



Guía de referencia de NFS para vSphere 8

NetApp Solutions

NetApp
December 19, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions/vmware/vmware_nfs_overview.html on December 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Guía de referencia de NFS para vSphere 8 1
 - Guía de referencia de NFS v3 para vSphere 8 1
 - La función nConnect de NFS con NetApp y VMware 9
 - Utilice las herramientas de ONTAP 10 para configurar almacenes de datos NFS para vSphere 8 13
 - Utilice Site Recovery Manager de VMware para la recuperación ante desastres de almacenes de datos NFS 45
 - Protección autónoma frente al ransomware para almacenamiento NFS 71

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:

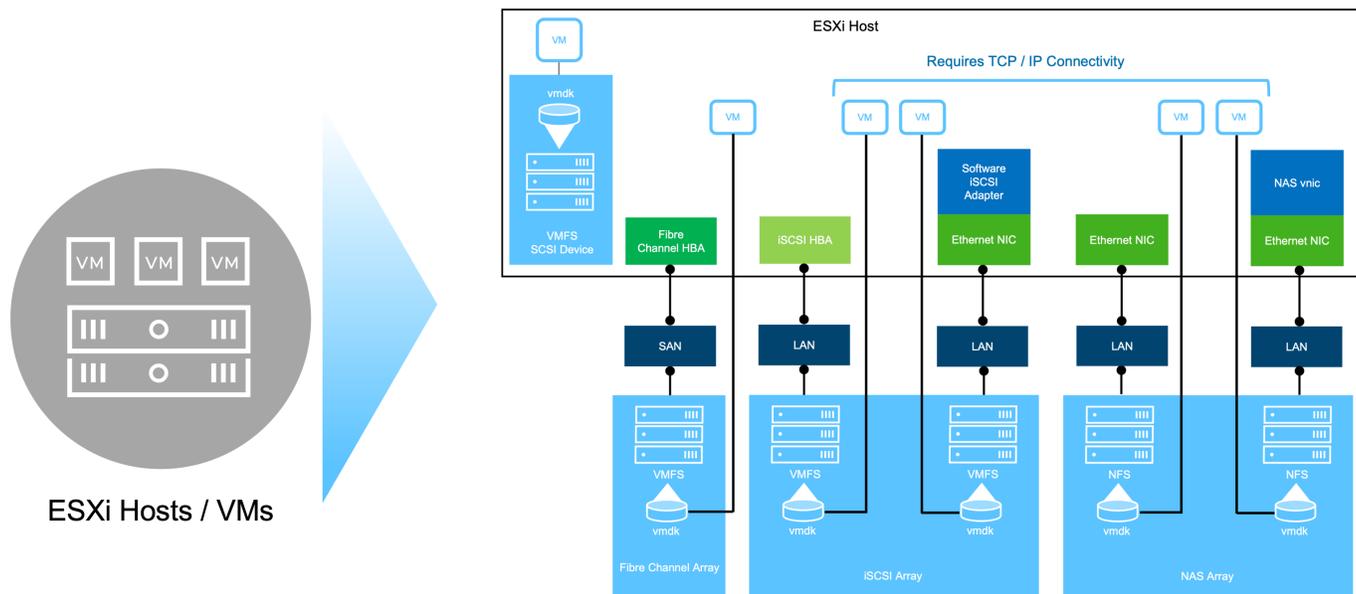
- vSphere de VMware
- vSAN de VMware
- Estándar ARIA
- Tanzu Kubernetes Grid Service para vSphere de VMware
- Switch distribuido de vSphere

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.

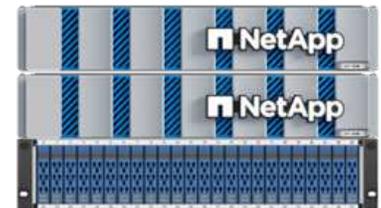
AFF A70



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.

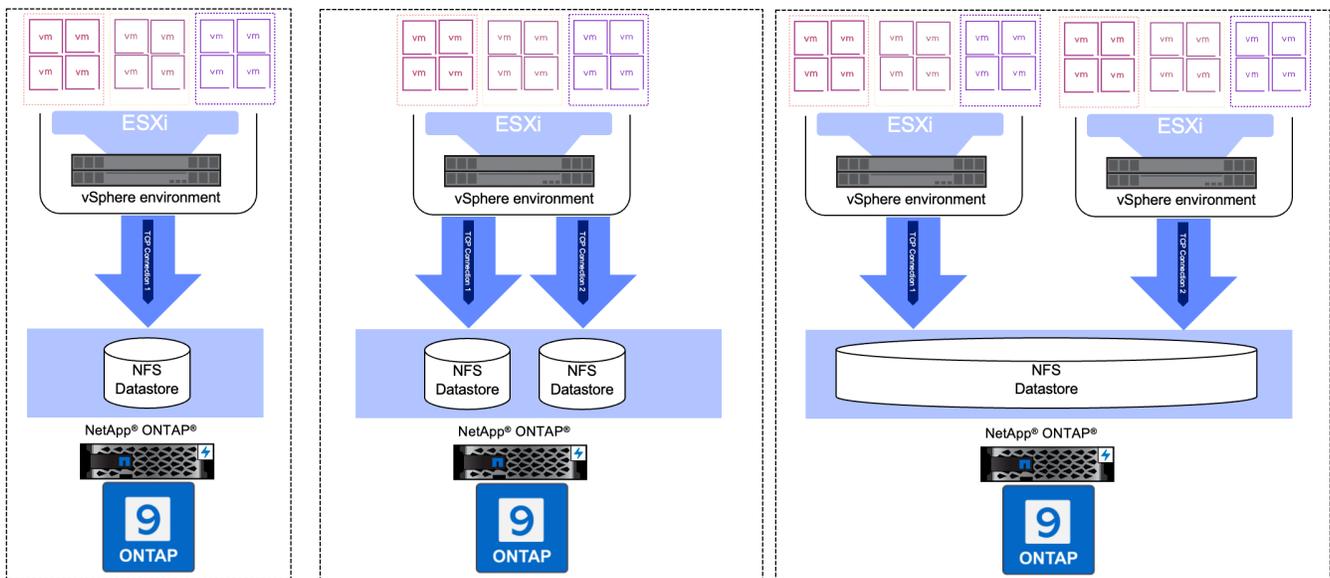
Detalles técnicos

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.

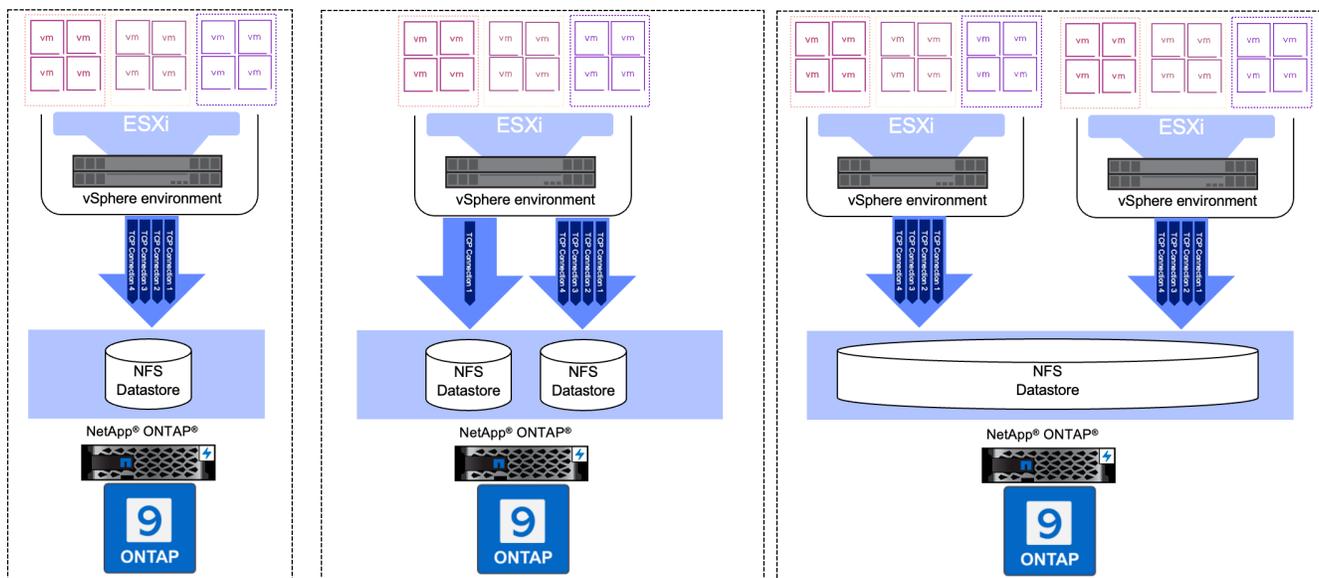
Without nConnect feature with NetApp and VMware



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. Compruebe "[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.

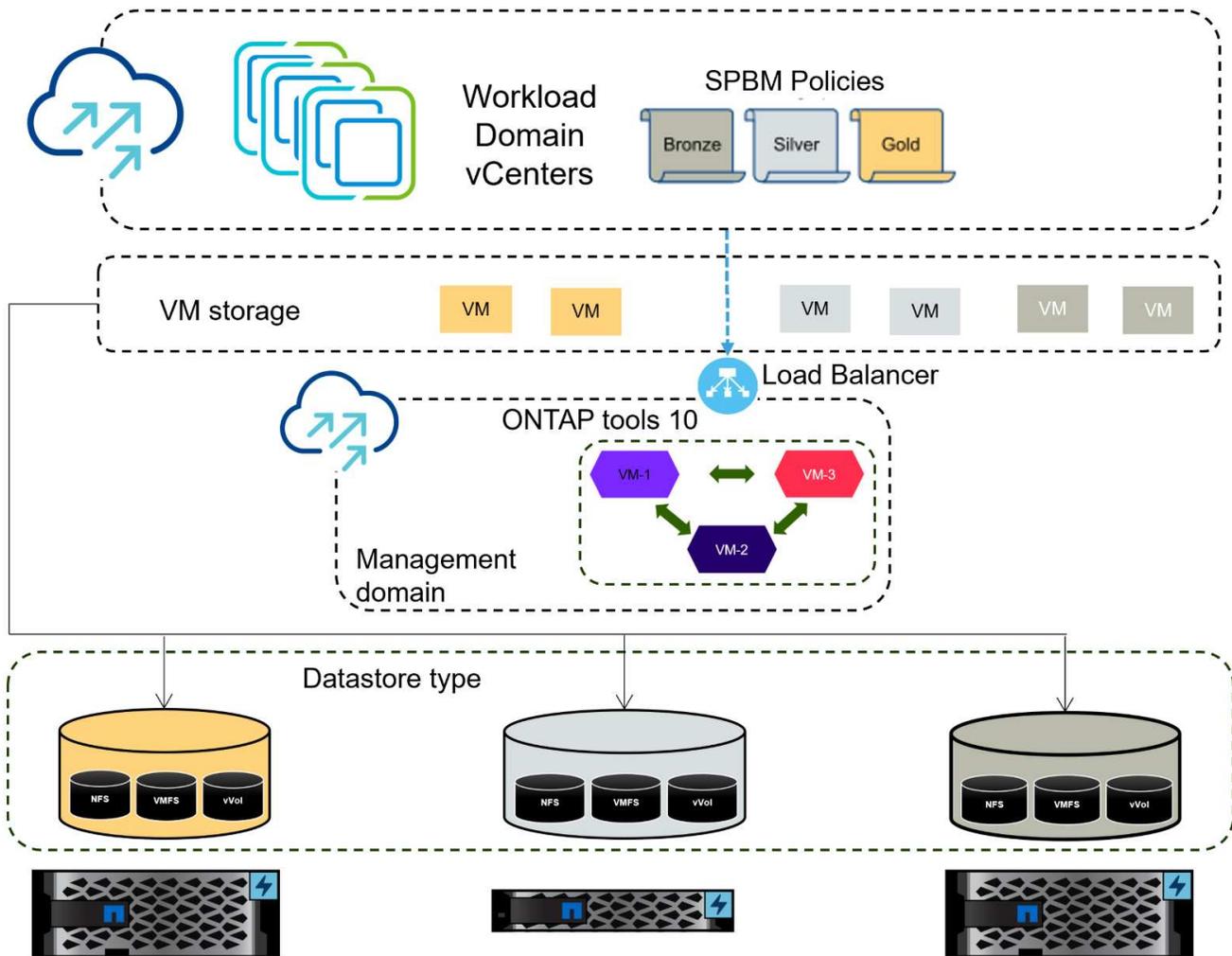
Descripción general de la solución

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:

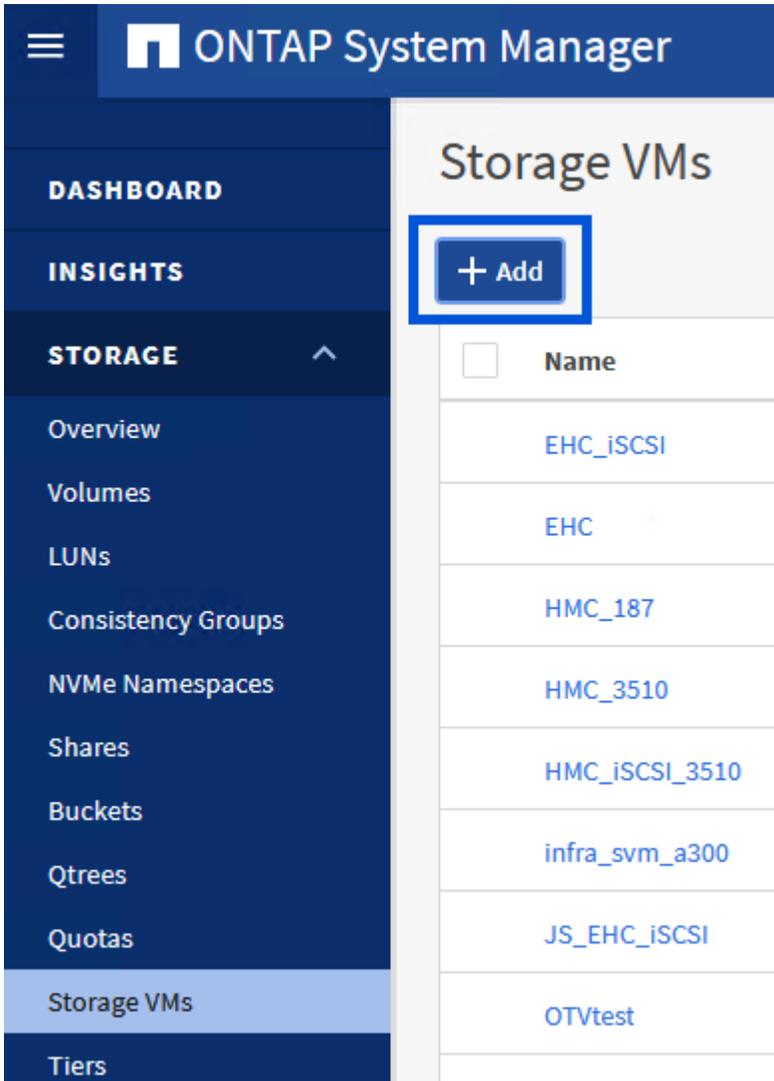
Crear SVM y LIF en el sistema de almacenamiento ONTAP

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

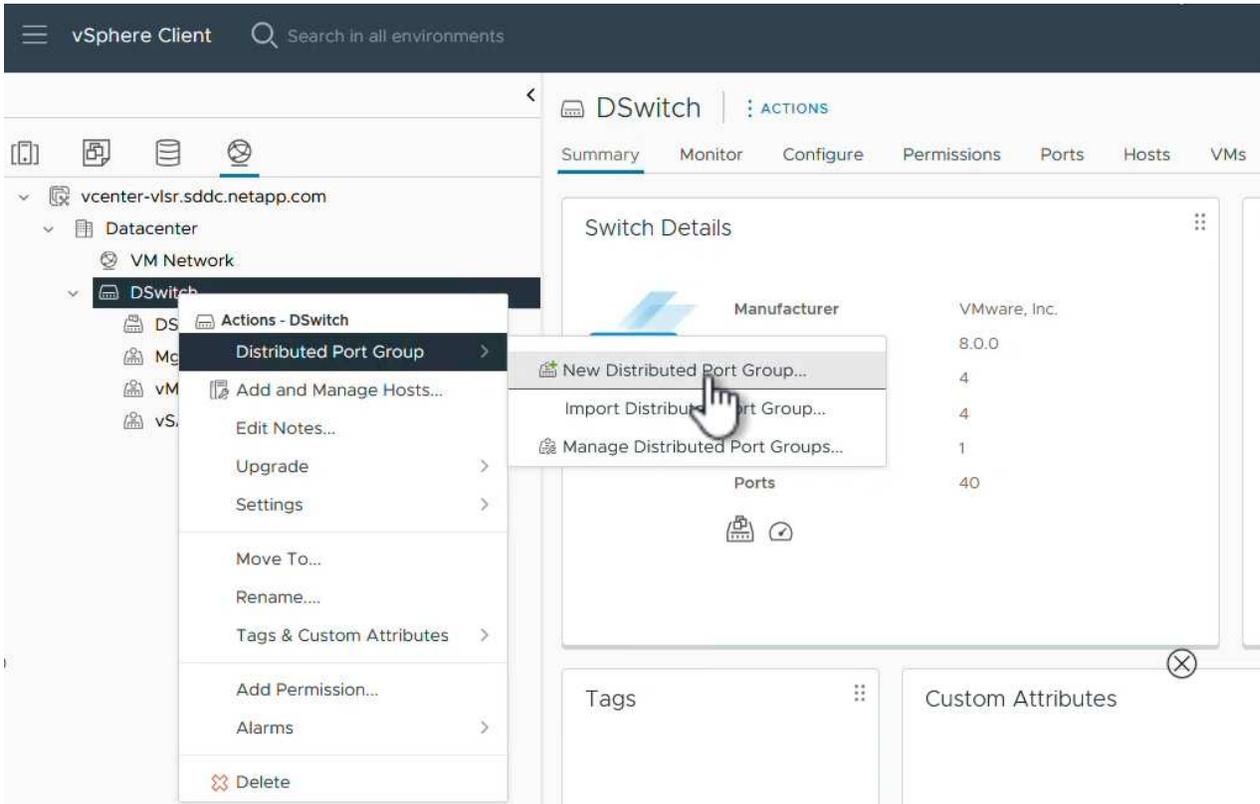
Configure las redes para NFS en los hosts ESXi

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.

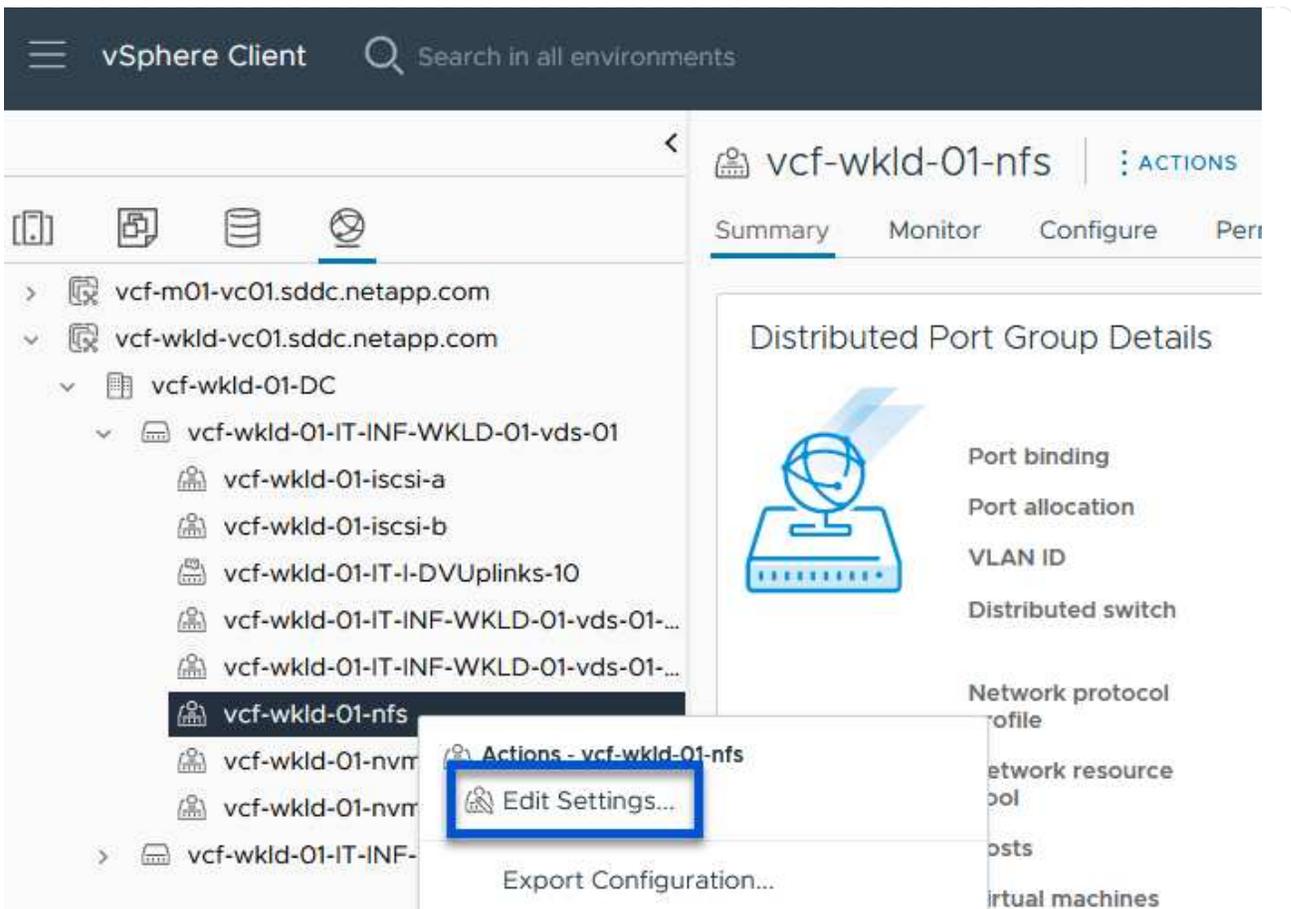
Port binding	Static binding
Port allocation	Elastic ?
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

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 por ▾

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

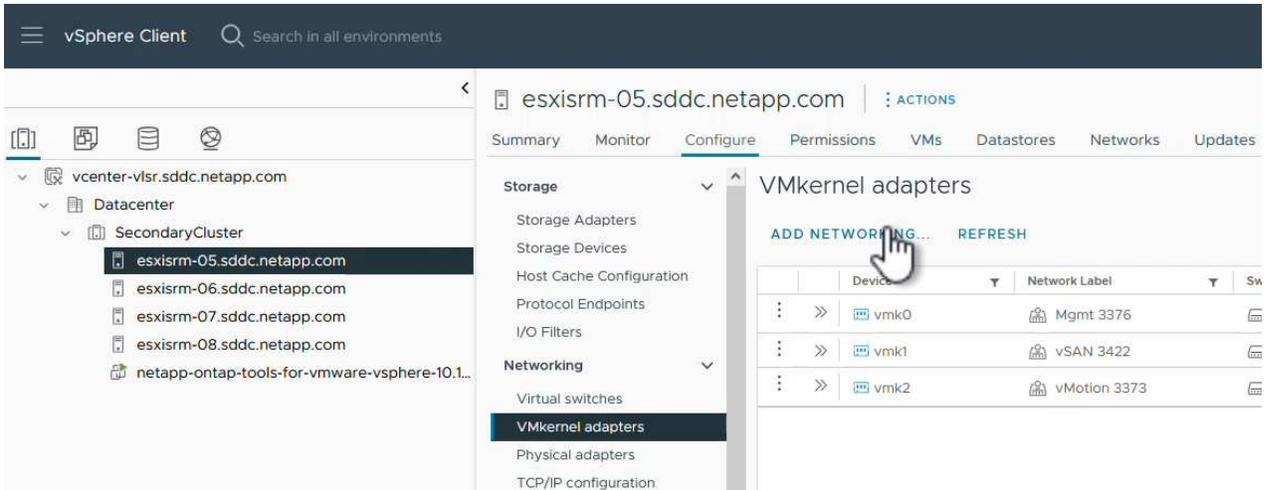
OK

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

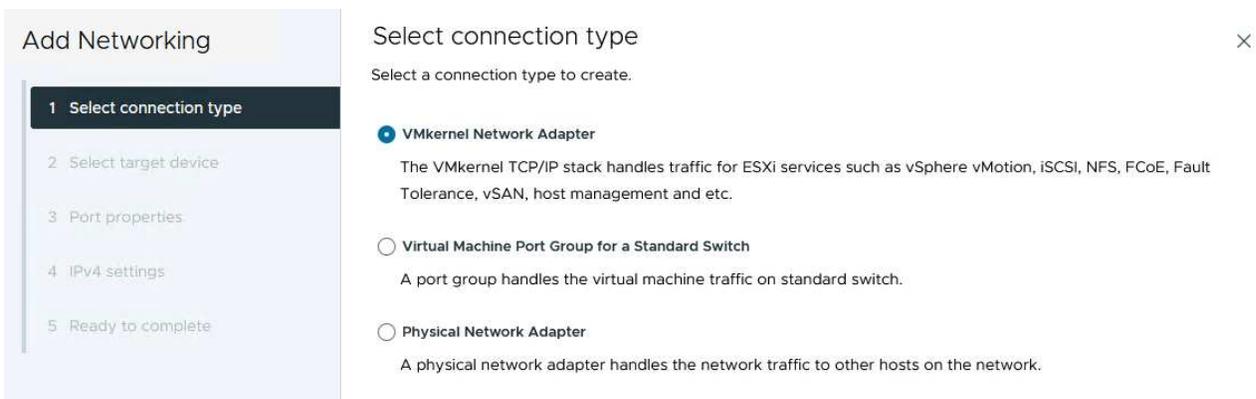
Crear un adaptador de VMkernel en cada host ESXi

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

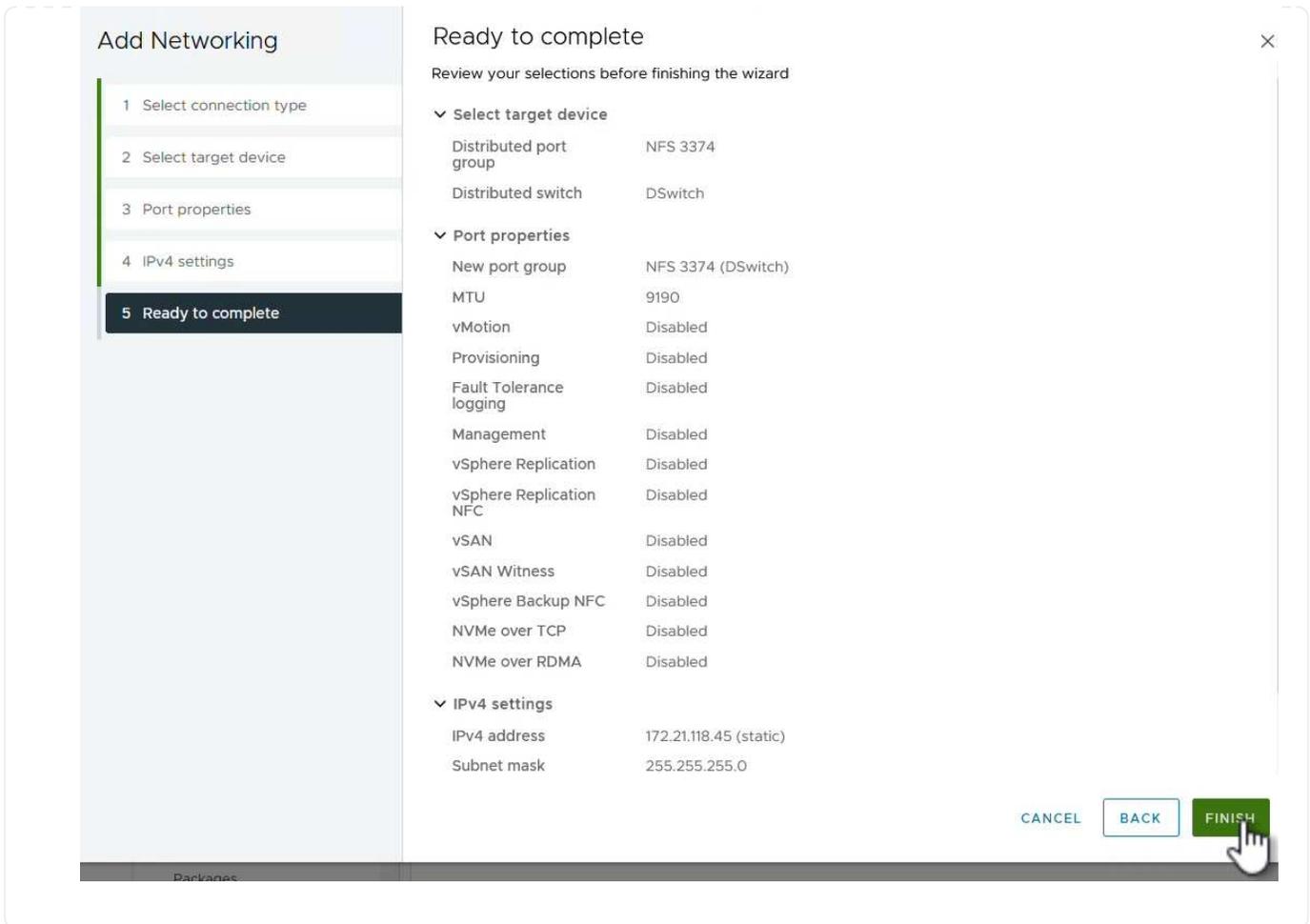
DNS server addresses

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

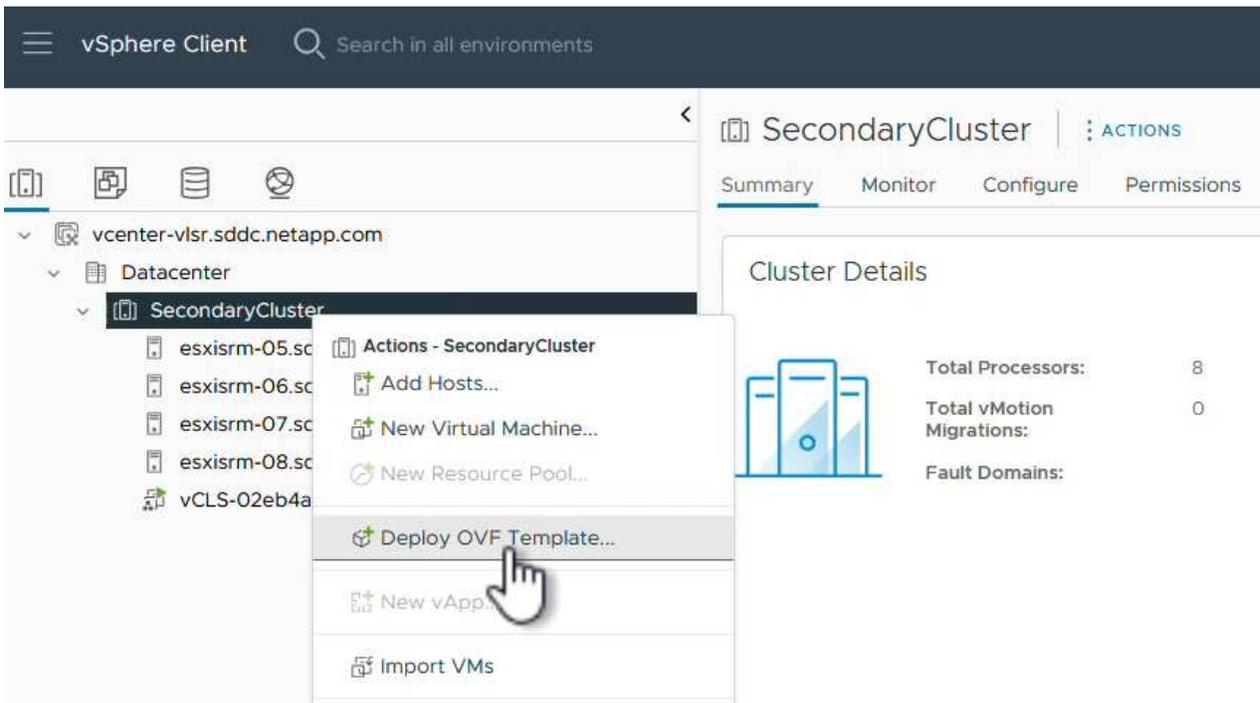
Las herramientas de ONTAP para VMware vSphere 10 se ponen en marcha como dispositivo de máquina virtual y proporcionan una interfaz de usuario integrada de vCenter para gestionar el almacenamiento de ONTAP. Las herramientas de ONTAP 10 cuenta con un nuevo portal de gestión global para gestionar conexiones 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-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 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	
vsanDatastore	--	799.97 GB	26.05 GB	783.98 GB	

Items per page 10 1 Item

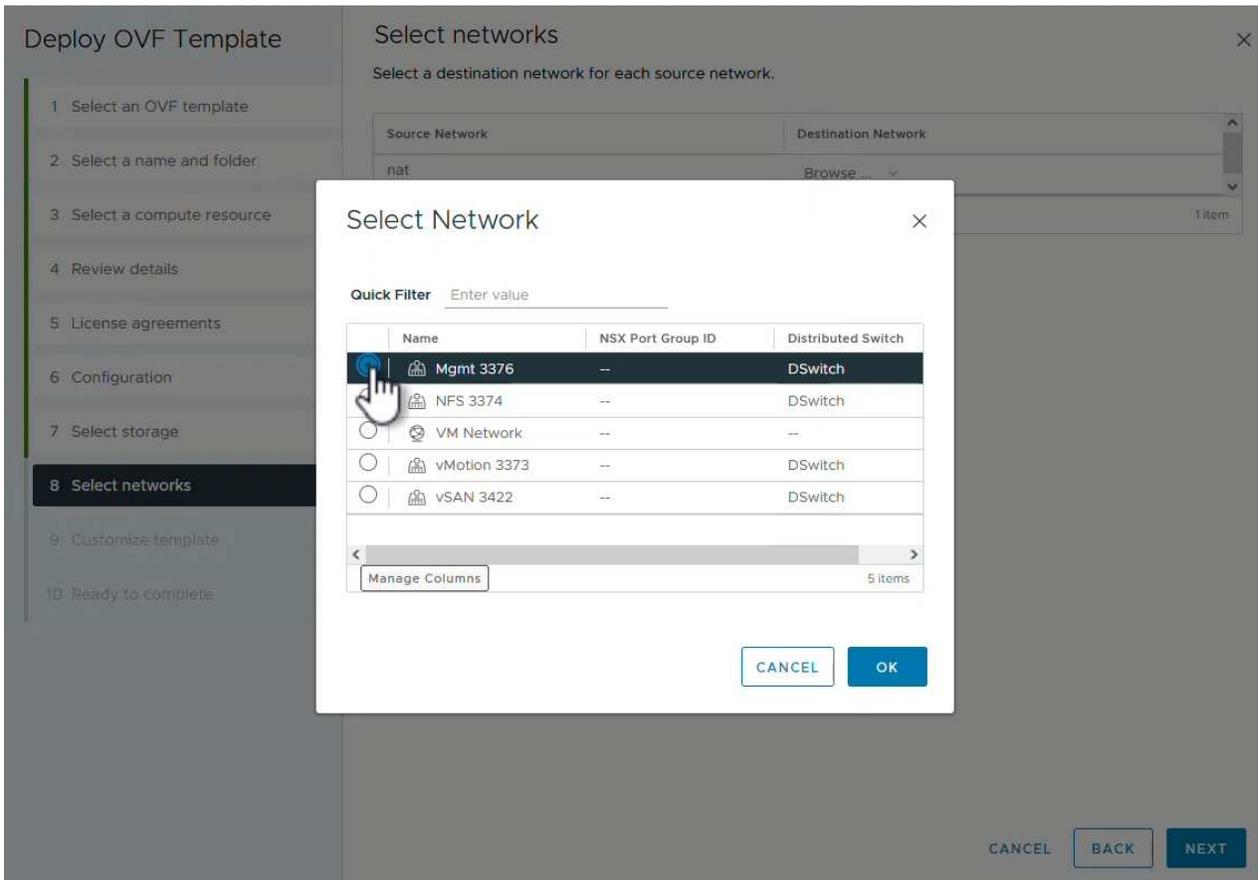
Compatibility

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 style="border: 2px solid #f00;" 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 style="border: 2px solid #f00;" type="text"/>
IP Address(*)	Specify the IP address for the appliance	<input style="border: 2px solid #f00;" 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](#)



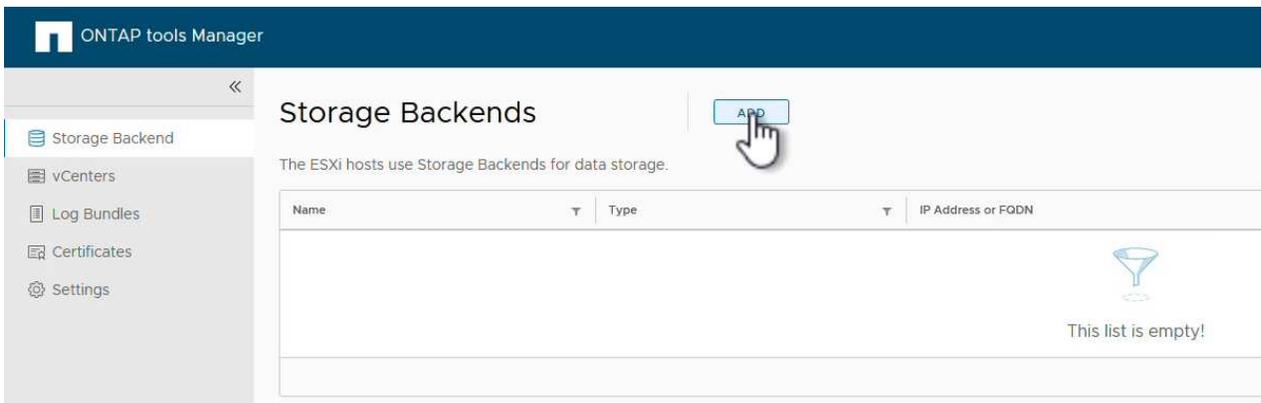
Log Bundles

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.

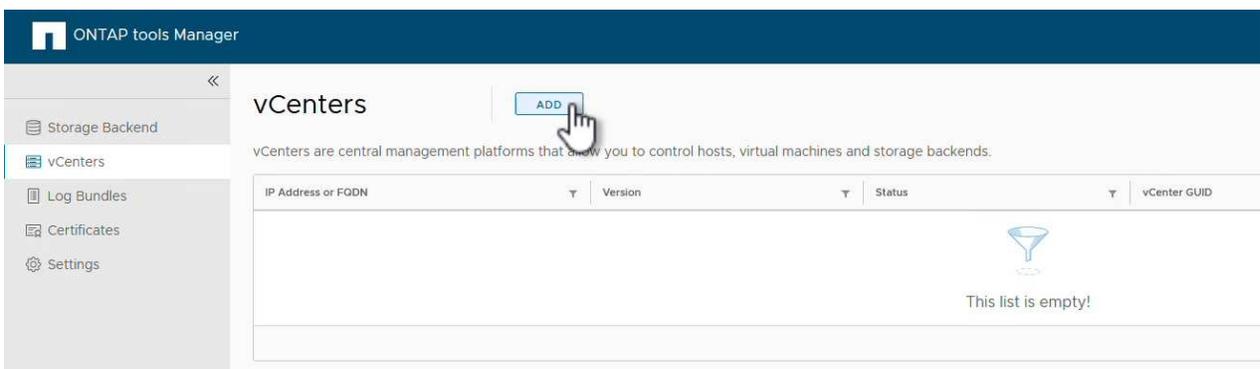
Add Storage Backend

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". A left sidebar contains a menu with items: Storage Backend, vCenters (highlighted), Log Bundles, Certificates, and Settings. The main content area is titled "vCenters" and features an "ADD" button with a hand cursor pointing to it. Below the title, there is a descriptive sentence: "vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends." Underneath is a table with columns: IP Address or FQDN, Version, Status, and vCenter GUID. The table is currently empty, with a funnel icon and the text "This list is empty!" centered below it.

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

Add vCenter

Server IP Address or FQDN: *

Username: *

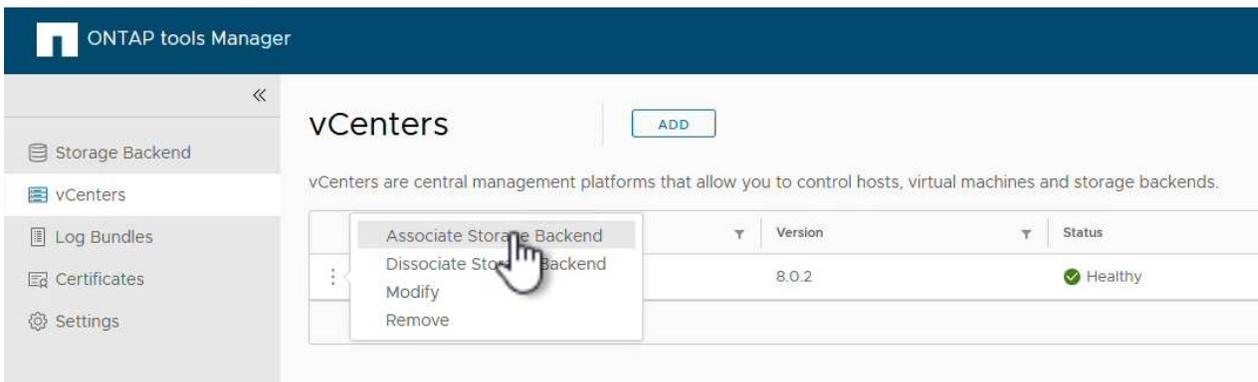
Password: * 

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, with the 'Associate Storage Backend' option highlighted by a hand cursor. The table contains one row with the version '8.0.2' and status 'Healthy'.

	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

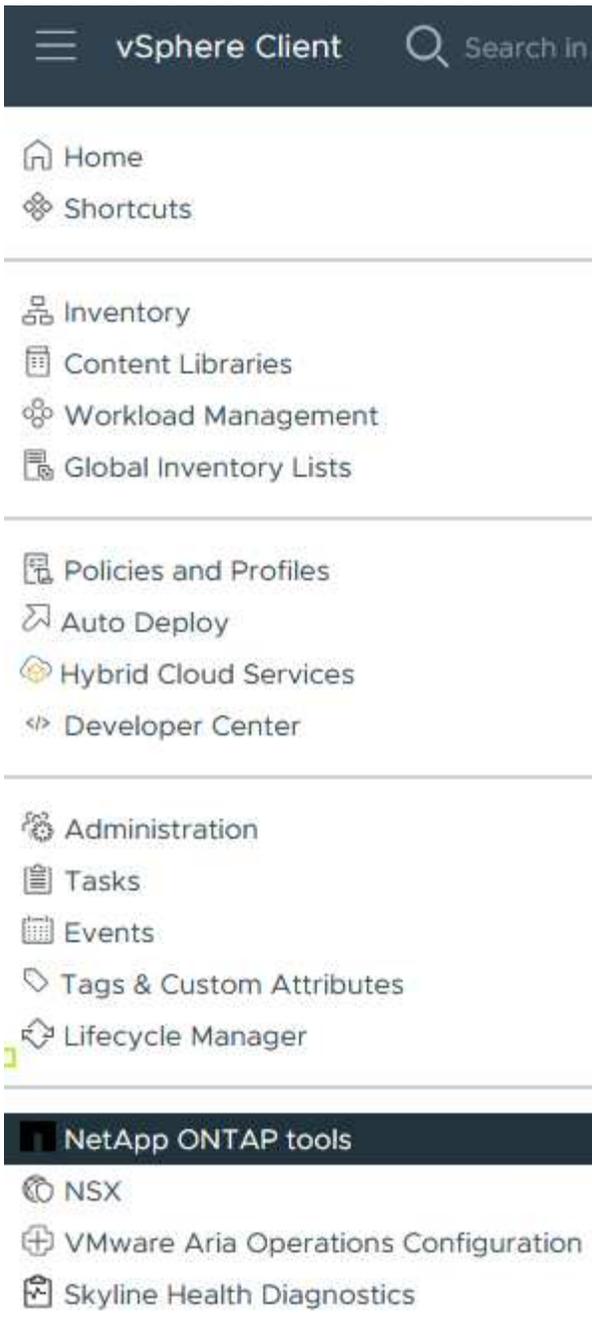


CANCEL

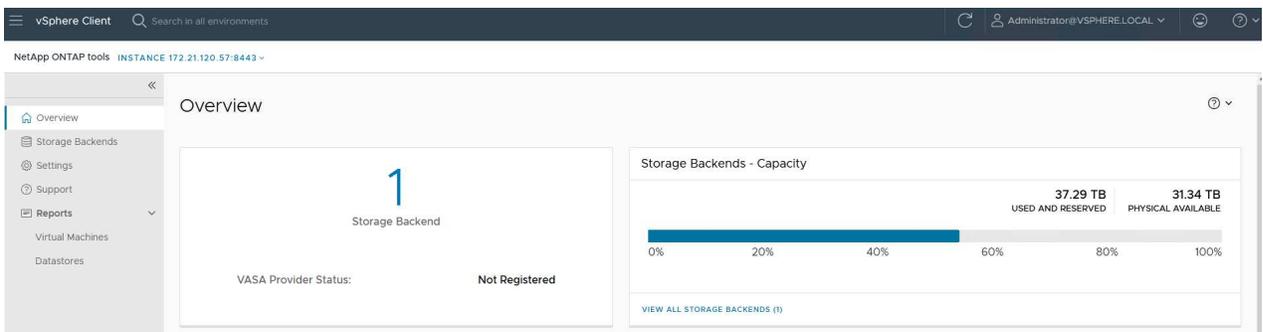
ASSOCIATE



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.

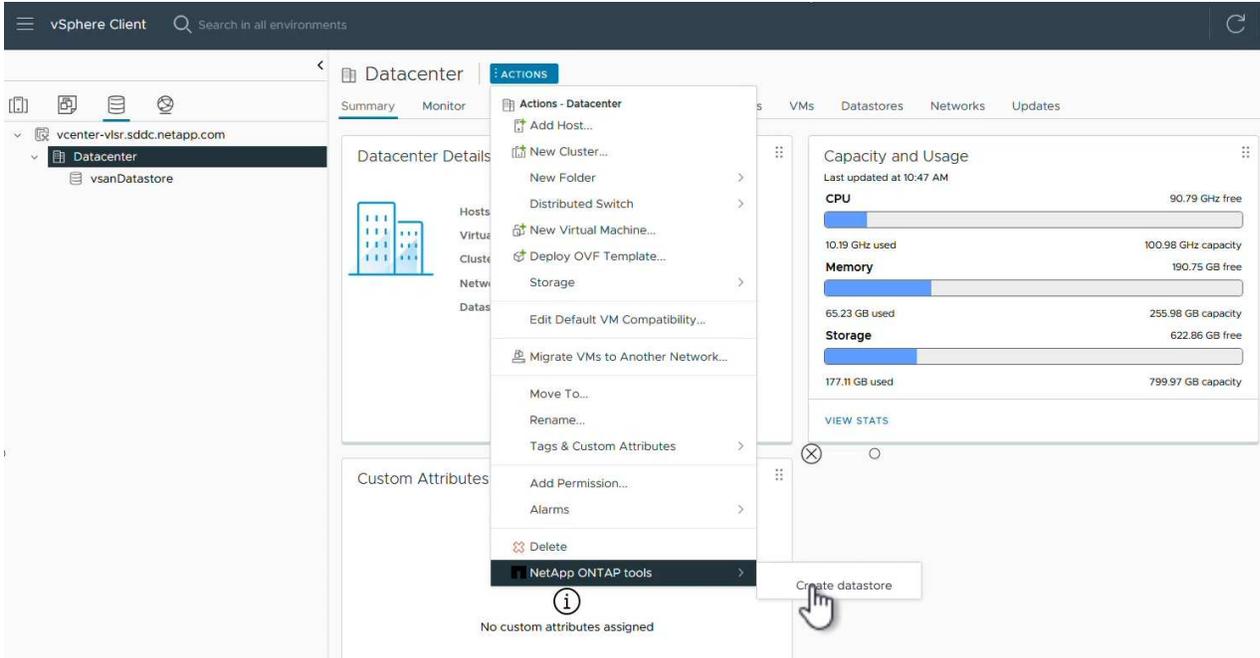




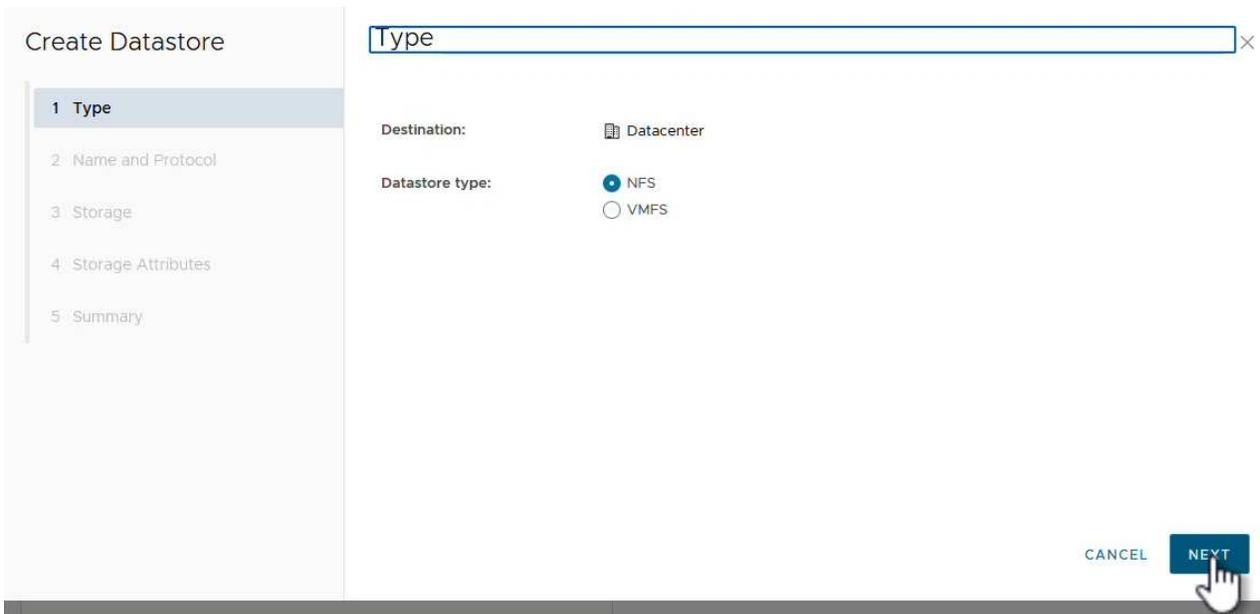
Cree un almacén de datos NFS con las herramientas de ONTAP 10

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 dropdown arrow). Below this field, it says 'Minimum supported size is 1 GB.'
- Protocol:** NFS 3 (with a dropdown arrow).
- Advanced Options:** A section header with a chevron icon.
- Datastore Cluster:** (with a dropdown arrow).

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at 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) (with a dropdown arrow).
- Storage VM: *** VCF_NFS (with a dropdown arrow). Below this field, it says 'ntaphci-a300e9u25 (172.16.9.25)'. There is also a small 'x' icon in the top right corner of the main area.
- Advanced Options:** A section header with a chevron icon.
- Custom Export Policy:** Search or specify policy name (with a dropdown arrow). Below this field, it says '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 pointing at 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

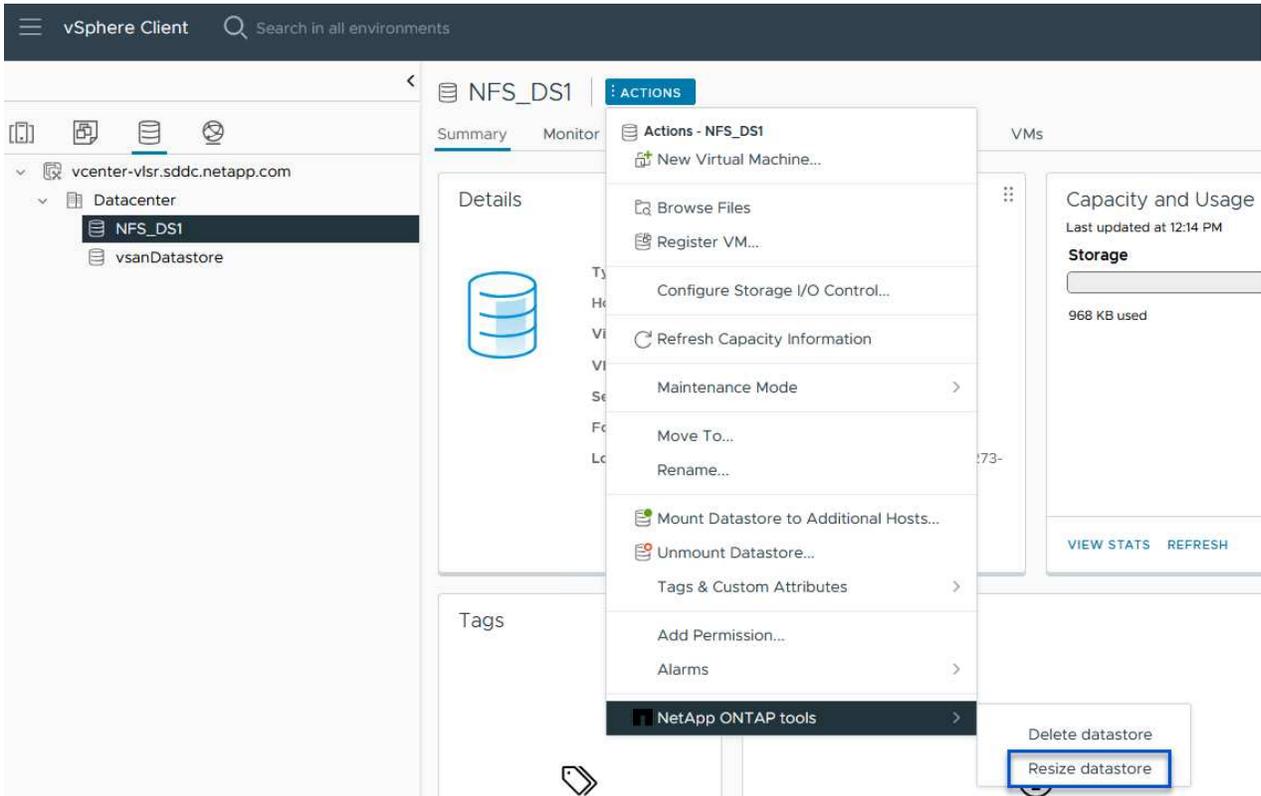
BACK

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 <input type="text"/>

CANCEL

RESIZE

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	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.

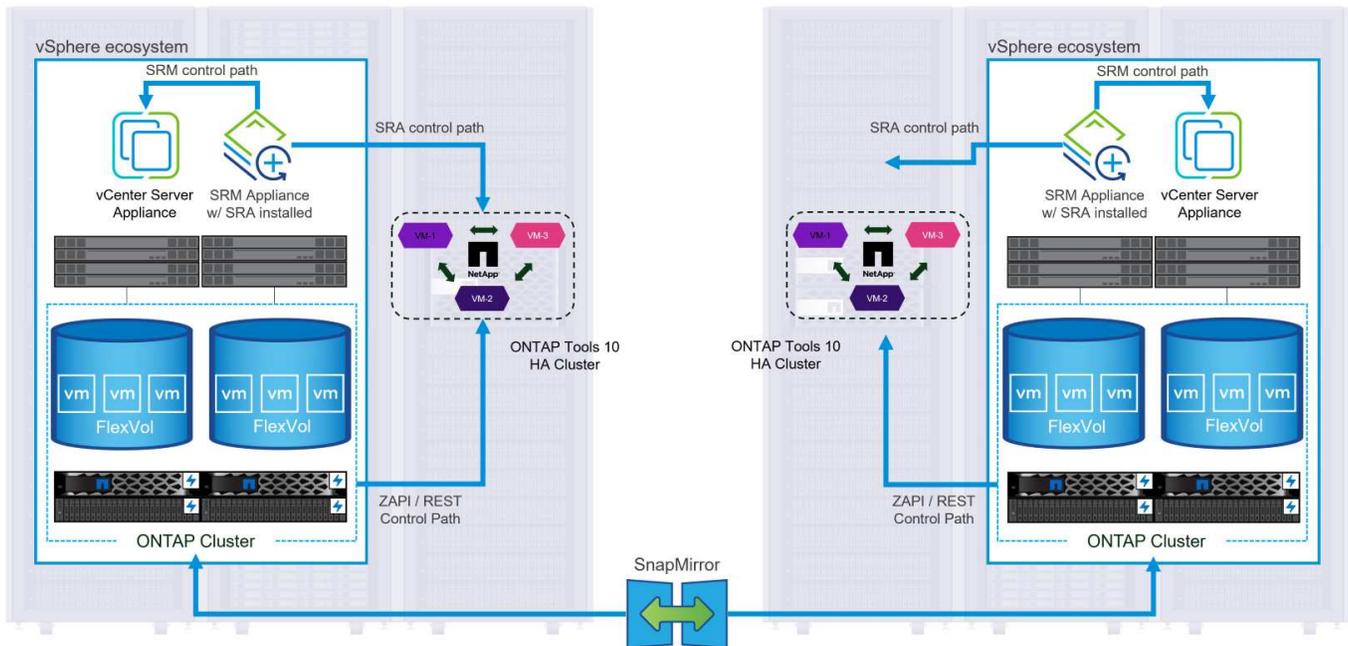
Descripción general del escenario

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.

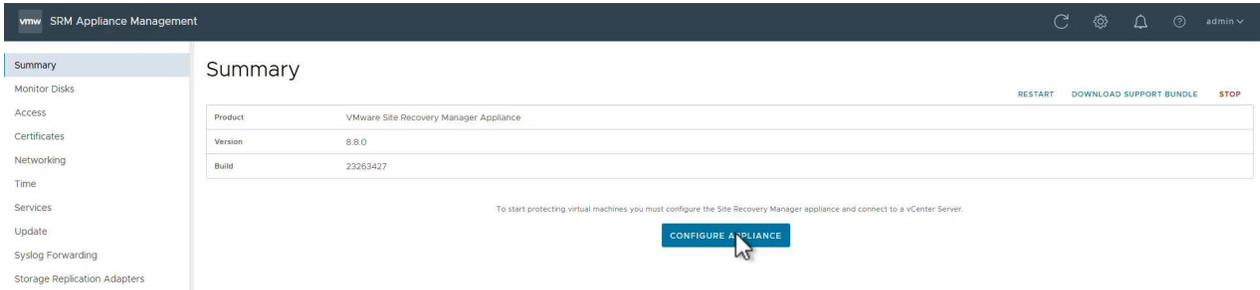
Configure el dispositivo SRM

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

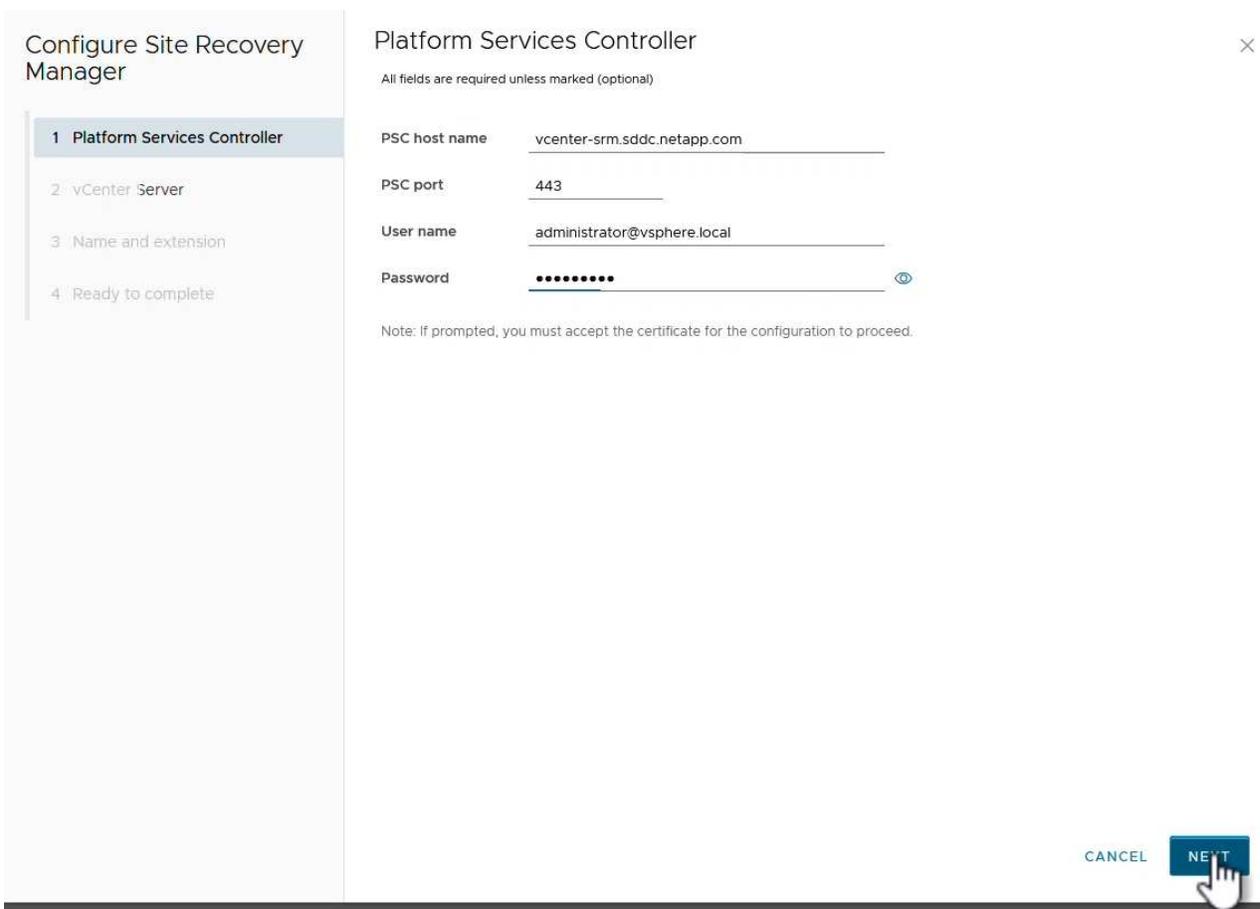
Conecte el dispositivo SRM para sitios primarios y secundarios

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 for Site Recovery Manager. On the left, a sidebar titled 'Configure Site Recovery Manager' lists 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 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)

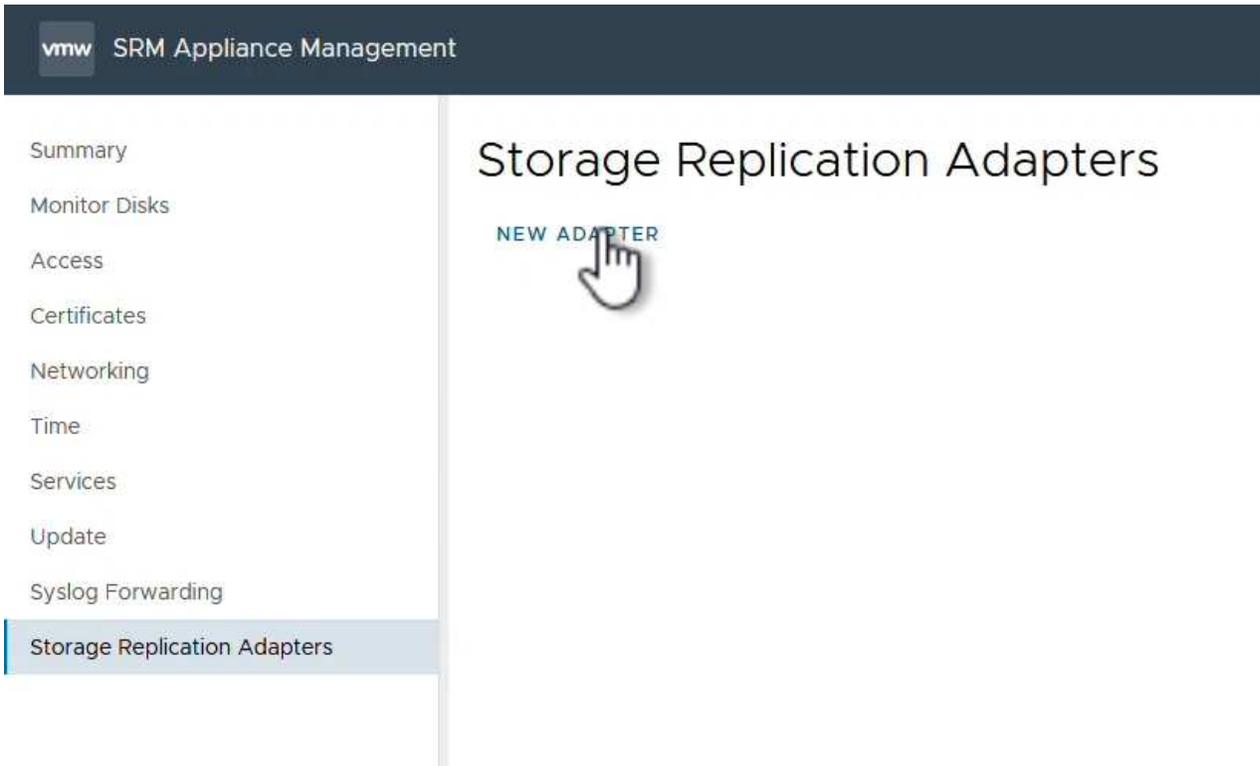
At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is clicking the NEXT button.

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.

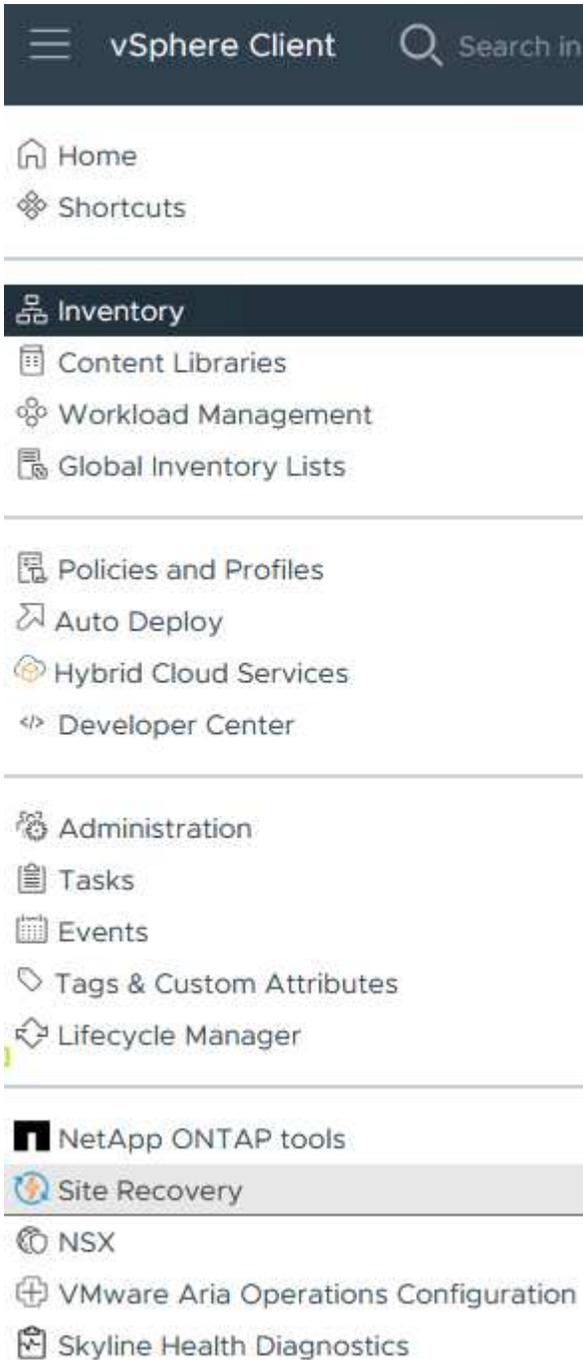
Configurar Site Recovery para SRM

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, showing 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

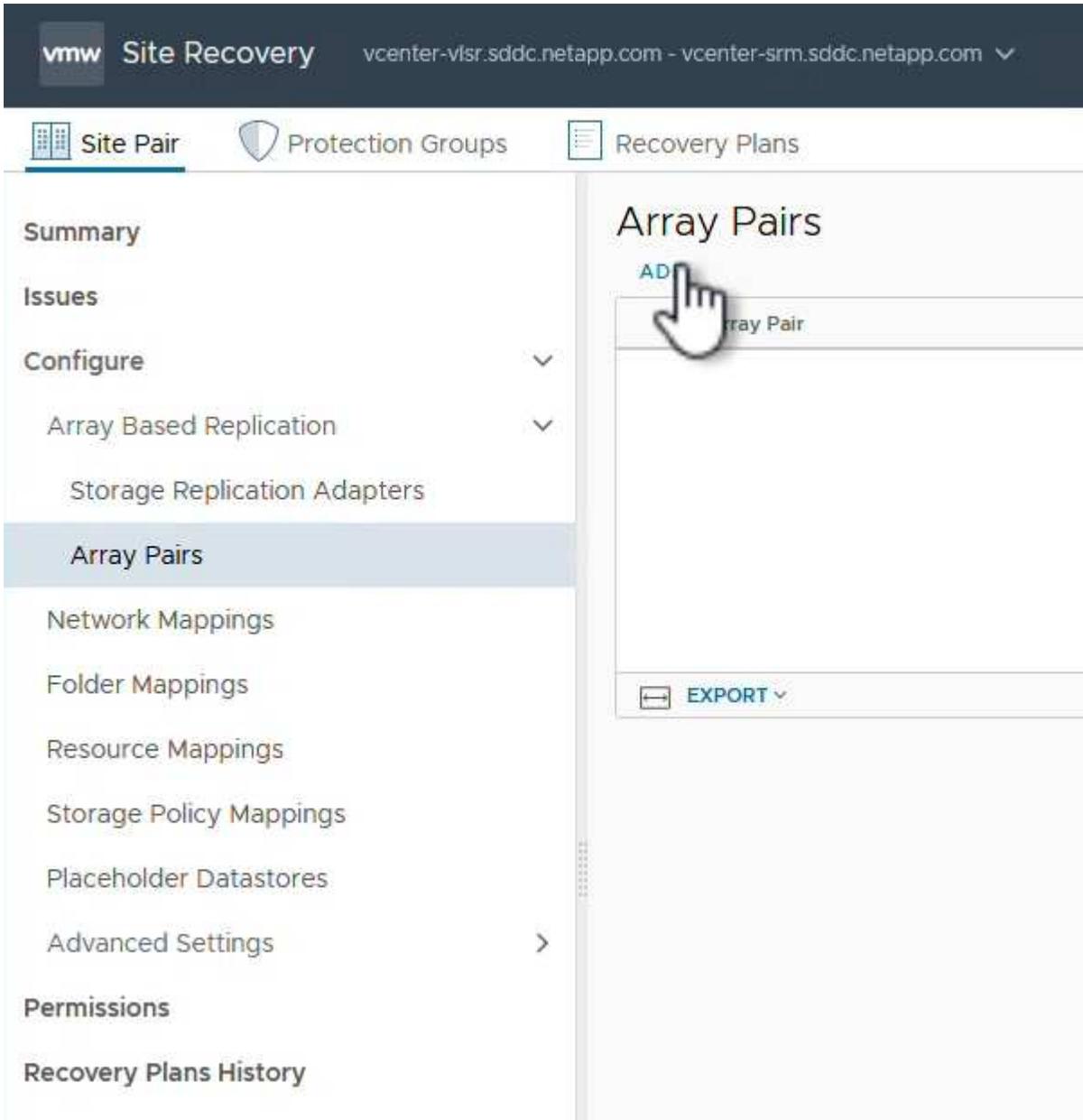
Protection Groups:0 Recovery Plans:0

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":

Storage Array Parameters

Storage System connection parameters

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

Storage Virtual Machine(SVM) Name
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

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

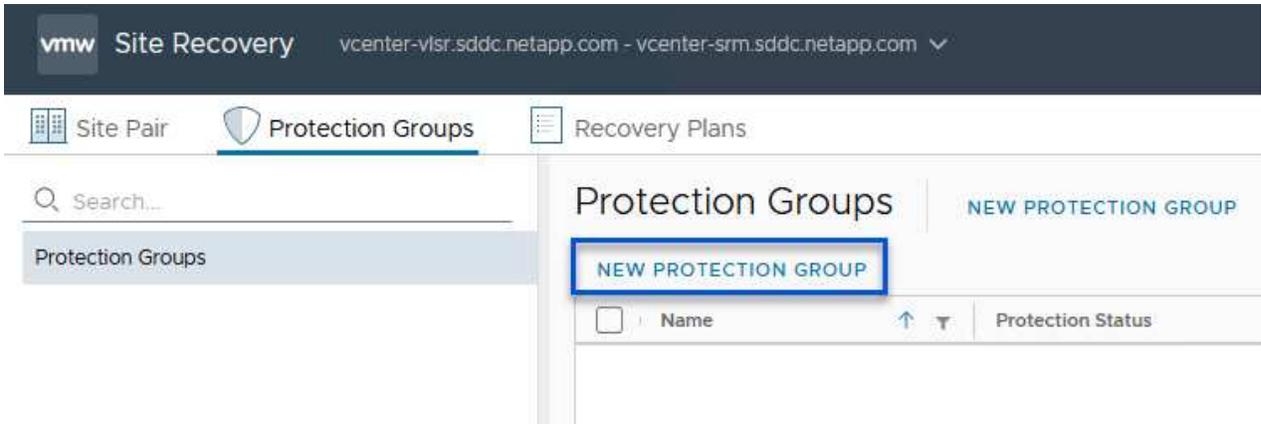
NEXT

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

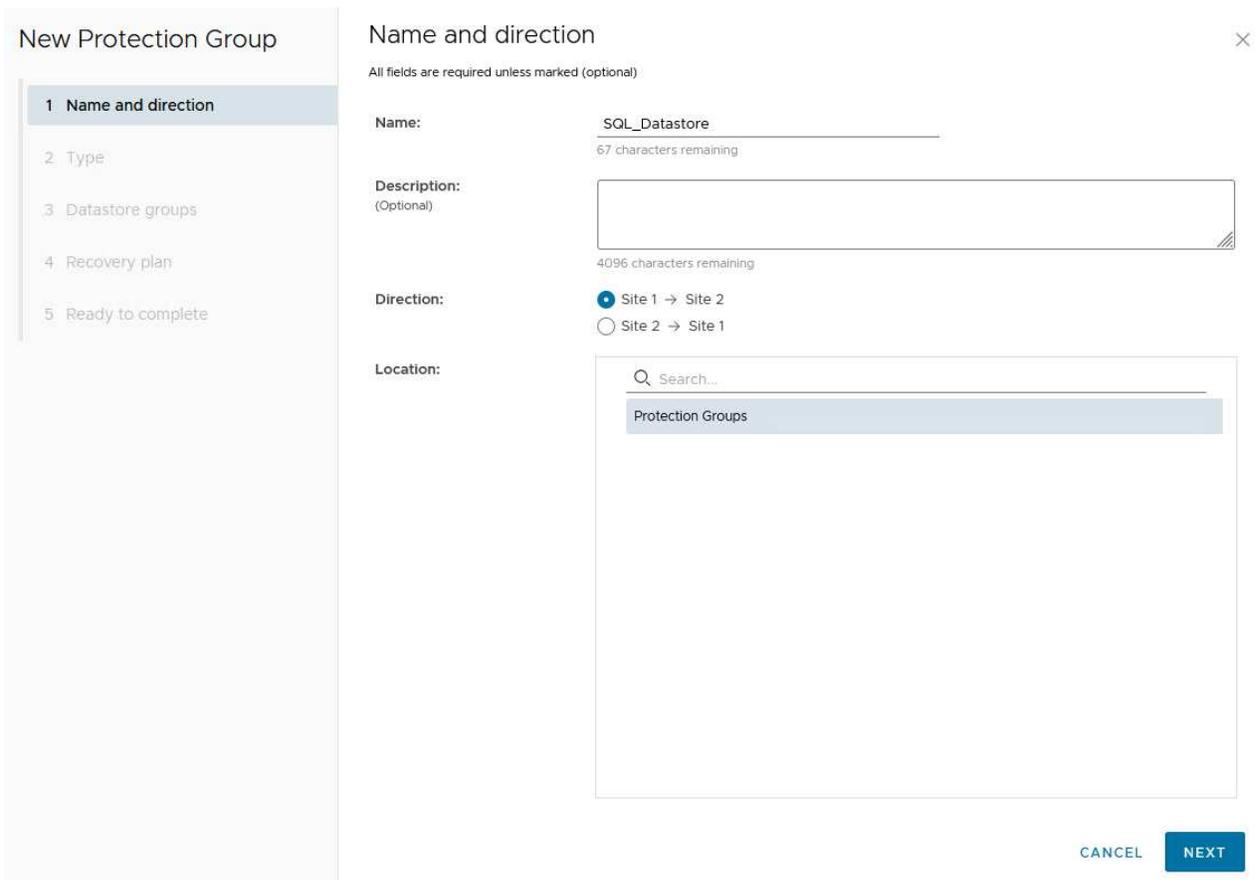
Configure los grupos de protección para el SRM

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.



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

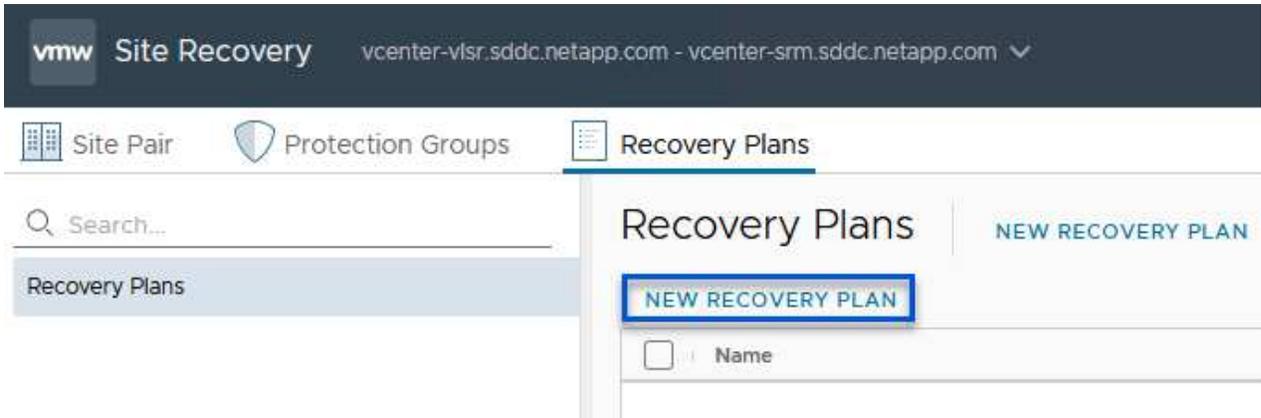
BACK

FINISH

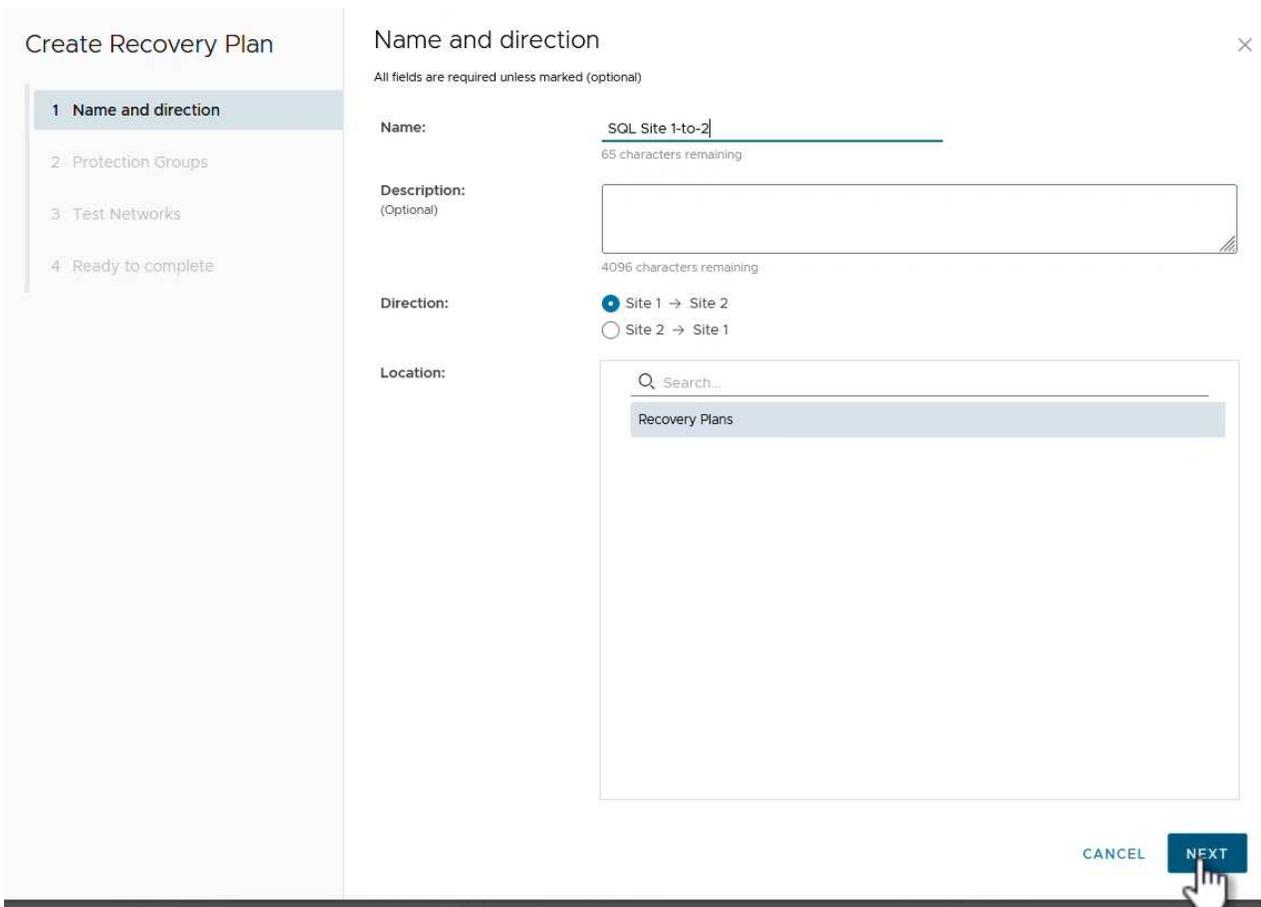
Configurar el plan de recuperación para SRM

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.

Create Recovery Plan

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

Protection Groups [Close]

All Selected (1)

<input checked="" type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	SQL_Datastore	

Items per page: AUTO 1 group(s)

CANCEL BACK **NEXT**

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

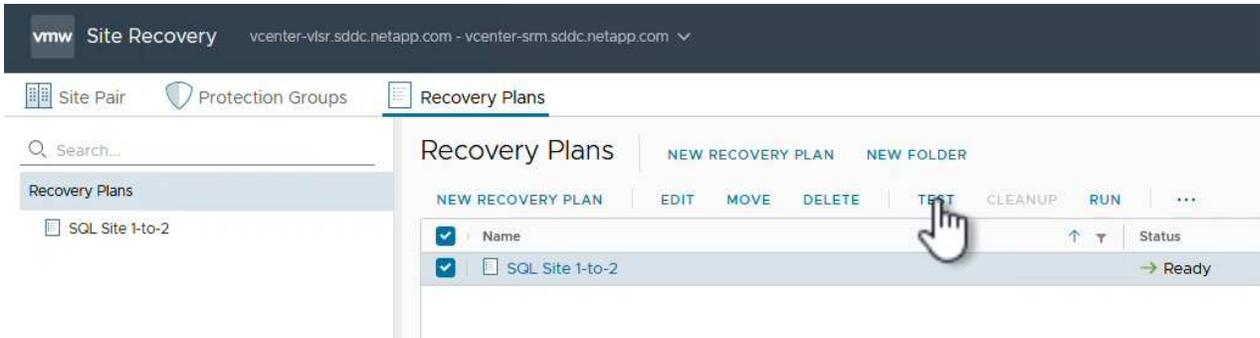
En esta sección se tratarán varias funciones de uso de la recuperación ante desastres con SRM, como la prueba de recuperación tras fallos, la realización de recuperación tras fallos, la realización de reprotcción y la conmutación tras recuperación.

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

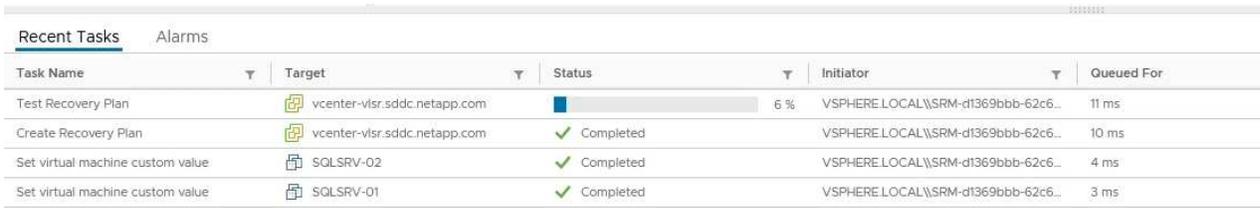
Pruebas de recuperación tras fallos con SRM

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.



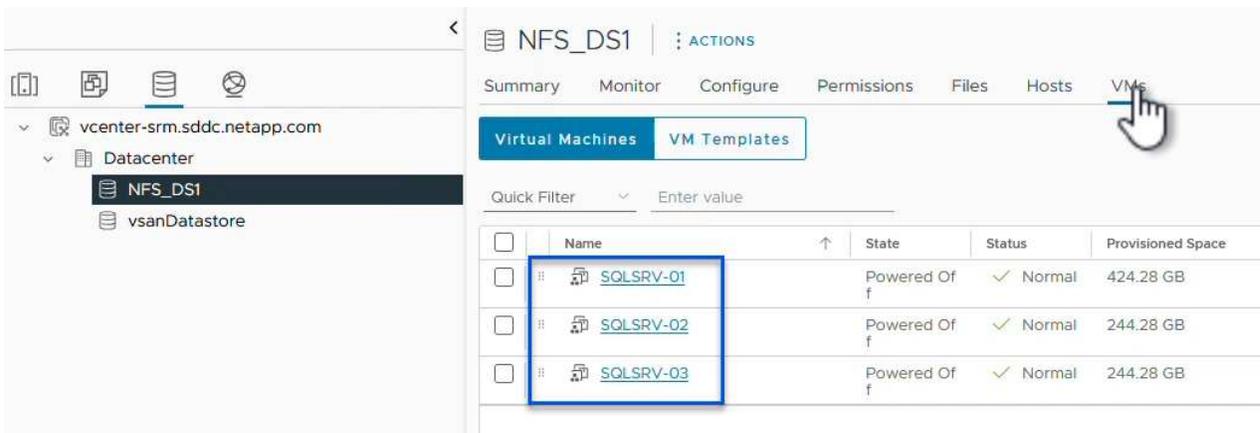
2. Es posible ver el progreso de la prueba desde el panel de tareas Site Recovery y el panel de tareas de vCenter.



The screenshot shows the 'Recent Tasks' panel in the VMware Site Recovery Manager interface. The panel has two tabs: 'Recent Tasks' and 'Alarms'. The 'Recent Tasks' tab is active. Below the tabs, there's a table 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'.

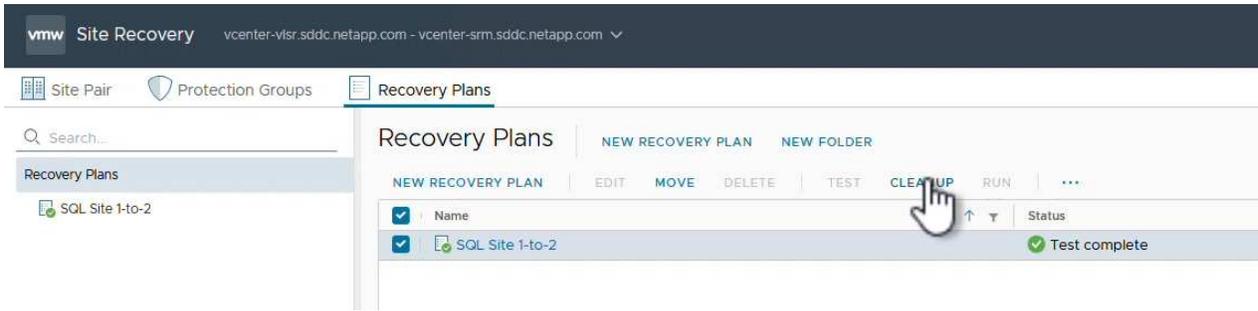
Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...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

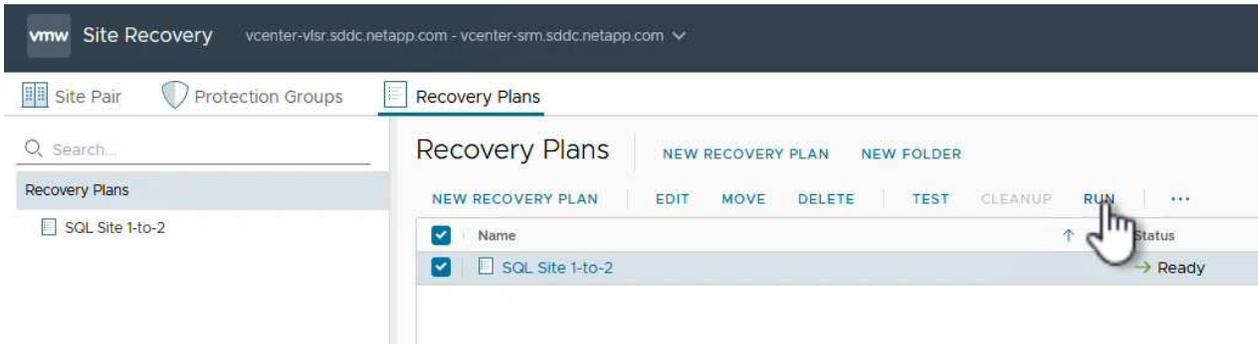
entorno original.



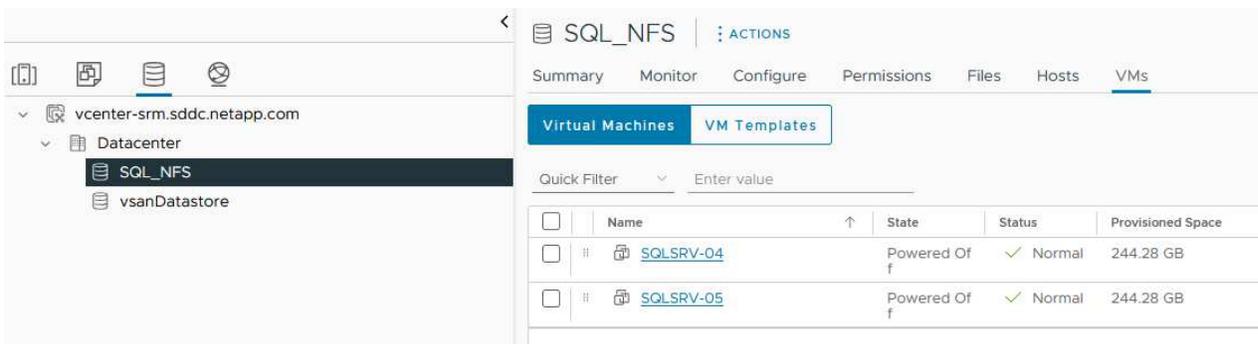
Ejecute el plan de recuperación con SRM

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"](#)

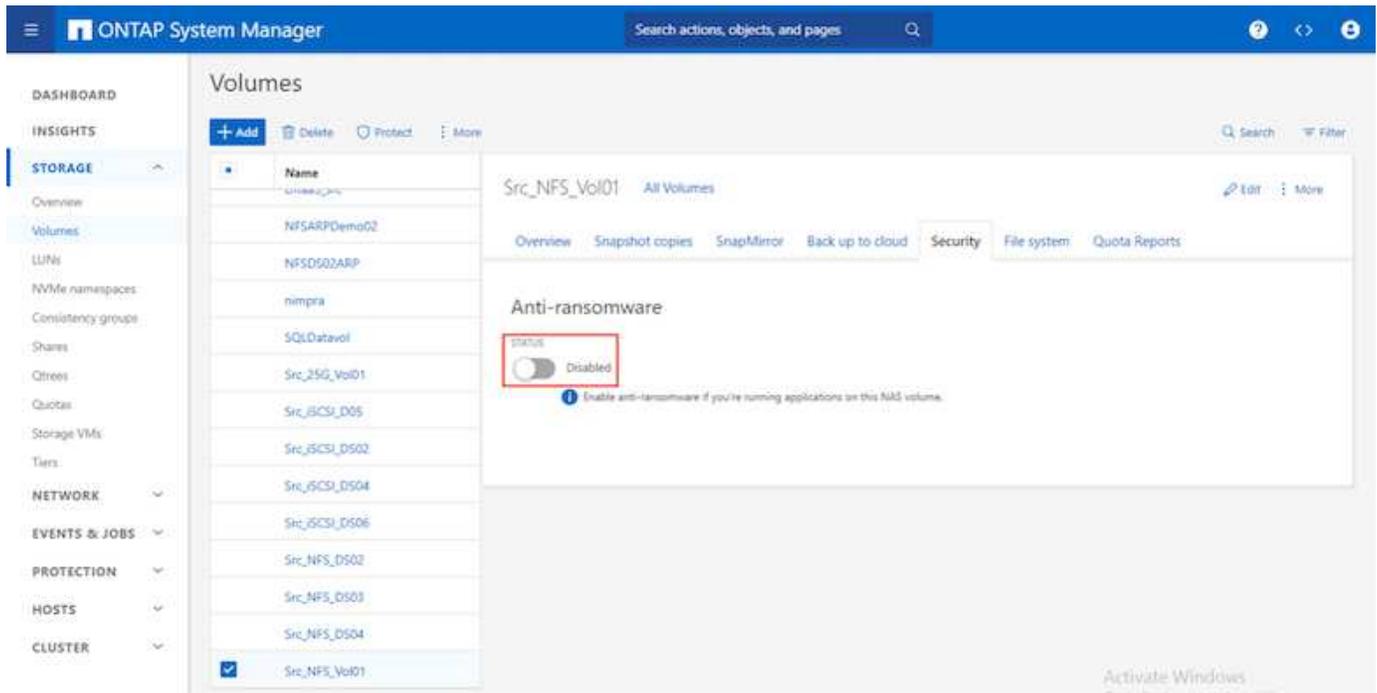
Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

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.

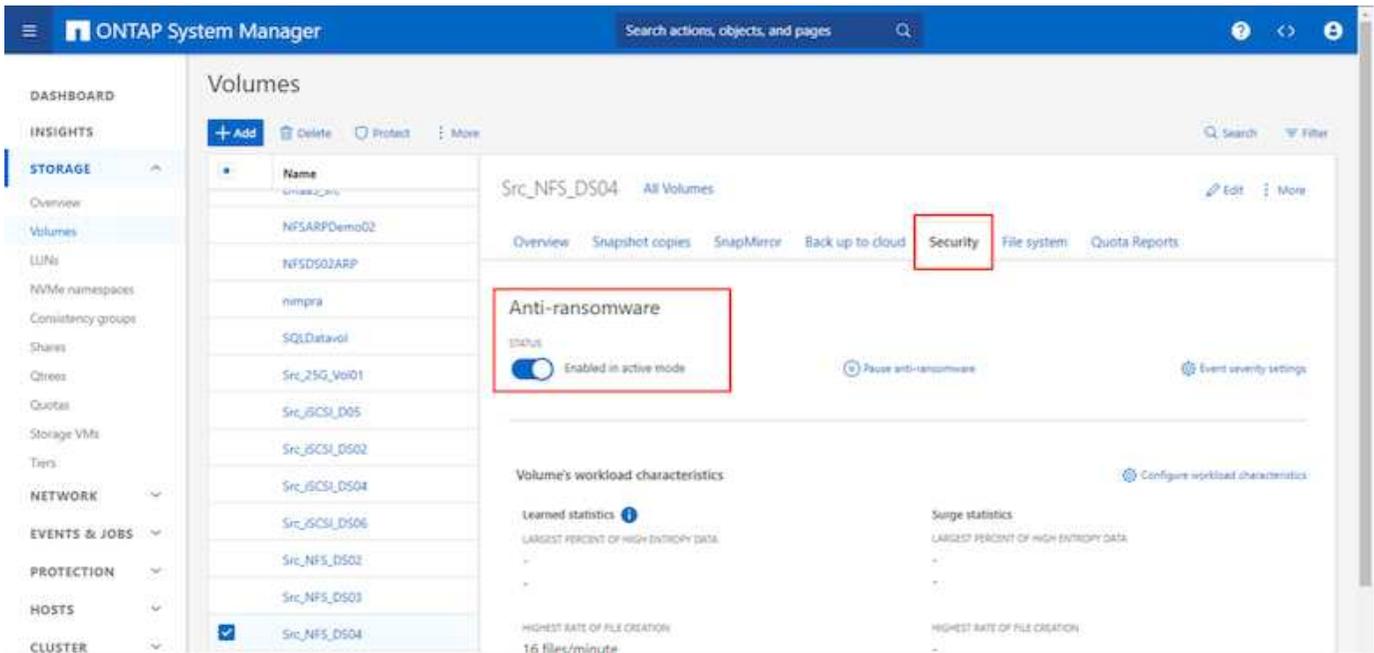


Con el nuevo ARP/AI de NetApp, que actualmente se encuentra en versión preliminar tecnológica, no es necesario un modo de aprendizaje. En su lugar, puede pasar directamente al modo activo con su función de detección de ransomware impulsada por la IA.



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.

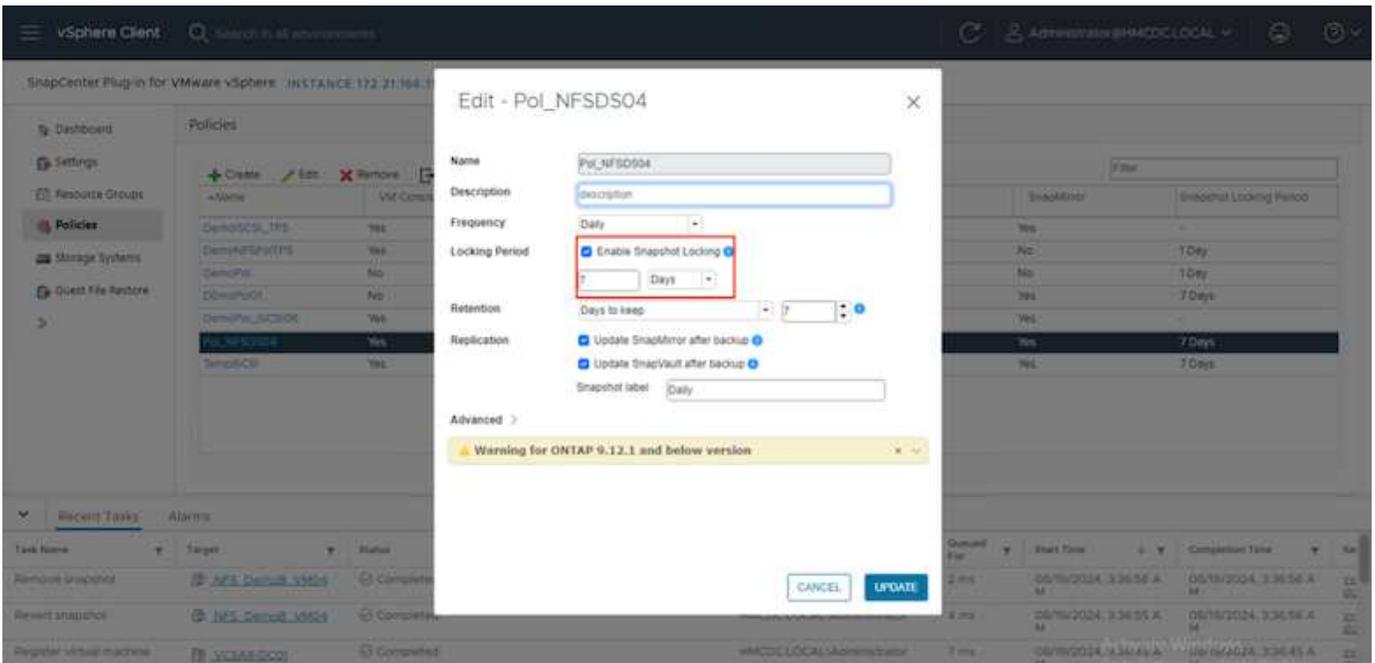
Una vez en el modo activo, se inicia a buscar la actividad anormal del volumen que podría ser potencialmente ransomware. Si se detecta una actividad anormal, se realiza inmediatamente una copia snapshot automática que proporciona un punto de restauración lo más cercano posible a la infección del archivo. 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.



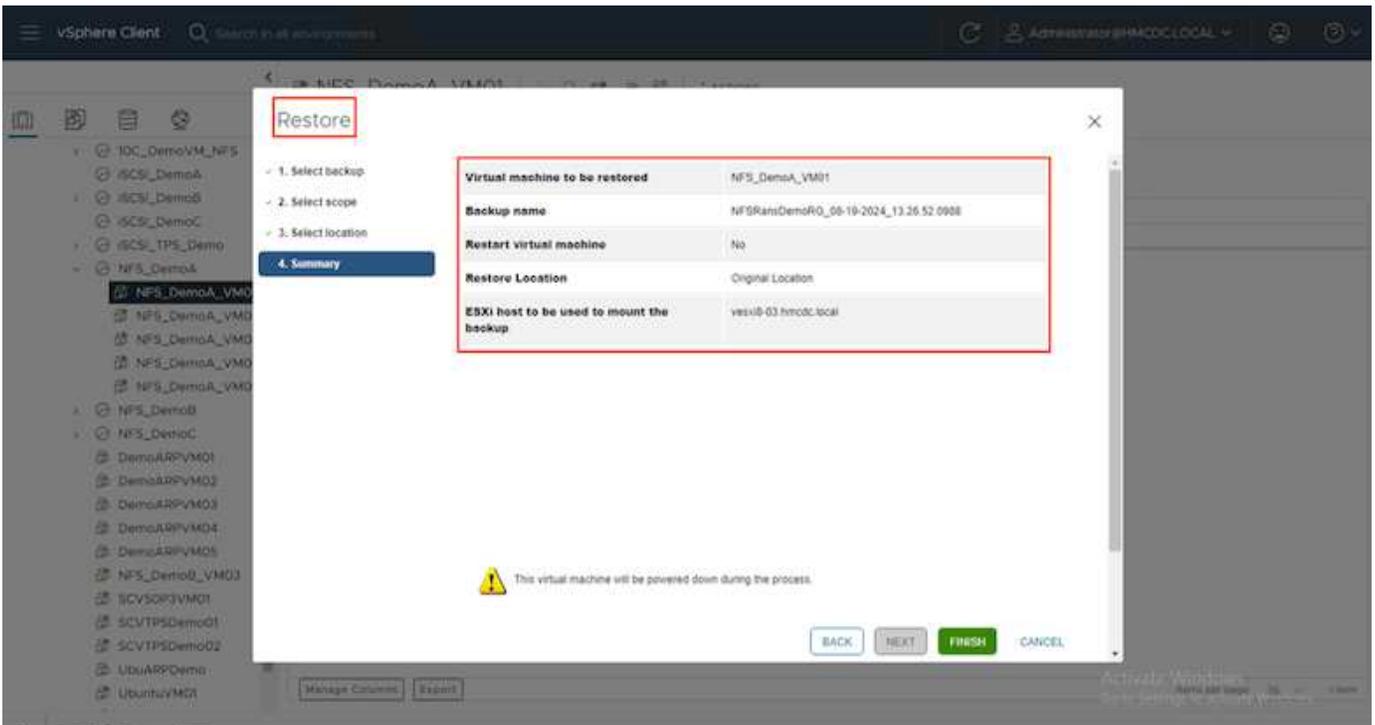
Si un ataque de ransomware se dirige a la máquina virtual (VM) y altera los archivos dentro de la máquina virtual sin hacer cambios fuera de la máquina virtual, la protección avanzada contra ransomware (ARP) seguirá detectando la amenaza si la entropía predeterminada de la máquina virtual es baja, por 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

0 Alerts

Not marked for recovery

VM datastore

Location: urn:acvs:svm:U1:Resou...

vCenter server: vvcas01-01.hmc:dc: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

Protection

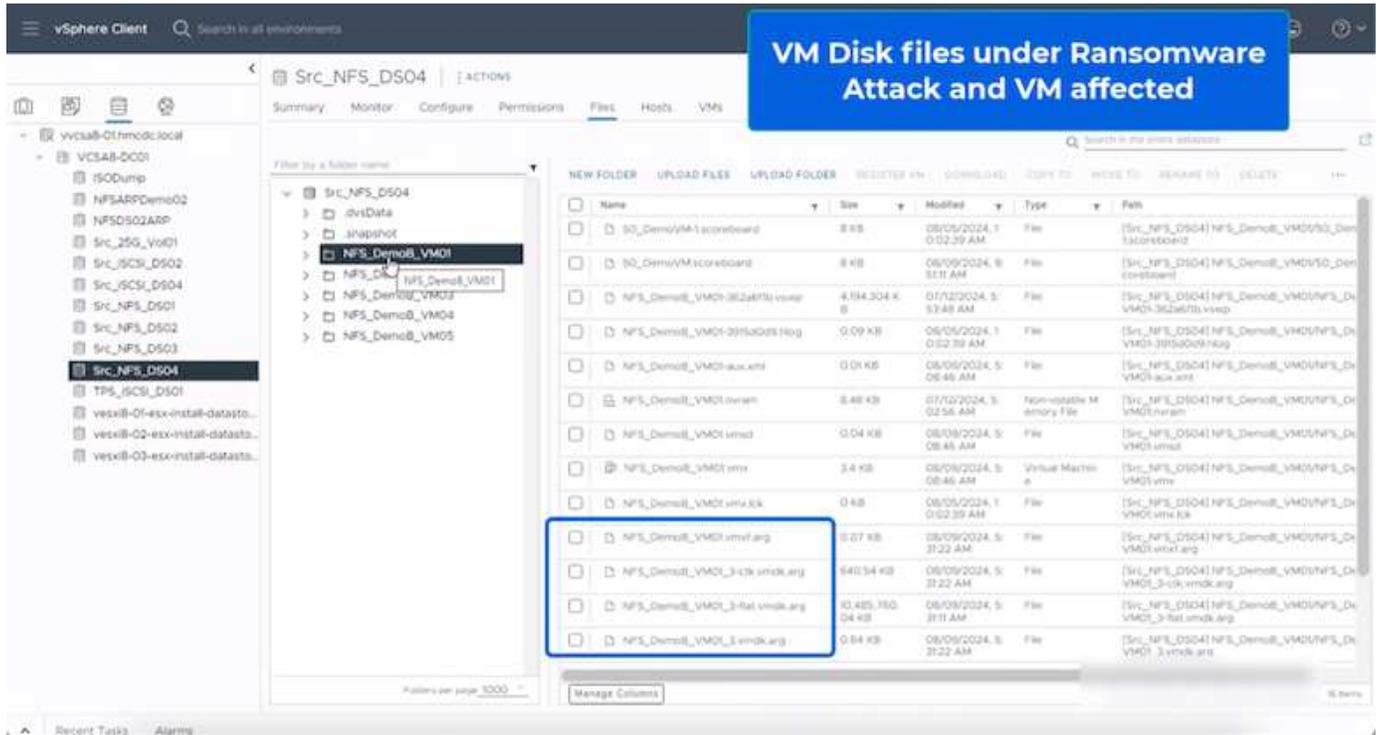
These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

- Pol_NFSDS04 Snapshot policy
- 1 Year Daily LTR Backup policy

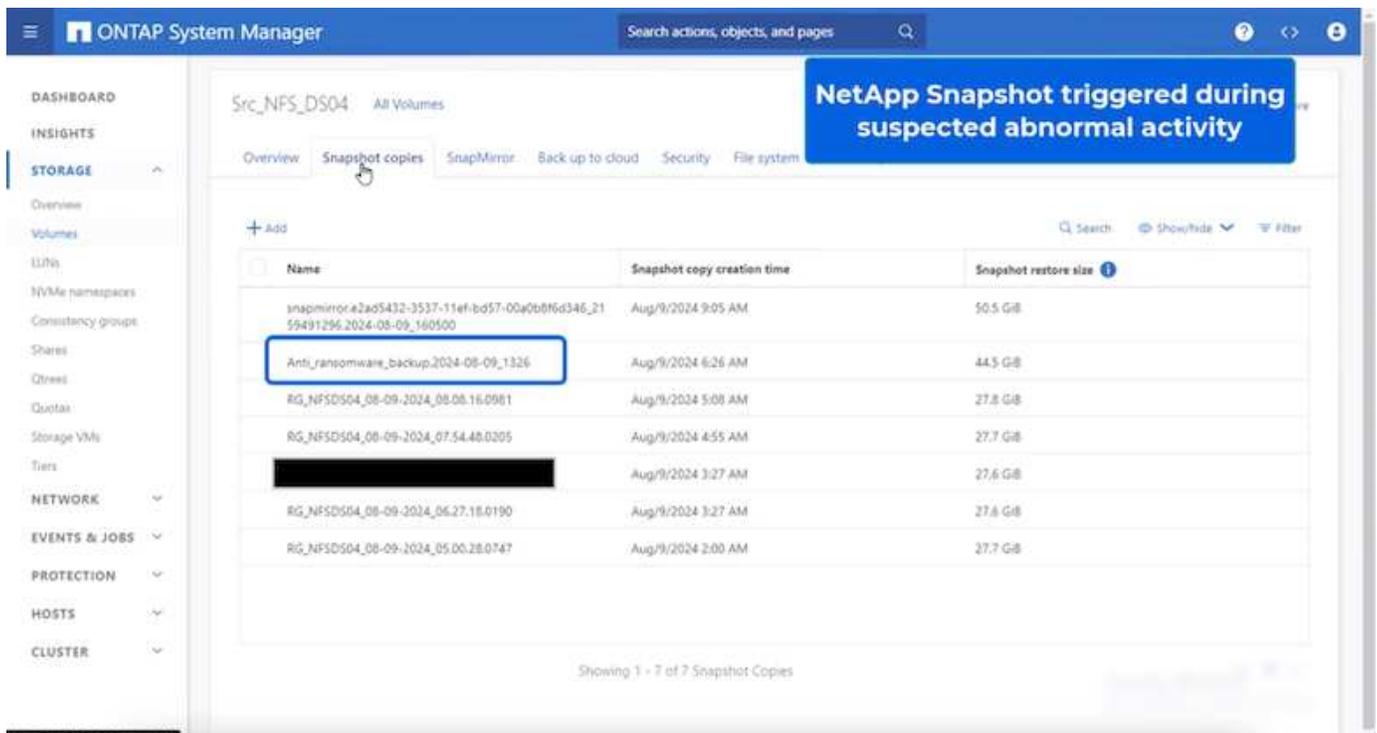
Para obtener información detallada sobre cómo configurar la protección contra ransomware de BlueXP , consulte "Configura la protección frente al ransomware de BlueXP" y "Configura las opciones de protección

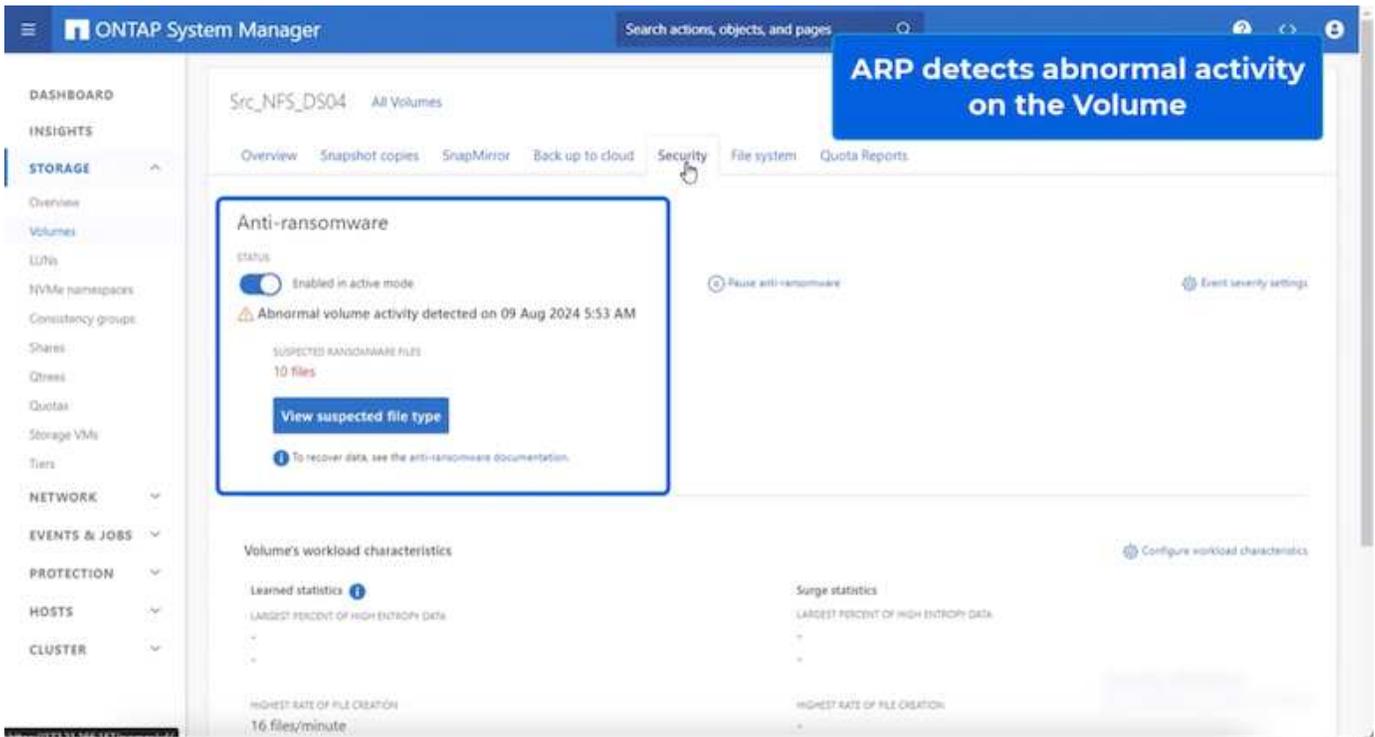
contra ransomware de BlueXP".

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

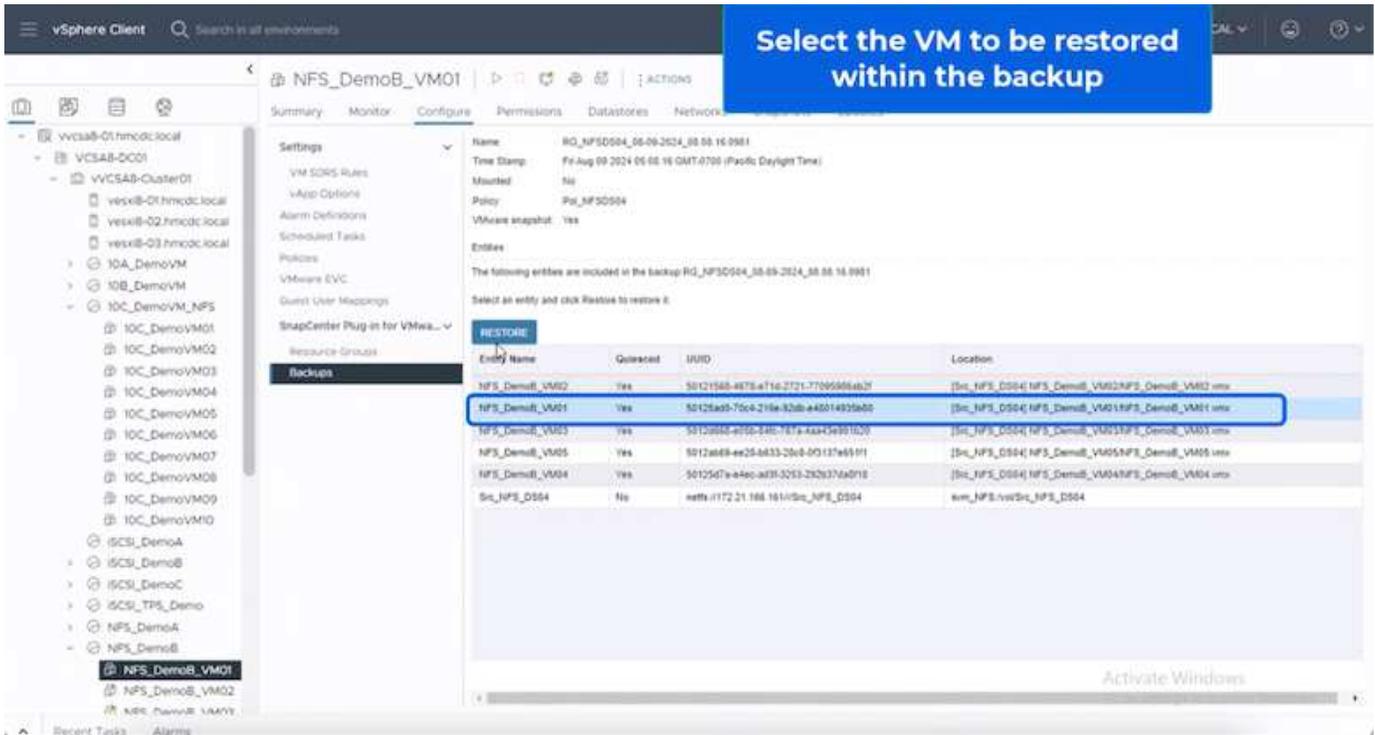


ARP activó inmediatamente una instantánea en el volumen después de la detección.





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.

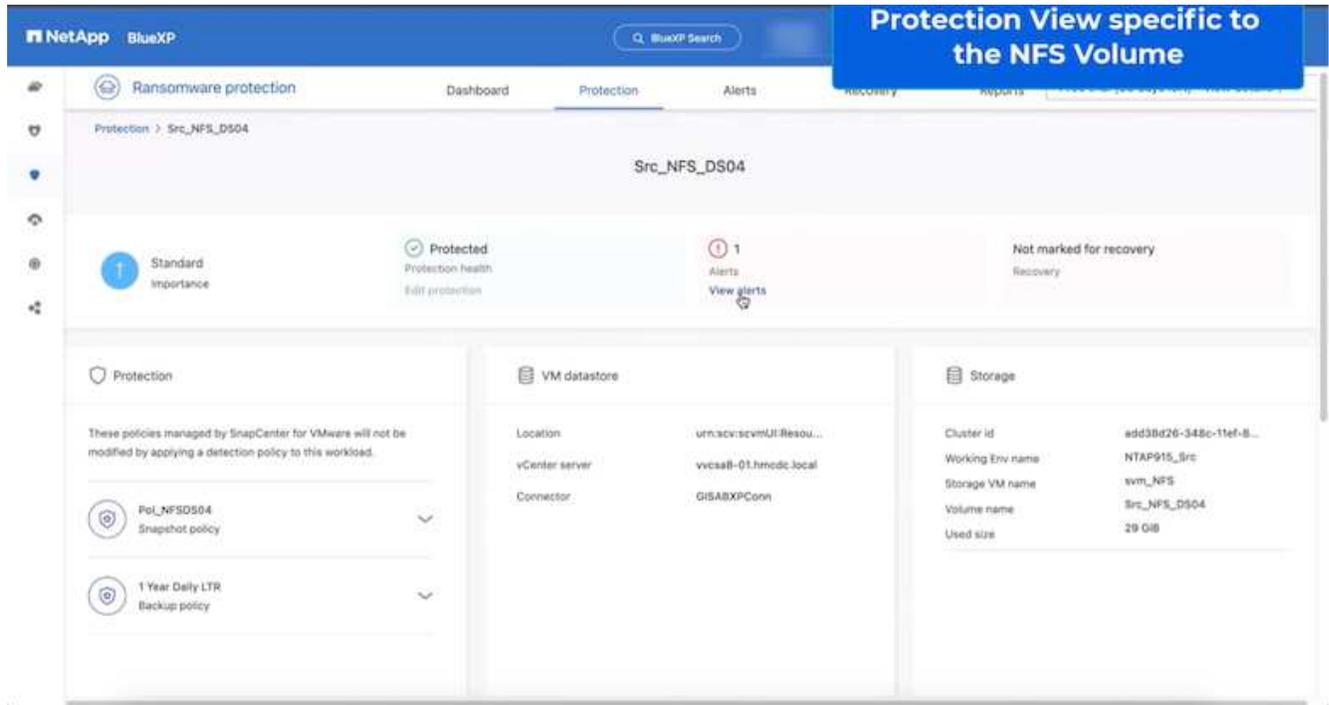


Esta sección muestra cómo la protección contra ransomware de BlueXP orquesta la recuperación de un incidente de ransomware en el que los archivos de VM están cifrados.

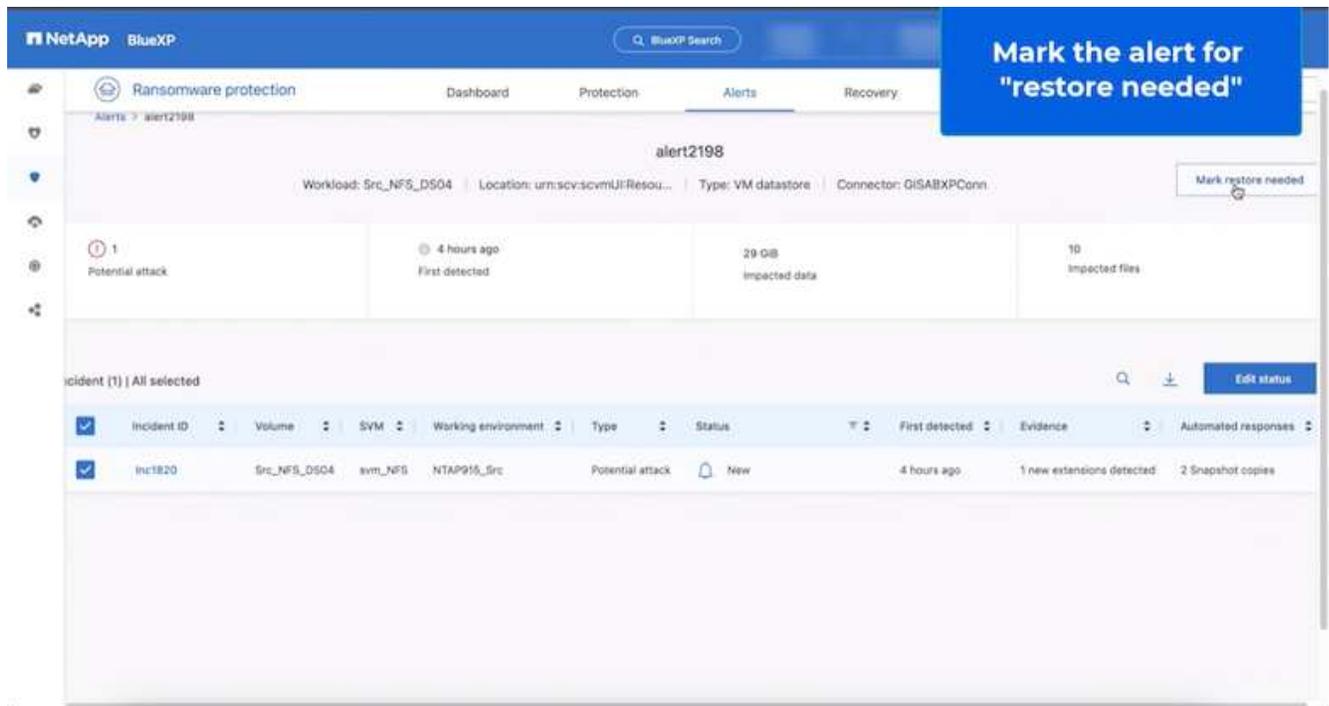


Si SnapCenter gestiona la máquina virtual, la protección frente al ransomware de BlueXP restaura la máquina virtual a su estado anterior mediante el proceso consistente con la máquina virtual.

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



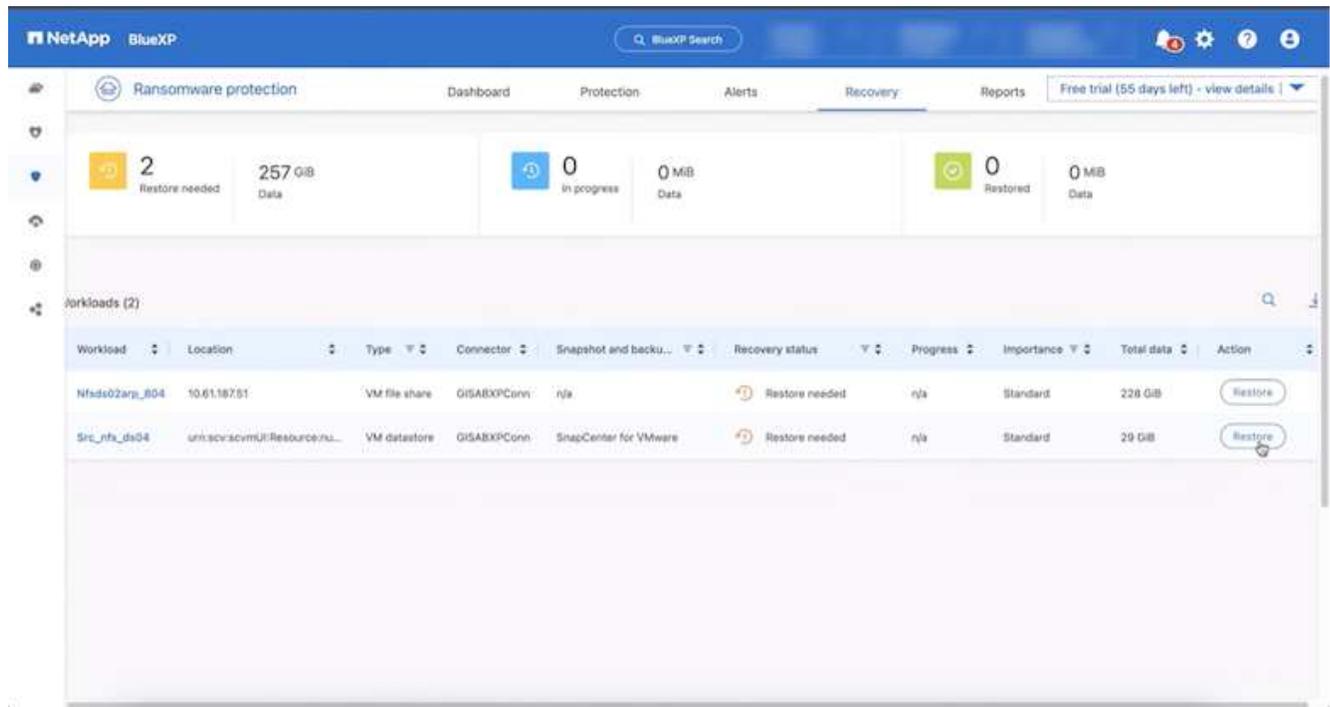
3. Marque el incidente de ransomware como listo para la recuperación (después de que se neutralicen los incidentes) seleccionando «Mark restore needed» (Mark restore needed).



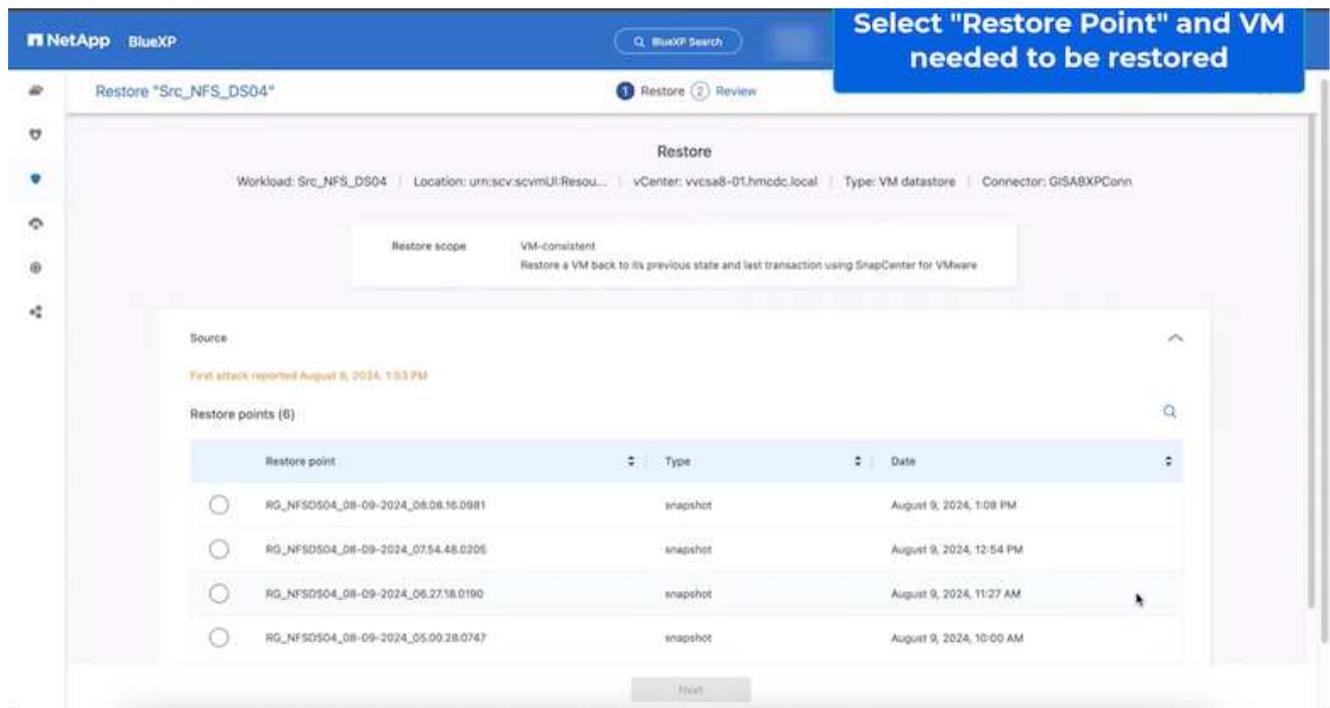


La alerta se puede descartar si el incidente resulta ser falso positivo.

- 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

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.

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.