTAP, seleccione las opciones de migración de máquinas virtuales anteriores.

Migración de la versión anterior a la última versión de vSphere.

- Si no es posible realizar una actualización in situ, puede crear un nuevo entorno y utilizar las opciones de migración anteriores.



En la opción de migración Cross vCenter, importe desde destino si la opción de exportación no está disponible en el origen. Para este procedimiento, compruebe ["Importe o clone una máquina virtual con Advanced Cross vCenter vMotion"](#)

Migración al dominio de carga de trabajo de VCF.

- Migre las 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 de la instancia de vCenter de origen, amplíe el segmento de NSX añadiendo los hosts de vcenter vSphere de origen a la zona de transporte o use el puente L2 en el perímetro para permitir la comunicación de L2 en la VLAN. Consulte la documentación de NSX de ["Configurar una VM de Edge para Bridging"](#)

Recursos adicionales

- ["Migración de máquinas virtuales vSphere"](#)
- ["Novedades de vSphere 8 para vMotion"](#)
- ["Recursos de vMotion de vSphere"](#)
- ["Configuraciones de puerta de enlace Tier-0 en la federación NSX"](#)
- ["Guía del usuario DE HCX 4,8"](#)
- ["Documentación de VMware Site Recovery Manager"](#)
- ["Recuperación ante desastres de BlueXP para VMware"](#)

Migre sus máquinas virtuales a Amazon EC2 mediante Amazon FSx para ONTAP

Migre las máquinas virtuales a Amazon EC2 mediante Amazon FSx for ONTAP: Descripción general

Las organizaciones están acelerando sus migraciones a soluciones de cloud computing en AWS, aprovechando servicios como las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y Amazon FSx para NetApp ONTAP (FSx ONTAP) para modernizar sus INFRAESTRUCTURAS TECNOLÓGICAS, ahorrar en costes y mejorar la eficiencia operativa. Estas ofertas de AWS permiten realizar migraciones que optimizan el coste total de propiedad (TCO) mediante modelos de precios basados en el consumo, funciones de almacenamiento empresarial, lo que proporciona la flexibilidad y la escalabilidad necesarias para satisfacer las cambiantes demandas empresariales globales.

Descripción general

Para las empresas que invierten profundamente en VMware vSphere, la migración a AWS es una opción rentable dadas las condiciones actuales del mercado, una oportunidad única.

A medida que estas organizaciones realizan la transición a AWS, tratan de aprovechar la agilidad y los beneficios económicos del cloud y, al mismo tiempo, mantener los conjuntos de funciones que ya conocen, sobre todo en lo que se refiere al almacenamiento. Mantener operaciones fluidas con los protocolos de almacenamiento ya conocidos, especialmente iSCSI, los procesos, las herramientas y las competencias es crucial para la migración de cargas de trabajo o la configuración de soluciones de recuperación de desastres.

Mediante el servicio de almacenamiento gestionado de AWS FSx ONTAP para conservar las funcionalidades de almacenamiento empresarial, que también proviene de almacenamientos de terceros de las instalaciones,

las empresas pueden desplegar la potencia de AWS a la vez que minimizan las interrupciones y maximizan sus futuras inversiones.

En este informe técnico se explica cómo migrar máquinas virtuales de VMware vSphere on-premises a una instancia de Amazon EC2 con discos de datos ubicados en las LUN iSCSI de FSx ONTAP usando la funcionalidad de «movilidad de datos como código» de MigrateOps de Cirrus Migrate Cloud (CMC).

Requisitos de la solución

Existen varios retos que los clientes de VMware quieren resolver actualmente. Estas organizaciones desean:

1. Aproveche las capacidades de almacenamiento empresarial, como thin provisioning, tecnologías de eficiencia del almacenamiento, clones con espacio cero, backups integrados, replicación a nivel de bloque y organización en niveles. Esto ayuda a optimizar los esfuerzos de migración y a preparar la puesta en marcha para el futuro en AWS desde el día 1.
2. Optimice las puestas en marcha de almacenamiento que actualmente están en AWS que utilizan instancias de Amazon EC2 incorporando FSx ONTAP y las funciones de optimización de costes que ofrece.
3. Reduzca el coste total de propiedad (TCO) que se obtiene al usar instancias de Amazon EC2 con soluciones de almacenamiento en bloque ajustando el tamaño de las instancias de Amazon EC2 para satisfacer los parámetros de IOPS y rendimiento necesarios. Con el almacenamiento en bloques, las operaciones en los discos de Amazon EC2 tienen un tope en las tasas de I/O y ancho de banda. El almacenamiento de archivos con FSx ONTAP usa ancho de banda de red. En otras palabras, FSx ONTAP no tiene límites de I/O a nivel de máquina virtual.

Descripción general de los componentes técnicos

Conceptos de FSx ONTAP

Amazon FSx ONTAP es un servicio de almacenamiento de AWS totalmente gestionado que proporciona sistemas de archivos NetApp® ONTAP® con todas las funciones, el rendimiento y las API de administración de datos de ONTAP en AWS. Su almacenamiento de alto rendimiento admite diversos protocolos (NFS, SMB, iSCSI), lo que proporciona un único servicio para cargas de trabajo que utilizan instancias de Windows, Linux y macOS EC2.

Dado que FSx ONTAP es un sistema de archivos ONTAP, trae consigo una gran cantidad de funciones y servicios de NetApp familiares, incluyendo la tecnología de replicación de datos SnapMirror®, clones delgados y copias Snapshot™ de NetApp. Al aprovechar un nivel de capacidad de bajo coste a través de la organización de los datos en niveles, FSx ONTAP es elástico y puede alcanzar una escala prácticamente ilimitada. Además, con la firma de la tecnología de eficiencia del almacenamiento de NetApp, reduce aún más los costes de almacenamiento en AWS. Para obtener más información, consulte "[Cómo empezar a usar Amazon FSx ONTAP](#)".

Sistema de archivos

El recurso central de FSx ONTAP es su sistema de archivos basado en almacenamiento en unidades de estado sólido (SSD). Al aprovisionar un sistema de archivos FSx ONTAP, el usuario introduce el rendimiento deseado y la capacidad de almacenamiento, y selecciona una Amazon VPC donde residirá el sistema de archivos.

Los usuarios también pueden elegir entre dos modelos de implementación de alta disponibilidad integrados para el sistema de archivos: Zona de disponibilidad múltiple (AZ) o implementación de zona única. Cada una de estas opciones ofrece su propio nivel de durabilidad y disponibilidad, que los clientes pueden seleccionar en función de los requisitos de continuidad del negocio de su caso de uso. Las puestas en marcha de varias

zonas de disponibilidad constan de nodos dobles que replican sin problemas entre dos zonas de disponibilidad. La opción de implementación de un solo AZ más rentable estructura el sistema de archivos en dos nodos divididos entre dos dominios de fallo independientes que residen en un único AZ.

Máquinas virtuales de almacenamiento

Se accede a los datos en el sistema de archivos FSx ONTAP a través de una partición de almacenamiento lógico que se denomina máquina virtual de almacenamiento. Un SVM es su propio servidor de archivos equipado con sus propios puntos de acceso de datos y administradores. Al acceder a los LUN de iSCSI en un sistema de archivos FSx ONTAP, la instancia de Amazon EC2 se comunica directamente con la SVM mediante la dirección IP del extremo de iSCSI de la SVM.

Aunque es posible mantener una única SVM en un clúster, la opción de ejecutar varias SVM en un clúster tiene una gran variedad de usos y beneficios. Los clientes pueden determinar el número óptimo de SVM que deben configurar teniendo en cuenta sus necesidades empresariales, incluidos sus requisitos en cuanto al aislamiento de cargas de trabajo.

Volúmenes

Los datos en una SVM de FSx ONTAP se almacenan y organizan en estructuras conocidas como volúmenes, que actúan como contenedores virtuales. Un volumen individual se puede configurar con una o varias LUN. Los datos almacenados en cada volumen consumen capacidad de almacenamiento en el sistema de archivos. Sin embargo, como FSx ONTAP aprovisiona poco el volumen, el volumen solo ocupa capacidad de almacenamiento para la cantidad de datos que se va a almacenar.

El concepto de Cirrus Migrate Cloud MigrateOps

CMC es una oferta de software como servicio (SaaS) transaccional de Cirrus Data Solutions, Inc. Que está disponible a través de AWS Marketplace. MigrateOps es una función de automatización de datos como código de CMC que le permite gestionar de forma declarativa sus operaciones de movilidad de datos a escala utilizando configuraciones de operación simples en YAML. Una configuración de MigrateOps determina cómo desea que se ejecuten las tareas de movilidad de datos. Para obtener más información sobre MigrateOps, consulte "[Acerca de MigrateOps](#)".

MigrateOps adopta un enfoque que da prioridad a la automatización, el cual está creado específicamente para optimizar todo el proceso, garantizando la movilidad de datos empresariales a escala cloud sin interrupciones operativas. Además de las ya ricas funcionalidades que CMC ofrece para la automatización, MigrateOps añade otras automatizaciones que a menudo se administran externamente, como:

- Corrección del SO
- Planificación de aprobaciones y transición de aplicaciones
- Migración de clúster con cero tiempo de inactividad
- Integración de plataformas de cloud público/privado
- Integración de plataforma de virtualización
- Integración de la gestión del almacenamiento empresarial
- CONFIGURACIÓN DE SAN (iSCSI)

Con las tareas anteriores totalmente automatizadas, todos los tediosos pasos para preparar la máquina virtual de origen on-premises (como añadir agentes y herramientas de AWS), crear LUN FSx de destino, configurar iSCSI y Multipath/MPIO en la instancia de destino de AWS, y todas las tareas de detener/iniciar servicios de aplicaciones se eliminan simplemente especificando parámetros en un archivo YAML.

FSX ONTAP se utiliza para proporcionar los LUN de datos y ajustar el tamaño adecuado del tipo de instancia de Amazon EC2, a la vez que proporciona todas las funciones que las organizaciones tenían previamente en sus entornos en las instalaciones. La función MigrateOps de CMC se utilizará para automatizar todos los pasos involucrados, incluido el aprovisionamiento de LUN iSCSI asignados, lo que lo convierte en una operación predecible y declarativa.

Nota: CMC requiere que se instale un agente muy delgado en las instancias de la máquina virtual de origen y destino para garantizar la transferencia segura de datos desde el almacenamiento de origen de almacenamiento a FSX ONTAP.

Beneficios de usar Amazon FSx ONTAP con instancias EC2

El almacenamiento FSx ONTAP para instancias de Amazon EC2 ofrece varios beneficios:

- Almacenamiento de alto rendimiento y baja latencia que proporcionan un alto rendimiento constante para las cargas de trabajo más exigentes
- El almacenamiento en caché NVMe inteligente mejora el rendimiento
- La capacidad ajustable, el rendimiento y las IOPS pueden cambiarse sobre la marcha y adaptarse rápidamente a las demandas de almacenamiento cambiantes
- La replicación de datos basada en bloques del almacenamiento de ONTAP on-premises a AWS
- Accesibilidad multiprotocolo, incluido para iSCSI, que está ampliamente utilizado en puestas en marcha de VMware en las instalaciones
- La tecnología Snapshot™ de NetApp y la recuperación ante desastres orquestada por SnapMirror evitan la pérdida de datos y aceleran la recuperación
- Funciones de eficiencia del almacenamiento que reducen el espacio y los costes del almacenamiento, incluidos el thin provisioning, la deduplicación de datos, la compresión y la compactación
- Una replicación eficiente reduce el tiempo de creación de backups de horas a tan solo minutos, lo que optimiza el objetivo de tiempo de recuperación
- Opciones granulares para copias de seguridad de archivos y restauraciones usando NetApp SnapCenter®

La puesta en marcha de las instancias de Amazon EC2 con FSx ONTAP como capa de almacenamiento basado en iSCSI ofrece funciones de gestión de datos esenciales de alto rendimiento y funciones de eficiencia del almacenamiento rentables que pueden transformar su puesta en marcha en AWS.

Al ejecutar una memoria Flash Cache, múltiples sesiones iSCSI y aprovechar un tamaño de conjunto de trabajo del 5 %, es posible que FSx ONTAP ofrezca IOPS de aprox. 350K M, lo que proporciona niveles de rendimiento que satisfacen incluso las cargas de trabajo más intensivas.

Dado que solo los límites de ancho de banda de red se aplican en FSx ONTAP, y no en los límites de ancho de banda de almacenamiento basado en bloques, los usuarios pueden aprovechar tipos de instancias de Amazon EC2 reducidos al tiempo que logran las mismas tasas de rendimiento que los tipos de instancias mucho más grandes. El uso de tipos de instancia tan pequeños también mantiene los costes de computación bajos, lo que optimiza el TCO.

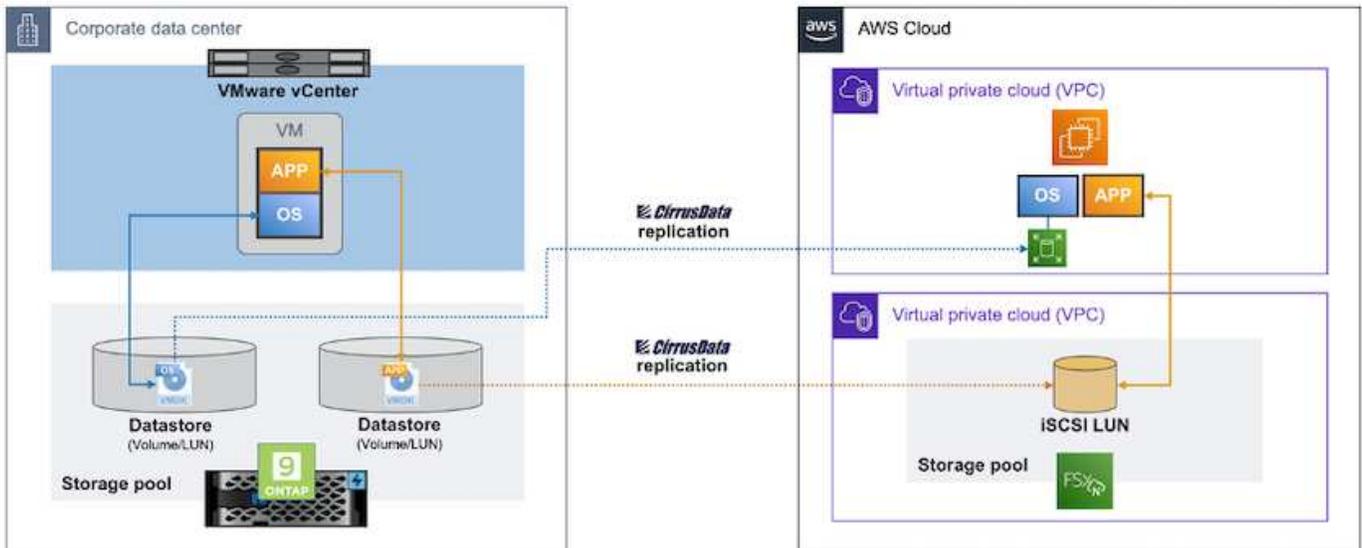
La capacidad de FSx ONTAP para ofrecer servicio a varios protocolos es otra ventaja que ayuda a estandarizar un único servicio de almacenamiento de AWS para una amplia gama de requisitos de servicios de archivos y datos existentes. Para las empresas que invierten profundamente en VMware vSphere, la migración a AWS es una opción rentable dadas las condiciones actuales del mercado, una oportunidad única.

Migre las máquinas virtuales a Amazon EC2 mediante Amazon FSx para NetApp ONTAP: Arquitectura y requisitos previos

En este artículo se muestran los requisitos previos de la arquitectura de alto nivel y la puesta en marcha para completar la migración.

Arquitectura de alto nivel

El siguiente diagrama ilustra la arquitectura de alto nivel de migración de datos de disco de máquina virtual (VMDK) en VMware a AWS mediante CMC MigrateOps:



Cómo migrar tus máquinas virtuales de VMware a AWS mediante Amazon EC2 y FSx ONTAP iSCSI

Requisitos previos

Antes de iniciar los pasos del tutorial, asegúrese de que se cumplen los siguientes requisitos previos:

En AWS

- Una cuenta de AWS. Esto incluye permisos para subredes, configuración de VPC, tablas de enrutamiento, migración de reglas de seguridad, grupos de seguridad, y otros requisitos para la red, como el equilibrio de carga. Al igual que con cualquier migración, el mayor esfuerzo y consideración debe ir a la conexión en red.
- Roles de IAM adecuados que le permiten aprovisionar instancias de FSX ONTAP y Amazon EC2.
- Las tablas de rutas y los grupos de seguridad pueden comunicarse con FSX ONTAP.
- Agregue una regla de entrada al grupo de seguridad apropiado (consulte a continuación para obtener más detalles) para permitir la transferencia segura de datos desde su centro de datos local a AWS.
- Un DNS válido que puede resolver nombres de dominio de Internet públicos.
- Compruebe que la resolución de DNS es funcional y le permite resolver nombres de host.
- Para obtener un rendimiento y un ajuste del tamaño óptimos, usa los datos de rendimiento de tu entorno de origen para ajustar el tamaño de tu almacenamiento de FSx ONTAP.
- Cada sesión de MigrateOps utiliza un EIP, por lo que la cuota para EIP debe aumentarse para un mayor paralelismo. Tenga en cuenta que la cuota EIP predeterminada es 5.

- (Si se están migrando cargas de trabajo basadas en Active Directory) Un dominio de Windows Active Directory en Amazon EC2.

Para Cirrus Migrate Cloud

- Una cuenta de Cirrus Data Cloud en "cloud.cirrusdata.com" Debe crearse antes de utilizar CMC. Se debe permitir la comunicación saliente con la CDN, los puntos finales de Cirrus Data y el repositorio de software a través de HTTPS.
- Permitir la comunicación (saliente) con los servicios de Cirrus Data Cloud a través del protocolo HTTPS (puerto 443).
- Para que un host sea gestionado por el proyecto CMC, el software CMC implementado debe iniciar una conexión TCP de salida unidireccional a Cirrus Data Cloud.
- Permitir el acceso del protocolo TCP, puerto 443 a portal-gateway.cloud.cirrusdata.com que está actualmente en 208.67.222.222.
- Permitir solicitudes POST HTTP (a través de conexión HTTPS) con carga útil de datos binarios (aplicación/octet-stream). Esto es similar a una carga de archivos.
- Asegúrese de que el DNS puede resolver portal-gateway.cloud.cirrusdata.com (o a través del archivo host del sistema operativo).
- Si tiene reglas estrictas para prohibir las instancias de productos para realizar conexiones salientes, la función "Management Relay" de CMC se puede usar donde la conexión 443 saliente es de un único host no de producción seguro.

Nota: Nunca se envían datos de almacenamiento al punto final de Cirrus Data Cloud. Solo se envían metadatos de gestión, y esto puede enmascarse opcionalmente, de modo que no se incluya nombre de host real, nombre del volumen ni IP de red.

Para migrar datos de repositorios de almacenamiento on-premises a AWS, MigrateOps automatiza la gestión de una conexión de host a host (H2H). Se trata de conexiones de red optimizadas, unidireccionales y basadas en TCP que CMC utiliza para facilitar la migración remota. Este proceso incluye una compresión y un cifrado siempre disponibles que pueden reducir la cantidad de tráfico hasta ocho veces en función de la naturaleza de los datos.

Nota: CMC está diseñado para que ningún dato de producción / E/S salga de la red de producción durante toda la fase de migración. Como resultado, se necesita conectividad directa entre el host de origen y el de destino.

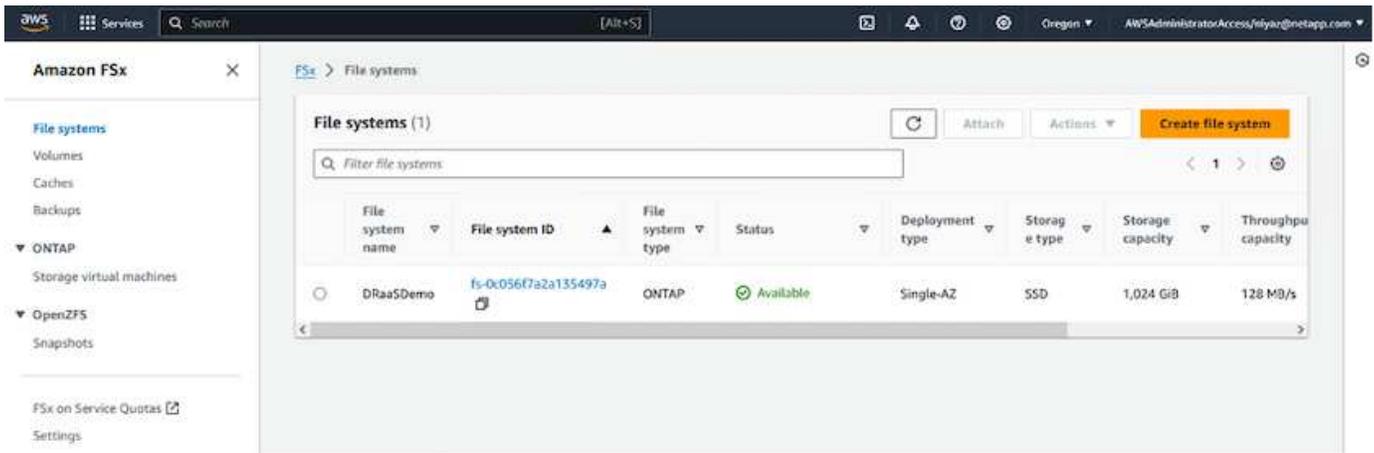
Migre las máquinas virtuales a Amazon EC2 mediante Amazon FSx para ONTAP: Guía de puesta en marcha

En este artículo se describe el procedimiento de implementación de estas soluciones de migración.

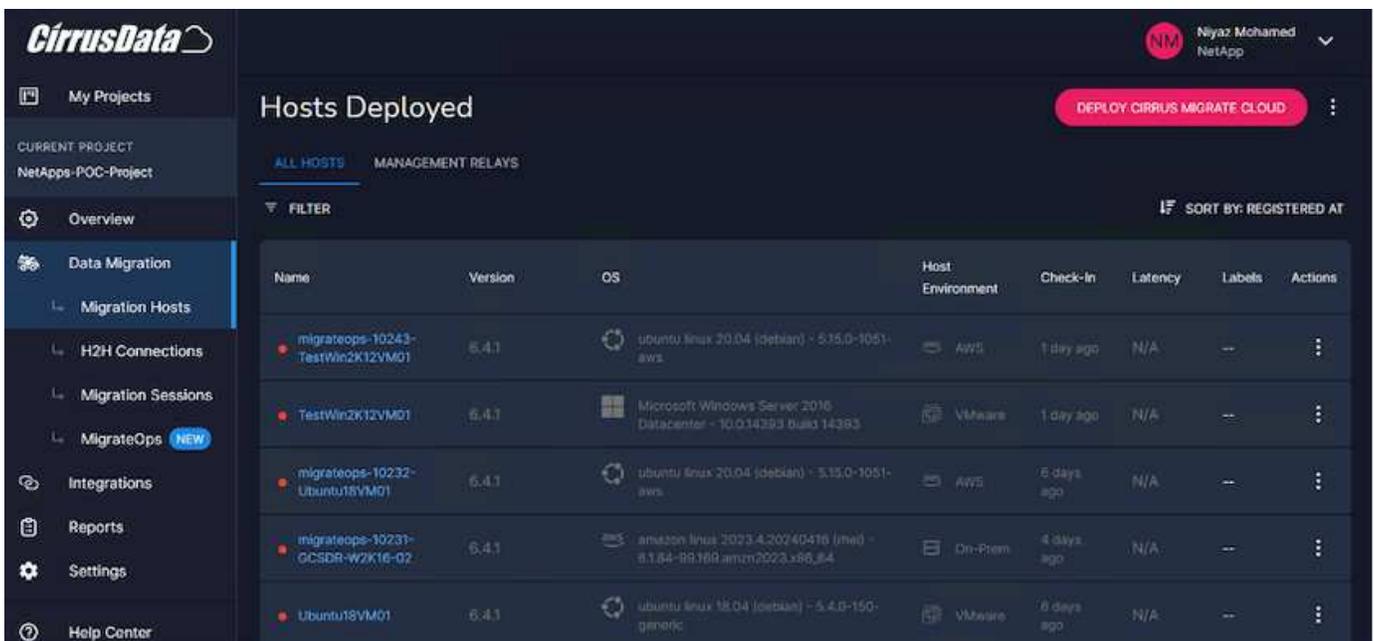
Configuración de FSx ONTAP y Cirrus Data para las operaciones de migración

Esto "[guía de puesta en marcha paso a paso](#)" muestra cómo añadir un volumen de FSx ONTAP a una VPC. Dado que estos pasos son de naturaleza secuencial, asegúrese de que estén cubiertos en orden.

A efectos de esta demostración, "DRaaS Demo" es el nombre del sistema de archivos creado.



Una vez que AWS VPC está configurado y FSx ONTAP se aprovisiona en función de tus requisitos de rendimiento, inicia sesión en ["cloud.cirrusdata.com"](https://cloud.cirrusdata.com) " Cree un nuevo proyecto" un proyecto existente o accede a él.



Antes de crear la receta para MigrationOps, hay que añadir la nube de AWS como una integración. CMC proporciona integración integrada con FSx ONTAP y AWS. La integración de FSx ONTAP proporciona las siguientes funcionalidades automatizadas:

Prepara tu sistema de archivos FSX ONTAP:

- Cree nuevos volúmenes y LUN que coincidan con los volúmenes de origen

Nota: Un disco de destino en el modelo FSX ONTAP FS es un "LUN" que se crea en un "Volumen" que tiene suficiente capacidad para contener el LUN más una cantidad razonable de sobrecarga para facilitar instantáneas y metadatos. La automatización de CMC se encarga de todos estos detalles para crear el volumen y la LUN adecuados con parámetros opcionales definidos por el usuario.

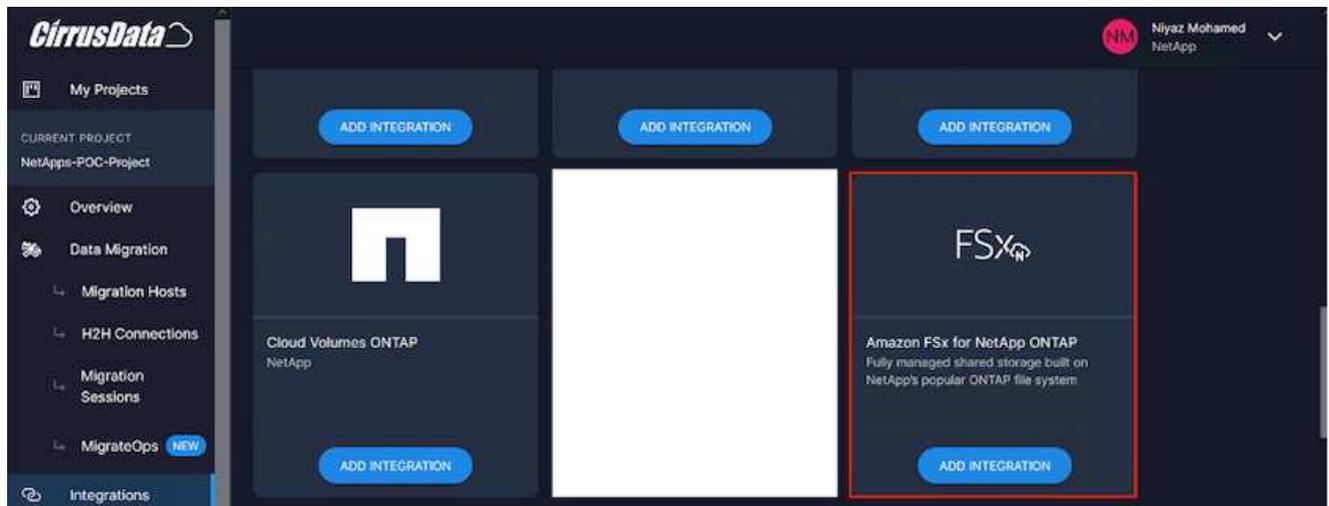
- Cree una entidad de host (denominada iGroups en FSx) con el IQN del iniciador de host
- Asigne los volúmenes recién creados a entidades host apropiadas mediante asignaciones
- Crear todas las demás configuraciones necesarias

Prepare el host de producción para la conexión iSCSI:

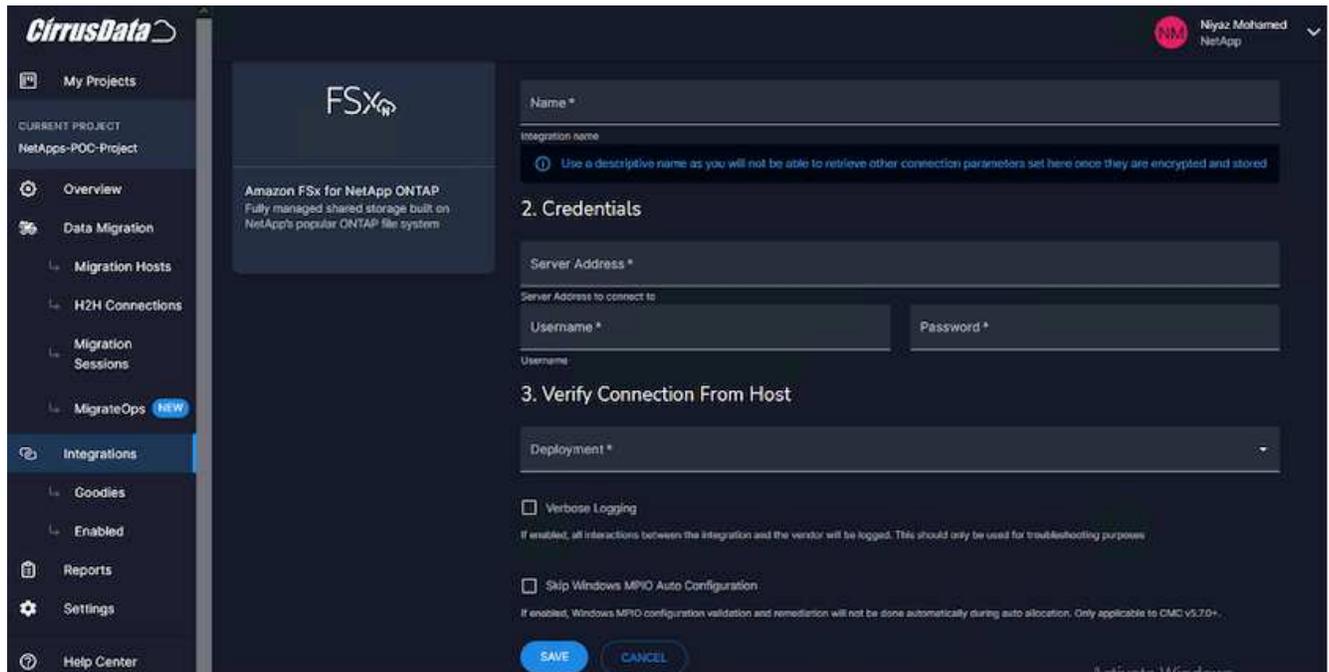
- Si es necesario, instale y configure la función iSCSI y configure el iniciador.
- Si es necesario, instale y configure multipath (MPIO para Windows) con los identificadores de proveedor adecuados.
- Ajuste la configuración del sistema, si es necesario, de acuerdo con las mejores prácticas del proveedor, por ejemplo, con la configuración udev en Linux.
- Cree y gestione conexiones iSCSI como destinos iSCSI persistentes/favoritos en Windows.

Para configurar la integración de CMC para FSx ONTAP y AWS, realice los siguientes pasos:

1. Inicie sesión en el portal de Cirrus Data Cloud.
2. Vaya al proyecto para el que desea activar la integración.
3. Vaya a Integraciones → Goodies.
4. Desplácese hasta encontrar FSx ONTAP y haga clic en AGREGAR INTEGRACIÓN.



5. Proporcione un nombre descriptivo (estrictamente para fines de visualización) y agregue las credenciales adecuadas.



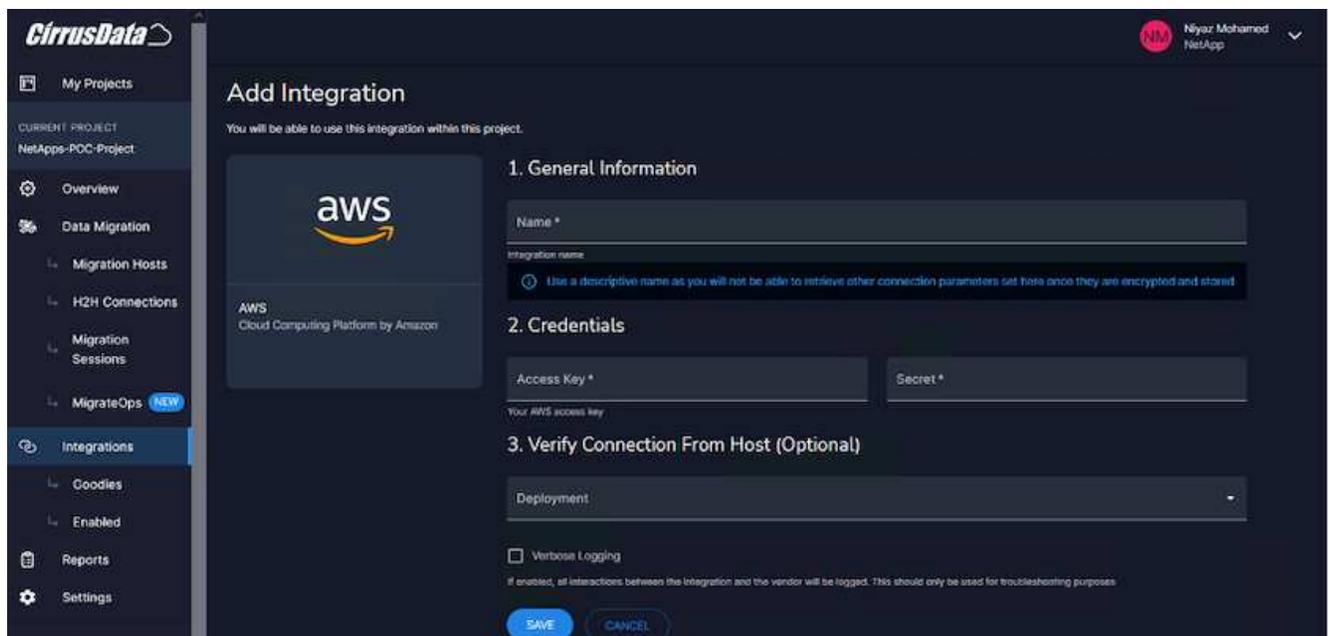
- Una vez creada la integración, durante la creación de una nueva sesión de migración, seleccione Asignar volúmenes de destino automáticamente para asignar automáticamente nuevos volúmenes en FSx ONTAP.

Nota: Se crearán nuevas LUN con el mismo tamaño que el tamaño del volumen de origen, a menos que "Migrate to small volumes" (Migración a volúmenes más pequeños) esté habilitado para la migración.

Nota: Si una entidad host (iGroup) no existe todavía, se creará una nueva. Se añadirán todos los IQN de iniciador iSCSI de host a la nueva entidad de host.

Nota: Si ya existe una entidad host existente con alguno de los iniciadores iSCSI, se reutilizará.

- Una vez hecho esto, agrega la integración para AWS, siguiendo los pasos en la pantalla.



Nota: Esta integración se utiliza al migrar máquinas virtuales del almacenamiento local a AWS junto con la

integración de FSX ONTAP.

Nota: Utilice relés de administración para comunicarse con Cirrus Data Cloud si no hay conexión saliente directa para migrar instancias de producción.

Con Integraciones agregadas, es hora de registrar hosts con el Proyecto. Vamos a cubrir esto con un escenario de ejemplo.

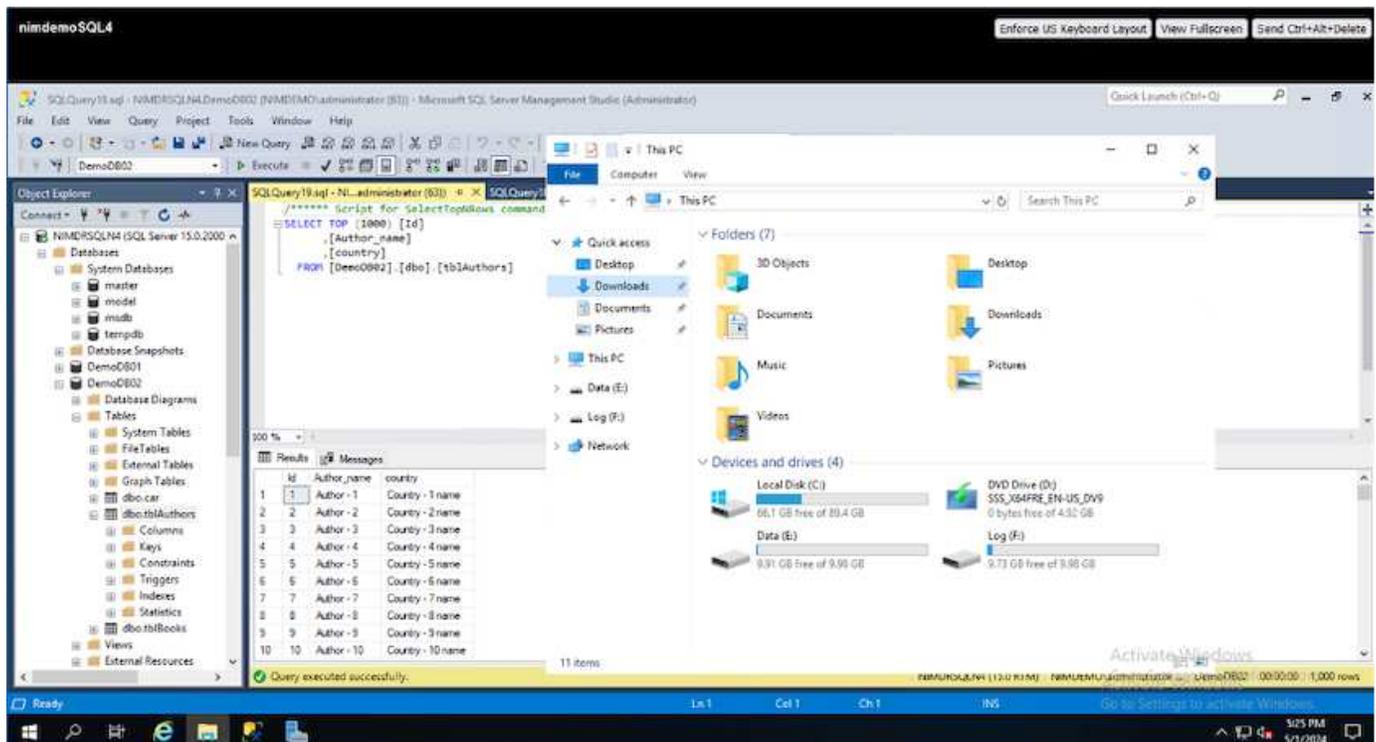
Escenario de registro de host

Equipos virtuales VMware invitados que residen en vCenter en el centro de datos en las instalaciones:

- Windows 2016 se ejecuta con SQL Server con tres VMDK, incluidos los sistemas operativos y los discos de datos. Está ejecutando una base de datos activa. La base de datos se encuentra en un volumen de datos respaldado por dos VMDK.

Nota: Dado que el origen es un entorno VMware y se utilizan VMDK, el software del iniciador iSCSI de Windows no está configurado actualmente en esta máquina virtual invitada. Para conectar con nuestro almacenamiento de destino mediante iSCSI, se deberán instalar y configurar tanto iSCSI como MPIO. La integración de Cirrus Data Cloud realizará esta instalación automáticamente durante el proceso.

Nota: La integración configurada en la sección anterior automatiza la configuración del nuevo almacenamiento de destino en la creación de los nuevos discos, la configuración de las entidades host y sus IQN, e incluso la corrección de la aplicación VM (host) para configuraciones iSCSI y multivía.



Esta demostración migrará los VMDK de aplicación desde cada equipo virtual a un volumen iSCSI provisionado y asignado automáticamente desde FSx ONTAP. El VMDK del sistema operativo en este caso se migrará a un volumen de Amazon EBS, ya que las instancias de Amazon EC2 admiten este Amazon EBS solo como disco de arranque.

Nota: El factor de escala con este enfoque de migración es el ancho de banda de la red y la tubería que conecta en las instalaciones a AWS VPC. Como cada equipo virtual tiene configurada 1:1 sesión de host, el

rendimiento de migración general depende de dos factores:

- Ancho de banda de red
- Tipo de instancia de destino y ancho de banda ENI

Los pasos de migración son los siguientes:

1. Instalar el agente CMC en cada host (Windows y Linux) designado para la etapa de migración. Esto se puede realizar ejecutando un comando de instalación de una línea.

Para ello, acceda a Data Migration > Migration Hosts > haga clic en «Deploy Cirrus Migrate Cloud» y seleccione «Windows».

A continuación, copie el iex Comando al host y ejecutarlo mediante PowerShell. Una vez que el despliegue del agente se realiza correctamente, el host se agregará al proyecto bajo “Hosts de migración”.

The screenshot shows the CirrusData console interface. On the left, the 'Migration Hosts' menu item is highlighted with a red box. A modal dialog titled 'Deploy Cirrus Migrate Cloud' is open, showing the 'WINDOWS' tab. The dialog contains the following text:

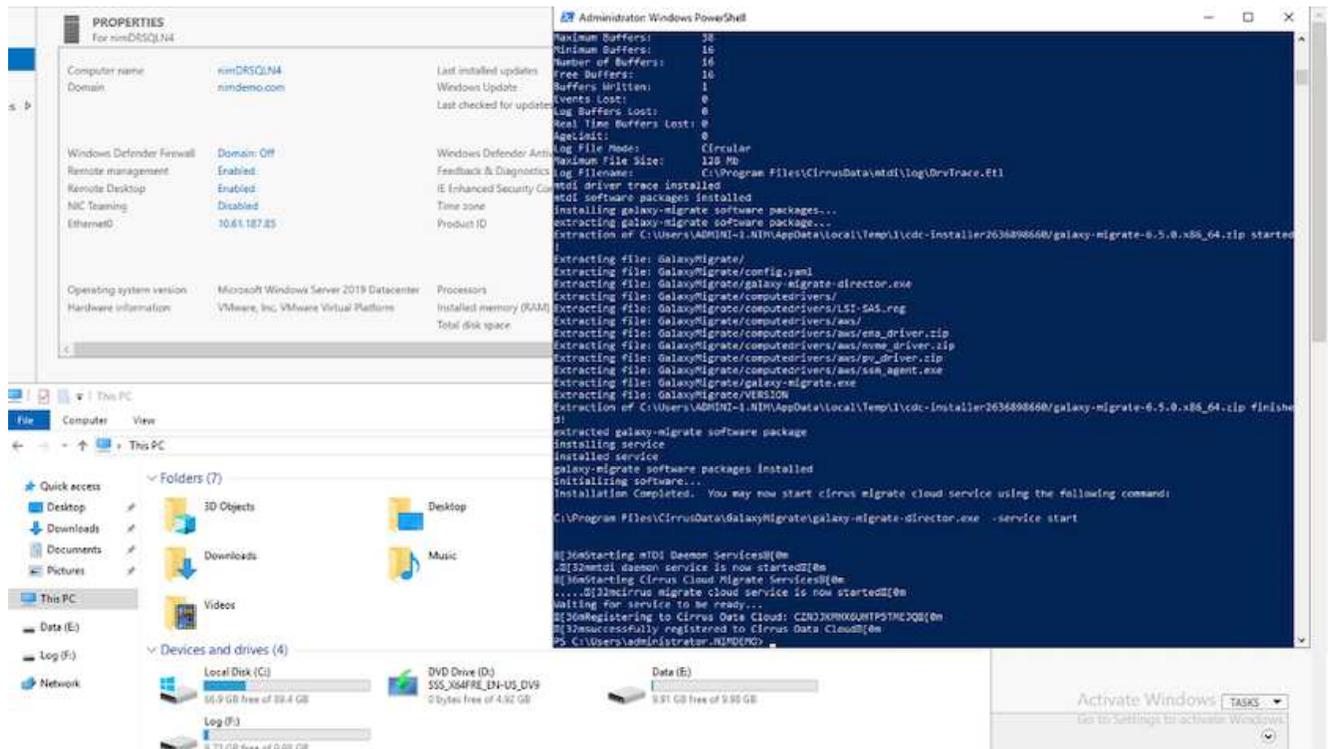
Installation - Windows
In your Windows administrator account, run the following command in powershell to install Cirrus Migrate Cloud:

```
iex "&($irm https://get.cirrusdata.cloud/install-cmc-win) -rgc CZNJJKMHXBUHTP5TMEJQ"
```

Uninstall - Windows
Run the following Command to uninstall Cirrus Migrate Cloud after migration is completed:

```
iex "&($irm https://get.cirrusdata.cloud/install-cmc-win) -uninstall"
```

The background shows a table of hosts with columns: Name, Check-in, Latency, Labels, and Actions. The table is currently empty.



2. Prepare el YAML para cada máquina virtual.

Nota: Es un paso vital tener un YAML para cada VM que especifique la receta o el plan necesario para la tarea de migración.

El YAML proporciona el nombre de la operación, las notas (descripción) junto con el nombre de la receta como `MIGRATEOPS_AWS_COMPUTE`, el nombre del host (`system_name`) y nombre de integración (`integration_name`) y la configuración de origen y destino. Los scripts personalizados se pueden especificar como una acción antes y después de la transición.

```
operations:
  - name: Win2016 SQL server to AWS
    notes: Migrate OS to AWS with EBS and Data to FSx ONTAP
    recipe: MIGRATEOPS_AWS_COMPUTE
    config:
      system_name: Win2016-123
      integration_name: NimAWSHybrid
      migrateops_aws_compute:
        region: us-west-2
        compute:
          instance_type: t3.medium
          availability_zone: us-west-2b
        network:
          vpc_id: vpc-05596abe79cb653b7
          subnet_id: subnet-070aeb9d6b1b804dd
          security_group_names:
            - default
      destination:
```

```

        default_volume_params:
            volume_type: GP2
        iscsi_data_storage:
            integration_name: DemoDRaaS
        default_volume_params:
            netapp:
                qos_policy_name: ""
    migration:
        session_description: Migrate OS to AWS with EBS and
Data to FSx ONTAP
        qos_level: MODERATE
    cutover:
        stop_applications:
            - os_shell:
                script:
                    - stop-service -name 'MSSQLSERVER'
-Force
                    - Start-Sleep -Seconds 5
                    - Set-Service -Name 'MSSQLSERVER'
-StartupType Disabled
                    - write-output "SQL service stopped
and disabled"

            - storage_unmount:
                mountpoint: e
            - storage_unmount:
                mountpoint: f
    after_cutover:
        - os_shell:
            script:
                - stop-service -name 'MSSQLSERVER'
-Force
                - write-output "Waiting 90 seconds to
mount disks..." > log.txt
                - Start-Sleep -Seconds 90
                - write-output "Now re-mounting disks
E and F for SQL..." >>log.txt
            - storage_unmount:
                mountpoint: e
            - storage_unmount:
                mountpoint: f
            - storage_mount_all: {}
            - os_shell:
                script:
                    - write-output "Waiting 60 seconds to
restart SQL Services..." >>log.txt

```

```

-Force

>>log.txt

-StartupType Automatic

- Start-Sleep -Seconds 60
- stop-service -name 'MSSQLSERVER'

- Start-Sleep -Seconds 3
- write-output "Start SQL Services..."

- Set-Service -Name 'MSSQLSERVER'

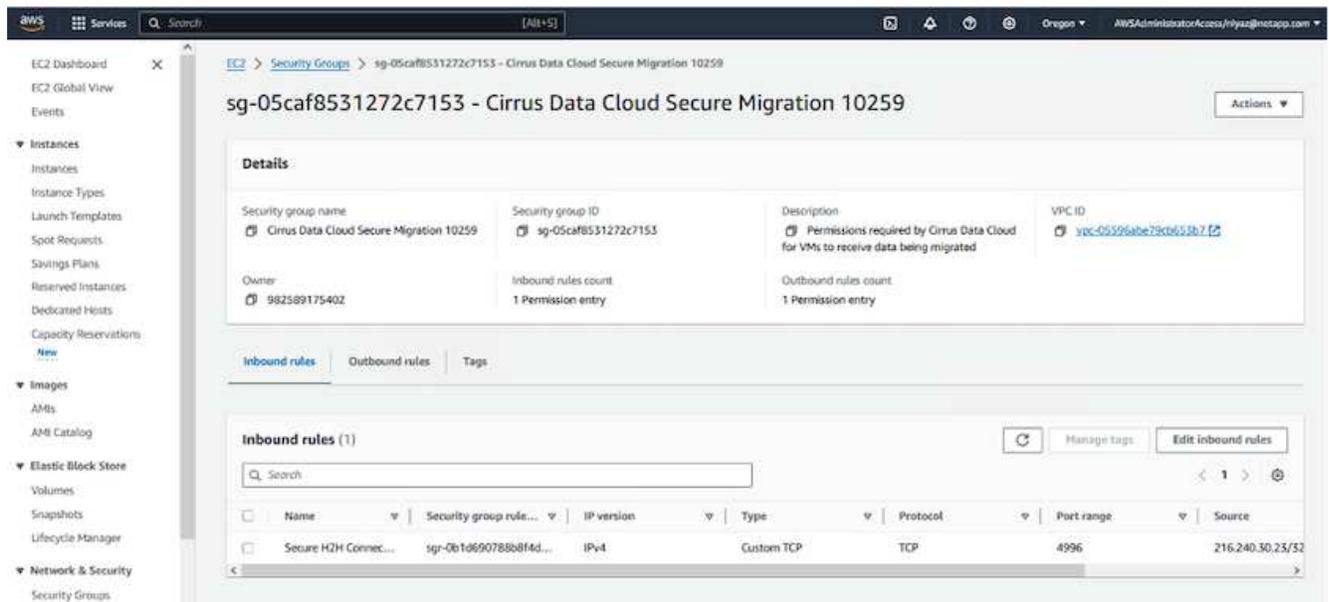
- start-service -name 'MSSQLSERVER'
- write-output "SQL started" >>log.txt

```

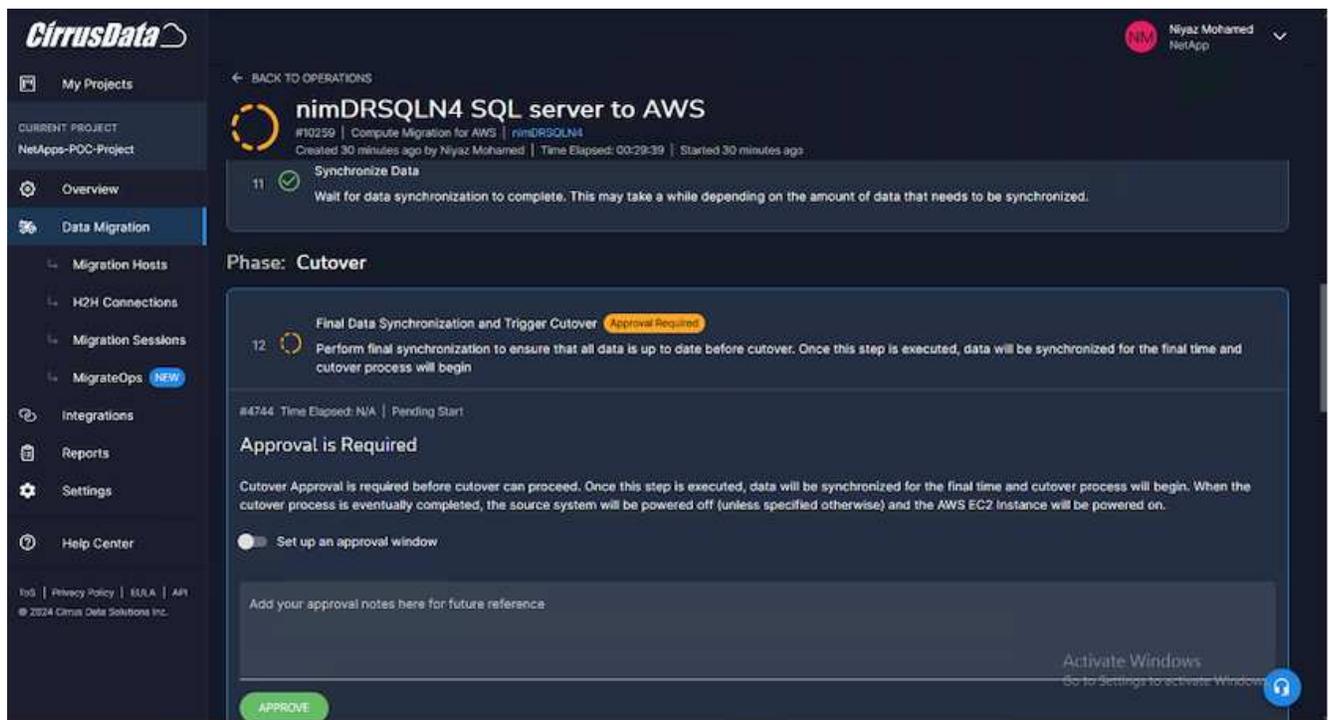
- Una vez instalados los YAML, crea la configuración de MigrateOps. Para ello, vaya a Data Migration > MigrateOps, haga clic en “Start New Operation” (Iniciar nueva operación) e introduzca la configuración en formato YAML válido.
 - Haga clic en “Crear operación”.
- Nota:** Para lograr el paralelismo, cada host necesita tener un archivo YAML especificado y configurado.
- A menos que el `scheduled_start_time` el campo se especifica en la configuración, la operación se iniciará inmediatamente.
 - La operación se ejecutará y continuará. Desde la interfaz de usuario de Cirrus Data Cloud, puede supervisar el progreso con mensajes detallados. Estos pasos incluyen automáticamente tareas que normalmente se realizan manualmente, como la asignación automática y la creación de sesiones de migración.



Nota: Durante la migración host-a-host, se creará un grupo de seguridad adicional con una regla que permita el puerto 4996 entrante, que permitirá el puerto requerido para la comunicación y se eliminará automáticamente una vez que se complete la sincronización.



7. Mientras esta sesión de migración se está sincronizando, hay un paso futuro en la fase 3 (transposición) con la etiqueta «Aprobación requerida». En una receta de MigrateOps, las tareas críticas (como los cortes de migración) requieren la aprobación del usuario antes de que puedan ejecutarse. Los operadores o administradores de proyectos pueden aprobar estas tareas desde la interfaz de usuario. También se puede crear una ventana de aprobación futura.



8. Una vez aprobada, la operación de MigrateOps continúa con la transición.
 9. Después de un breve momento, la operación se completará.



Nota: Con la ayuda de la tecnología Cirrus Data cMotion™, el almacenamiento de destino se ha mantenido actualizado con todos los cambios más recientes. Por lo tanto, una vez aprobada, el proceso final de transición llevará muy poco tiempo, menos de un minuto, en completarse.

Verificación posterior a la migración

Veamos la instancia de Amazon EC2 migrada que ejecuta el sistema operativo Windows Server y los siguientes pasos que se han completado:

1. Los servicios SQL de Windows se han iniciado ahora.
2. La base de datos vuelve a estar en línea y está utilizando el almacenamiento del dispositivo iSCSI Multipath.
3. Todos los registros nuevos de la base de datos agregados durante la migración se pueden encontrar en la base de datos recién migrada.
4. El almacenamiento antiguo ahora se encuentra desconectado.

Nota: Con solo un clic para enviar la operación de movilidad de datos como código, y un clic para aprobar la transposición, la VM ha migrado con éxito de VMware en las instalaciones a una instancia de Amazon EC2 usando FSx ONTAP y sus capacidades iSCSI.

Nota: Debido a la limitación de la API de AWS, las VM convertidas se mostrarían como “Ubuntu”. Esto es estrictamente un problema de visualización y no afecta a la funcionalidad de la instancia migrada. Una próxima versión resolverá este problema.

Nota: Se puede acceder a las instancias migradas de Amazon EC2 utilizando las credenciales que se utilizaron en el lado local.

Migra máquinas virtuales a Amazon EC2 mediante Amazon FSx para ONTAP: Otras posibilidades y conclusiones

Este artículo destaca otras posibilidades para esta solución de migración, así como la conclusión del tema.

Otras posibilidades

El mismo método se puede ampliar para migrar máquinas virtuales utilizando almacenamiento en invitado en máquinas virtuales on-premises. El VMDK del sistema operativo se puede migrar usando CMC, y los LUN iSCSI internos se pueden replicar mediante SnapMirror. El proceso requiere interrumpir la duplicación y conectar el LUN a la instancia recién migrada de Amazon EC2, como se muestra en el siguiente diagrama.



Conclusión

Este documento ha proporcionado un tutorial completo sobre el uso de la función MigrateOps de CMC para migrar los datos almacenados en repositorios de VMware locales a AWS mediante instancias de Amazon EC2 y FSx ONTAP.

En el siguiente vídeo se muestra el proceso de migración de principio a fin:

[Migre máquinas virtuales de VMware a Amazon EC2](#)

Para ver la interfaz gráfica de usuario y la migración local básica de Amazon EBS a FSx ONTAP, vea este vídeo de demostración de cinco minutos:



Local Migration with
MigrateOps

Migración a cualquier almacenamiento a escala con Cirrus Migrate Cloud

Multicloud híbrido de NetApp con soluciones de VMware

Casos de uso de multicloud híbrido de VMware

Casos de uso del multicloud híbrido de NetApp con VMware

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

Casos de uso populares

Sus casos de uso son:

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

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

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

- Migración
- Extender

En el camino hacia la TECNOLOGÍA

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

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

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

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

Consideremos este caso:

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

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

Automatización de VMware vSphere

Introducción a la automatización para ONTAP y vSphere

Esta página describe las ventajas de automatizar la funcionalidad básica de ONTAP en un entorno VMware vSphere.

Automatización de VMware

La automatización ha sido un aspecto integral de la gestión de entornos VMware desde los primeros días de VMware ESX. La capacidad de poner en marcha infraestructura como código y ampliar las prácticas en operaciones de cloud privado ayuda a paliar las cuestiones relacionadas con el escalado, la flexibilidad, el aprovisionamiento automático y la eficiencia.

La automatización se puede organizar en las siguientes categorías:

- **Implementación de infraestructura virtual**
- **Operaciones de máquina invitada**
- **Operaciones en la nube**

Los administradores tienen a su disposición muchas opciones en lo que respecta a la automatización de su infraestructura. Ya sea mediante el uso de funciones nativas de vSphere como Perfiles de host o especificaciones de personalización para máquinas virtuales hasta las API disponibles en los componentes de software, los sistemas operativos y los sistemas de almacenamiento de NetApp, existe una documentación y guía significativas disponibles.

Data ONTAP 8.0.1 y versiones posteriores admiten ciertas funciones de API de VMware vSphere para la integración de cabinas (VAAI) cuando el host ESX ejecuta ESX 4.1 o versiones posteriores. VAAI es un conjunto de API que permiten la comunicación entre hosts ESXi de VMware vSphere y dispositivos de almacenamiento. Estas funciones ayudan a descargar las operaciones del host ESX al sistema de almacenamiento y aumentan el rendimiento de la red. El host ESX habilita las funciones automáticamente en el entorno correcto. Puede determinar la extensión hasta la cual el sistema utiliza las funciones de VAAI si se comprueban las estadísticas contenidas en los contadores VAAI.

El punto de partida más común para automatizar la puesta en marcha de un entorno VMware es el aprovisionamiento de almacenes de datos basados en bloques o archivos. Es importante trazar el mapa de los requisitos de las tareas reales antes de desarrollar la automatización correspondiente.

Si quiere más información sobre la automatización de los entornos VMware, consulte los siguientes recursos:

- ["ThePub de NetApp"](#). Gestión y automatización de la configuración de NetApp.
- ["La comunidad de Ansible Galaxy para VMware"](#). Una colección de recursos de Ansible para VMware.
- ["Recursos de VMware {code}"](#). Los recursos necesarios para diseñar soluciones para el centro de datos definido mediante software, incluidos foros, estándares de diseño, código de muestra y herramientas de desarrollo.

Aprovisionamiento de almacenamiento en bloques tradicional

Aprovisionamiento de almacenamiento en bloques vSphere tradicional con ONTAP

VMware vSphere admite las siguientes opciones de almacenes de datos VMFS con la compatibilidad con el protocolo SAN de ONTAP indicada.

Opciones de almacén de datos VMFS	Compatibilidad con el protocolo SAN de ONTAP
"Fibre Channel (FC)"	sí

Opciones de almacén de datos VMFS	Compatibilidad con el protocolo SAN de ONTAP
"Fibre Channel sobre Ethernet (FCoE)"	sí
"iSCSI"	sí
Extensiones iSCSI para RDMA (Iser)	no
"NVMe sobre estructura con FC (NVMe/FC)"	sí
NVMe over Fabric con RDMA sobre Ethernet convergente (NVMe/roce)	no



Si se requiere Iser o VMFS NVMe/roce, compruebe los sistemas de almacenamiento basados en SANtricity.

Almacén de datos VMFS de vSphere: Back-end de almacenamiento de Fibre Channel con ONTAP

En esta sección se describe la creación de un almacén de datos VMFS con el almacenamiento Fibre Channel (FC) de ONTAP.

Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP
- Un sistema de almacenamiento ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) que ejecuta {ontap_version}
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- WWPN de ONTAP con información sobre el host, el destino y la SVM y LUN
- ["La hoja de datos de configuración de FC completada"](#)
- Credenciales de vCenter Server
- Información sobre los hosts de vSphere
 - {vsphere_version}
- Switch(es) de estructura
 - Con los puertos de datos FC de ONTAP conectados y los hosts de vSphere
 - Con la función de virtualización N_Port ID (NPIV) habilitada
 - Cree una zona de destino única de iniciador.
 - Cree una zona para cada iniciador (zona iniciador única).
 - 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.
- Una herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar.

Aprovisionamiento de un almacén de datos VMFS

Para aprovisionar un almacén de datos VMFS, complete los siguientes pasos:

1. Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#)

2. Compruebe que el ["Es compatible con la configuración de FCP"](#).

Tareas de ONTAP

1. ["Comprobar que tiene una licencia de ONTAP para FCP."](#)
 - a. Utilice la `system license show` Comando para comprobar que FCP aparece.
 - b. Uso `licen se add -license-code <license code>` para añadir la licencia.
2. Asegúrese de que el protocolo FCP esté habilitado en la SVM.
 - a. ["Comprobar el FCP en una SVM existente."](#)
 - b. ["Configure el FCP en una SVM existente."](#)
 - c. ["Cree una nueva SVM con FCP."](#)
3. Asegúrese de que las interfaces lógicas FCP estén disponibles en una SVM.
 - a. Uso `Network Interface show` Para comprobar el adaptador FCP.
 - b. Cuando se crea una SVM con la interfaz gráfica de usuario, las interfaces lógicas forman parte de ese proceso.
 - c. Para cambiar el nombre de las interfaces de red, utilice `Network Interface modify`.
4. ["Cree y asignar una LUN."](#) Omita este paso si utiliza herramientas de ONTAP para VMware vSphere.

Tareas de VMware vSphere

1. Es decir, que están instalados los controladores HBA. Los HBA compatibles con VMware tienen controladores instalados de fábrica y deben estar visibles en la ["Información del adaptador de almacenamiento"](#).
2. ["Aprovisione un almacén de datos VMFS con herramientas de ONTAP"](#).

Almacén de datos VMFS de vSphere: Protocolo de almacenamiento Fibre Channel sobre Ethernet con ONTAP

En esta sección se describe la creación de un almacén de datos VMFS con el protocolo de transporte Fibre Channel over Ethernet (FCoE) al almacenamiento de ONTAP.

Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP
- Un sistema de almacenamiento ONTAP (FAS/AFF/CVO/ONTAP Select) que ejecuta {ontap_version}
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- ["Una combinación de FCoE compatible"](#)
- ["Una hoja de datos de configuración completada"](#)
- Credenciales de vCenter Server
- Información sobre los hosts de vSphere
 - {vsphere_version}
- Switch(es) de estructura
 - Con los puertos de datos FC de ONTAP o los hosts de vSphere conectados

- Con la función de virtualización N_Port ID (NPIV) habilitada
- Cree una zona de destino única de iniciador.
- ["Se ha configurado la división en zonas de FC/FCoE"](#)
- Switches de red
 - Compatibilidad con FCoE
 - Compatibilidad con DCB
 - ["Tramas gigantes para FCoE"](#)
- Herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar

Aprovisione un almacén de datos de VMFS

- Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#).
- ["Compruebe que la configuración de FCoE es compatible"](#).

Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para FCP."](#)
 - a. Utilice la `system license show` Comando para verificar que el FCP aparece.
 - b. Uso `license add -license-code <license code>` para añadir una licencia.
2. Compruebe que el protocolo FCP esté habilitado en la SVM.
 - a. ["Comprobar el FCP en una SVM existente."](#)
 - b. ["Configure el FCP en una SVM existente."](#)
 - c. ["Cree una nueva SVM con el FCP."](#)
3. Comprobar que las interfaces lógicas FCP están disponibles en la SVM.
 - a. Uso `Network Interface show` Para comprobar el adaptador FCP.
 - b. Cuando se crea la SVM con la interfaz gráfica de usuario, las interfaces lógicas forman parte de ese proceso.
 - c. Para cambiar el nombre de la interfaz de red, utilice `Network Interface modify`.
4. ["Cree y asigne una LUN"](#); Omita este paso si utiliza las herramientas de ONTAP para VMware vSphere.

Tareas de VMware vSphere

1. Compruebe que los controladores HBA están instalados. Los HBA compatibles con VMware tienen controladores instalados de fábrica y deben estar visibles en la ["información del adaptador de almacenamiento"](#).
2. ["Aprovisione un almacén de datos VMFS con herramientas de ONTAP"](#).

Almacén de datos VMFS de vSphere: Entorno de administración del almacenamiento iSCSI con ONTAP

En esta sección, se describe la creación de un almacén de datos VMFS con almacenamiento ONTAP iSCSI.

Para el aprovisionamiento automatizado, utilice el siguiente script: [\[Ansible\]](#).

Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP.
- Un sistema de almacenamiento ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) que ejecuta {ontap_version}
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- Información sobre los puertos de red de ONTAP, SVM y LUN para iSCSI
- ["Hoja de datos de configuración de iSCSI completada"](#)
- Credenciales de vCenter Server
- Información sobre los hosts de vSphere
 - {vsphere_version}
- Información de IP del adaptador de VMkernel de iSCSI
- Switches de red
 - Con los puertos de datos de red del sistema ONTAP y los hosts de vSphere conectados
 - VLAN configuradas para iSCSI
 - (Opcional) agregación de enlaces configurada para los puertos de datos de red ONTAP
- Herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar

Pasos

1. Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#).
2. ["Compruebe que la configuración de iSCSI es compatible."](#)
3. Complete las siguientes tareas de ONTAP y vSphere.

Tareas de ONTAP

1. ["Compruebe la licencia de ONTAP para iSCSI"](#).
 - a. Utilice la `system license show` Comando para comprobar si iSCSI aparece.
 - b. Use `license add -license-code <license code>` para añadir la licencia.
2. ["Compruebe que el protocolo iSCSI está habilitado en la SVM."](#)
3. Confirmar que las interfaces lógicas de red iSCSI están disponibles en la SVM.



Cuando se crea una SVM mediante la interfaz gráfica de usuario, también se crean interfaces de red iSCSI.

4. Utilice la `Network interface` comando para ver o realizar cambios en la interfaz de red.



Se recomiendan dos interfaces de red iSCSI por nodo.

5. ["Cree una interfaz de red iSCSI."](#) Puede usar la política de servicio de bloques de datos predeterminada.
6. ["Comprobar que el servicio de datos iscsi está incluido en la normativa de servicio."](#) Puede utilizar `network interface service-policy show` para verificar.
7. ["Compruebe que las tramas gigantes están habilitadas."](#)
8. ["Cree y asigne la LUN."](#) Omite este paso si utiliza herramientas de ONTAP para VMware vSphere. Repita

este paso con cada LUN.

Tareas de VMware vSphere

1. Verifique que hay al menos un NIC disponible para la VLAN iSCSI. Se prefieren dos NIC para mejorar el rendimiento y la tolerancia a fallos.
2. "Identifique la cantidad de NIC físicas disponibles en el host vSphere."
3. "Configure el iniciador de iSCSI." Un caso de uso típico es un iniciador iSCSI de software.
4. "Compruebe que la pila TCP/IP para iSCSI está disponible".
5. "Compruebe que los grupos de puertos iSCSI estén disponibles".
 - Normalmente utilizamos un único switch virtual con varios puertos de enlace ascendente.
 - Utilice la asignación de adaptador 1:1.
6. Compruebe que los adaptadores de VMkernel iSCSI están habilitados para coincidir con el número de NIC y que las IP están asignadas.
7. "Vincule el adaptador de software iSCSI a los adaptadores de VMkernel iSCSI."
8. "Aprovisione el almacén de datos VMFS con herramientas de ONTAP". Repita este paso para todos los almacenes de datos.
9. "Comprobar la compatibilidad con la aceleración de hardware."

El futuro

Una vez completadas estas tareas, el almacén de datos VMFS estará listo para consumir para aprovisionar máquinas virtuales.

Libro de estrategia de Ansible

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
        password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
      register: vclogin

    # Generate Session ID for ONTAP tools with vCenter
```

```

- name: Generate a Session ID for ONTAP tools with vCenter
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/security/user/login"
    validate_certs: false
    method: POST
    return_content: yes
    body_format: json
    body:
      vcenterUserName: "{{ vcenter_username }}"
      vcenterPassword: "{{ vcenter_password }}"
  register: login

# Get existing registered ONTAP Cluster info with ONTAP tools
- name: Get ONTAP Cluster info from ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
    validate_certs: false
    method: Get
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  register: clusterinfo

- name: Get ONTAP Cluster ID
  set_fact:
    ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
  vars:
    clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

- name: Get ONTAP SVM ID
  set_fact:
    ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
  vars:
    svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

- name: Get Aggregate detail
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
    validate_certs: false
    method: GET

```

```

    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      cluster-id: "{{ ontap_svm_id }}"
    when: ontap_svm_id != ''
    register: aggrinfo

- name: Select Aggregate with max free capacity
  set_fact:
    aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
  vars:
    aggrquery: "max_by(records, &freeCapacity).name"

- name: Convert datastore size in MB
  set_fact:
    datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

- name: Get vSphere Cluster Info
  uri:
    url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
    validate_certs: false
    method: GET
    return_content: yes
    body_format: json
    headers:
      vmware-api-session-id: "{{ vclogin.json.value }}"
  when: vsphere_cluster != ''
  register: vcenterclusterid

- name: Create iSCSI VMFS-6 Datastore with ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
    validate_certs: false
    method: POST
    return_content: yes
    status_code: [200]
    body_format: json
    body:
      traditionalDatastoreRequest:
        name: "{{ iscsi_datastore_name }}"
        datastoreType: VMFS
        protocol: ISCSI
        spaceReserve: Thin

```

```

        clusterID: "{{ ontap_cluster_id }}"
        svmID: "{{ ontap_svm_id }}"
        targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
        datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
        vmfsFileSystem: VMFS6
        aggrName: "{{ aggr_name }}"
        existingFlexVolName: ""
        volumeStyle: FLEXVOL
        datastoreClusterMoref: ""
    headers:
        vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
    when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''
    register: result
    changed_when: result.status == 200

```

Almacén de datos VMFS de vSphere: NVMe/FC con ONTAP

En esta sección se describe la creación de un almacén de datos VMFS con almacenamiento ONTAP mediante NVMe/FC.

Lo que necesita

- Se necesitan habilidades básicas para gestionar un entorno de vSphere y ONTAP.
- ["Comprensión básica de NVMe/FC"](#).
- Un sistema de almacenamiento ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) que ejecuta {ontap_version}
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- WWPN de ONTAP para información sobre el host, el destino y las SVM y la LUN
- ["Una hoja de datos de configuración de FC completada"](#)
- VCenter Server
- Información de hosts de vSphere ({vsphere_version})
- Switch(es) de estructura
 - Con los puertos de datos FC de ONTAP y los hosts de vSphere conectados.
 - Con la función de virtualización N_Port ID (NPIV) habilitada.
 - Cree una sola zona de destino de iniciador.
 - Cree una zona para cada iniciador (zona iniciador única).
 - 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.

Aprovisione el almacén de datos VMFS

1. Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#).
2. ["Compruebe que la configuración de NVMe/FC sea compatible."](#)

Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para FCP."](#) Utilice `system license show` el comando y compruebe si `NVMe_oF` está en la lista. Se utiliza `license add -license-code <license code>` para agregar una licencia.
2. Compruebe que el protocolo NVMe esté habilitado en la SVM.
 - a. ["Configure SVM para NVMe."](#)
3. Compruebe que las interfaces lógicas de NVMe/FC estén disponibles en las SVM.
 - a. Use `Network Interface show` Para comprobar el adaptador FCP.
 - b. Cuando se crea una SVM con la interfaz gráfica de usuario, las interfaces lógicas se forman parte de ese proceso.
 - c. Para cambiar el nombre de la interfaz de red, utilice el comando `Network Interface modify`.
4. ["Cree el espacio de nombres y el subsistema NVMe"](#)

Tareas de VMware vSphere

1. Compruebe que los controladores HBA están instalados. Los HBA compatibles con VMware tienen los controladores instalados de fábrica y deben ser visibles en ["Información del adaptador de almacenamiento"](#)
2. ["Realice tareas de instalación y validación del controlador vSphere NVMe host"](#)
3. ["Crear almacén de datos VMFS"](#)

Aprovisionamiento de almacenamiento de ficheros tradicional

Aprovisionamiento de almacenamiento de archivos tradicional de vSphere con ONTAP

VMware vSphere admite los siguientes protocolos NFS, los cuales son compatibles con ONTAP.

- ["NFS Versión 3"](#)
- ["NFS Versión 4.1"](#)

Si necesita ayuda para seleccionar la versión de NFS correcta para vSphere, compruebe ["Esta comparativa de las versiones del cliente NFS"](#).

Referencia

["Funciones de protocolo y almacén de datos de vSphere: NFS"](#)

Almacén de datos NFS de vSphere: Versión 3 con ONTAP

Creación de un almacén de datos de NFS versión 3 con almacenamiento NAS de ONTAP.

Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP.
- Un sistema de almacenamiento de ONTAP (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) que ejecuta `{ONTAP_VERSION}`

- Credenciales de ONTAP (nombre de SVM, ID de usuario, contraseña)
- Información sobre el puerto de red de ONTAP, SVM y LUN para NFS
 - ["Una hoja de trabajo de configuración de NFS completada"](#)
- Credenciales de vCenter Server
- Información de los hosts de vSphere para {vsphere_version}
- Información de IP del adaptador de VMkernel de NFS
- Switches de red
 - Con los puertos de datos de red del sistema ONTAP y los hosts de vSphere conectados
 - VLAN configuradas para NFS
 - (Opcional) agregación de enlaces configurada para los puertos de datos de red ONTAP
- Herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar

Pasos

- Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#)
 - ["Compruebe que la configuración de NFS es compatible."](#)
- Complete las siguientes tareas de ONTAP y vSphere.

Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para NFS."](#)
 - a. Utilice la `system license show` Y compruebe que NFS aparece en la lista.
 - b. Uso `license add -license-code <license code>` para añadir una licencia.
2. ["Siga el flujo de trabajo de configuración de NFS."](#)

Tareas de VMware vSphere

["Siga el flujo de trabajo de configuración del cliente NFS para vSphere."](#)

Referencia

["Funciones de protocolo y almacén de datos de vSphere: NFS"](#)

El futuro

Una vez completadas estas tareas, el almacén de datos NFS estará listo para consumir para aprovisionar máquinas virtuales.

Almacén de datos NFS de vSphere: Versión 4.1 con ONTAP

En esta sección se describe la creación de un almacén de datos de NFS versión 4.1 con almacenamiento NAS de ONTAP.

Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP

- Sistema de almacenamiento ONTAP (FAS/AFF/CVO/ONTAP Select/Servicio de volumen de cloud/Azure NetApp Files) con {ontap_version}
- Credenciales de ONTAP (nombre de SVM, ID de usuario, contraseña)
- Información sobre el puerto de red de ONTAP, SVM y LUN para NFS
- ["Una hoja de trabajo de configuración de NFS completada"](#)
- Credenciales de vCenter Server
- Información de los hosts de vSphere {vsphere_version}
- Información de IP del adaptador de VMkernel de NFS
- Switches de red
 - Con los puertos de datos de red del sistema ONTAP, los hosts de vSphere y los están conectados
 - VLAN configuradas para NFS
 - (Opcional) agregación de enlaces configurada para los puertos de datos de red ONTAP
- Herramientas de ONTAP para VMware vSphere puestas en marcha, configuradas y listas para usar

Pasos

- Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)."](#)
 - ["Compruebe que la configuración de NFS es compatible."](#)
- Complete las tareas de ONTAP y vSphere que se proporcionan a continuación.

Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para NFS"](#)
 - a. Úselos `system license show` Comando para comprobar si NFS aparece en la lista.
 - b. Uso `license add -license-code <license code>` para añadir una licencia.
2. ["Siga el flujo de trabajo de configuración de NFS"](#)

Tareas de VMware vSphere

["Siga el flujo de trabajo de configuración del cliente de NFS para vSphere."](#)

El futuro

Una vez completadas estas tareas, el almacén de datos NFS estará listo para consumir para aprovisionar máquinas virtuales.

Recopilador de datos de máquina virtual (VMDC)

El recopilador de datos de máquina virtual (VMDC) es un kit de herramientas gratuito, ligero y sencillo basado en una interfaz gráfica de usuario para entornos de VMware que permite a los usuarios recopilar información detallada de inventario sobre sus máquinas virtuales, hosts, almacenamiento y redes.

Descripción general

La función principal de VMDC es generar informes sobre la configuración de vCenter, servidores ESXi y máquinas virtuales (VM) que residen en un entorno de vSphere, incluidos los datos de configuración del clúster, de redes, del almacenamiento y de rendimiento. Una vez que se han recopilado datos ambientales integrales, se pueden utilizar para producir información detallada sobre la infraestructura. La pantalla de salida de informes es una GUI de estilo hoja de cálculo con varias pestañas en sus distintas secciones. Facilita informes fáciles de leer y ayuda a optimizar el uso de recursos y la planificación de la capacidad.

VMDC es solo una piedra angular para recopilar estadísticas rápidas e instantáneas para proyectar posibilidades de optimización para las licencias de núcleo de VMware junto con vCPU y RAM. ["Información sobre la infraestructura de datos de NetApp"](#) Lo que requiere la instalación de AUS y recopiladores de datos debe ser el siguiente paso obvio para comprender la topología detallada de VM, agrupar VM mediante anotación para ajustar el tamaño adecuado de las cargas de trabajo y proteger la infraestructura para el futuro.

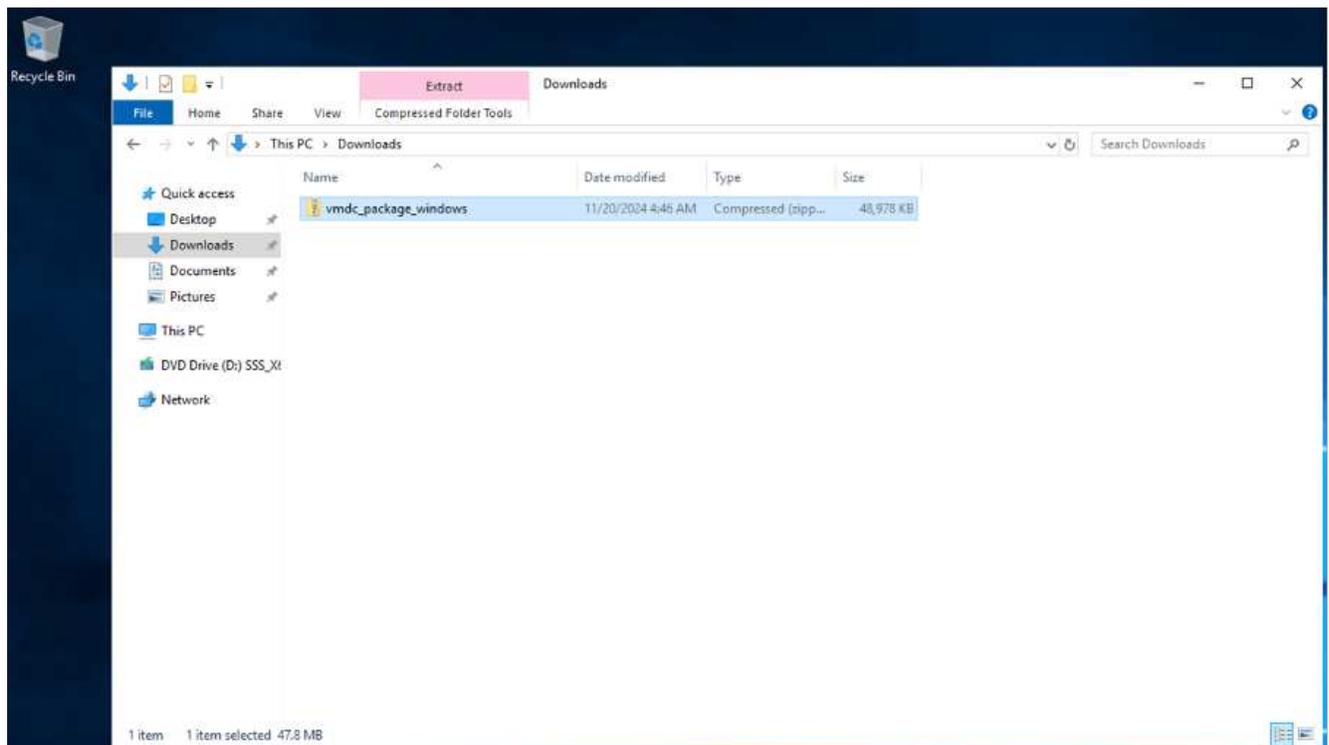
VMDC se puede descargar ["aquí"](#) y solo está disponible para sistemas Windows.

Instalación y configuración de VMDC

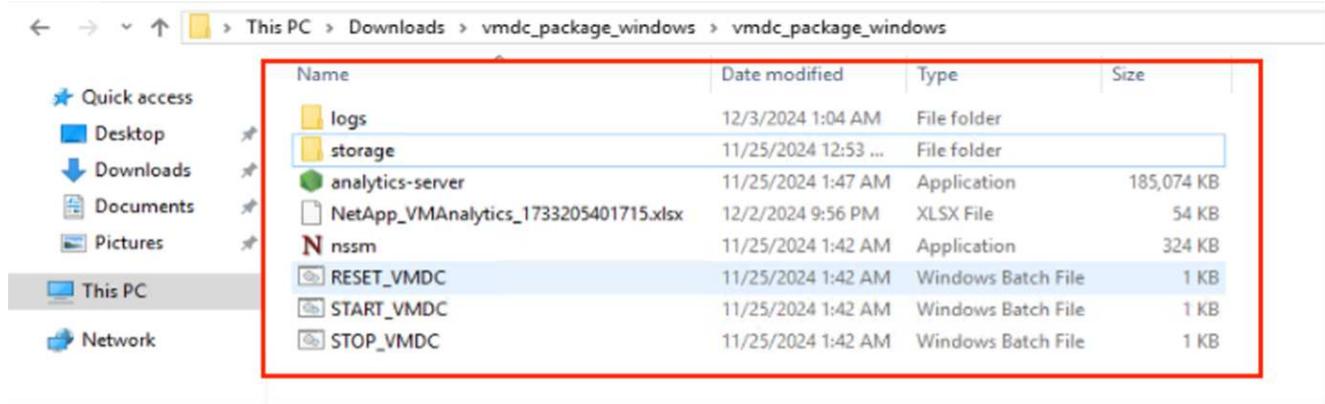
VMDC se puede ejecutar en Windows 2019, versión 2022. El requisito previo es contar con conectividad de red desde la instancia de VMDC a los servidores de vCenter designados. Una vez verificado, descargue el paquete VMDC desde ["Toolchest de NetApp"](#) y, a continuación, descomprima el paquete y ejecute el archivo por lotes para instalar e iniciar el servicio.

Una vez instalado VMDC, acceda a la interfaz de usuario con la dirección IP mencionada durante la instalación. Esto abrirá la interfaz de inicio de sesión VMDC, donde se puede añadir el para vCenter; para ello, introduzca la dirección IP o el nombre DNS y las credenciales de una instancia de vCenter Server.

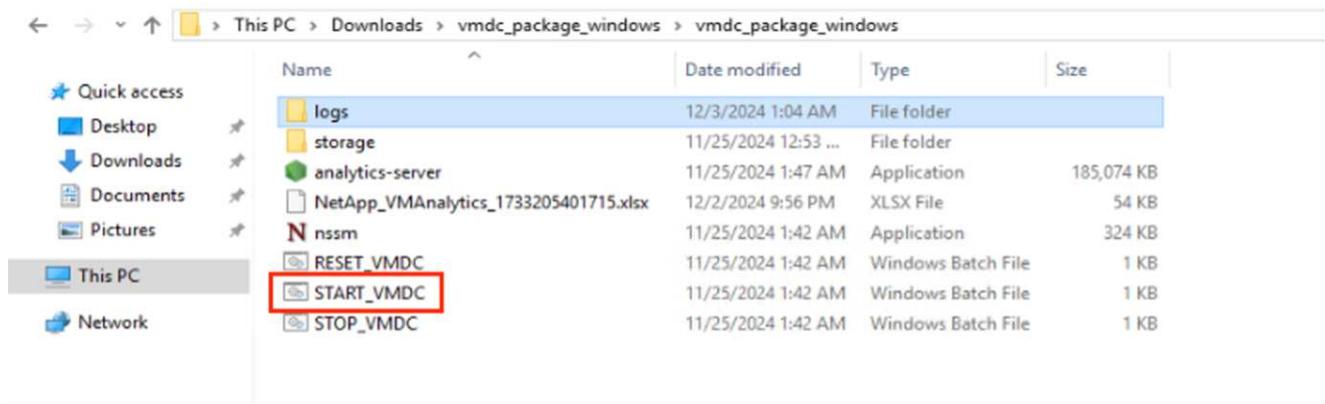
1. Descargar ["Paquete VMDC"](#).



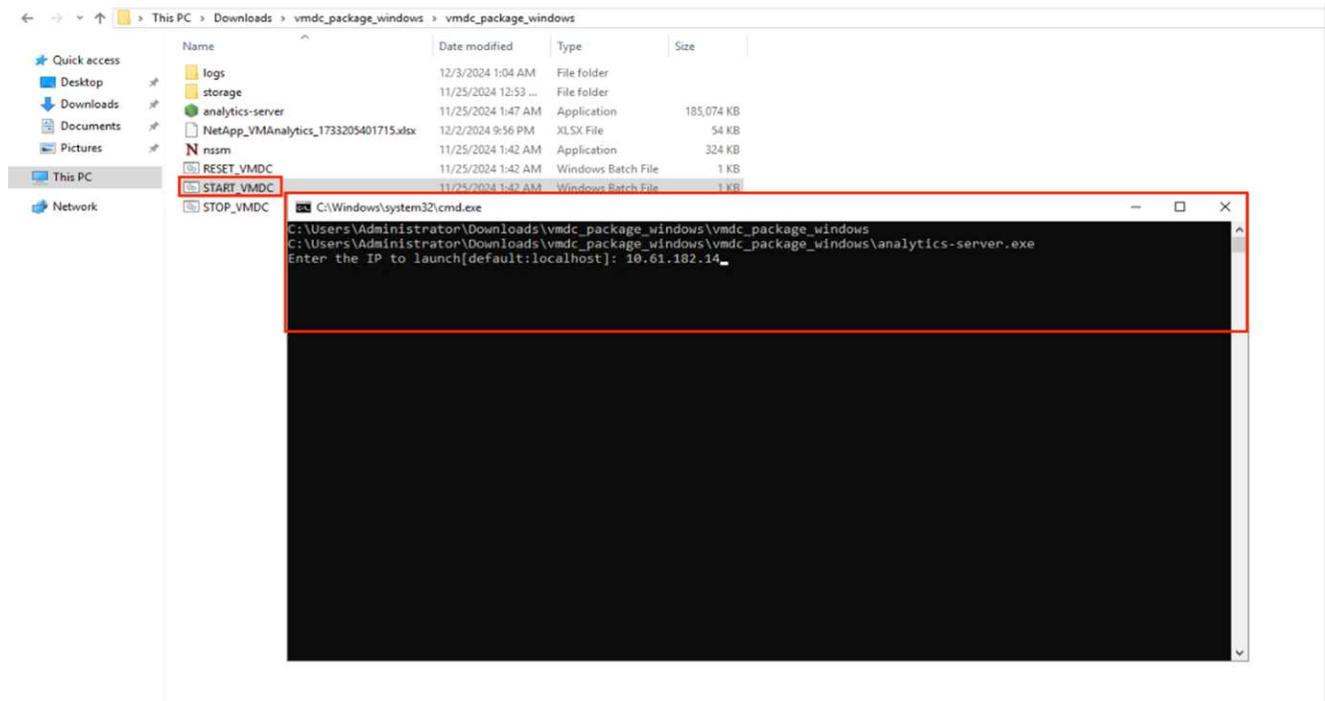
2. Extraiga el paquete en la carpeta designada.

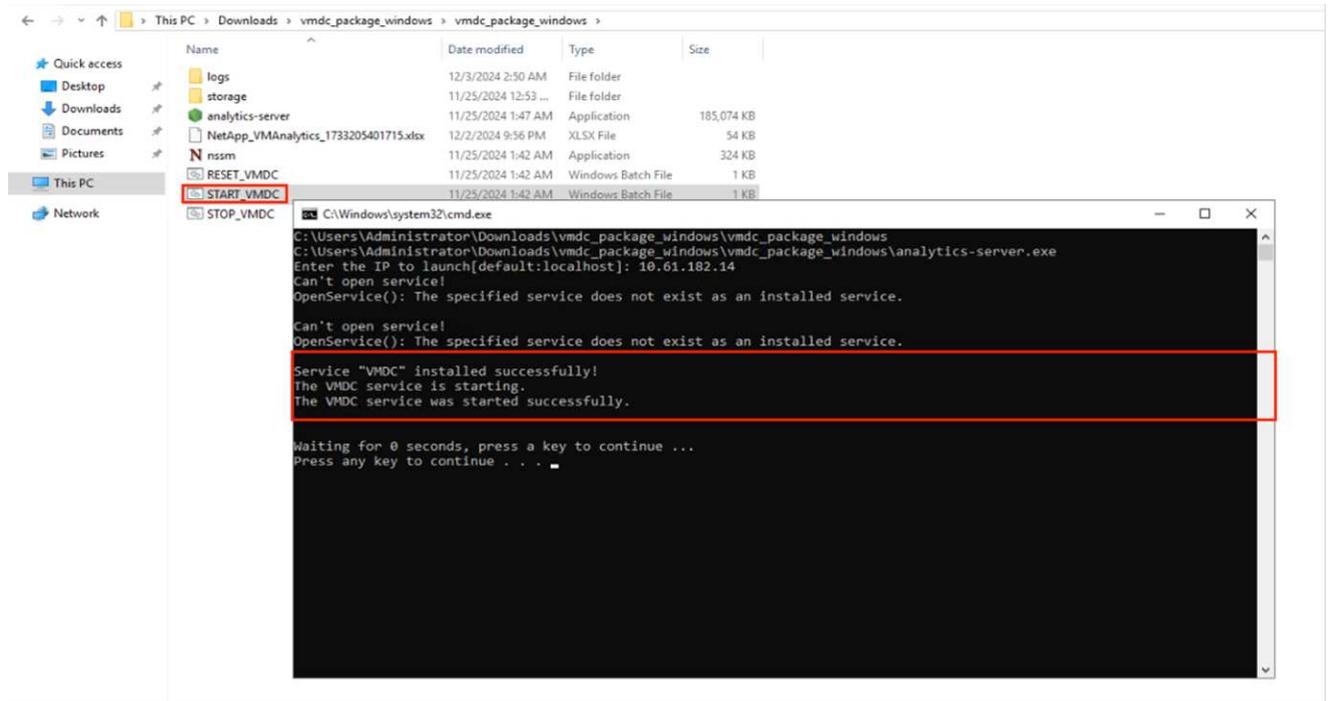


3. Ejecute el paquete VMDC haciendo clic en el archivo por lotes Start_VMDC. Esto abrirá el símbolo del sistema y solicitará que introduzca la dirección IP.

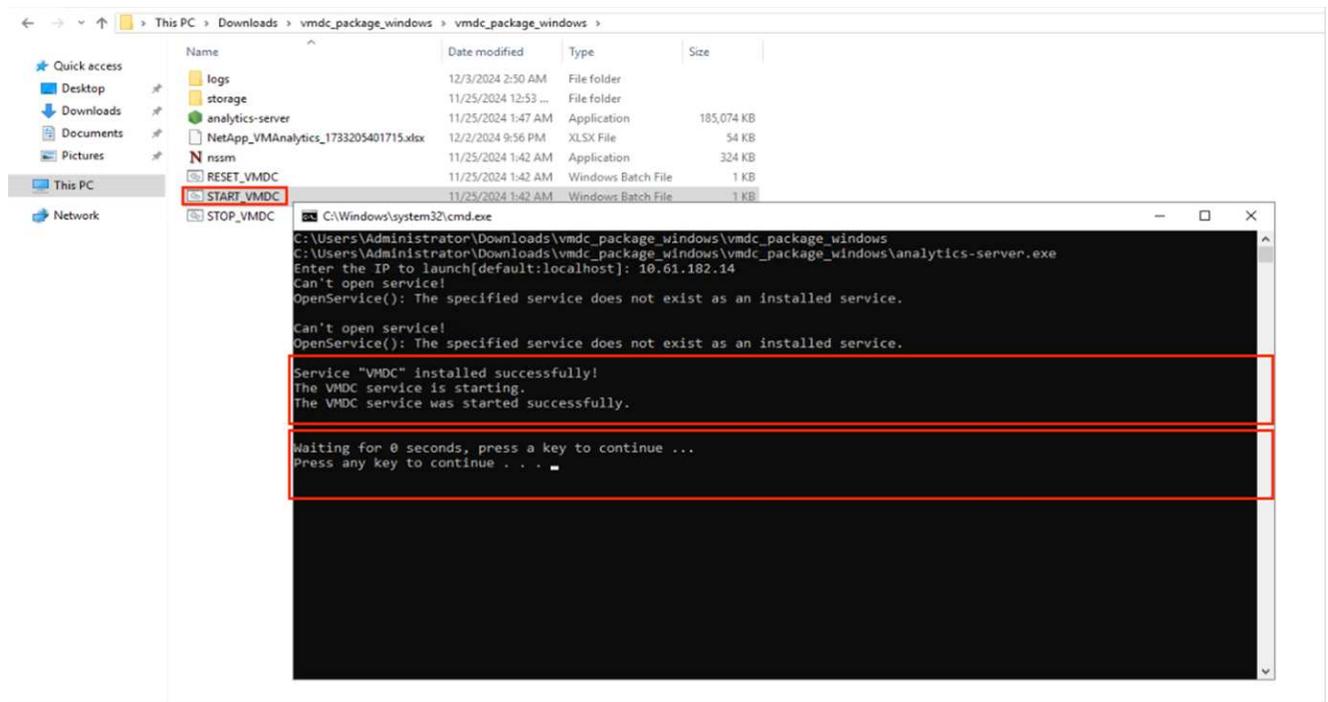


4. El instalador iniciará el proceso de instalación e iniciará el servicio VMDC.





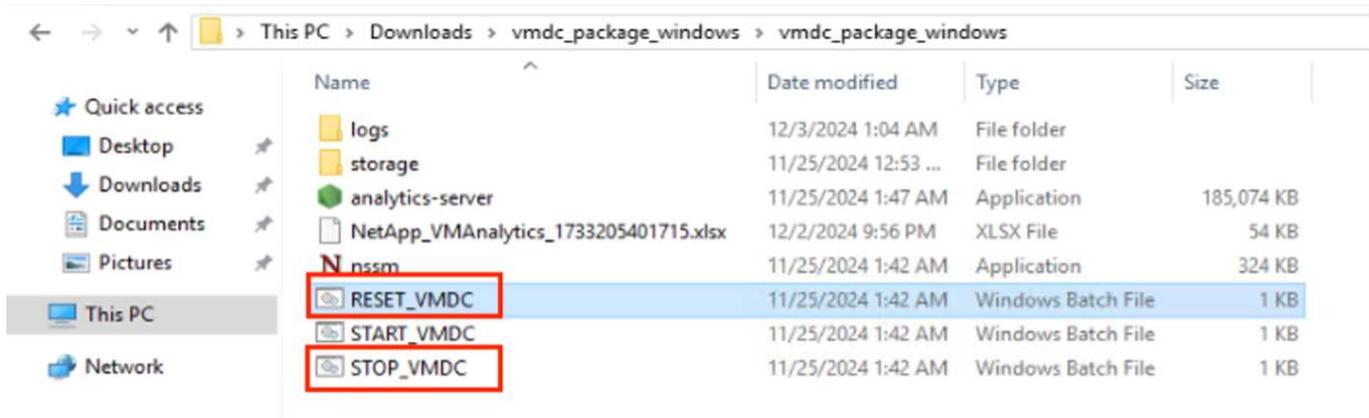
5. Una vez hecho esto, “Presione cualquier tecla para continuar” para cerrar el símbolo del sistema.



Para detener la recopilación de datos, haga clic en el archivo por lotes Stop_VMDC.



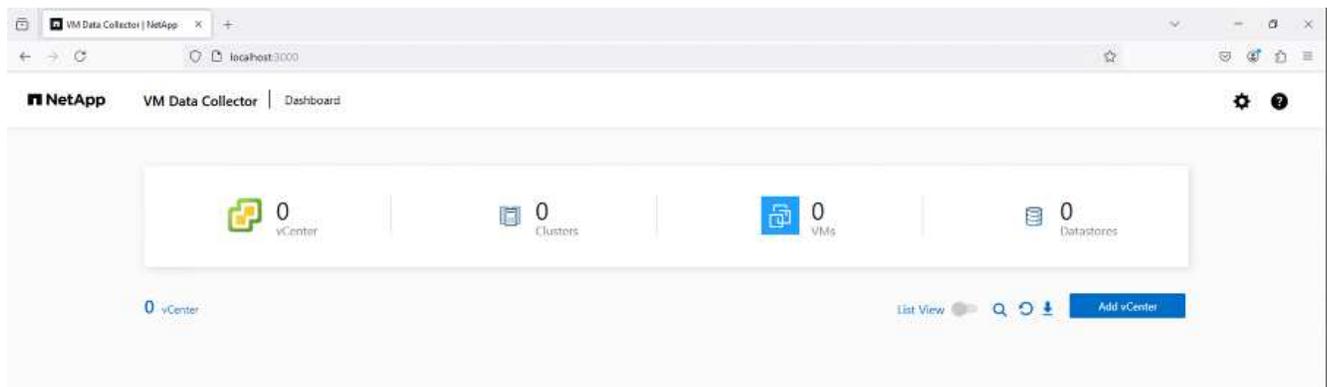
Para eliminar los datos recopilados y restablecer VMDC, ejecute el archivo por lotes reset_VMDC. Tenga en cuenta que la ejecución de reset bat file eliminará todos los datos existentes y comenzará desde cero.



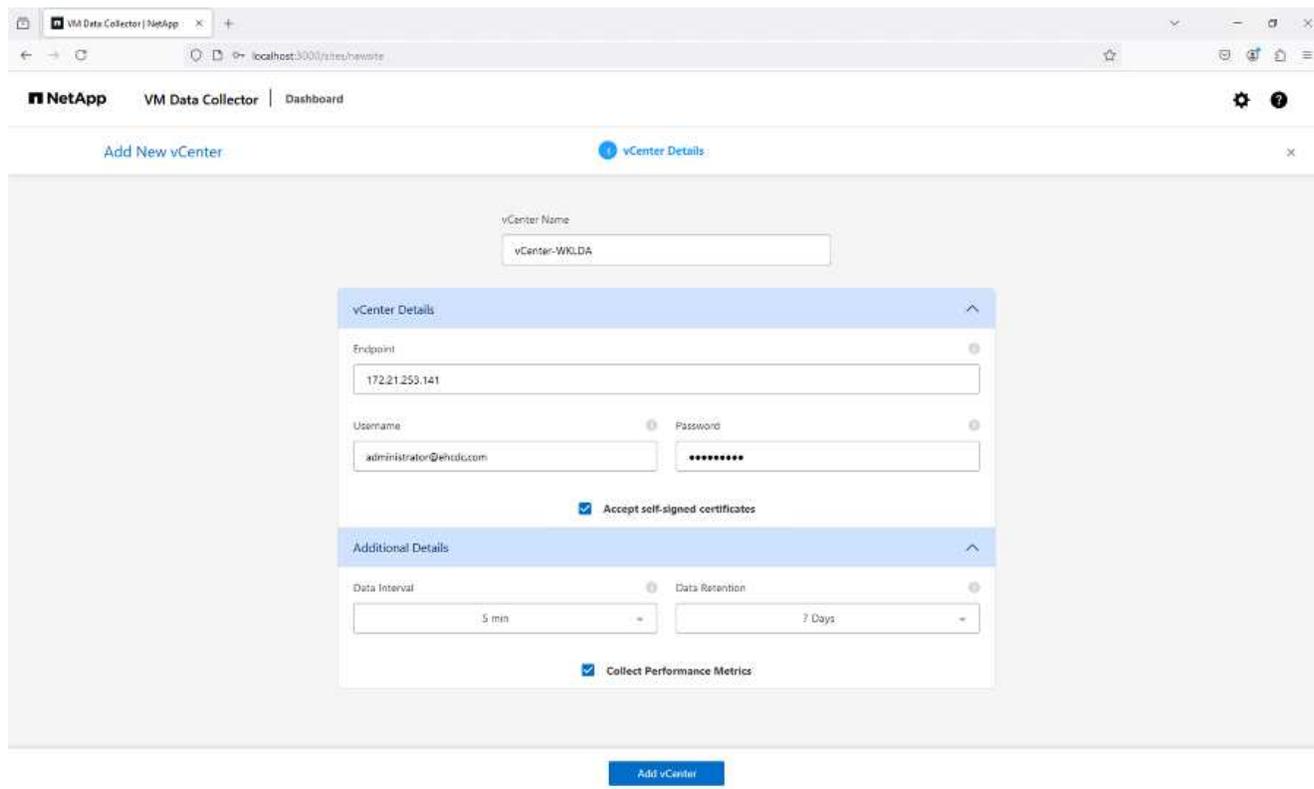
Uso de GUI

Ejecute VMDC

- Acceda a la interfaz de usuario de VMDC en el explorador



- Añada el vCenter designado mediante la opción «Add vCenter»
 - VCenter Name: Proporcione un nombre para el para vCenter
 - Endpoint: Introduzca la dirección IP o el FQDN del servidor vCenter
 - Username: Nombre de usuario para acceder al para vCenter (en formato UPN: username@domain.com)
 - Contraseña
- Modifique los “Detalles Adicionales” según los requisitos
 - Tiempo de Intervalo de Datos: Especifica el rango de tiempo de agregación de muestras. El valor predeterminado es 5 minutos, sin embargo, se puede modificar a 30sec o 1 minutos según sea necesario.
 - Retención de Datos: Especifica el período de retención para almacenar las métricas históricas.
 - Recopilar métricas de rendimiento: Cuando está activado, recopila las métricas de rendimiento de cada equipo virtual. Si no se selecciona, VMDC proporciona funcionalidad como RVtools solo proporcionando los detalles de máquina virtual, host y almacén de datos.
- Una vez hecho esto, haga clic en “Add vCenter”



La recogida de datos se inicia inmediatamente una vez que se añade el para vCenter. No es necesario programar una hora para la recopilación, ya que el proceso obtendría los datos disponibles en la base de datos de vCenter y empezaría a agregarlos en función del tipo de tiempo de intervalo de datos especificado.

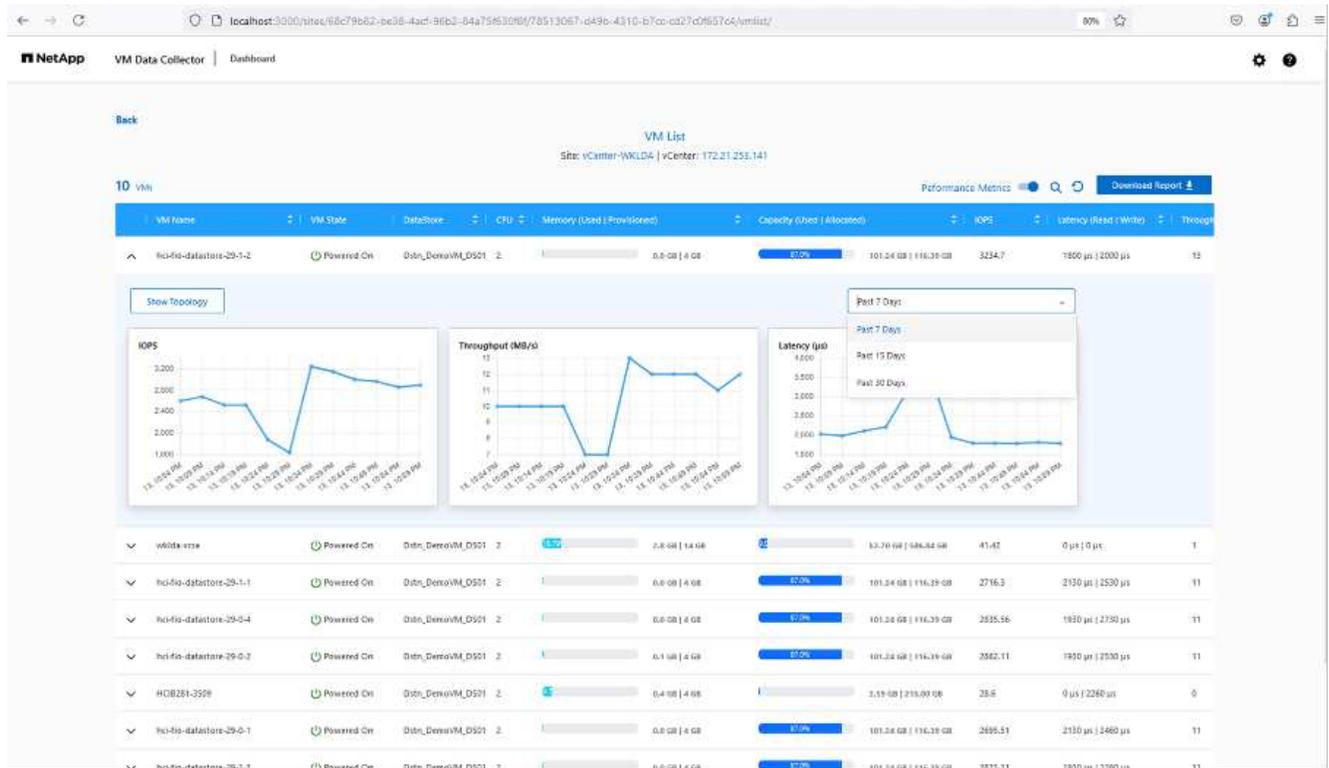
Para ver los datos de un vCenter concreto, vaya a la consola, haga clic en «View Inventory» con el nombre de vCenter apropiado. La página mostrará el inventario de VM junto con los atributos de VM. De forma predeterminada, “Performance Metrics” está desactivado en la interfaz de usuario, sin embargo, se puede ACTIVAR mediante la opción de alternar. Una vez habilitadas las métricas de rendimiento, se mostrarán los datos de rendimiento de cada equipo virtual. Para obtener información sobre el rendimiento en tiempo real, haga clic en el botón Actualizar.

Ver la topología de VM

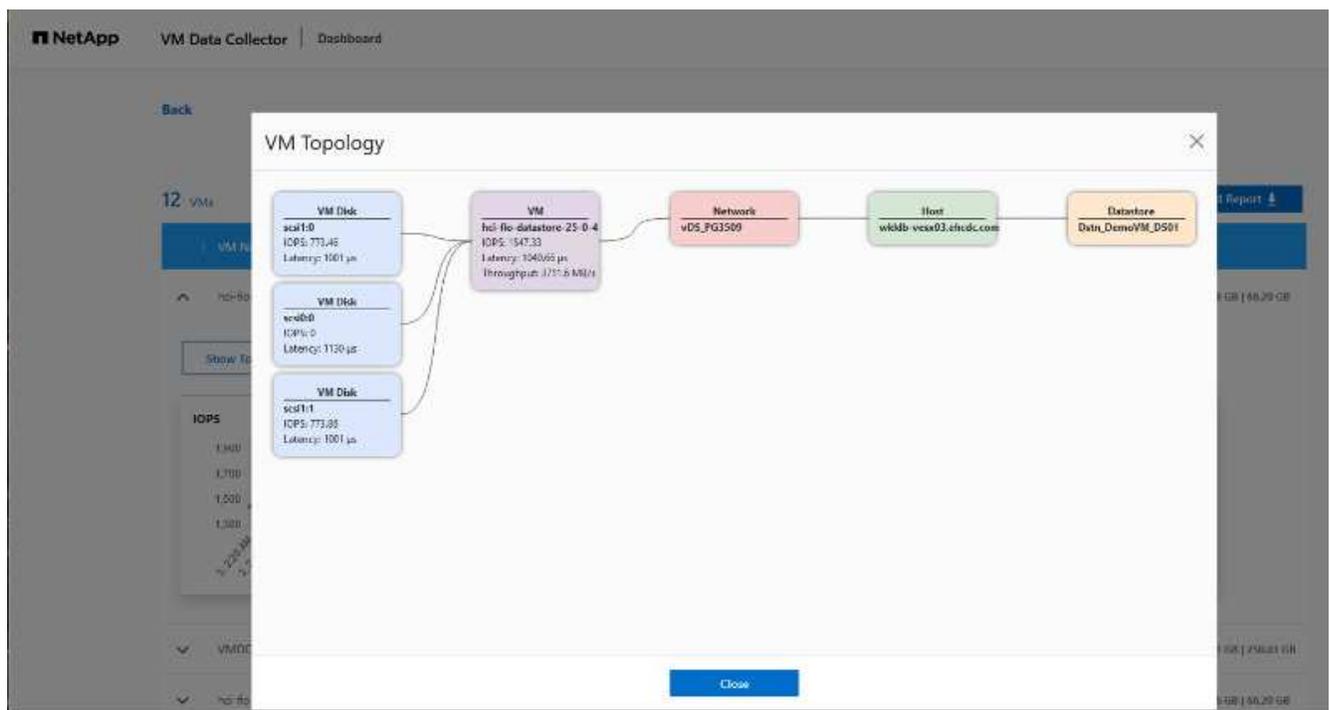
VMDC proporciona la opción “Mostrar Topología” para cada VM que proporciona una interfaz interactiva para ver los recursos y sus relaciones en disco de VM, VM, host ESXi, almacenes de datos y redes. Ayuda a gestionar y supervisar con información de los datos de rendimiento recopilados. La topología ayuda a realizar diagnósticos básicos y a resolver problemas utilizando los datos actuales. Para obtener una solución de problemas detallada y un MTTR rápido, utilice ["Información sobre la infraestructura de datos de NetApp"](#) el que proporciona una vista de topología detallada con asignación de dependencia de extremo a extremo.

Para acceder a la vista de topología, siga estos pasos:

- Acceda al panel de control de VMDC.
- Seleccione el nombre de vCenter y haga clic en «View Inventory».



- Seleccione la VM y haga clic en "Mostrar Topología".

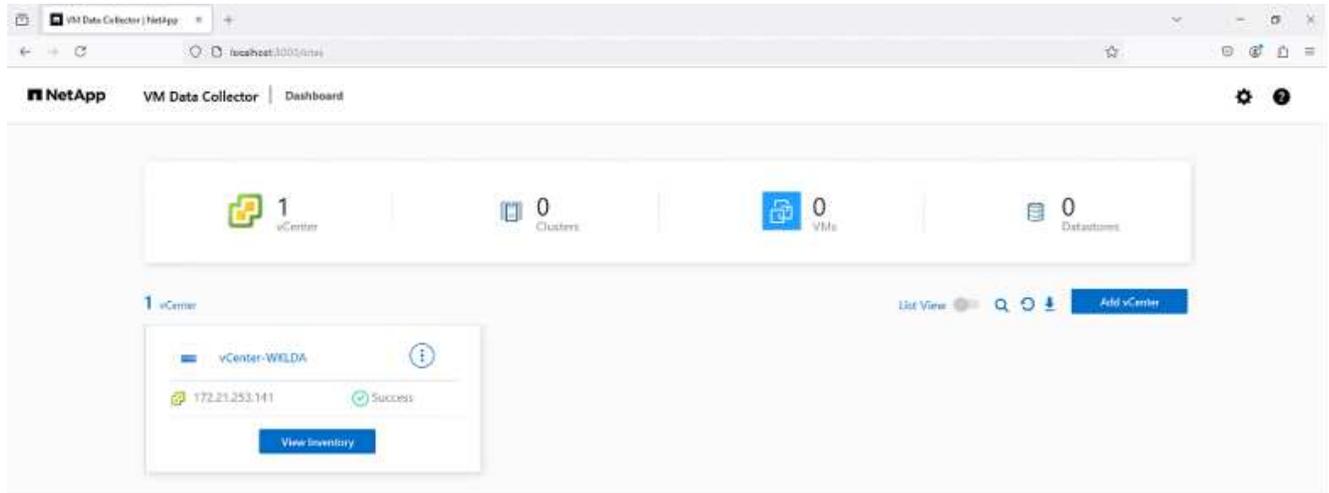


Exportar a Excel

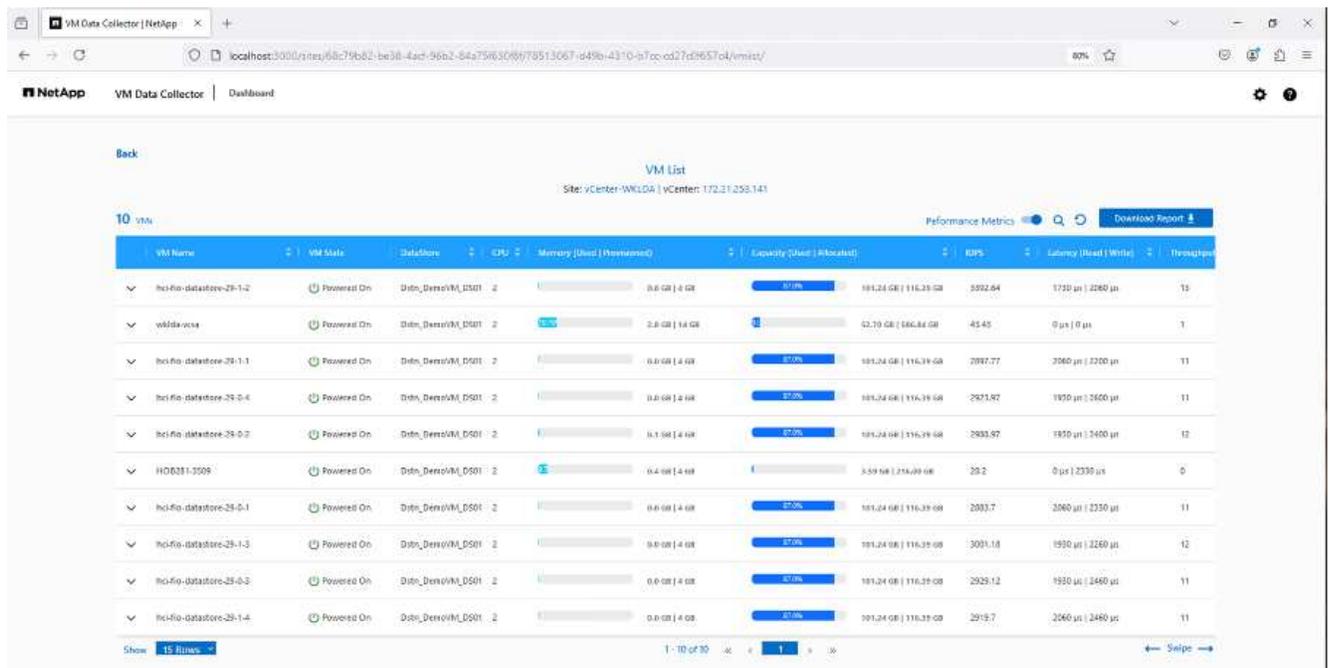
Para capturar el recopilado en un formato utilizable, use la opción "Descargar informe" para descargar el archivo XLSX.

Para descargar el informe, siga los siguientes pasos:

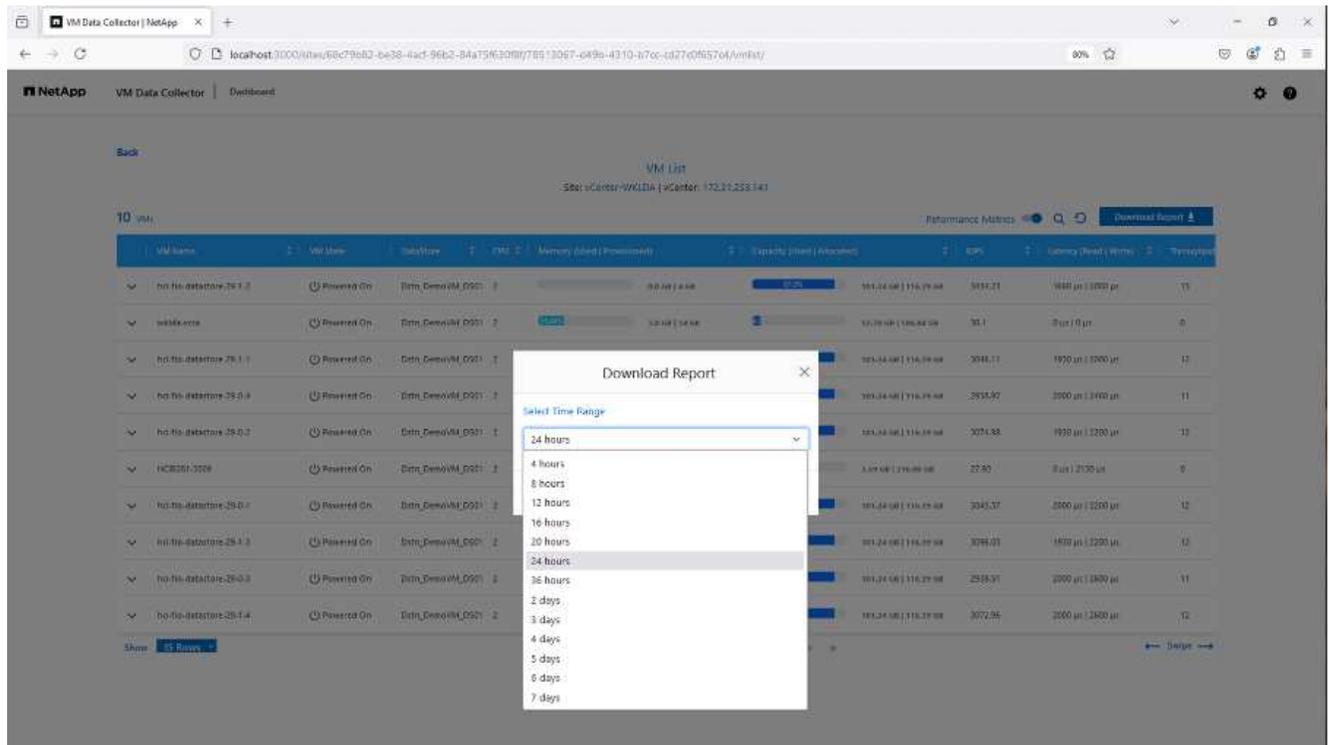
- Acceda al panel de control de VMDC.
- Seleccione el nombre de vCenter y haga clic en «View Inventory».



- Se selecciona la opción «Descargar informe»



- Seleccione el intervalo de tiempo. El intervalo de tiempo proporciona varias opciones que comienzan de 4 horas a 7 días.



Por ejemplo, si los datos necesarios son para las últimas 4 horas, seleccione 4 o elija el valor adecuado para capturar los datos de ese período determinado. Los datos generados se agregan de forma continua. Por lo tanto, seleccione el rango de tiempo para asegurarse de que el informe generado captura las estadísticas de carga de trabajo necesarias.

Contadores de datos VMDC

Una vez descargada, la primera hoja que muestra VMDC es «VM Info», una hoja que contiene información sobre los equipos virtuales que residen en el entorno vSphere. Muestra información genérica sobre las máquinas virtuales: Nombre de VM, Estado de Energía, CPU, Memoria Provisionada (MB), Memoria Utilizada (MB), Capacidad Provisionada (GB), Capacidad Utilizada (GB), Versión de Herramientas de VMware, Versión del SO, Tipo de Entorno, Centro de Datos, Clúster, Host, Carpeta, Almacén de Datos Primario, Discos, NIC, ID de VM y UUID de VM.

La pestaña 'Rendimiento de VM' captura los datos de rendimiento de cada VM muestreada en el nivel de intervalo seleccionado (el valor predeterminado es 5 minutos). El ejemplo de cada máquina virtual cubre: Promedio de IOPS de lectura, promedio de IOPS de escritura, promedio total de IOPS, pico de IOPS de lectura, pico de IOPS de escritura, pico total de IOPS, rendimiento promedio de lectura (KB/s), rendimiento medio de escritura (KB/s), rendimiento máximo de lectura (KB/s), rendimiento máximo total de escritura (KB/s), promedio de latencia de lectura (ms), promedio de latencia máxima (ms), latencia total de lectura (ms).

La pestaña «Información de host ESXi» captura para cada host: Centro de datos, vCenter, clúster, sistema operativo, fabricante, modelo, zócalos de CPU, núcleos de CPU, velocidad de reloj de red (GHz), subprocesos de CPU, memoria (GB), memoria usada (%), uso de CPU (%), recuento de VM de invitado y número de NIC.

Siguientes pasos

Utilice el archivo XLSX descargado para los ejercicios de optimización y refactorización.

Descripción de atributos de VMDC

Esta sección del documento cubre la definición de cada contador utilizado en la hoja de excel.

Hoja de información VM

Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
CPUs	The number of vCPUs provisioned on the Guest Virtual Machine
Memory Provisioned (MB)	The Memory Provisioned on the Guest Virtual Machine. Units MB
Memory Utilized (MB)	Active Memory Utilized by the Guest Virtual Machine during the phase of metrics collection. Units MB
Capacity Provisioned (GB)	Total Capacity of the Virtual Disks provisioned on the Guest Virtual Machine. Units GB
Capacity Utilized (GB)	Total Utilized Virtual Disks capacity on the Guest Virtual Machine. Units GB
VMware tools version	Version of the VMware Tools installed on the Guest Virtual machine
OS Version	The Operating System installed on the Guest Virtual Machine
Environment Type	
Datacenter	Name of the Datacenter containing the Guest Virtual Machine
Cluster	Name of the Cluster containing the Guest Virtual Machine
Host	Name of the ESXi Server on which the Guest Virtual Machine is hosted
Folder	Name of the folder under the VMs Tab containing the Guest Virtual Machine
Primary Datastore	Name of the Datastore on which the Guest Virtual Machine's disks reside
Disks	Number of Virtual Disks connected to the Guest Virtual Machine
NICs	Number of Virtual Network Interface connections to the Guest Virtual Machine
VM ID	The Guest Virtual Machine Identifier String within the scope of vCenter Server Monitoring
VM UUID	The Unique Identifier value for the Guest Virtual Machine

Hoja de rendimiento de VM

Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
Number of CPUs	Number of vCPUs provisioned on the Guest Virtual Machine
Average CPU (%)	Average vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Peak CPU (%)	Maximum vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Average Read IOPS	Average read IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Write IOPS	Average Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Average IOPS	Combined Average Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Read IOPS	Maximum Read IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Write IOPS	Maximum Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Peak IOPS	Combined Maximum Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Read Throughput (KB/s)	Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Write Throughput (KB/s)	Average rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Average Throughput (KB/s)	Combined Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Read Throughput (KB/s)	Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Write Throughput (KB/s)	Peak rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Peak Throughput (KB/s)	Combined Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Read Latency (ms)	Average Read latency for the Guest Virtual Machine. Units milliseconds
Average Write Latency (ms)	Average Write latency for the Guest Virtual Machine. Units milliseconds
Total Average Latency (ms)	Combined Average Read & Write latency for the Guest Virtual Machine. Units milliseconds
Peak Read Latency (ms)	Maximum Read latency for the Guest Virtual Machine. Units milliseconds
Peak Write Latency (ms)	Maximum Write latency for the Guest Virtual Machine. Units milliseconds
Total Peak Latency (ms)	Combined Maximum Read & Write latency for the Guest Virtual Machine. Units milliseconds

ESXi Host Info

Counter Name	Counter Description
Host	Hostname of the ESXi Hypervisor Server
Datacenter	Virtual DataCenter Name under which the ESXi Hypervisor Hosts exists
vCenter	Version of the VMware vCenter Server used to Manage & Monitor the ESXi Hosts
Cluster	Name of the Cluster under which the ESXi Hypervisor Hosts exists
OS	Version of VMware ESXi Hypervisor that is installed on the Host / Server
Manufacturer	Vendor Company name of the Physical Server of the Host
Model	Server Model / Model Number of the Physical Server
CPU Sockets	Total number of CPU Sockets installed on the Physical Server
CPU Cores	Total number of Cores across all CPU Sockets installed on the Physical Server
CPU Description	Vendor Company & Model Information of the CPU Type installed on the Physical Server
Net Clock Speed (GHz)	Sum of CPU Clock Speed of all CPU cores running on the Physical Server. Units GHz
CPU Clock Speed (GHz)	Clock Speed of each CPU core running on the Physical Server. Units GHz
CPU Threads	Total Number of threads supported for all Cores on the Physical Server
Memory (GB)	Total RAM installed on the Physical Server. Units GB
Memory Used (%)	Percentage of Memory Used on the Physical Server / Host
CPU usage (%)	Percentage of CPU Used on the Physical Server / Host
Guest VM Count	Total Number of Guest Virtual Machines running on the Physical Server / Host
Number of NICs	Total Number of Network Interface Connection Ports on the Physical Hypervisor Server / Host

Conclusión

Con los próximos cambios en las licencias, las organizaciones están abordando de forma proactiva el aumento potencial del coste total de propiedad (TCO). Están optimizando estratégicamente su infraestructura de VMware mediante la agresiva gestión de recursos y el dimensionamiento para mejorar la utilización de

recursos y optimizar la planificación de la capacidad. Gracias al uso eficaz de herramientas especializadas, las organizaciones pueden identificar y recuperar de manera eficiente los recursos desperdiciados, lo que permite reducir el número de núcleos y los gastos generales de licencias. VMDC proporciona la capacidad de recopilar rápidamente datos de VM que se pueden dividir para informar y optimizar el entorno existente.

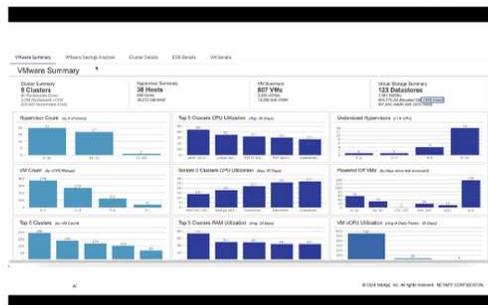
Con VMDC, lleve a cabo una evaluación rápida para determinar los recursos infrutilizados y, a continuación, utilice la información sobre la infraestructura de datos (DII) de NetApp para proporcionar análisis detallados y recomendaciones para la reclamación de máquinas virtuales. Esto permite a los clientes comprender el ahorro potencial de costes y la optimización mientras que el análisis de la infraestructura de datos de NetApp (DII) está instalado y configurado. Data Infrastructure Insights (DII) de NetApp puede ayudar a las empresas a tomar decisiones informadas para optimizar su entorno de máquinas virtuales. Puede identificar dónde se pueden reclamar los recursos o dónde se pueden retirar los hosts con un impacto mínimo en la producción, lo que ayuda a las empresas a navegar por los cambios provocados por la adquisición de VMware por Broadcom de forma reflexiva y estratégica. En otras palabras, VMDC y DII como mecanismo de análisis detallado ayudan a las empresas a eliminar la emoción de la decisión. En lugar de reaccionar a los cambios con pánico o frustración, pueden utilizar los conocimientos proporcionados por estas dos herramientas para tomar decisiones racionales y estratégicas que equilibran la optimización de costos con la eficiencia operativa y la productividad.

Con NetApp, ajusta el tamaño adecuado de tus entornos virtualizados e introduce un rendimiento rentable del almacenamiento flash, junto con una gestión de datos simplificada y soluciones de ransomware para garantizar que las organizaciones están preparadas para el nuevo modelo de suscripción, mientras optimizan los recursos TECNOLÓGICOS que se encuentran en la actualidad.

Optimize VMware core licensing

Optimize VMware core licensing and right-size workloads

25-50% optimization savings (based on VMDC reports showing CPU utilization of ~30% or less)



Optimize:

- VMware core licensing
- VM CPU and memory

NetApp® Data Infrastructure Insights

- Understand topology
- Drive density
- Right-size workloads

Siguientes pasos

Descargue el paquete VMDC y recopile los datos y utilícelos "Estimación del coste total de propiedad de VSAN" para una fácil proyección y, a continuación, utilícelos "DII" para proporcionar la inteligencia de forma continua, IMPACTÁNDOLO ahora y en el futuro para garantizar que se adapte a medida que surjan nuevas necesidades.

Demostraciones y tutoriales

Vídeos y demostraciones sobre virtualización

Vea los siguientes vídeos y demostraciones en los que se destacan características específicas de las soluciones de cloud híbrido, virtualización y contenedores.

Herramientas de ONTAP de NetApp para VMware vSphere

[Herramientas de ONTAP para VMware: Información general](#)

[Aprovisionamiento de almacén de datos iSCSI de VMware con ONTAP](#)

[Aprovisionamiento del almacén de datos NFS de VMware con ONTAP](#)

Plugin de SnapCenter para VMware vSphere

El software SnapCenter de NetApp es una plataforma empresarial fácil de usar para coordinar y administrar de un modo seguro la protección de datos en todas las aplicaciones, bases de datos y sistemas de archivos.

El plugin de SnapCenter para VMware vSphere permite ejecutar operaciones de backup, restauración y conexión para máquinas virtuales, así como operaciones de backup y montaje para almacenes de datos que se registran en SnapCenter directamente en VMware vCenter.

Para obtener más información sobre el plugin de SnapCenter para VMware vSphere, consulte "[Información general sobre el plugin de SnapCenter de NetApp para VMware vSphere](#)".

[Plugin de SnapCenter para VMware vSphere: Requisitos previos de la solución](#)

[Plugin de SnapCenter para VMware vSphere: Implementación](#)

[Plugin de SnapCenter para VMware vSphere: Flujo de trabajo de backup](#)

[Plugin de SnapCenter para VMware vSphere: Flujo de trabajo de restauración](#)

[SnapCenter - flujo de trabajo de restauración SQL](#)

Soluciones de protección de datos 3-2-1

Las soluciones de protección de datos 3-2-1 combinan backups primarios y secundarios en las instalaciones mediante la tecnología SnapMirror y copias replicadas en almacenamiento de objetos mediante el backup y la recuperación de datos de BlueXP.

[3-2-1 Protección de datos para almacenes de datos VMFS con plugin SnapCenter para VMware vSphere y backup y recuperación de BlueXP para máquinas virtuales](#)

VMware Cloud en AWS con AWS FSx ONTAP

[Almacenamiento conectado como invitado de Windows con FSX ONTAP mediante iSCSI](#)

[Almacenamiento conectado invitado de Linux con FSX ONTAP mediante NFS](#)

[Ahorro en el TCO de VMware Cloud en AWS con Amazon FSx ONTAP](#)

[Almacén de datos complementario de VMware Cloud en AWS con Amazon FSx ONTAP](#)

[Instalación y configuración de VMware HCX para VMC](#)

[Demostración de la migración de VMotion con VMware HCX para VMC y FSx ONTAP](#)

[Demostración de migración en frío con VMware HCX para VMC y FSx ONTAP](#)

Azure VMware Services en Azure con Azure NetApp Files (ANF)

[Descripción general adicional del almacén de datos de la solución para VMware Azure con Azure NetApp Files](#)

[Recuperación ante desastres de la solución VMware para Azure con Cloud Volumes ONTAP, SnapCenter y JetStream](#)

[Demostración de migración en frío con VMware HCX para AVS y ANF](#)

[Demostración de VMotion con VMware HCX para AVS y ANF](#)

[Demostración de migración masiva con VMware HCX para AVS y ANF](#)

VMware Cloud Foundation con NetApp ONTAP

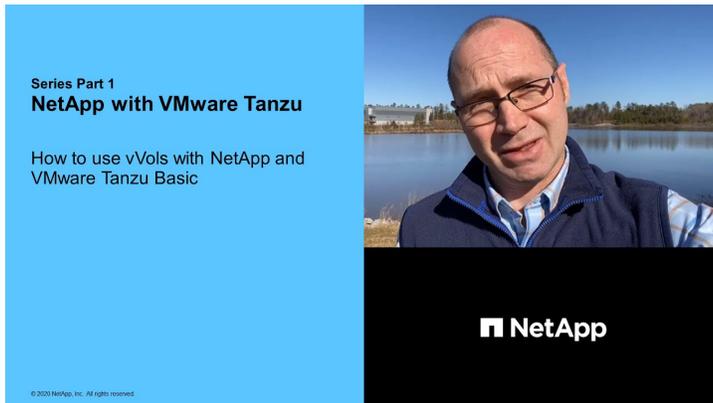
[Almacenes de datos NFS como almacenamiento principal para dominios de carga de trabajo de VCF](#)

[Almacenes de datos iSCSI como almacenamiento complementario para dominios de gestión de VCF](#)

NetApp con VMware Tanzania

VMware Tanzania permite a los clientes poner en marcha, administrar y gestionar su entorno de Kubernetes a través de vSphere o de VMware Cloud Foundation. Esta cartera de productos de VMware permite a los clientes gestionar todos sus clústeres de Kubernetes relevantes desde un único plano de control al elegir la edición de VMware Tanzu que mejor se adapte a sus necesidades.

Si quiere más información sobre VMware Tanzania, consulte "[Descripción general de VMware Tanzania](#)". Esta revisión incluye casos de uso, adiciones disponibles y mucho más sobre VMware Tanzu.



Cómo usar vVols con NetApp y VMware Tanzu Basic, parte 1



Cómo usar vVols con NetApp y VMware Tanzu Basic, parte 2



Cómo utilizar vVols con NetApp y VMware Tanzu Basic, parte 3

Cloud Insights de NetApp

NetApp Cloud Insights es una plataforma completa de análisis y supervisión diseñada para proporcionar visibilidad y control sobre tu infraestructura on-premises y en la nube.

[NetApp Cloud Insights: Observabilidad para el centro de datos moderno](#)

Información de copyright

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

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

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN 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.