



# **VMware**

## Enterprise applications

NetApp  
January 12, 2026

# Tabla de contenidos

|  |     |
|--|-----|
| VMware   | 1   |
| VMware vSphere con ONTAP   | 1   |
| VMware vSphere con ONTAP   | 1   |
| ¿Por qué elegir ONTAP para VMware vSphere?   | 1   |
| Almacenamiento unificado   | 3   |
| Herramientas de virtualización para ONTAP  | 5   |
| Volúmenes virtuales (vVols) y gestión basada en políticas de almacenamiento (SPBM) | 7   |
| Almacenes de datos y protocolos  | 8   |
| Configuración de red   | 23  |
| Clonado de máquinas virtuales y almacenes de datos                                 | 26  |
| Protección de datos  | 28  |
| Calidad de servicio (QoS)  | 31  |
| Migración al cloud y backup  | 36  |
| Cifrado para datos de vSphere  | 37  |
| Active IQ Unified Manager  | 38  |
| Gestión basada en políticas de almacenamiento y vVols                              | 40  |
| Planificador de recursos distribuidos de almacenamiento de VMware                  | 42  |
| Host ESXi recomendado y otra configuración de ONTAP                                | 43  |
| Virtual Volumes (vVols) con herramientas de ONTAP 10                               | 47  |
| Descripción general  | 47  |
| Lista de comprobación  | 53  |
| Usar vVols con ONTAP   | 55  |
| Puesta en marcha de vVols en sistemas AFF, ASA, ASA R2 y FAS                       | 61  |
| Protección de vVols  | 72  |
| Resolución de problemas  | 77  |
| VMware Site Recovery Manager con ONTAP   | 78  |
| Recuperación de sitios en vivo de VMware con ONTAP                                 | 78  |
| Mejores prácticas de puesta en marcha  | 80  |
| Mejores prácticas operativas   | 81  |
| Topologías de replicación  | 86  |
| Solución de problemas de VLSRM/SRM cuando se usa la replicación de vVols           | 95  |
| Información adicional  | 96  |
| Clúster de almacenamiento vSphere Metro con ONTAP                                  | 96  |
| Clúster de almacenamiento vSphere Metro con ONTAP                                  | 96  |
| Descripción general de la solución de VMware vSphere                               | 99  |
| Directrices de implementación y diseño de VMSC                                     | 104 |
| Resiliencia para eventos planificados y no planificados                            | 115 |
| Situaciones de fallo para VMSC con MetroCluster                                    | 116 |
| Seguridad de los productos   | 127 |
| Herramientas de ONTAP para VMware vSphere  | 127 |
| Complemento de SnapCenter, VMware vSphere  | 129 |
| Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere         | 132 |
| Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere 9,13    | 132 |

|   |     |
|---|-----|
| Verificación de la integridad de las herramientas de ONTAP para los paquetes de instalación de VMware vSphere 9,13 . . . . .                              | 132 |
| Puertos y protocolos para las herramientas de ONTAP 9,13 . . . . .  | 134 |
| Herramientas de ONTAP para puntos de acceso de VMware vSphere 9,13 (usuarios) . . . . .   | 135 |
| ONTAP TOOLS 9,13 TLS mutuo (autenticación basada en certificados) . . . . .   | 136 |
| Certificado HTTPS de ONTAP TOOLS 9,13 . . . . .   | 143 |
| Banner de inicio de sesión de ONTAP tools 9,13 . . . . .  | 144 |
| Tiempo de espera de inactividad para las herramientas de ONTAP 9,13 . . . . .   | 144 |
| Número máximo de solicitudes simultáneas por usuario (protección de seguridad de red/ataque DOS) herramientas de ONTAP para VMware vSphere 9,13 . . . . . | 144 |
| Configuración del Protocolo de hora de red (NTP) para las herramientas ONTAP 9,13 . . . . .   | 145 |
| Políticas de contraseñas para las herramientas de ONTAP 9,13 . . . . .  | 145 |

# VMware

## VMware vSphere con ONTAP

### VMware vSphere con ONTAP

ONTAP ha servido como solución de almacenamiento líder para VMware vSphere y, más recientemente, entornos de Cloud Foundation desde su introducción en el centro de datos moderno en 2002. Sigue introduciendo funciones innovadoras que simplifican la gestión y reducen los costes.

Este documento presenta la solución ONTAP para vSphere, donde se destaca la información de producto más reciente y las prácticas recomendadas para simplificar la puesta en marcha, mitigar los riesgos y simplificar la gestión.



Esta documentación sustituye a los informes técnicos publicados anteriormente *TR-4597: VMware vSphere para ONTAP*

Las prácticas recomendadas complementan otros documentos, como guías y listas de compatibilidad. Se desarrollan según pruebas de laboratorio y una amplia experiencia de campo por parte de ingenieros y clientes de NetApp. Puede que no sean las únicas prácticas compatibles que funcionan en todos los entornos, pero suelen ser las soluciones más sencillas que satisfacen las necesidades de la mayoría de los clientes.

Este documento se centra en las funcionalidades de los lanzamientos recientes de ONTAP (9.x) ejecutados en vSphere 7,0 o posterior. Consulte la "["Herramienta de matriz de interoperabilidad \(IMT\)"](#)" y "["Guía de compatibilidad de VMware"](#)" para obtener detalles relacionados con versiones específicas.

### ¿Por qué elegir ONTAP para VMware vSphere?

Los clientes eligen con confianza ONTAP for vSphere para soluciones de almacenamiento SAN y NAS. La nueva arquitectura de almacenamiento desagregado simplificada, que se incluye en las últimas matrices All SAN, ofrece una experiencia simplificada familiar para los administradores de almacenamiento SAN y, al mismo tiempo, conserva la mayoría de las integraciones y el conjunto de características de los sistemas ONTAP tradicionales. Los sistemas ONTAP proporcionan una protección excepcional de instantáneas y herramientas de gestión sólidas. Al descargar funciones al almacenamiento dedicado, ONTAP maximiza los recursos del host, reduce costos y mantiene un rendimiento óptimo. Además, las cargas de trabajo se pueden migrar fácilmente mediante Storage vMotion a través de VMFS, NFS o vVols.

### Las ventajas de usar ONTAP para vSphere

Hay muchas razones por las que decenas de miles de clientes han seleccionado ONTAP como solución de almacenamiento para vSphere, como un sistema de almacenamiento unificado que admite los protocolos SAN y NAS, sólidas funcionalidades de protección de datos mediante copias Snapshot con gestión eficiente del espacio y una gran cantidad de herramientas para ayudar a gestionar los datos de aplicaciones. 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 de hardware del host y software VMware. También puede proteger sus datos a un menor coste y con un alto rendimiento constante. Debido a que las cargas de trabajo virtualizadas son móviles, puede explorar diferentes enfoques usando Storage vMotion para mover máquinas virtuales entre almacenes de datos VMFS, NFS o vVols, todo en el mismo sistema de almacenamiento.

Estos son los factores clave que los clientes valoran hoy en día:

- **Almacenamiento unificado.** Los sistemas que ejecutan ONTAP están unificados de varias maneras importantes. Originalmente, este enfoque se refería a los protocolos NAS y SAN, y ONTAP continúa siendo una plataforma líder para SAN, junto con su fortaleza original en NAS. En el mundo vSphere, este enfoque también podría significar un sistema unificado para la infraestructura de escritorio virtual (VDI) junto con la infraestructura de servidor virtual (VSI). Los sistemas que ejecutan ONTAP suelen ser menos costosos para VSI que las matrices empresariales tradicionales y, además, tienen capacidades avanzadas de eficiencia de almacenamiento para manejar VDI en el mismo sistema. ONTAP también unifica una variedad de medios de almacenamiento, desde SSD hasta SATA, y puede extenderlo fácilmente a la nube. No es necesario comprar un sistema operativo de almacenamiento para el rendimiento, otro para los archivos y otro más para la nube. ONTAP los une a todos.
- **Cabina All SAN (ASA).** Los sistemas de ONTAP ASA más recientes (a partir de A1K, A90, A70, A50, A30 y A20) se basan en una nueva arquitectura de almacenamiento que elimina el paradigma de almacenamiento tradicional de ONTAP relativo a la gestión de agregados y volúmenes. Como no hay recursos compartidos del sistema de archivos, no se necesitan volúmenes. Todo el almacenamiento conectado a un par de alta disponibilidad se trata como una zona de disponibilidad de almacenamiento común (SAZ) dentro de la que los LUN y los espacios de nombres de NVMe se aprovisionan como «unidades de almacenamiento» (SUS). Los últimos sistemas ASA han sido diseñados para ser fáciles de gestionar, gracias a una experiencia familiar para los administradores de almacenamiento SAN. Esta nueva arquitectura es ideal para entornos de vSphere, ya que permite una gestión sencilla de los recursos de almacenamiento y ofrece una experiencia simplificada para los administradores de almacenamiento SAN. La arquitectura de ASA también es compatible con la tecnología NVMe over Fabrics (NVMe-oF) más reciente, que proporciona un rendimiento y una escalabilidad aún mayores para las cargas de trabajo de vSphere.
- **Tecnología Snapshot.** ONTAP fue el primero en ofrecer tecnología Snapshot para la protección de datos y sigue siendo la más avanzada en el sector. Este método de protección de datos con un uso eficiente del espacio se ha ampliado para dar soporte a las API de VMware vSphere para la integración de cabinas (VAAI). Esta integración le permite aprovechar las capacidades Snapshot de ONTAP en las operaciones de backup y restauración, y reducir el impacto en su entorno de producción. Este método también permite utilizar copias Snapshot para una rápida recuperación de equipos virtuales, lo que reduce el tiempo y el esfuerzo necesarios para restaurar datos. Además, la tecnología Snapshot de ONTAP se integra con las soluciones Live Site Recovery (VLSR, anteriormente Site Recovery Manager [SRM]) de VMware, por lo que proporciona una estrategia de protección de datos completa para su entorno virtualizado.
- **Volúmenes virtuales y gestión de almacenamiento basada en políticas.** NetApp fue uno de los primeros socios de diseño de VMware en el desarrollo de vSphere Virtual Volumes (vVols), aportando información arquitectónica y soporte temprano para vVols y VMware vSphere API for Storage Awareness (VASA). Este enfoque no solo aportó una gestión granular del almacenamiento de máquinas virtuales a VMFS, sino que también respaldó la automatización del aprovisionamiento de almacenamiento a través de una gestión de almacenamiento basada en políticas. Este enfoque permite a los arquitectos de almacenamiento diseñar grupos de almacenamiento con diferentes capacidades que los administradores de máquinas virtuales pueden utilizar fácilmente. ONTAP lidera la industria del almacenamiento en escala vVol, y admite cientos de miles de vVols en un solo clúster, mientras que los proveedores de matrices empresariales y matrices flash más pequeñas admiten tan solo varios miles de vVols por matriz. NetApp también está impulsando la evolución de la gestión granular de máquinas virtuales con sus próximas

capacidades.

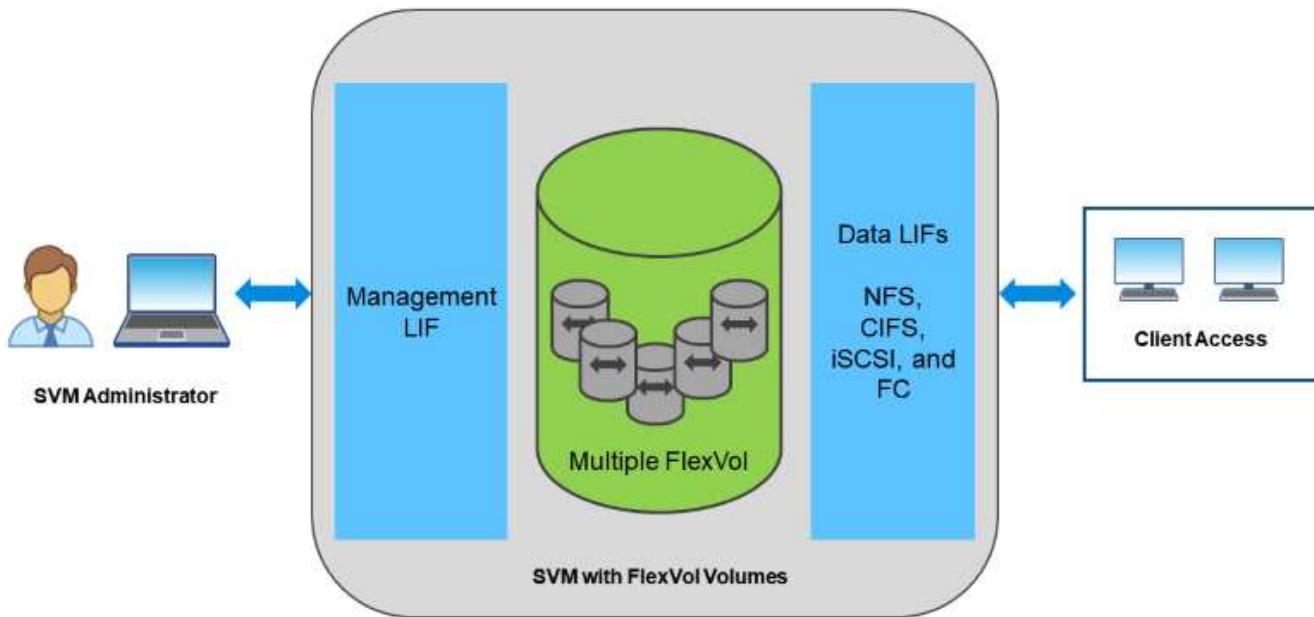
- **Eficiencia de almacenamiento.** Si bien NetApp fue el primero en ofrecer deduplicación para cargas de trabajo de producción, esta innovación no fue la primera ni la última en esta área. Todo comenzó con instantáneas, un mecanismo de protección de datos que ahorra espacio y no afecta el rendimiento, junto con la tecnología FlexClone para hacer instantáneamente copias de lectura y escritura de máquinas virtuales para uso en producción y respaldo. NetApp continuó ofreciendo capacidades en línea, incluidas deduplicación, compresión y deduplicación de bloque cero, para aprovechar al máximo el almacenamiento de los costosos SSD. ONTAP también agregó la capacidad de empaquetar operaciones de E/S y archivos más pequeños en un bloque de disco usando compactación. La combinación de estas capacidades ha permitido que los clientes experimenten comúnmente ahorros de hasta 5:1 para VSI y hasta 30:1 para VDI. La última generación de sistemas ONTAP también incluye compresión y deduplicación aceleradas por hardware, lo que puede mejorar aún más la eficiencia del almacenamiento y reducir los costos. Este enfoque permite almacenar más datos en menos espacio, lo que reduce el costo general de almacenamiento y mejora el rendimiento. NetApp confía tanto en sus capacidades de eficiencia de almacenamiento que ofrece un enlace: <https://www.netapp.com/pdf.html?item=/media/79014-ng-937-Efficiency-Guarantee-Customer-Flyer.pdf> [Garantía de eficiencia<sup>4</sup>].
- **Multitenencia.** ONTAP ha sido durante mucho tiempo líder en multitenencia, lo que le permite crear múltiples máquinas virtuales de almacenamiento (SVM) en un solo clúster. Este enfoque le permite aislar cargas de trabajo y brindar diferentes niveles de servicio a diferentes inquilinos, lo que lo hace ideal para proveedores de servicios y grandes empresas. La última generación de sistemas ONTAP también incluye soporte para la gestión de la capacidad de los inquilinos. Esta función le permite establecer límites de capacidad para cada inquilino, garantizando que ningún inquilino pueda consumir todos los recursos disponibles. Este enfoque ayuda a garantizar que todos los inquilinos reciban el nivel de servicio que esperan, al tiempo que proporciona un alto nivel de seguridad y aislamiento entre ellos. Además, las capacidades multitenencia de ONTAP están integradas con la plataforma vSphere de VMware, lo que le permite administrar y monitorear fácilmente su entorno virtualizado a través de "[Herramientas de ONTAP para VMware vSphere](#)" y "[Información sobre la infraestructura de datos](#)" .
- **Nube híbrida.** Ya sea que se utilicen para una nube privada local, una infraestructura de nube pública o una nube híbrida que combina lo mejor de ambas, las soluciones ONTAP lo ayudan a construir su estructura de datos para agilizar y optimizar la administración de datos. Comience con sistemas all-flash de alto rendimiento y luego combínelos con sistemas de almacenamiento en disco o en la nube para la protección de datos y la computación en la nube. Elija entre Azure, AWS, IBM o Google Cloud para optimizar costos y evitar la dependencia. Aproveche el soporte avanzado para OpenStack y tecnologías de contenedores según sea necesario. NetApp también ofrece copias de seguridad basadas en la nube (SnapMirror Cloud, Cloud Backup Service y Cloud Sync) y herramientas de archivado y niveles de almacenamiento (FabricPool) para ONTAP para ayudar a reducir los gastos operativos y aprovechar el amplio alcance de la nube.
- **Y mucho más.** saque partido del rendimiento extremo de las cabinas AFF A-Series de NetApp para acelerar su infraestructura virtualizada a la vez que gestiona los costes. Disfrute de operaciones no disruptivas, desde el mantenimiento hasta las actualizaciones, pasando por la sustitución completa de su sistema de almacenamiento, mediante clústeres ONTAP de escalado horizontal. Proteja los datos en reposo con funcionalidades de cifrado de NetApp sin coste adicional. Asegúrese de que el rendimiento cumple los niveles de servicio empresarial a través de funcionalidades de calidad de servicio de gran precisión. Todos ellos forman parte de la amplia gama de funcionalidades que incluyen ONTAP, el software para la gestión de datos empresariales líder del sector.

## Almacenamiento unificado

ONTAP unifica el almacenamiento mediante un enfoque simplificado definido por software para una gestión segura y eficiente, un rendimiento mejorado y una escalabilidad fluida. Este enfoque mejora la protección de datos y permite usar eficazmente los recursos cloud.

En un principio, este método unificado hacía referencia a la compatibilidad de los protocolos NAS y SAN en un solo sistema de almacenamiento, y ONTAP sigue siendo una plataforma líder para SAN junto con su solidez original en NAS. ONTAP ahora también ofrece compatibilidad con el protocolo de objetos S3. Aunque S3 no se utiliza para almacenes de datos, puede usarlo para aplicaciones «in-guest». Puede obtener más información sobre la compatibilidad con el protocolo S3 en ONTAP en el ["Información general de la configuración de S3"](#). El término almacenamiento unificado ha evolucionado para suponer un método unificado de la gestión del almacenamiento que incluye la capacidad de gestionar todos tus recursos de almacenamiento desde una única interfaz. Esto incluye la capacidad de gestionar recursos de almacenamiento en cloud y en las instalaciones, los sistemas de cabinas All SAN (ASA) más recientes y la capacidad de gestionar varios sistemas de almacenamiento desde una única interfaz.

Una máquina virtual de almacenamiento (SVM) es la unidad de multi-tenancy seguro en ONTAP. Es una construcción lógica que permite al cliente acceder a los sistemas que ejecutan ONTAP. Las SVM pueden servir datos de forma simultánea mediante varios protocolos de acceso a los datos a través de interfaces lógicas (LIF). Los SVM proporcionan acceso a los datos de nivel de archivo mediante protocolos NAS, como CIFS y NFS, y acceso a datos de nivel de bloque mediante protocolos SAN, como iSCSI, FC/FCoE y NVMe. Los SVM pueden servir datos a clientes SAN y NAS de forma independiente a la vez, así como con S3.



En el mundo de vSphere, este enfoque también podría significar un sistema unificado para una infraestructura de puestos de trabajo virtuales (VDI) junto con una infraestructura de servidores virtuales (VSI). Los sistemas que ejecutan ONTAP suelen ser más económicos para VSI que las cabinas empresariales tradicionales y, al mismo tiempo, cuentan con funcionalidades de eficiencia del almacenamiento avanzadas para gestionar VDI en el mismo sistema. ONTAP también unifica varios medios de almacenamiento, desde SSD a SATA, y puede ampliarlos fácilmente al cloud. No es necesario comprar una cabina flash para el rendimiento, una cabina SATA para archivos y sistemas independientes para la nube. ONTAP los une a todos.

**NOTA:** Para obtener más información sobre SVM, almacenamiento unificado y acceso de clientes, consulte ["Virtualización del almacenamiento"](#) En el centro de documentación de ONTAP 9.

## Herramientas de virtualización para ONTAP

NetApp proporciona varias herramientas de software independientes compatibles con sistemas ONTAP y ASA tradicionales, integrando vSphere para administrar de forma eficaz su entorno virtualizado.

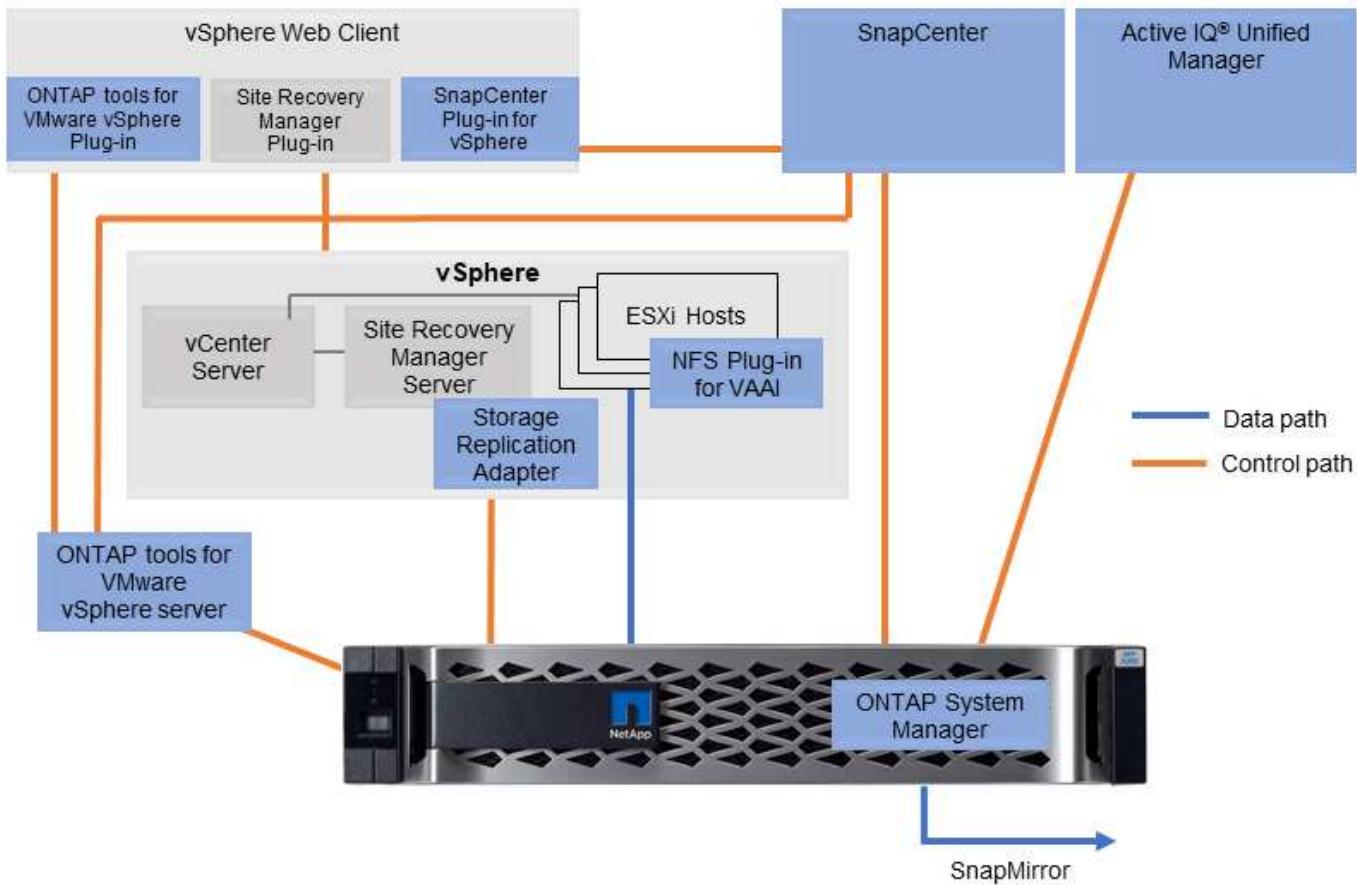
Las siguientes herramientas están incluidas con la licencia ONTAP One sin coste adicional. Consulte la figura 1 para obtener una descripción de cómo funcionan estas herramientas juntas en su entorno vSphere.

### Herramientas de ONTAP para VMware vSphere

["Herramientas de ONTAP para VMware vSphere"](#) Es un conjunto de herramientas para usar el almacenamiento de ONTAP junto con vSphere. El complemento de vCenter, anteriormente conocido como Virtual Storage Console (VSC), simplifica las funciones de gestión y eficiencia del almacenamiento, mejora la disponibilidad y reduce los costes de almacenamiento y la sobrecarga operativa, tanto si usa 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 obtener todos estos beneficios, NetApp recomienda el uso de estas herramientas de ONTAP como mejor práctica al utilizar vSphere con sistemas que ejecuten ONTAP. Incluye un dispositivo de servidor, extensiones de interfaz de usuario para vCenter, VASA Provider y Storage Replication Adapter. Casi todo lo que incluye las herramientas de ONTAP se puede automatizar mediante API de REST sencillas, consumibles gracias a las herramientas de automatización más modernas.

- **Extensiones de la interfaz de usuario de vCenter.** Las extensiones de interfaz de usuario de las herramientas de ONTAP simplifican el trabajo de los equipos de operaciones y los administradores de vCenter al integrar menús contextuales fáciles de usar para gestionar hosts y almacenamiento, portlets informativos y funcionalidades de alertas nativas directamente en la interfaz de usuario de vCenter para flujos de trabajo optimizados.
- **Proveedor VASA para ONTAP.** el Proveedor VASA para ONTAP es compatible con el marco de trabajo VMware vStorage APIs for Storage Awareness (VASA). Se suministra como parte de las herramientas de ONTAP para VMware vSphere como un dispositivo virtual único para facilitar la puesta en marcha. EL proveedor DE VASA conecta vCenter Server con ONTAP para ayudar en el aprovisionamiento y la supervisión del almacenamiento de máquinas virtuales. Permite el soporte de VMware Virtual Volumes (vVols), la gestión de los perfiles de las funcionalidades del almacenamiento y el rendimiento vVols individual, y las alarmas para supervisar la capacidad y el cumplimiento de los perfiles.
- **Adaptador de replicación de almacenamiento.** SRA se utiliza junto con VMware Live Site Recovery (VLSR)/Site Recovery Manager (SRM) para administrar la replicación de datos entre sitios de producción y recuperación ante desastres mediante SnapMirror para la replicación basada en matrices. Puede automatizar la tarea de conmutación por error en caso de desastre y puede ayudar a probar las réplicas de DR de forma no disruptiva para garantizar la confianza en su solución de DR.

La figura siguiente muestra las herramientas de ONTAP para vSphere.



### Complemento de SnapCenter para VMware vSphere

El ["Complemento de SnapCenter para VMware vSphere"](#) es un complemento para vCenter Server que le permite administrar copias de seguridad y restauraciones de máquinas virtuales (VM) y almacenes de datos. Proporciona una interfaz única para administrar copias de seguridad, restauraciones y clones de máquinas virtuales y almacenes de datos en múltiples sistemas ONTAP. SnapCenter admite la replicación y recuperación desde sitios secundarios mediante SnapMirror. Las últimas versiones también admiten SnapMirror en la nube (S3), instantáneas a prueba de manipulaciones, SnapLock y sincronización activa de SnapMirror. El complemento SnapCenter para VMware vSphere se puede integrar con los complementos de aplicaciones SnapCenter para proporcionar copias de seguridad consistentes con las aplicaciones.

### Plugin NFS para VAAI de VMware

El ["Plugin NFS de NetApp para VAAI de VMware"](#) es un plugin para hosts ESXi que permite utilizar funciones VAAI con almacenes de datos NFS en ONTAP. Es compatible con copias de descarga para operaciones de clonado, reserva de espacio para archivos de disco virtual gruesos y descarga de copias Snapshot. La descarga de operaciones de copia en el almacenamiento no es necesariamente más rápida de completarse, pero reduce los requisitos de ancho de banda de red y libera a recursos del host, como ciclos de CPU, búferes y colas. Puede usar las herramientas de ONTAP para VMware vSphere para instalar el plugin en hosts ESXi o, si es compatible, vSphere Lifecycle Manager (VLCM).

### Opciones de software premium

Los siguientes productos de software premium están disponibles en NetApp. No están incluidos con la licencia de ONTAP One y deben comprarse por separado.

- ["NetApp Disaster Recovery"](#) para VMware vSphere. Este es un servicio basado en la nube que proporciona

recuperación ante desastres y respaldo para entornos VMware. Se puede utilizar con o sin SnapCenter y admite recuperación ante desastres de local a local mediante SAN o NAS, y de local a/desde la nube mediante NFS, donde sea compatible.

- **"Información sobre la infraestructura de datos (DII)".** Este es un servicio basado en la nube que proporciona monitoreo y análisis para entornos VMware. Admite otros proveedores de almacenamiento en entornos de almacenamiento heterogéneos, así como múltiples proveedores de conmutadores y otros hipervisores. DII proporciona información completa de extremo a extremo sobre el rendimiento, la capacidad y el estado de su entorno VMware.

## **Volúmenes virtuales (vVols) y gestión basada en políticas de almacenamiento (SPBM)**

Anunciada por primera vez en 2012, NetApp fue un partner de diseño temprano con VMware en el desarrollo de VMware vSphere APIs for Storage Awareness (VASA), la base de la gestión basada en políticas de almacenamiento (SPBM) con cabinas de almacenamiento empresarial. Este enfoque trajo una gestión granular del almacenamiento de las máquinas virtuales limitada al almacenamiento de VMFS y NFS.

Como partner de diseño tecnológico, NetApp proporcionó información sobre la arquitectura y en 2015 anunció la compatibilidad con vVols. Esta nueva tecnología ahora permitió la automatización del aprovisionamiento de almacenamiento granular de equipos virtuales y realmente nativo de la cabina a través de SPBM.

### **Volúmenes virtuales (vVols)**

Los vVols son una revolucionaria arquitectura de almacenamiento que permite gestionar el almacenamiento de forma granular de las máquinas virtuales y no solo por equipo virtual (incluidos los metadatos de las máquinas virtuales), sino incluso por VMDK. Los vVols son un componente clave de la estrategia de centro de datos definido por software (SDDC) que forma la base de VMware Cloud Foundation (VCF), lo que proporciona una arquitectura de almacenamiento más eficiente y escalable para entornos virtualizados.

VVols permite que las máquinas virtuales consuman almacenamiento por equipo virtual, ya que cada objeto de almacenamiento de equipo virtual es una entidad única en NetApp ONTAP. En los sistemas ASA R2 que ya no requieren gestión de volúmenes, esto significa que cada objeto de almacenamiento de VM es una única unidad de almacenamiento (SU) en la matriz que se puede controlar de forma independiente. De este modo, se pueden crear normativas de almacenamiento que se pueden aplicar a VMDK o máquinas virtuales individuales (y, por lo tanto, SUS individual), lo que proporciona un control granular sobre los servicios de almacenamiento como el rendimiento, la disponibilidad y la protección de datos.

### **Gestión basada en la política de almacenamiento (SPBM)**

La SPBM proporciona un marco que funciona como capa de abstracción entre los servicios de almacenamiento disponibles para su entorno de virtualización y los elementos de almacenamiento aprovisionados mediante políticas. Este método permite a los arquitectos de almacenamiento diseñar pools de almacenamiento con diferentes funcionalidades. Los administradores de equipos virtuales pueden consumir fácilmente estos pools. De este modo, los administradores pueden ajustar los requisitos de las cargas de trabajo de las máquinas virtuales con los pools de almacenamiento aprovisionados. Este enfoque simplifica la gestión del almacenamiento y permite usar los recursos de almacenamiento de forma más eficiente.

El SPBM es un componente clave de vVols, que ofrece un marco basado en normativas para gestionar los servicios de almacenamiento. Los administradores de vSphere crean políticas usando reglas y funcionalidades expuestas por el proveedor de VASA (VP) del proveedor. Es posible crear políticas para diferentes servicios de almacenamiento, tales como rendimiento, disponibilidad y protección de datos. Las políticas se pueden asignar a máquinas virtuales o VMDK individuales, lo que proporciona control granular

sobre los servicios de almacenamiento.

## NetApp ONTAP y vVols

NetApp ONTAP lidera la industria del almacenamiento en vVols Scale, que admite cientos de miles de vVols en un único clúster\*. Por el contrario, las cabinas empresariales y los proveedores de cabinas Flash más pequeños admiten hasta varios miles de vVols por cabina. ONTAP proporciona una solución de almacenamiento escalable y eficiente para entornos VMware vSphere que admite vVols con un amplio conjunto de servicios de almacenamiento, que incluye deduplicación de datos, compresión, thin provisioning y protección de datos. SPBM permite una integración perfecta con entornos VMware vSphere.

Anteriormente ya hemos mencionado que los administradores de equipos virtuales pueden consumir capacidad como pools de almacenamiento. Esto se realiza mediante el uso de contenedores de almacenamiento que se representan en vSphere como almacenes de datos lógicos.

Los contenedores de almacenamiento los crean los administradores de almacenamiento y se utilizan para agrupar los recursos de almacenamiento que pueden consumir los administradores de las máquinas virtuales. Los contenedores de almacenamiento se pueden crear de forma diferente en función del tipo de sistema ONTAP que use. Con los clústeres tradicionales de ONTAP 9, se asignan a los contenedores uno o varios volúmenes FlexVol de respaldo que, juntos, forman el pool de almacenamiento. Con los sistemas R2 de ASA, el clúster entero es el pool de almacenamiento.



Para obtener más información sobre VMware vSphere Virtual Volumes, SPBM y ONTAP, consulte "[TR-4400: VMware vSphere Virtual Volumes con ONTAP](#)".

\*Dependiendo de la plataforma y el protocolo

## Almacenes de datos y protocolos

### Información general sobre las funciones de protocolo y almacenes de datos de vSphere

Se utilizan seis protocolos para conectar VMware vSphere a almacenes de datos en un sistema que ejecuta ONTAP:

- FCP
- NVMe/FC
- NVMe/TCP
- iSCSI
- NFS v3
- NFS v4,1

FCP, NVMe/FC, NVMe/TCP e iSCSI son protocolos de bloque que utilizan el sistema de archivos de máquina virtual de vSphere (VMFS) para almacenar máquinas virtuales dentro de LUN de ONTAP o espacios de nombres de NVMe que se encuentran en un ONTAP FlexVol volume. NFS es un protocolo de archivos que coloca equipos virtuales en almacenes de datos (que son simplemente volúmenes de ONTAP) sin necesidad de VMFS. SMB (CIFS), iSCSI, NVMe/TCP o NFS también se puede utilizar directamente de un sistema operativo invitado a ONTAP.

Las siguientes tablas presentan funciones de almacén de datos tradicionales compatibles con vSphere con ONTAP. Esta información no se aplica a almacenes de datos vVols, pero, generalmente, se aplica a vSphere 6.x y versiones posteriores mediante versiones ONTAP compatibles. También se puede consultar el

"Herramienta VMware Configuration Maximums" para conocer versiones de vSphere específicas para confirmar límites específicos.

| Característica/función                                   | FC   | ISCSI                 | NVMe-of                  | NFS   |
|--|--|-----------------------|--------------------------|---|
| Formato  | Asignación de dispositivo sin formato (RDM) o VMFS | VMFS o RDM            | VMFS                     | n.a.  |
| Número máximo de almacenes de datos o LUN                | 1024 LUN por host                                  | 1024 LUN por servidor | 256 nombres por servidor | 256 conexiones NFS por host (afectadas por nconnect y trunking de sesiones) NFS predeterminado. MaxVolumes tiene 8 años. Utilice las herramientas de ONTAP para VMware vSphere para aumentar a 256. |
| Tamaño máximo de almacén de datos                        | 64 TB  | 64 TB                 | 64 TB                    | 300 TB de volumen FlexVol o superior con volumen FlexGroup  |
| Tamaño máximo de archivo del almacén de datos            | 62 TB  | 62 TB                 | 62 TB                    | 62TB con ONTAP 9.12.1P2 y posterior   |
| Profundidad de cola óptima por LUN o sistema de archivos | 64-256   | 64-256                | Autonegociar             | Consulte NFS.MaxQueueDepth en <a href="#">"Host ESXi recomendado y otra configuración de ONTAP"</a> .   |

En la siguiente tabla se enumeran las funcionalidades relacionadas con el almacenamiento de VMware admitidas.

| Capacidad/función  | FC | ISCSI | NVMe-of | NFS |
|--|----|-------|---------|-----|
| VMotion  | Sí | Sí    | Sí      | Sí  |
| VMotion de almacenamiento                                      | Sí | Sí    | Sí      | Sí  |
| Ha de VMware   | Sí | Sí    | Sí      | Sí  |
| Planificador de recursos distribuidos de almacenamiento (SDRS) | Sí | Sí    | Sí      | Sí  |

| Capacidad/función  | FC | ISCSI           | NVMe-of         | NFS   |
|--|----|-----------------|-----------------|---|
| Software de backup habilitado para VMware vStorage APIs for Data Protection (VADP)             | Sí | Sí              | Sí              | Sí  |
| Microsoft Cluster Service (MSCS) o clustering de recuperación tras fallos en un equipo virtual | Sí | Sí <sup>1</sup> | Sí <sup>1</sup> | No admitido   |
| Tolerancia a fallos  | Sí | Sí              | Sí              | Sí  |
| Recuperación de sitios activos/Gestor de recuperación de sitios                                | Sí | Sí              | No <sup>2</sup> | v3 Solo <sup>2</sup>  |
| Equipos virtuales con thin provisioning (discos virtuales)                                     | Sí | Sí              | Sí              | Sí<br>Esta configuración es la predeterminada para todas las máquinas virtuales de NFS cuando no se utiliza VAAI. |
| Accesos múltiples nativos de VMware  | Sí | Sí              | Sí              | La conexión de enlaces de sesión NFS v4.1 requiere ONTAP 9.14.1 y posterior                                       |

En la siguiente tabla se enumeran las funciones de gestión de almacenamiento de ONTAP admitidas.

| Característica/función   | FC                     | ISCSI                  | NVMe-of             | NFS  |
|--|------------------------|------------------------|---------------------|--|
| Deduplicación de datos   | Ahorro en la cabina    | Ahorro en la cabina    | Ahorro en la cabina | De ahorro en el almacén de datos           |
| Aprovisionamiento ligero   | Almacén de datos o RDM | Almacén de datos o RDM | Almacén de datos    | Almacén de datos                           |
| Redimensión de almacén de datos  | Crezca solo            | Crezca solo            | Crezca solo         | Crecer, crecimiento automático y reducción |
| Complementos de SnapCenter para aplicaciones Windows y Linux (en invitado) | Sí                     | Sí                     | Sí                  | Sí   |

| Característica/función  | FC | iSCSI | NVMe-of | NFS |
|---|----|-------|---------|-----|
| Supervisión y configuración del host mediante herramientas de ONTAP para VMware vSphere | Sí | Sí    | Sí      | Sí  |
| Aprovisionar mediante las herramientas de ONTAP para VMware vSphere                     | Sí | Sí    | Sí      | Sí  |

En la siguiente tabla se enumeran las funciones de backup admitidas.

| Característica/función                | FC  | iSCSI   | NVMe-of   | NFS   |
|---------------------------------------|---|---|---|---|
| Snapshots de ONTAP                    | Sí  | Sí  | Sí  | Sí  |
| SRM compatible con backups replicados | Sí  | Sí  | No <sup>2</sup>   | v3 Solo <sup>2</sup>  |
| SnapMirror para volúmenes             | Sí  | Sí  | Sí  | Sí  |
| Acceso a imagen VMDK                  | Software de backup habilitado para SnapCenter y VADP                    | Software de backup habilitado para SnapCenter y VADP                    | Software de backup habilitado para SnapCenter y VADP                    | El software de backup habilitado para SnapCenter y VADP, vSphere Client y el explorador de almacén de datos de vSphere Web Client |
| Acceso de nivel de ficheros VMDK      | Software de backup habilitado para SnapCenter y VADP, solamente Windows | Software de backup habilitado para SnapCenter y VADP, solamente Windows | Software de backup habilitado para SnapCenter y VADP, solamente Windows | Software de backup y aplicaciones de terceros habilitados para SnapCenter y VADP  |
| Granularidad de NDMP                  | Almacén de datos  | Almacén de datos  | Almacén de datos  | Almacén de datos o máquina virtual  |

<sup>1</sup> **NetApp recomienda** usar iSCSI en invitado para clústeres de Microsoft en lugar de VMDK con capacidad para múltiples escritores en un almacén de datos VMFS. Este enfoque es totalmente compatible con Microsoft y VMware, ofrece una gran flexibilidad con ONTAP (SnapMirror para sistemas ONTAP en las instalaciones o en el cloud), es fácil de configurar y automatizar y se puede proteger con SnapCenter. VSphere 7 añade una nueva opción de VMDK en clúster. Es diferente de los VMDK habilitados para el multiescritor, que requieren un almacén de datos VMFS 6 que tenga habilitada la compatibilidad con VMDK en clúster. Se aplican otras restricciones. Consulte la documentación de VMware "Configuración de clústeres de comutación por error de Windows Server" para conocer las directrices de configuración.

<sup>2</sup> Los almacenes de datos que utilizan NVMe-oF y NFS v4.1 requieren replicación de vSphere. Actualmente, SRM no admite la replicación basada en cabinas para NFS v4.1. Actualmente, las herramientas de ONTAP para vSphere Storage Replication Adapter (SRA) de VMware no admiten la replicación basada en cabinas con NVMe-oF.

### Seleccionar un protocolo de almacenamiento

Los sistemas que se ejecutan en ONTAP son compatibles con los principales protocolos de almacenamiento, de modo que los clientes pueden elegir el que mejor se adapte a su entorno, en función de la infraestructura de red existente y las aptitudes previstas para el personal. Históricamente, las pruebas de NetApp generalmente han mostrado poca diferencia entre los protocolos que se ejecutan a velocidades de línea similares y el número de conexiones. Sin embargo, NVMe-oF (NVMe/TCP y NVMe/FC) muestra aumentos notables en IOPS, reducción de la latencia y hasta un 50 % o más de reducción en el consumo de CPU del host según la I/O de almacenamiento. En el otro extremo, NFS ofrece la mayor flexibilidad y facilidad de gestión, especialmente para un gran número de máquinas virtuales. Todos estos protocolos pueden usarse y gestionarse con las herramientas de ONTAP para VMware vSphere, lo que ofrece una interfaz sencilla para crear y gestionar almacenes de datos.

Los siguientes factores pueden ser útiles a la hora de considerar una opción de protocolo:

- **Entorno operativo actual.** Aunque los EQUIPOS DE TI suelen especializarse en la gestión de la infraestructura IP de Ethernet, no todos tienen experiencia a la hora de gestionar una estructura SAN FC. Sin embargo, es posible que el uso de una red IP de uso general que no está diseñada para el tráfico de almacenamiento no funcione bien. Considere la infraestructura de red de que dispone, las mejoras planificadas y las capacidades y la disponibilidad del personal para gestionarlos.
- **Facilidad de configuración.** más allá de la configuración inicial de la estructura FC (comutadores y cableado adicionales, zonificación y verificación de interoperabilidad de HBA y firmware), los protocolos de bloque también requieren la creación y asignación de LUN y descubrimiento y formato por parte del SO invitado. Una vez creados y exportados los volúmenes de NFS, el host ESXi los monta y está listo para usarse. NFS no tiene ninguna cualificación de hardware o firmware especial que gestionar.
- **Facilidad de gestión.** Con los protocolos SAN, si se necesita más espacio, son necesarios varios pasos: Ampliar una LUN, volver a analizar para descubrir el nuevo tamaño y, posteriormente, aumentar el sistema de archivos). Aunque sea posible aumentar una LUN, reducir el tamaño de una LUN no lo es. NFS permite ajustar fácilmente el tamaño, y el sistema de almacenamiento puede automatizar este ajuste de tamaño. SAN ofrece recuperación de espacio mediante comandos de DESASIGNAR/TRIM/UNMAP del sistema operativo invitado, para que se pueda devolver espacio de los archivos eliminados a la cabina. Este tipo de recuperación de espacio no es difícil con los almacenes de datos NFS.
- **Transparencia del espacio de almacenamiento.** la utilización del almacenamiento suele ser más fácil de ver en entornos NFS, ya que Thin Provisioning devuelve ahorros inmediatamente. Del mismo modo, los ahorros en deduplicación y clonado están disponibles inmediatamente para otras máquinas virtuales en el mismo almacén de datos o para otros volúmenes del sistema de almacenamiento. La densidad de las máquinas virtuales también es superior en un almacén de datos NFS, que puede mejorar el ahorro de la deduplicación y reducir los costes de gestión al tener menos almacenes de datos que gestionar.

### Distribución de almacenes de datos

Los sistemas de almacenamiento ONTAP ofrecen una gran flexibilidad a la hora de crear almacenes de datos para equipos virtuales y discos virtuales. Aunque muchas prácticas recomendadas de ONTAP se aplican al usar las herramientas de ONTAP para aprovisionar almacenes de datos para vSphere (se muestran en la sección "["Host ESXi recomendado y otra configuración de ONTAP"](#)"), estas son algunas directrices adicionales a tener en cuenta:

- La puesta en marcha de vSphere con almacenes de datos NFS de ONTAP da como resultado una implementación de alto rendimiento y fácil de gestionar que proporciona ratios de máquina virtual a

almacén de datos que no pueden obtenerse con protocolos de almacenamiento basados en bloques. Esta arquitectura puede provocar un aumento diez veces en la densidad de los almacenes de datos con una reducción correlacionada en el número de almacenes de datos. Aunque un almacén de datos de mayor tamaño puede beneficiar a la eficiencia del almacenamiento y proporcionar ventajas operativas, considere la posibilidad de utilizar al menos cuatro almacenes de datos (volúmenes FlexVol) por nodo para almacenar sus máquinas virtuales en una sola controladora ONTAP para obtener el máximo rendimiento de los recursos de hardware. Este enfoque también permite establecer almacenes de datos con diferentes políticas de recuperación. Algunas se pueden hacer backups o replicarse con una frecuencia mayor que otras en función de las necesidades de las empresas. No se necesitan varios almacenes de datos en los volúmenes de FlexGroup para mejorar el rendimiento, ya que se escalan por diseño.

- **NetApp recomienda** el uso de volúmenes FlexVol para la mayoría de los almacenes de datos NFS. A partir de la versión ONTAP 9,8, se admiten los volúmenes FlexGroup también para su uso como almacenes de datos y, por lo general, se recomienda en determinados casos de uso. No se recomiendan normalmente otros contenedores de almacenamiento de ONTAP, como qtrees, porque actualmente no son compatibles con las herramientas de ONTAP para VMware vSphere o con el complemento de NetApp SnapCenter para VMware vSphere.
- Un buen tamaño para un almacén de datos con volúmenes FlexVol es de entre 4 y 8 TB. Este tamaño es un buen punto de equilibrio entre rendimiento, facilidad de gestión y protección de datos. Empiece con poco (digamos, 4 TB) y crezca el almacén de datos según sea necesario (hasta el máximo de 300 TB). Los almacenes de datos más pequeños son más rápidos de recuperar desde un backup o después de un desastre y se pueden mover rápidamente en el clúster. Considere la posibilidad de utilizar el ajuste de tamaño automático de ONTAP para aumentar y reducir automáticamente el volumen a medida que se modifique el espacio utilizado. De forma predeterminada, las herramientas de ONTAP para el asistente de aprovisionamiento de almacenes de datos de VMware vSphere utilizan el tamaño automático para nuevos almacenes de datos. System Manager o la línea de comandos pueden personalizarse los umbrales de crecimiento y reducción, y el tamaño máximo y mínimo.
- Como alternativa, los almacenes de datos VMFS se pueden configurar con espacios de nombres NVMe o LUN (denominados unidades de almacenamiento en nuevos sistemas ASA) a los que se accede mediante FC, iSCSI, NVMe/FC o NVMe/TCP. VMFS permite a los almacenes de datos acceder de forma simultánea a cada servidor ESX de un clúster. Los almacenes de datos VMFS pueden tener un tamaño de hasta 64 TB y constan de hasta 32 LUN de 2 TB (VMFS 3) o una única LUN de 64 TB (VMFS 5). El tamaño máximo de LUN de ONTAP es de 128TB TB en los sistemas AFF, ASA y FAS. NetApp siempre recomienda utilizar un único LUN grande para cada almacén de datos en vez de intentar utilizar extensiones. Al igual que sucede con NFS, considere la posibilidad de utilizar varios almacenes de datos (volúmenes o unidades de almacenamiento) para maximizar el rendimiento en una única controladora de ONTAP.
- Los sistemas operativos invitados (SO) antiguos necesitaban alineación con el sistema de almacenamiento para obtener el mejor rendimiento y eficiencia del almacenamiento. Sin embargo, los sistemas operativos modernos admitidos por el proveedor de distribuidores de Microsoft y Linux como Red Hat ya no requieren ajustes para alinear la partición del sistema de archivos con los bloques del sistema de almacenamiento subyacente en un entorno virtual. Si utiliza un antiguo sistema operativo que pueda requerir la alineación, busque en la base de conocimientos de soporte de NetApp los artículos mediante «alineación de VM» o solicite una copia de TR-3747 a partir de un contacto de ventas o partner de NetApp.
- Evite el uso de utilidades de desfragmentación en el sistema operativo invitado, ya que no ofrece beneficios de rendimiento y afecta a la eficiencia del almacenamiento y al uso del espacio de instantáneas. Considere también desactivar la indización de búsquedas en el sistema operativo invitado para escritorios virtuales.
- ONTAP ha dirigido el sector mediante funciones innovadoras de eficiencia del almacenamiento, que le permiten sacar el máximo partido a su espacio en disco utilizable. Los sistemas AFF llevan esta eficiencia aún más allá gracias a la compresión y la deduplicación inline predeterminadas. Los datos se deduplican en todos los volúmenes de un agregado, por lo que ya no necesita agrupar sistemas operativos similares y aplicaciones similares en un único almacén de datos para optimizar el ahorro.

- En algunos casos, es posible que ni siquiera se necesite un almacén de datos. Piense en sistemas de archivos propiedad del invitado como NFS, SMB, NVMe/TCP o iSCSI gestionados por el invitado. Para obtener orientación específica sobre las aplicaciones, consulte los informes técnicos de NetApp para su aplicación. Por ejemplo, ["Bases de datos de Oracle en ONTAP"](#) tiene una sección sobre la virtualización con detalles útiles.
- Los discos de primera clase (o discos virtuales mejorados) permiten discos gestionados por vCenter independientemente de una máquina virtual con vSphere 6.5 y versiones posteriores. Aunque son gestionados principalmente por la API, pueden ser útiles con vVols, sobre todo cuando las herramientas de OpenStack o Kubernetes las gestionan. Son compatibles tanto con ONTAP como con herramientas de ONTAP para VMware vSphere.

### **Migración de almacenes de datos y máquinas virtuales**

Al migrar las máquinas virtuales desde un almacén de datos existente en otro sistema de almacenamiento a ONTAP, estas son algunas prácticas que deben tenerse en cuenta:

- Use Storage vMotion para mover la mayoría de los equipos virtuales a ONTAP. Este método no solo no es disruptivo para la ejecución de equipos virtuales, sino que también permite funciones de eficiencia del almacenamiento de ONTAP como deduplicación y compresión inline para procesar los datos a medida que migran. Considere usar funcionalidades de vCenter para seleccionar varias máquinas virtuales de la lista de inventario y programar la migración (utilice la tecla Ctrl mientras hace clic en acciones) en un momento adecuado.
- Aunque podría planificar con cuidado la migración a los almacenes de datos de destino adecuados, a menudo es más sencillo migrar de forma masiva y luego organizarse más tarde, según sea necesario. Puede que desee utilizar este enfoque para guiar la migración a diferentes almacenes de datos si tiene necesidades específicas de protección de datos, como distintas programaciones de Snapshot. Asimismo, una vez que los equipos virtuales se encuentran en el clúster de NetApp, Storage vMotion puede utilizar descargas de VAAI para mover equipos virtuales entre los almacenes de datos del clúster sin necesidad de realizar una copia basada en host. Tenga en cuenta que NFS no descarga vMotion de almacenamiento de equipos virtuales encendidos, pero VMFS sí lo hace.
- Los equipos virtuales que necesitan una migración más cuidadosa incluyen las bases de datos y las aplicaciones que utilizan almacenamiento conectado. En general, considere el uso de las herramientas de la aplicación para gestionar la migración. Para Oracle, considere la posibilidad de utilizar herramientas de Oracle como RMAN o ASM para migrar los archivos de base de datos. Consulte ["Migración de bases de datos de Oracle a sistemas de almacenamiento de ONTAP"](#) para obtener más información. Del mismo modo, para SQL Server, plantéese utilizar SQL Server Management Studio o herramientas de NetApp, como SnapManager para SQL Server o SnapCenter.

### **Herramientas de ONTAP para VMware vSphere**

La mejor práctica más importante cuando se usa vSphere con sistemas que ejecutan ONTAP es instalar y utilizar las herramientas de ONTAP para el complemento VMware vSphere (anteriormente conocido como Virtual Storage Console). Este complemento de vCenter simplifica la gestión del almacenamiento, mejora la disponibilidad y reduce los costes de almacenamiento y la sobrecarga operativa, tanto si se utiliza SAN o NAS, en ASA, AFF, FAS o incluso en ONTAP Select (una versión definida por software de ONTAP que se ejecuta en una máquina virtual VMware o KVM). Utiliza prácticas recomendadas para el aprovisionamiento de almacenes de datos y optimiza la configuración del host ESXi para los tiempos de espera de multivía y HBA (que se describen en el apéndice B). Dado que es un complemento de vCenter, está disponible para todos los clientes web de vSphere que se conectan al servidor vCenter.

El plugin también le ayuda a utilizar otras herramientas ONTAP en entornos de vSphere. Le permite instalar el complemento de NFS para VMware VAAI, que permite realizar copias de datos descargados en ONTAP para las operaciones de clonado de equipos virtuales, reservar espacio para archivos de disco virtual gruesos y

descargar la copia Snapshot de ONTAP.



En los clústeres de vSphere basados en imágenes, seguirá queriendo añadir el plugin NFS a su imagen para que no cumplan las normativas al instalarlo con las herramientas de ONTAP.

Las herramientas de ONTAP también son la interfaz de gestión para numerosas funciones de VASA Provider para ONTAP, compatible con la gestión basada en políticas de almacenamiento con vVols.

En general, **NetApp recomienda** el uso de las herramientas de ONTAP para la interfaz de VMware vSphere en vCenter para aprovisionar almacenes de datos tradicionales y vVols a fin de garantizar que se siguen las mejores prácticas.

### Redes generales

La configuración de los ajustes de red cuando se utiliza vSphere con sistemas que ejecutan ONTAP es sencilla y similar a otra configuración de red. Estas son algunas cosas a tener en cuenta:

- Hay que separar el tráfico de la red de almacenamiento de otras redes. Se puede lograr una red independiente a través de una VLAN dedicada o switches independientes para el almacenamiento. Si la red de almacenamiento comparte rutas físicas como los enlaces ascendentes, puede que necesite calidad de servicio o puertos adicionales para garantizar el ancho de banda suficiente. No conecte los hosts directamente al almacenamiento; utilice switches para que tengan rutas redundantes y permita que VMware HA funcione sin intervención alguna. Consulte "["Conexión de red directa"](#)" para obtener más información.
- Las tramas gigantes se pueden utilizar si se desean y admiten en la red, especialmente si se utiliza iSCSI. Si se usan, asegúrese de que estén configurados de la misma forma en todos los dispositivos de red, VLAN, etc., en la ruta entre el almacenamiento y el host ESXi. De lo contrario, puede que observe problemas de rendimiento o conexión. La MTU también debe establecerse de forma idéntica en el switch virtual ESXi, el puerto de VMkernel y, además, en los puertos físicos o los grupos de interfaces de cada nodo ONTAP.
- NetApp solo recomienda deshabilitar el control de flujo de red en los puertos de interconexión de clúster de un clúster de ONTAP. NetApp no ofrece otras recomendaciones para seguir las prácticas recomendadas para los puertos de red restantes que se usan para el tráfico de datos. Debe activar o desactivar según sea necesario. Consulte "["CONSULTE TR-4182"](#)" para obtener más información sobre el control de flujo.
- Cuando las cabinas de almacenamiento ESXi y ONTAP están conectadas a redes de almacenamiento Ethernet, **NetApp recomienda** configurar los puertos Ethernet a los que se conectan estos sistemas como puertos periféricos del protocolo de árbol de expansión rápido (RSTP) o mediante la función PortFast de Cisco. **NetApp recomienda** habilitar la función de troncal PortFast de árbol de expansión en entornos que utilizan la característica PortFast de Cisco y que tienen habilitado el troncalización de VLAN 802,1Q para el servidor ESXi o las cabinas de almacenamiento ONTAP.
- **NetApp recomienda** las siguientes mejores prácticas para la agregación de enlaces:
  - Utilice switches que admitan la agregación de enlaces de puertos en dos chasis de switch separados mediante un enfoque de grupo de agregación de enlaces de varios chasis, como Virtual PortChannel (VPC) de Cisco.
  - Deshabilite LACP para los puertos del switch conectados a ESXi a menos que utilice dvSwitch 5.1 o una versión posterior con LACP configurado.
  - Utilice LACP para crear agregados de enlaces para sistemas de almacenamiento de ONTAP con grupos de interfaces dinámicas multimodo con puerto o hash IP. Consulte "["Gestión de redes"](#)" para obtener más orientación.

- Utilice una política de agrupación de hash IP en ESXi cuando utilice la agregación de enlaces estáticos (por ejemplo, EtherChannel) y vSwitch estándar, o la agregación de enlaces basada en LACP con switches distribuidos de vSphere. Si no se utiliza la agregación de enlaces, utilice en su lugar «Ruta basada en el identificador de puerto virtual de origen».

## SAN (FC, FCoE, NVMe/FC, iSCSI), RDM

En vSphere, hay cuatro formas de utilizar dispositivos de almacenamiento de bloques:

- Con almacenes de datos VMFS
- Con asignación de dispositivos sin formato (RDM)
- Como LUN conectado a iSCSI o espacio de nombres conectado a NVMe/TCP, al que accede y controla un iniciador de software desde un sistema operativo invitado de máquina virtual
- Como almacén de datos vVols

VMFS es un sistema de archivos en clúster de alto rendimiento que proporciona almacenes de datos que son pools de almacenamiento compartido. Los almacenes de datos VMFS se pueden configurar con LUN a los que se accede mediante espacios de nombres FC, iSCSI, FCoE o NVMe a los que se accede mediante los protocolos NVMe/FC o NVMe/TCP. VMFS permite a cada servidor ESX de un clúster acceder al almacenamiento de forma simultánea. El tamaño máximo de LUN suele ser de 128TB TB a partir de ONTAP 9.12.1P2 (y versiones anteriores con los sistemas ASA). Por lo tanto, es posible crear un almacén de datos VMFS 5 o 6 de tamaño máximo de 64TB TB utilizando una única LUN.

 Las extensiones son un concepto de almacenamiento de vSphere por el que puede unir varios LUN para crear un único almacén de datos de mayor tamaño. Nunca se deben utilizar extensiones para alcanzar el tamaño deseado del almacén de datos. Una única LUN es la mejor práctica para un almacén de datos VMFS.

vSphere incluye soporte incorporado para varias rutas hacia los dispositivos de almacenamiento. vSphere puede detectar el tipo de dispositivo de almacenamiento en los sistemas de almacenamiento compatibles y configurar automáticamente la pila multivía para admitir las capacidades del sistema de almacenamiento que se esté utilizando, el uso del protocolo utilizado o si se utiliza ASA, AFF, FAS o ONTAP definido por software.

Tanto vSphere como ONTAP admiten el acceso asimétrico de unidad lógica (ALUA) para establecer rutas activo/optimizado y activo/no optimizado para Fibre Channel e iSCSI, y Acceso asimétrico a espacios de nombres (ANA) para espacios de nombres NVMe mediante NVMe/FC y NVMe/TCP. En ONTAP, una ruta optimizada para ALUA o ANA sigue una ruta de datos directa, mediante un puerto de destino en el nodo que aloja el LUN o el espacio de nombres al que se está accediendo. ALUA/ANA está activado de manera predeterminada en vSphere y ONTAP. El software multivía de vSphere reconoce el clúster de ONTAP como ALUA o ANA y utiliza el complemento nativo adecuado con la política de equilibrio de carga round robin.

Con los sistemas ASA de NetApp, las LUN y los espacios de nombres se presentan a los hosts ESXi con rutas simétricas. Lo que significa que todas las rutas están activas y optimizadas. El software multivía en vSphere reconoce el sistema ASA como simétrico y utiliza el plugin nativo adecuado con la política de equilibrio de carga round robin.

 Consulte ["Host ESXi recomendado y otra configuración de ONTAP"](#) para obtener información sobre los ajustes de acceso múltiple optimizados.

ESXi no ve ninguna LUN, espacios de nombres o rutas más allá de sus límites. En un clúster de ONTAP mayor, es posible alcanzar el límite de ruta antes del límite de LUN. Para solucionar esta limitación, ONTAP admite una asignación de LUN selectiva (SLM) en la versión 8.3 y posteriores.



Consulte el ["Herramienta VMware Configuration Maximums"](#) para obtener los límites admitidos más actualizados en ESXi.

SLM limita los nodos que anuncian rutas a un LUN determinado. Una mejor práctica de NetApp es tener al menos dos LIF por nodo y utilizar SLM para limitar las rutas anunciadas al nodo que aloja el LUN y su partner de alta disponibilidad. Aunque existen otras rutas, no se anuncian por defecto. Es posible modificar las rutas anunciadas con los argumentos de nodo de informes Agregar y quitar dentro de SLM. Tenga en cuenta que las LUN creadas en versiones anteriores a la 8,3 anuncian todas las rutas y deben modificarse únicamente para anunciar las rutas al par de alta disponibilidad que aloja. Para obtener más información sobre SLM, consulte la sección 5,9 de ["CONSULTE TR-4080"](#). El método anterior de conjuntos de puertos también puede utilizarse para reducir aún más las rutas disponibles para una LUN. Los conjuntos de puertos ayudan a reducir el número de rutas visibles a través de las cuales los iniciadores de un igroup pueden ver LUN.

- SLM está habilitado de forma predeterminada. A menos que utilice conjuntos de puertos, no se requiere ninguna configuración adicional.
- Para las LUN creadas antes de Data ONTAP 8,3, aplique manualmente SLM ejecutando `lun mapping remove-reporting-nodes` el comando para quitar los nodos de informe de LUN y restringir el acceso de las LUN al nodo propietario del LUN y su partner de alta disponibilidad.

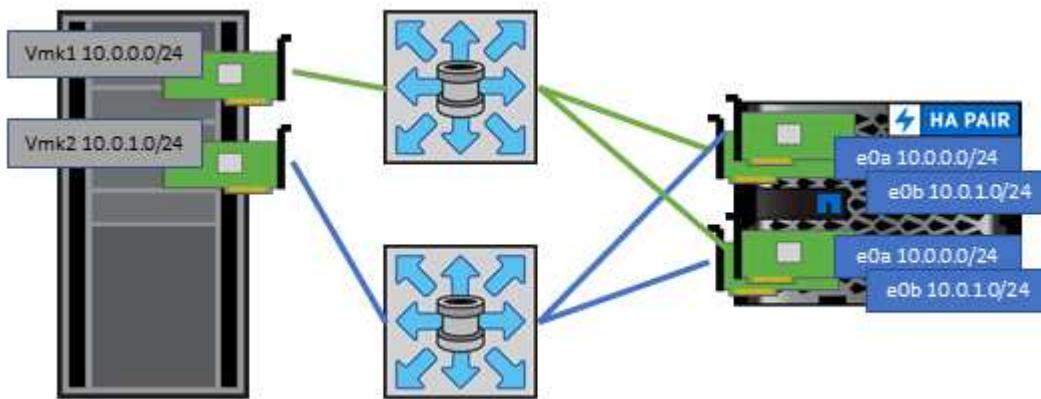
Los protocolos de bloque basados en SCSI (iSCSI, FC y FCoE) acceden a los LUN usando ID de LUN y números de serie, junto con nombres únicos. FC y FCoE utilizan nombres a nivel mundial (WWN y WWPN), e iSCSI utiliza nombres completos de iSCSI (IQN) para establecer rutas en función de las asignaciones de LUN a igroup filtradas por conjuntos de puertos y SLM. Los protocolos de bloques basados en NVMe se gestionan asignando el espacio de nombres con un ID de espacio de nombres generado automáticamente a un subsistema NVMe y asignando dicho subsistema al nombre completo de NVMe (NQN) de los hosts. Independientemente de FC o TCP, los espacios de nombres de NVMe se asignan mediante el NQN y no el puerto WWPN o WWNN. A continuación, el host crea una controladora definida por software para que el subsistema asignado acceda a sus espacios de nombres. La ruta a las LUN y los espacios de nombres dentro de ONTAP no tiene sentido para los protocolos de bloques y no se presenta en ninguna parte del protocolo. Por lo tanto, no es necesario montar de forma interna un volumen que solo contiene LUN; por lo tanto, no es necesaria una ruta de unión para los volúmenes que contengan LUN usadas en los almacenes de datos.

Otras prácticas recomendadas a tener en cuenta:

- Compruebe ["Host ESXi recomendado y otra configuración de ONTAP"](#) los ajustes recomendados por NetApp en colaboración con VMware.
- Asegúrese de que se crea una interfaz lógica (LIF) para cada SVM en cada nodo del clúster de ONTAP para garantizar la máxima disponibilidad y movilidad. La práctica recomendada para SAN de ONTAP es usar dos puertos físicos y LIF por nodo, uno para cada estructura. ALUA se utiliza para analizar las rutas e identificar las rutas activas optimizadas (directas) en comparación con las rutas activas no optimizadas. ALUA se utiliza para FC, FCoE e iSCSI.
- En el caso de las redes iSCSI, utilice varias interfaces de red de VMkernel en distintas subredes de la red con la agrupación de NIC cuando haya varios switches virtuales. También puede utilizar varias NIC físicas conectadas a varios switches físicos para proporcionar alta disponibilidad y mayor rendimiento. En la figura siguiente se proporciona un ejemplo de conectividad multivía. En ONTAP, configure un grupo de interfaces de un único modo para realizar la conmutación al nodo de respaldo con dos o más enlaces conectados a dos o más switches, o bien utilice LACP u otra tecnología de agregación de enlaces con grupos de interfaces multimodo para proporcionar alta disponibilidad y las ventajas de la agregación de enlaces.
- Si el protocolo de autenticación por desafío mutuo (CHAP) se utiliza en ESXi para la autenticación de destino, también debe configurarse en ONTAP mediante la CLI (`vserver iscsi security create`) O con System Manager (edite Initiator Security en almacenamiento > SVM > SVM Settings > Protocols >

iSCSI).

- Utilice las herramientas de ONTAP para VMware vSphere para crear y gestionar LUN y iGroups. El plugin determina automáticamente los WWPN de los servidores y crea iGroups adecuados. También configura las LUN de acuerdo con las prácticas recomendadas y las asigna a los iGroups correctos.
- Use los DMR con cuidado porque pueden ser más difíciles de manejar, y también usan rutas, que son limitadas como se describió anteriormente. Las LUN de ONTAP son compatibles con ambos ["modo de compatibilidad físico y virtual"](#) RDM.
- Para obtener más información sobre cómo usar NVMe/FC con vSphere 7.0, consulte este tema ["Guía de configuración de hosts ONTAP NVMe/FC"](#) y.. ["CONSULTE TR-4684"](#). En la siguiente figura, se muestra la conectividad multivía de un host de vSphere a un LUN de ONTAP.



## NFS

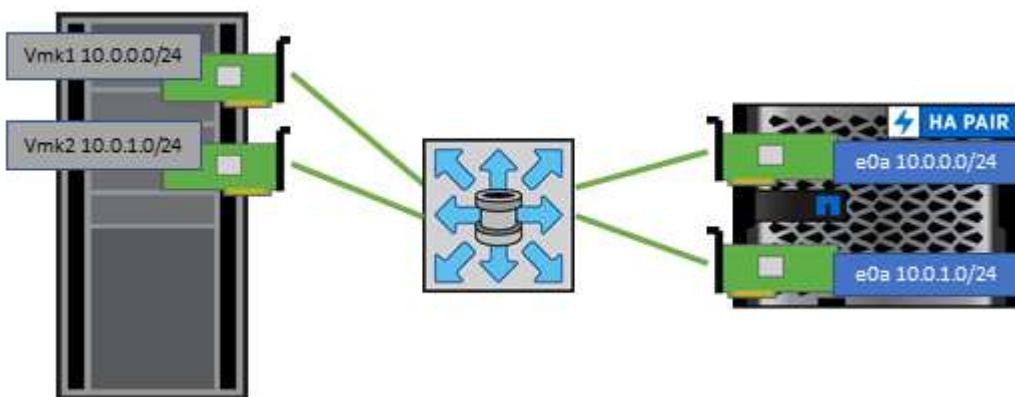
ONTAP representa, entre otras cosas, una cabina NAS de escalado horizontal para empresas. ONTAP proporciona acceso concurrente a los almacenes de datos conectados a NFS desde muchos hosts ESXi, lo que supera con creces los límites impuestos en los sistemas de archivos VMFS. El uso de NFS con vSphere proporciona cierta facilidad de uso y ventajas de visibilidad de la eficiencia del almacenamiento, como se menciona en ["almacenes de datos"](#) la sección.

Las siguientes prácticas recomendadas se recomiendan al usar NFS de ONTAP con vSphere:

- Use las herramientas de ONTAP para VMware vSphere (las mejores prácticas más importantes):
  - Utilizar herramientas de ONTAP para VMware vSphere para aprovisionar almacenes de datos, ya que simplifica la gestión automática de políticas de exportación.
  - Cuando se crean almacenes de datos para clústeres de VMware con el plugin, seleccione el clúster en lugar de un único servidor ESX. Esta opción la activa para montar automáticamente el almacén de datos en todos los hosts del clúster.
  - Use la función de montaje del plugin para aplicar almacenes de datos existentes a servidores nuevos.
  - Si no se utilizan las herramientas de ONTAP para VMware vSphere, utilice una única política de exportación para todos los servidores o para cada cluster de servidores donde se necesite un control de acceso adicional.
- Utilice una sola interfaz lógica (LIF) para cada SVM en cada nodo del clúster de ONTAP. Ya no son necesarias las recomendaciones anteriores de una LIF por almacén de datos. Aunque el acceso directo (LIF y almacén de datos en el mismo nodo) es el mejor, no se preocupe por el acceso indirecto, ya que el efecto sobre el rendimiento suele ser mínimo (microsegundos).

- Si usa fpolicy, asegúrese de excluir los archivos .lck, ya que los utiliza vSphere para bloquear cada vez que se enciende una máquina virtual.
- Todas las versiones de VMware vSphere compatibles en la actualidad pueden usar NFS v3 y v4.1. La compatibilidad oficial con nconnect se agregó a la actualización 2 de vSphere 8.0 para NFS v3 y a la actualización 3 para NFS v4.1. Para NFS v4.1, vSphere sigue admitiendo el truncado de sesión, la autenticación Kerberos y la autenticación Kerberos con integridad. Es importante tener en cuenta que el trunking de sesión requiere ONTAP 9.14.1 o una versión posterior. Puede obtener más información sobre la función nconnect y cómo mejora el rendimiento en "["La función de NFSv3 nconnect con NetApp y VMware"](#)".
  - El valor máximo para nconnect en vSphere 8 es 4 y el valor predeterminado es 1. El límite de valor máximo en vSphere se puede aumentar por host a través de una configuración avanzada, sin embargo, por lo general no es necesario.
  - Se recomienda un valor de 4 para los entornos que requieren más rendimiento del que puede proporcionar una única conexión TCP.
    - Tenga en cuenta que ESXi tiene un límite de 256 conexiones NFS y cada conexión nconnect cuenta para ese total. Por ejemplo, dos almacenes de datos con nconnect=4 contarían como ocho conexiones totales.
    - Es importante probar el impacto de nconnect en el rendimiento en su entorno antes de implementar cambios a gran escala en los entornos de producción.
- Vale la pena señalar que NFSv3 y NFSv4.1 utilizan diferentes mecanismos de bloqueo. NFSv3 utiliza bloqueo del lado del cliente, mientras que NFSv4.1 utiliza bloqueo del lado del servidor. Aunque un volumen ONTAP se puede exportar mediante ambos protocolos, ESXi solo puede montar un almacén de datos a través de un protocolo. Sin embargo, esto no significa que otros hosts ESXi no puedan montar el mismo almacén de datos mediante una versión diferente. Para evitar cualquier problema, es esencial especificar la versión del protocolo que se debe utilizar al montar, asegurándose de que todos los hosts utilicen la misma versión y, por lo tanto, el mismo estilo de bloqueo. Es crucial evitar mezclar versiones de NFS entre hosts. Si es posible, utilice perfiles de host para comprobar el cumplimiento.
  - Dado que no existe ninguna conversión automática de almacenes de datos entre NFSv3 y NFSv4.1, cree un nuevo almacén de datos NFSv4.1 y utilice Storage vMotion para migrar las máquinas virtuales al nuevo almacén de datos.
  - Consulte las notas de la tabla de interoperabilidad de NFS v4.1 en la "["Herramienta de matriz de interoperabilidad de NetApp"](#)" para ver los niveles de parches de ESXi específicos necesarios para el soporte.
- Tal como se ha mencionado en "["configuración"](#)", si no utiliza el CSI de vSphere para Kubernetes, debe establecer newSyncInterval por "["VMware KB 386364"](#)"
- Las reglas de políticas de exportación de NFS se usan para controlar el acceso de los hosts vSphere. Puede usar una política con varios volúmenes (almacenes de datos). Con NFS, ESXi utiliza el estilo de seguridad sys (UNIX) y requiere la opción de montaje root para ejecutar equipos virtuales. En ONTAP, esta opción se denomina superusuario y cuando se utiliza la opción superusuario, no es necesario especificar el ID de usuario anónimo. Tenga en cuenta que reglas de políticas de exportación con diferentes valores para -anon y -allow-suid pueden causar problemas de detección de SVM con las herramientas de ONTAP. Las direcciones IP deben ser una lista separada por comas sin espacios de las direcciones de puertos de vmkernel que montan los almacenes de datos. He aquí una regla de política de ejemplo:
  - Protocolo de acceso: nfs (que incluye nfs3 y nfs4)
  - Lista de nombres de host, direcciones IP, grupos de red o dominios de coincidencia de cliente: 192.168.42.21, 192.168.42.22

- Regla de acceso de RO: Cualquiera
- Regla de acceso RW: Cualquiera
- ID de usuario al que se asignan los usuarios anónimos: 65534
- Tipos de seguridad de superusuario: Cualquiera
- Honor setuid Bits en SETATTR: True
- Permitir la creación de dispositivos: True
- Si se utiliza el plugin de NFS de NetApp para VMware VAAI, el protocolo se debe establecer `nfs` como cuando se crea o se modifica la regla de política de exportación. El protocolo NFSv4 se requiere para que la copia de VAAI descargue el trabajo y especificando el protocolo como `nfs` automáticamente incluye las versiones NFSv3 y NFSv4. Esto es necesario incluso si el tipo de almacenamiento de datos se crea como NFS v3.
- Los volúmenes de almacenamiento de datos NFS se unen desde el volumen raíz de la SVM; por lo tanto, ESXi también debe tener acceso al volumen raíz para navegar y montar volúmenes de almacenamiento de datos. La política de exportación del volumen raíz y para cualquier otro volumen en el que esté anidada la unión del volumen de almacenamiento de datos, debe incluir una regla o reglas para los servidores ESXi que les otorgan acceso de solo lectura. A continuación, se muestra una política de ejemplo para el volumen raíz, que también utiliza el complemento VAAI:
  - Protocolo de acceso: `nfs`
  - Client Match Spec: 192.168.42.21, 192.168.42.22
  - Regla DE ACCESO DE RO: `Sys`
  - Regla de acceso RW: Nunca (mejor seguridad para el volumen raíz)
  - UID anónimo
  - Superusuario: `Sys` (también necesario para el volumen raíz con VAAI)
- Aunque ONTAP ofrece una estructura de espacio de nombres de volúmenes flexibles para organizar los volúmenes en un árbol mediante uniones, este enfoque no tiene valor para vSphere. Crea un directorio para cada equipo virtual en la raíz del almacenamiento de datos, independientemente de la jerarquía de espacio de nombres del almacenamiento. Por lo tanto, la práctica recomendada es simplemente montar la ruta de unión para volúmenes para vSphere en el volumen raíz de la SVM, que es la forma en que las herramientas de ONTAP para VMware vSphere aprovisionan almacenamiento de datos. No tener rutas de unión anidadas también significa que ningún volumen depende de ningún otro volumen que no sea el volumen raíz y que el hecho de desconectar un volumen o destruirlo, incluso intencionalmente, no afecta la ruta a otros volúmenes.
- El tamaño de bloque de 4K se ajusta a las particiones NTFS en almacenamientos de datos NFS. En la siguiente figura, se muestra la conectividad de un host vSphere a un almacenamiento de datos NFS de ONTAP.



En la siguiente tabla, se enumeran las versiones de NFS y las funciones compatibles.

| Funciones de vSphere                             | NFSv3 | NFSv4,1  |
|--|-------|--|
| VMotion y Storage vMotion                        | Sí    | Sí   |
| Alta disponibilidad                              | Sí    | Sí   |
| Tolerancia a fallos                              | Sí    | Sí   |
| DRS  | Sí    | Sí   |
| Perfiles de host                                 | Sí    | Sí   |
| DRS de almacenamiento                            | Sí    | No   |
| Control de la actividad de I/o de almacenamiento | Sí    | No   |
| SRM  | Sí    | No   |
| Volúmenes virtuales                              | Sí    | No   |
| Aceleración de hardware (VAAI)                   | Sí    | Sí   |
| Autenticación Kerberos                           | No    | Sí (mejorada con vSphere 6.5 y versiones posteriores para ser compatible con AES, krb5i) |
| Compatibilidad con accesos múltiples             | No    | Sí (ONTAP 9.14.1)  |

### Volúmenes de FlexGroup

Utilice ONTAP y FlexGroup Volumes con VMware vSphere para obtener almacenes de datos sencillos y escalables que aprovechan toda la potencia de todo un clúster de ONTAP.

ONTAP 9.8, junto con las herramientas de ONTAP para VMware vSphere 9.8-9.13 y el complemento SnapCenter para VMware 4.4, y otras versiones más recientes, añadieron compatibilidad con almacenes de datos respaldados por volúmenes de FlexGroup en vSphere. Los volúmenes FlexGroup simplifican la creación de grandes almacenes de datos y crean automáticamente los volúmenes constituyentes distribuidos necesarios en el clúster ONTAP para obtener el rendimiento máximo de un sistema ONTAP.

Utilice FlexGroup Volumes con vSphere si necesita un único almacén de datos de vSphere escalable con la potencia de un clúster ONTAP completo, o si cuenta con cargas de trabajo de clonado muy grandes que pueden beneficiarse del mecanismo de clonado de FlexGroup manteniendo constantemente la memoria caché de clonado caliente.

### Descarga de copias

Además de las amplias pruebas del sistema con cargas de trabajo de vSphere, ONTAP 9.8 añadió un nuevo mecanismo de descarga de copia para los almacenes de datos de FlexGroup. Este nuevo sistema emplea un motor de copia mejorado para replicar archivos entre componentes en segundo plano a la vez que permite el acceso al origen y al destino. A continuación, esta caché local de componente se utiliza para crear rápidamente instancias de clones de equipos virtuales bajo demanda.

Para habilitar la descarga de copias optimizada para FlexGroup, consulte ["Cómo configurar volúmenes de ONTAP FlexGroup para permitir la descarga de la copia de VAAI"](#)

Puede ocurrir que si utiliza la clonación de VAAI, pero no clona lo suficiente para mantener la caché caliente, es posible que los clones no sean más rápidos que una copia basada en host. Si ese es el caso, puede ajustar el tiempo de espera de la caché para adaptarse mejor a sus necesidades.

Considere el siguiente escenario:

- Ha creado un nuevo FlexGroup con 8 componentes
- El tiempo de espera de caché para el nuevo FlexGroup se establece en 160 minutos

En esta situación, los primeros 8 clones que se realizarán serán copias completas, no clones de archivos locales. Cualquier clonación adicional de ese equipo virtual antes de que caduque el tiempo de espera de 160 segundos utilizará el motor de clonado de archivos dentro de cada componente en turno rotatorio para crear copias casi inmediatas distribuidas uniformemente en los volúmenes constituyentes.

Cada trabajo de clon nuevo que recibe un volumen restablece el tiempo de espera. Si un volumen constituyente de FlexGroup de ejemplo no recibe una solicitud de clonado antes del tiempo de espera, se borrará la caché de esa máquina virtual en particular y el volumen se deberá volver a completar. Además, si el origen del clon original cambia (por ejemplo, ha actualizado la plantilla), la caché local de cada componente se invalidará para evitar cualquier conflicto. Como se ha indicado anteriormente, la caché se puede ajustar y se puede configurar para satisfacer las necesidades del entorno.

Para obtener más información sobre el uso de FlexGroup Volumes con VAAI, consulte este artículo de la base de conocimientos: "["VAAI: ¿Cómo funciona el almacenamiento en caché con volúmenes FlexGroup?"](#)"

En entornos donde no es posible aprovechar al máximo la caché FlexGroup, pero aún así requerir un clonado rápido entre volúmenes, considere el uso de vVols. La clonación entre volúmenes con vVols es mucho más rápida que el uso de almacenes de datos tradicionales y no utiliza una caché.

#### **Configuración de calidad de servicio**

Se admite la configuración de la calidad de servicio en el nivel de FlexGroup mediante ONTAP System Manager o el shell del clúster; sin embargo, no se proporciona para la máquina virtual ni la integración con vCenter.

La calidad de servicio (IOPS máx./mín.) se puede establecer en máquinas virtuales individuales o en todas las máquinas virtuales de un almacén de datos en ese momento en la interfaz de usuario de vCenter o mediante las API de REST con las herramientas de ONTAP. La configuración de la calidad de servicio en todas las máquinas virtuales sustituye cualquier configuración independiente por cada máquina virtual. Los ajustes no amplían en el futuro a máquinas virtuales nuevas o migradas; establezca la calidad de servicio en las nuevas máquinas virtuales o vuelva a aplicar la calidad de servicio a todas las máquinas virtuales del almacén de datos.

Tenga en cuenta que VMware vSphere trata todas las I/O de un almacén de datos NFS como una única cola por host, y la limitación de la calidad de servicio de un equipo virtual puede afectar al rendimiento de otras máquinas virtuales del mismo almacén de datos en ese host. Esto contrasta con vVols, que puede mantener su configuración de política de calidad de servicio si migran a otro almacén de datos y no afecta la I/O de otras máquinas virtuales cuando se acelera.

#### **Métricas**

ONTAP 9.8 también agregó nuevas métricas de rendimiento basadas en archivos (IOPS, rendimiento y latencia) para archivos FlexGroup. Estas métricas pueden visualizarse en la consola de herramientas de ONTAP para la consola de VMware vSphere e informes de VM. Las herramientas de ONTAP para el complemento VMware vSphere también le permiten establecer reglas de calidad de servicio (QoS) con una combinación de IOPS máximo o mínimo. Estos conjuntos se pueden establecer en todas las máquinas

virtuales de un almacén de datos o individualmente para máquinas virtuales específicas.

### Mejores prácticas

- Utilice las herramientas de ONTAP para crear almacenes de datos de FlexGroup a fin de garantizar que el FlexGroup se cree de forma óptima y que las políticas de exportación se configuren en consonancia con su entorno vSphere. Sin embargo, después de crear el volumen FlexGroup con herramientas de ONTAP, se dará cuenta de que todos los nodos del clúster de vSphere utilizan una sola dirección IP para montar el almacén de datos. Esto podría provocar un cuello de botella en el puerto de red. Para evitar este problema, desmonte el almacén de datos y vuelva a montarlo mediante el asistente para almacenes de datos estándar de vSphere mediante un nombre DNS round-robin que equilibre la carga entre las LIF en la máquina virtual de almacenamiento. Tras el montaje, las herramientas de ONTAP podrán volver a gestionar el almacén de datos. Si no hay herramientas de ONTAP disponibles, use los valores predeterminados de FlexGroup y cree la política de exportación siguiendo las directrices de ["Almacenes de datos y protocolos: NFS"](#).
- Al ajustar el tamaño a un almacén de datos FlexGroup, tenga en cuenta que FlexGroup consta de varios volúmenes FlexVol más pequeños que crean un espacio de nombres mayor. De este modo, configure el tamaño del almacén de datos para que sea al menos 8x (asumiendo los 8 componentes predeterminados) el tamaño del archivo VMDK más grande y un margen no utilizado del 10 al 20% para permitir flexibilidad en el reequilibrio. Por ejemplo, si tiene un VMDK de 6TB GB en el entorno, ajuste el tamaño del almacén de datos FlexGroup como mínimo 52,8TB (6x8+10 %).
- VMware y NetApp admiten el trunking de sesiones NFSv4.1 a partir de ONTAP 9.14.1. Consulte las notas de la herramienta de matriz de interoperabilidad (IMT) de NFS 4.1 de NetApp para ver detalles específicos de la versión. NFSv3 no admite varias rutas físicas de un volumen, pero admite nconnect a partir de vSphere 8.0U2. Puede encontrar más información sobre nconnect en el ["NFSv3 Función nConnect con NetApp y VMware"](#).
- Use el plugin de NFS para VAAI de VMware para la descarga de copias. Tenga en cuenta que, aunque el clonado se mejora dentro de un almacén de datos de FlexGroup, como se ha mencionado anteriormente, ONTAP no ofrece importantes ventajas de rendimiento con respecto a la copia del host ESXi al copiar máquinas virtuales entre FlexVol y/o volúmenes de FlexGroup. Por tanto, tenga en cuenta las cargas de trabajo de clonado cuando decida usar volúmenes de VAAI o FlexGroup. La modificación del número de volúmenes constituyentes es una forma de optimizar para la clonación basada en FlexGroup. Al igual que el ajuste del timeout de caché mencionado anteriormente.
- Utilice herramientas de ONTAP para VMware vSphere 9.8-9.13 para supervisar el rendimiento de las VM de FlexGroup mediante métricas de ONTAP (informes de la consola y de VM), y para gestionar la calidad de servicio en máquinas virtuales individuales. Estas métricas no están disponibles a través de los comandos o las API de ONTAP.
- El plugin de SnapCenter para VMware vSphere versión 4.4 y versiones posteriores admite el backup y la recuperación de máquinas virtuales en un almacén de datos FlexGroup en el sistema de almacenamiento principal. SCV 4.6 añade compatibilidad con SnapMirror para almacenes de datos basados en FlexGroup. La forma más eficiente de proteger los datos es usar copias Snapshot y replicación basadas en cabinas.

## Configuración de red

La configuración de los ajustes de red cuando se utiliza vSphere con sistemas que ejecutan ONTAP es sencilla y similar a otra configuración de red.

Estas son algunas cosas a tener en cuenta:

- Hay que separar el tráfico de la red de almacenamiento de otras redes. Se puede lograr una red independiente a través de una VLAN dedicada o switches independientes para el almacenamiento. Si la red de almacenamiento comparte rutas físicas como los enlaces ascendentes, puede que necesite calidad

de servicio o puertos adicionales para garantizar el ancho de banda suficiente. No conecte los hosts directamente al sistema de almacenamiento a menos que la guía de la solución lo indique específicamente; utilice switches para tener rutas redundantes y permita que VMware HA funcione sin intervención alguna.

- Se deben utilizar tramas gigantes si la red es compatible. Si se usan, asegúrese de que estén configurados de la misma forma en todos los dispositivos de red, VLAN, etc., en la ruta entre el almacenamiento y el host ESXi. De lo contrario, puede que observe problemas de rendimiento o conexión. La MTU también debe establecerse de forma idéntica en el switch virtual ESXi, el puerto de VMkernel y, además, en los puertos físicos o los grupos de interfaces de cada nodo ONTAP.
- NetApp solo recomienda deshabilitar el control de flujo de red en los puertos de interconexión del clúster de un clúster de ONTAP. NetApp no hace ninguna otra recomendación en cuanto a las mejores prácticas relativas al control de flujo para los puertos de red restantes que se usan para el tráfico de datos. Debe habilitarla o deshabilitarla según sea necesario. Consulte "[CONSULTE TR-4182](#)" para obtener más información sobre el control de flujo.
- Cuando las cabinas de almacenamiento ESXi y ONTAP están conectadas a redes de almacenamiento Ethernet, NetApp recomienda configurar los puertos Ethernet a los que se conectan estos sistemas como puertos periféricos del protocolo de árbol de expansión rápido (RSTP) o mediante la función PortFast de Cisco. NetApp recomienda habilitar la función de enlace troncal Spanning-Tree PortFast en entornos que utilizan la función Cisco PortFast y que tienen la conexión de enlaces VLAN 802.1Q habilitada tanto para el servidor ESXi como para las cabinas de almacenamiento ONTAP.
- NetApp recomienda las siguientes prácticas recomendadas para la agregación de enlaces:
  - Utilice switches que admitan la agregación de enlaces de puertos en dos chasis de switch separados mediante un enfoque de grupo de agregación de enlaces de varios chasis, como Virtual PortChannel (VPC) de Cisco.
  - Deshabilite LACP para los puertos del switch conectados a ESXi a menos que utilice dvSwitch 5.1 o una versión posterior con LACP configurado.
  - LACP se utiliza para crear agregados de enlaces para sistemas de almacenamiento ONTAP con grupos de interfaces dinámicas multimodo con hash IP.
  - Use una política de agrupación de hash IP en ESXi.

En la siguiente tabla se ofrece un resumen de los elementos de configuración de red e indica dónde se aplican los ajustes.

| Elemento                   | ESXi  | Conmutador                 | Nodo      | SVM |
|----------------------------|---|----------------------------|-----------|-----|
| Dirección IP               | VMkernel  | No**                       | No**      | Sí  |
| Agregación de enlaces      | Switch virtual                                  | Sí                         | Sí        | No* |
| VLAN                       | VMkernel y grupos de puertos de máquina virtual | Sí                         | Sí        | No* |
| Control de flujo           | NIC   | Sí                         | Sí        | No* |
| Árbol expansivo            | No  | Sí                         | No        | No  |
| MTU (para tramas gigantes) | Conmutador virtual y puerto de VMkernel (9000)  | Sí (configurado como máx.) | Sí (9000) | No* |

| Elemento                        | ESXi | Conmutador | Nodo       | SVM             |
|---------------------------------|------|------------|------------|-----------------|
| Grupos de conmutación por error | No   | No         | Sí (crear) | Sí (seleccione) |

\*Las LIF de SVM se conectan a puertos, grupos de interfaces o interfaces VLAN que tienen VLAN, MTU y otras configuraciones. Sin embargo, la configuración no se gestiona a nivel de SVM.

\*\*Estos dispositivos tienen direcciones IP propias para la administración, pero estas direcciones no se utilizan en el contexto de las redes de almacenamiento ESXi.

### **SAN (FC, NVMe/FC, iSCSI, NVMe/TCP), RDM**

ONTAP ofrece almacenamiento basado en bloques para VMware vSphere utilizando el protocolo iSCSI tradicional y Fibre Channel (FCP) así como el protocolo de bloque de nueva generación altamente eficiente y eficiente, NVMe over Fabrics (NVMe-oF), con soporte para NVMe/FC y NVMe/TCP.

Para obtener las mejores prácticas detalladas para implementar protocolos de bloque para almacenamiento de máquinas virtuales con vSphere y ONTAP, consulte "[Almacenes de datos y protocolos: SAN](#)"

### **NFS**

VSphere permite a los clientes utilizar cabinas NFS de nivel empresarial para proporcionar acceso simultáneo a los almacenes de datos en todos los nodos de un clúster ESXi. Como se ha mencionado en la "[almacenes de datos](#)" sección, existen algunas ventajas de facilidad de uso y visibilidad de la eficiencia del almacenamiento cuando se usa NFS con vSphere.

Para conocer las prácticas recomendadas, consulte "[Almacenes de datos y protocolos: NFS](#)"

### **Conexión de red directa**

A veces, los administradores de almacenamiento prefieren simplificar sus infraestructuras eliminando los switches de red de la configuración. Esto puede ser soportado en algunos escenarios. Sin embargo, hay algunas limitaciones y advertencias a tener en cuenta.

### **iSCSI y NVMe/TCP**

Un host que utilice iSCSI o NVMe/TCP se puede conectar directamente a un sistema de almacenamiento y funcionar normalmente. El motivo son las rutas. Las conexiones directas a dos controladoras de almacenamiento diferentes dan como resultado dos rutas independientes para el flujo de datos. La pérdida de una ruta, un puerto o una controladora no impide que se utilice la otra ruta.

### **NFS**

Se puede utilizar el almacenamiento NFS conectado directamente, pero con una limitación considerable: El fallo no funcionará si no se realiza una ejecución significativa de secuencias de comandos, que sería responsabilidad del cliente.

El motivo por el que la recuperación tras fallos sin interrupciones se complica gracias al almacenamiento NFS de conexión directa es el enrutamiento que se produce en el sistema operativo local. Por ejemplo, supongamos que un host tiene una dirección IP de 192.168.1.1/24 y está directamente conectado a una controladora ONTAP con la dirección IP 192.168.1.50/24. Durante la conmutación al nodo de respaldo, esa dirección 192.168.1.50 puede conmutar al nodo de respaldo a la otra controladora y estará disponible para el host, pero ¿cómo detecta el host su presencia? La dirección 192.168.1.1 original todavía existe en la NIC host

que ya no se conecta a un sistema operativo. El tráfico destinado a 192.168.1.50 seguiría enviándose a un puerto de red inoperable.

La segunda NIC del SO podría configurarse como 192.168.1.2 y sería capaz de comunicarse con la dirección fallida en 192.168.1.50, pero las tablas de enrutamiento locales tendrían un valor predeterminado de usar una dirección **y solo una** para comunicarse con la subred 192.168.1.0/24. Un administrador de sistema podría crear un marco de scripting que detectara una conexión de red fallida y alterara las tablas de enrutamiento locales o activara o desactivara las interfaces. El procedimiento exacto dependerá del sistema operativo en uso.

En la práctica, los clientes de NetApp disponen de NFS conectado directamente, pero normalmente solo para cargas de trabajo en las que se pueden pausar I/O durante las recuperaciones tras fallos. Cuando se utilizan montajes duros, no debe haber ningún error de E/S durante dichas pausas. El E/S se debe congelar hasta que se restaren los servicios, ya sea mediante una conmutación por recuperación o mediante intervención manual para mover las direcciones IP entre las NIC del host.

#### **Conexión directa FC**

No es posible conectar directamente un host a un sistema de almacenamiento ONTAP mediante el protocolo FC. La razón es el uso de NPIV. El WWN que identifica un puerto ONTAP FC con la red de FC utiliza un tipo de virtualización denominado NPIV. Cualquier dispositivo conectado a un sistema ONTAP debe poder reconocer un WWN de NPIV. No hay proveedores de HBA actuales que ofrezcan un HBA que se pueda instalar en un host que admite un destino NPIV.

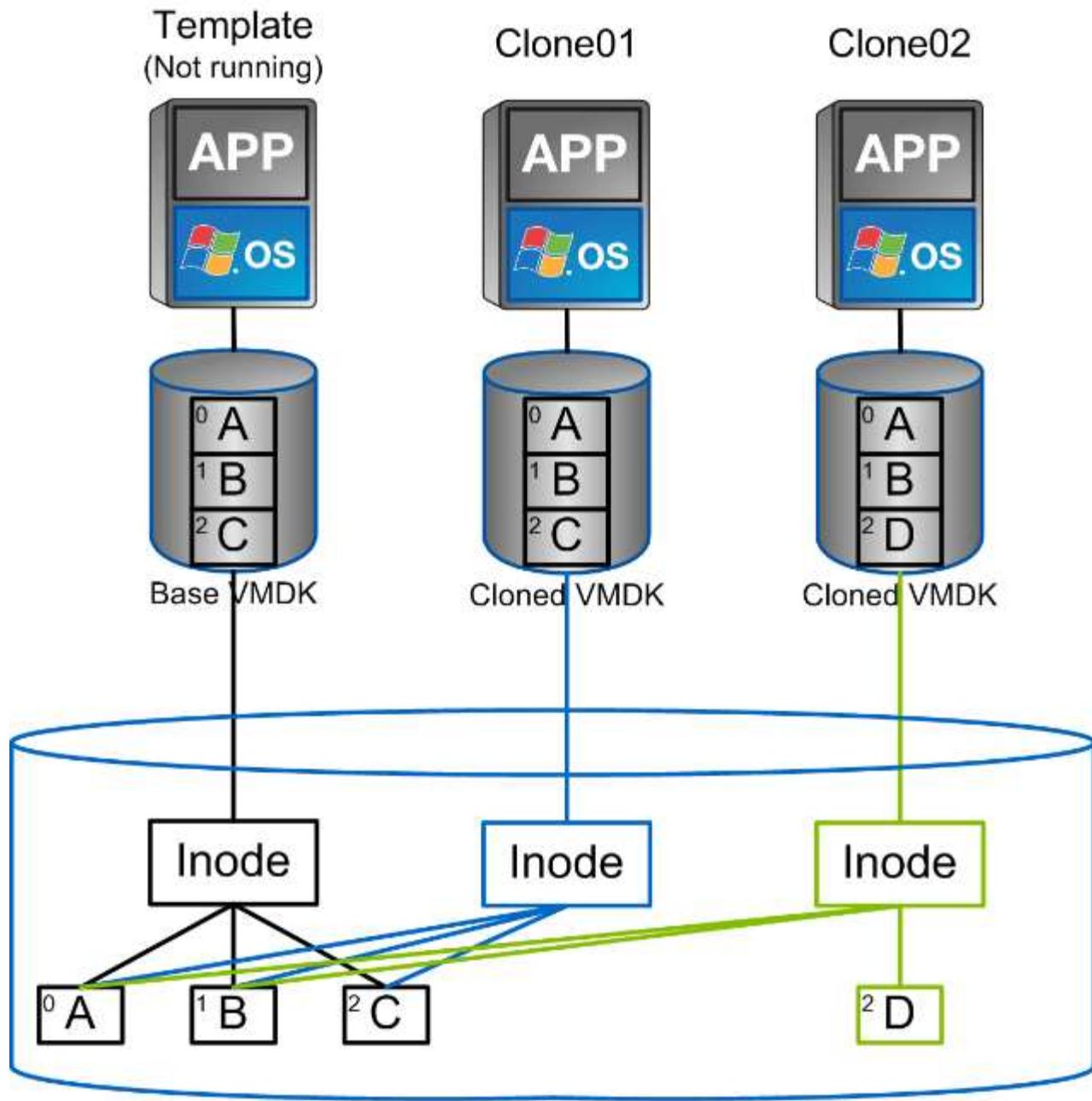
## **Clonado de máquinas virtuales y almacenes de datos**

El clonado de un objeto de almacenamiento le permite crear rápidamente copias para un uso adicional, como el aprovisionamiento de equipos virtuales adicionales, operaciones de backup/recuperación de datos, etc.

En vSphere, es posible clonar una máquina virtual, un disco virtual, VVol o un almacén de datos. Después de que se clona, el objeto se puede personalizar aún más, a menudo mediante un proceso automatizado. VSphere es compatible con ambos clones de copias completas, así como clones enlazados, donde sigue los cambios de forma independiente del objeto original.

Los clones enlazados son excelentes para ahorrar espacio, pero aumentan la cantidad de I/o que vSphere gestiona para el equipo virtual, lo que afecta al rendimiento de ese equipo virtual y, quizás, al host en general. Por eso los clientes de NetApp suelen usar clones basados en sistemas de almacenamiento para obtener lo mejor de ambos mundos: Un uso eficiente del almacenamiento y un mayor rendimiento.

La siguiente figura muestra la clonación de ONTAP.



## NetApp FlexVol Volume

La clonado puede descargarse en sistemas que ejecutan ONTAP a través de varios mecanismos, normalmente a nivel de máquina virtual, VVol o almacen de datos. Entre ellos se incluyen los siguientes:

- VVols utiliza el proveedor de API de vSphere para el reconocimiento del almacenamiento (VASA) de NetApp. Los clones de ONTAP se utilizan para admitir copias Snapshot VVOL gestionadas por vCenter, que gestionan el espacio de forma eficiente y tienen un efecto de I/O mínimo para crearlas y eliminarlas. Las máquinas virtuales también pueden clonarse mediante vCenter y también se descargan en ONTAP, ya sea en un único almacen de datos/volumen o entre almacenes de datos/volúmenes.
- Clonado y migración de vSphere mediante API de vSphere: Integración de cabina (VAAI). Las operaciones de clonado de máquinas virtuales se pueden descargar en ONTAP tanto en entornos SAN como NAS (NetApp proporciona un complemento ESXi para habilitar VAAI para NFS). VSphere solo libera las operaciones en máquinas virtuales frías (apagadas) de un almacen de datos NAS, mientras que las operaciones en máquinas virtuales activas (clonado y vMotion de almacenamiento) también se descargan

para SAN. ONTAP utiliza el método más eficaz basado en el origen y el destino. Esta capacidad también es utilizada por "[OmniSSA Horizon View](#)".

- SRA (utilizado con Live Site Recovery/Site Recovery Manager de VMware). Aquí, se utilizan clones para probar la recuperación de la réplica de recuperación ante desastres de forma no disruptiva.
- Backup y recuperación de datos con herramientas de NetApp como SnapCenter. Los clones de máquinas virtuales se utilizan para verificar las operaciones de backup, así como para montar un backup de equipo virtual para poder restaurar los archivos individuales.

El clonado descargado de ONTAP puede invocarse con VMware, NetApp y herramientas de terceros. Los clones que se descargan en ONTAP tienen varias ventajas. Ofrecen una gestión eficiente del espacio en la mayoría de los casos, y necesitan almacenamiento solo para los cambios en el objeto; no hay ningún efecto adicional en el rendimiento para leerlos y escribirlos; en algunos casos, el rendimiento mejora si se comparten los bloques en las cachés de alta velocidad. También descargan los ciclos de CPU y las operaciones de I/o de red del servidor ESXi. La copia de datos descargados dentro de un almacén de datos tradicional utilizando un FlexVol volume puede ser rápida y eficiente con licencia de FlexClone (incluida en la licencia ONTAP One), pero las copias entre volúmenes FlexVol pueden ser más lentas. Si mantiene las plantillas de equipos virtuales como origen de los clones, considere colocarlas en el volumen del almacén de datos (utilice carpetas o bibliotecas de contenido para organizarlas) para lograr clones rápidos con un uso eficiente del espacio.

También es posible clonar un volumen o LUN directamente en ONTAP para clonar un almacén de datos. Con almacenes de datos NFS, la tecnología FlexClone puede clonar un volumen completo, y el clon se puede exportar desde ONTAP y montar en ESXi como otro almacén de datos. En almacenes de datos VMFS, ONTAP puede clonar una LUN dentro de un volumen o un volumen entero, incluida una o varias LUN dentro de él. Una LUN que contiene un VMFS debe asignarse a un iGroup de ESXi y, a continuación, volver a firmar la bandeja de ESXi para que se monte y utilice como almacén de datos normal. Para algunos casos de uso temporales, se puede montar un VMFS clonado sin renuncias. Una vez que se ha clonado un almacén de datos, los equipos virtuales del interior se pueden registrar, volver a configurar y personalizar como si se clonaran individualmente.

En algunos casos, se pueden utilizar otras funciones con licencia para mejorar la clonación, como SnapRestore para backup o FlexClone. Estas licencias se incluyen a menudo en los paquetes de licencias sin coste adicional. Se necesita una licencia de FlexClone para las operaciones de clonado de VVol, así como para admitir Snapshot gestionadas de un VVol (que se descargan del hipervisor a ONTAP). Una licencia de FlexClone también puede mejorar ciertos clones basados en VAAI cuando se usan en un almacén de datos/volumen (crea copias instantáneas con gestión eficiente del espacio en lugar de copias de bloques). El SRA también usa para probar la recuperación de una réplica de DR, y el SnapCenter para las operaciones de clonado y para buscar copias de backup para restaurar archivos individuales.

## Protección de datos

El backup y la recuperación rápida de sus máquinas virtuales son ventajas clave de usar ONTAP para vSphere. Esta funcionalidad se puede gestionar fácilmente dentro de vCenter mediante el complemento SnapCenter para VMware vSphere. Muchos clientes mejoran sus soluciones de backup de terceros con SnapCenter para aprovechar la tecnología Snapshot de ONTAP, ya que ofrece la forma más rápida y sencilla de recuperar una máquina virtual con ONTAP. SnapCenter está disponible de forma gratuita para los clientes que tengan la licencia ONTAP One, mientras que otros paquetes de licencia también pueden estar disponibles.

Además, el complemento SnapCenter para VMware puede integrarse con "[NetApp Backup and Recovery para máquinas virtuales](#)", lo que permite soluciones de respaldo efectivas 3-2-1 para la mayoría de los sistemas ONTAP. Tenga en cuenta que pueden aplicarse algunas tarifas si utiliza Backup and Recovery para máquinas

virtuales con servicios premium, como almacenes de objetos para almacenamiento de respaldo adicional. En esta sección se describen las distintas opciones disponibles para proteger sus máquinas virtuales y almacenes de datos.

## Snapshots de volumen de NetApp ONTAP

Use copias Snapshot para realizar copias rápidas de sus máquinas virtuales o almacenes de datos sin afectar al rendimiento y, a continuación, envíelas a un sistema secundario usando SnapMirror para la protección de datos fuera del sitio a largo plazo. Este método minimiza el espacio de almacenamiento y el ancho de banda de red porque solo almacena la información modificada.

Las copias Snapshot son una función clave de ONTAP, que le permite crear copias de un momento específico de sus datos. Permiten una gestión eficiente del espacio y se pueden crear rápidamente, por lo que son ideales para proteger equipos virtuales y almacenes de datos. Las copias Snapshot pueden utilizarse para distintos fines, como backup, recuperación de datos y pruebas. Estas copias Snapshot son diferentes de las copias snapshot de VMware (coherencia) y son adecuadas para la protección a largo plazo. Las copias Snapshot gestionadas con vCenter de VMware solo se recomiendan para su uso a corto plazo debido al rendimiento y otros efectos. Consulte ["Limitaciones de Snapshot"](#) si desea obtener más información.

Las snapshots se crean a nivel de volumen, y se pueden usar para proteger todas las máquinas virtuales y los almacenes de datos que hay en ese volumen. Esto significa que puede crear una copia de Snapshot de todo un almacén de datos, lo que incluye todas las máquinas virtuales que contiene.

En almacenes de datos NFS, puede ver fácilmente archivos de máquinas virtuales en snapshots navegando por el directorio .snapshots. De este modo, puede acceder rápidamente a ficheros y restaurarlos desde una instantánea sin necesidad de utilizar una solución de backup específica.

Para los almacenes de datos VMFS, se puede crear un FlexClone del almacén de datos a partir de la snapshot que desee. Esto permite crear un nuevo almacén de datos que esté basado en la snapshot, que se puede usar con fines de prueba o desarrollo. La FlexClone solo consumirá espacio para los cambios realizados después de realizar la snapshot, por lo que constituye una forma con gestión eficiente del espacio de crear una copia del almacén de datos. Una vez creada la FlexClone, puede asignar el LUN o el espacio de nombres a un host ESXi, como un almacén de datos normal. Esto no solo permite restaurar archivos específicos de equipos virtuales, sino que también le permite crear rápidamente entornos de prueba o desarrollo basados en datos de producción sin que el rendimiento del entorno de producción se vea afectado.

Para obtener más información sobre las instantáneas, consulte la documentación de ONTAP. Los siguientes enlaces proporcionan detalles adicionales: ["Copias Snapshot locales de ONTAP"](#) ["Flujo de trabajo de replicación de SnapMirror de ONTAP"](#)

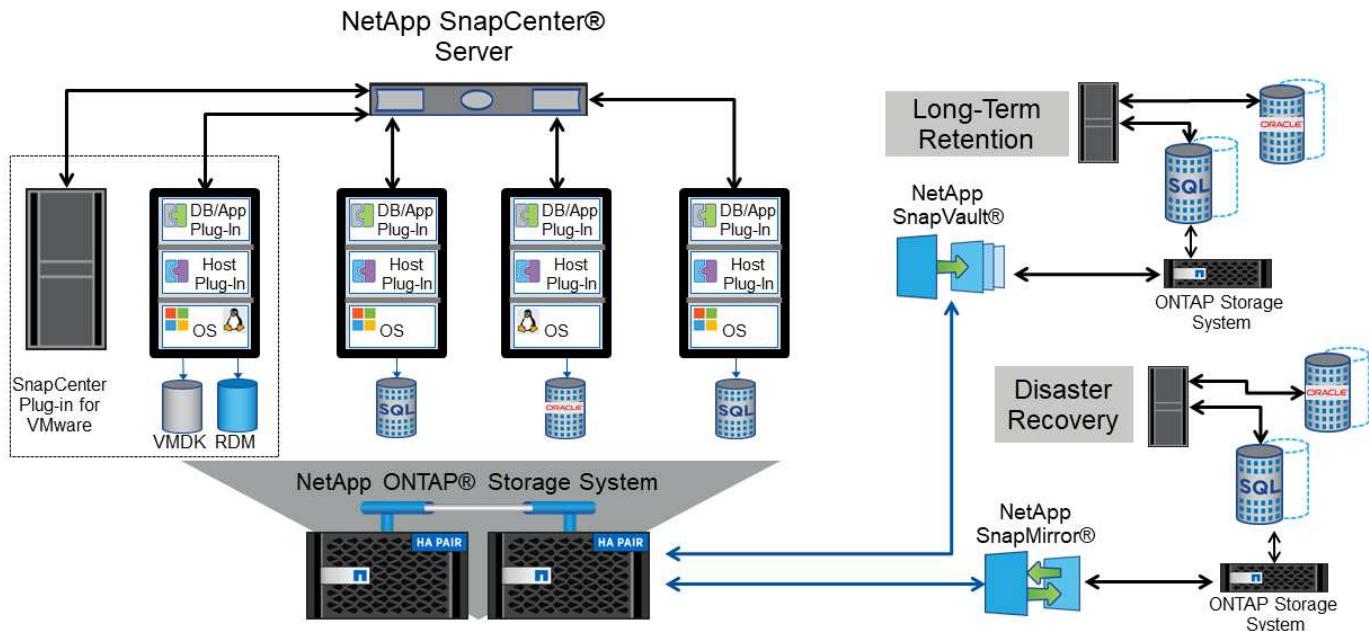
## Complemento de SnapCenter para VMware vSphere

SnapCenter permite crear políticas de backup que se pueden aplicar a varias tareas. Estas políticas pueden definir programaciones, retención, replicación y otras funcionalidades. Continúan permitiendo una selección opcional de snapshots consistentes con las máquinas virtuales, lo que aprovecha la capacidad del hipervisor para poner en modo inactivo las operaciones de I/O antes de tomar una snapshot de VMware. Sin embargo, debido al efecto sobre el rendimiento de las snapshots de VMware, generalmente no se recomiendan a menos que necesite que el sistema de archivos invitados se coloque en modo inactivo. En su lugar, utilice los snapshots para protección general y use herramientas de aplicaciones como los complementos de aplicaciones de SnapCenter para proteger los datos transaccionales, como SQL Server u Oracle.

Estos complementos ofrecen funcionalidades ampliadas para proteger las bases de datos tanto en entornos físicos como virtuales. Con vSphere, puede utilizarlos para proteger bases de datos de SQL Server u Oracle donde los datos se almacenan en LUN de RDM, vVols o espacios de nombres NVMe/TCP y LUN iSCSI directamente conectados al sistema operativo invitado o archivos VMDK en almacenes de datos VMFS o

NFS. Estos plugins permiten especificar distintos tipos de backups de bases de datos, ya sea compatible con backups en línea o sin conexión, y proteger archivos de base de datos junto con archivos de registro. Además de backup y recuperación de datos, los plugins también admiten la clonado de bases de datos para fines de prueba o desarrollo.

En la siguiente figura se muestra un ejemplo de la instalación de SnapCenter.



Para obtener información sobre el tamaño, consulte la ["Guía de configuración del complemento de SnapCenter para VMware vSphere"](#)

### Herramientas de ONTAP para VMware vSphere con VMware Live Site Recovery

Las herramientas de ONTAP para VMware vSphere (OT4VS) son un complemento gratuito que proporciona una integración sin problemas entre VMware vSphere y NetApp ONTAP. Le permite gestionar el almacenamiento de ONTAP directamente desde vSphere Web Client, lo que facilita la realización de tareas como el aprovisionamiento del almacenamiento, la gestión de la replicación y la supervisión del rendimiento.

Para funcionalidades mejoradas de recuperación ante desastres, considere el uso del SRA de NetApp para ONTAP, que forma parte de las herramientas de ONTAP para VMware vSphere, junto con Live Site Recovery de VMware (antes conocido como Site Recovery Manager). Esta herramienta no solo admite la replicación de almacenes de datos a un sitio de recuperación ante desastres mediante SnapMirror, sino que también permite realizar pruebas no disruptivas en el entorno de recuperación ante desastres mediante el clonado de los almacenes de datos replicados. Además, la recuperación tras un desastre y la reprotectación de la producción después de resolver una interrupción del servicio se optimiza gracias a las funciones de automatización integradas.

### NetApp Disaster Recovery

Disaster Recovery (DR) es un servicio basado en la nube que proporciona una solución integral para proteger sus datos y aplicaciones en caso de desastre. Ofrece una variedad de funciones, que incluyen comutación por error y recuperación automatizadas, múltiples puntos de recuperación en un momento determinado, recuperación ante desastres consistente con las aplicaciones y soporte para sistemas ONTAP locales y basados en la nube. NetApp Disaster Recovery está diseñado para funcionar sin problemas con ONTAP y su entorno VMware vSphere, proporcionando una solución unificada para la recuperación ante desastres.

## **vSphere Metro Storage Cluster (VMSC) con sincronización activa NetApp MetroCluster y SnapMirror**

Por último, para obtener el nivel más elevado de protección de datos, considere la configuración de clúster de almacenamiento Metro (VMSC) vSphere de VMware con NetApp MetroCluster. VMSC es una solución compatible con NetApp certificada por VMware que utiliza replicación síncrona, lo que le ofrece las mismas ventajas de un clúster de alta disponibilidad pero distribuido en diferentes ubicaciones para protegerse frente a desastres en el sitio. NetApp SnapMirror Active Sync, con ASA y AFF y MetroCluster con AFF, ofrece configuraciones rentables para replicación síncrona con recuperación transparente desde cualquier fallo de componente de almacenamiento individual así como recuperación transparente en el caso de sincronización activa de SnapMirror o recuperación con un único comando en caso de desastre en el centro con MetroCluster. ["CONSULTE TR-4128"](#)

## **Calidad de servicio (QoS)**

Los límites de rendimiento son útiles para controlar los niveles de servicio, gestionar cargas de trabajo desconocidas o probar las aplicaciones antes de la puesta en marcha para asegurarse de que no afecten a otras cargas de trabajo en la producción. También se pueden utilizar para limitar una carga de trabajo abusivas una vez que se identifica.

### **Compatibilidad con las políticas de calidad de servicio de ONTAP**

Los sistemas que ejecutan ONTAP pueden utilizar la función de calidad de servicio del almacenamiento para limitar el rendimiento en MB/s y/o I/O por segundo (IOPS) para diferentes objetos de almacenamiento, como archivos, LUN, volúmenes o SVM completas.

También admite niveles mínimos de servicio basados en IOPS para proporcionar un rendimiento constante para los objetos SAN en ONTAP 9.2 y para los objetos NAS en ONTAP 9.3.

El límite máximo de rendimiento de calidad de servicio en un objeto se puede establecer en Mbps o IOPS. Si se utilizan ambos, ONTAP aplica el primer límite alcanzado. Una carga de trabajo puede contener varios objetos y una política de calidad de servicio se puede aplicar a una o más cargas de trabajo. Cuando se aplica una política a varias cargas de trabajo, las cargas de trabajo comparten el límite total de la política. No se admiten los objetos anidados (por ejemplo, los archivos de un volumen no pueden tener cada uno su propia política). Los valores mínimos de calidad de servicio solo se pueden establecer en IOPS.

Las siguientes herramientas están disponibles en este momento para gestionar las políticas de calidad de servicio de ONTAP y aplicarlas a los objetos:

- CLI de ONTAP
- System Manager de ONTAP
- OnCommand Workflow Automation
- Active IQ Unified Manager
- Kit de herramientas NetApp PowerShell para ONTAP
- Herramientas de ONTAP para VASA Provider de VMware vSphere

Para asignar una normativa de calidad de servicio a un LUN, incluidos VMFS y RDM, la SVM de ONTAP (mostrada como Vserver), la ruta de LUN y el número de serie pueden obtenerse en el menú sistemas de almacenamiento de la página de inicio de ONTAP Tools para VMware vSphere. Seleccione el sistema de almacenamiento (SVM) y, a continuación, Related Objects > SAN. Use este enfoque cuando especifique la calidad de servicio mediante una de las herramientas de ONTAP.

Consulte ["Información general sobre la gestión y el control del rendimiento"](#) si quiere más información.

## Almacenes de datos NFS sin vVols

Una política de calidad de servicio de ONTAP puede aplicarse a todo el almacén de datos o archivos VMDK individuales que contiene. Sin embargo, es importante entender que todas las máquinas virtuales de un almacén de datos NFS tradicional (sin vVols) comparten una cola de I/O común desde un host determinado. Si alguna máquina virtual está regulada por una política de calidad de servicio de ONTAP, esta opción, en la práctica, provoca que todas las operaciones de I/O de ese almacén de datos parezcan aceleradas para ese host.

### Ejemplo:

- \* Se configura un límite de QoS en vm1.vmdk para un volumen que se monta como almacén de datos NFS tradicional mediante el host esxi-01.
- \* El mismo host (esxi-01) está usando vm2.vmdk y está en el mismo volumen.
- \* Si vm1.vmdk se acelera, entonces vm2.vmdk también parecerá estar estrangulado ya que comparte la misma cola de IO con vm1.vmdk.



Esto no se aplica a vVols.

A partir de vSphere 6,5, puede gestionar los límites granulares de archivos en almacenes de datos que no son vVols aprovechando la gestión basada en políticas de almacenamiento (SPBM) con Storage I/O Control (SIOC) v2.

Consulte los siguientes enlaces para obtener más información sobre la gestión del rendimiento con las políticas de SIOC y SPBM.

["Reglas basadas en host de SPBM: SIOC v2"](#)

["Gestione los recursos de I/O de almacenamiento con vSphere"](#)

Para asignar una política de calidad de servicio a un VMDK en NFS, tenga en cuenta las siguientes directrices:

- La política debe aplicarse a la `vmname-flat.vmdk` que contiene la imagen del disco virtual real, no la `vmname.vmdk` (archivo de descriptor de disco virtual) o. `vmname.vmx` (Archivo descriptor de máquina virtual).
- No aplique políticas a otros archivos del equipo virtual, como archivos de intercambio virtual (`vmname.vswp`).
- Cuando utilice el cliente web de vSphere para buscar rutas de archivos (Datastore > Files), tenga en cuenta que combina la información del `- flat.vmdk` y `.. vmdk` y simplemente muestra un archivo con el nombre del `. vmdk` pero el tamaño del `- flat.vmdk`. Agregar `-flat` en el nombre del archivo para obtener la ruta correcta.

Los almacenes de datos de FlexGroup ofrecen funcionalidades de calidad de servicio mejoradas al usar las herramientas de ONTAP para VMware vSphere 9.8 y versiones posteriores. Puede establecer fácilmente la calidad de servicio en todas las máquinas virtuales de un almacén de datos o en máquinas virtuales específicas. Consulte la sección FlexGroup de este informe para obtener más información. Tenga en cuenta que se siguen aplicando las limitaciones de la calidad de servicio mencionadas anteriormente con almacenes de datos NFS tradicionales.

## Almacenes de datos de VMFS

Al usar los LUN de ONTAP, las políticas de calidad de servicio se pueden aplicar al volumen de FlexVol que contiene los LUN o los LUN individuales, pero no archivos VMDK individuales, ya que ONTAP no es consciente del sistema de archivos VMFS.

## Almacenes de datos de vVols

La calidad de servicio mínima o máxima se puede establecer fácilmente en máquinas virtuales o VMDK individuales sin que ello afecte a ningún otro equipo virtual o VMDK gracias a la gestión basada en políticas de almacenamiento y vVols.

Al crear el perfil de funcionalidad de almacenamiento para el contenedor de VVol, especifique un valor de IOPS máximo y/o mínimo con la funcionalidad de rendimiento y, a continuación, haga referencia a este SCP con la política de almacenamiento de la máquina virtual. Use esta política cuando cree la máquina virtual o aplique la política a una máquina virtual existente.



VVols requiere el uso de herramientas de ONTAP para VMware vSphere, que funciona como proveedor VASA para ONTAP. Consulte "["VMware vSphere Virtual Volumes \(vVols\) con ONTAP"](#) para ver las prácticas recomendadas de vVols.

## ONTAP QoS y VMware SIOC

La calidad de servicio de ONTAP y el control de I/O de almacenamiento de VMware vSphere (SIOC) son tecnologías complementarias que los administradores de vSphere y de almacenamiento pueden utilizar conjuntamente para gestionar el rendimiento de las máquinas virtuales de vSphere alojadas en sistemas que ejecutan ONTAP. Cada herramienta tiene sus propias fuerzas, como se muestra en la siguiente tabla. Debido a los distintos ámbitos de VMware vCenter y ONTAP, algunos objetos pueden verse y gestionarse mediante un sistema, no el otro.

| Propiedad   | Calidad de servicio de ONTAP   | VMware SIOC  |
|---|--|--|
| Cuando está activo  | La directiva está siempre activa   | Activo cuando existe una contención (latencia por encima del umbral de los almacenes de datos) |
| Tipo de unidades  | IOPS, Mbps   | IOPS, recursos compartidos   |
| Alcance de vCenter o aplicaciones                                     | Varios entornos de vCenter, otros hipervisores y aplicaciones  | Un único servidor vCenter  |
| ¿Establecer QoS en la máquina virtual?                                | VMDK solo en NFS   | VMDK en NFS o VMFS   |
| ¿Establecer QoS en el LUN (RDM)?                                      | Sí   | No   |
| ¿Configurar QoS en LUN (VMFS)?  | Sí   | Sí (el almacén de datos puede acelerarse)  |
| ¿Configurar calidad de servicio en el volumen (almacén de datos NFS)? | Sí   | Sí (el almacén de datos puede acelerarse)  |
| ¿Configurar la calidad de servicio en SVM (inquilino)?                | Sí   | No   |
| ¿Enfoque basado en políticas?   | Sí, pueden compartirse todas las cargas de trabajo de la política o aplicarse por completo a cada carga de trabajo de la política. | Sí, con vSphere 6.5 y posterior.   |
| Se requiere licencia  | Incluido con ONTAP   | Enterprise Plus  |

## Planificador de recursos distribuidos de almacenamiento de VMware

El planificador de recursos distribuidos de almacenamiento (SDRS) de VMware es una función de vSphere que coloca los equipos virtuales en el almacenamiento en función de la latencia de I/o actual y el uso del espacio. A continuación, mueve la máquina virtual o los VMDK de forma no disruptiva entre los almacenes de datos de un clúster de almacenes de datos (también conocido como "pod"), seleccionando el mejor almacén de datos en el que colocar la máquina virtual o los VMDK en el clúster de almacenes de datos. Un clúster de almacenes de datos es una colección de almacenes de datos similares que se agregan en una única unidad de consumo desde la perspectiva del administrador de vSphere.

Cuando se usan SDRS con herramientas de ONTAP para VMware vSphere, primero debe crear un almacén de datos con el plugin, utilizar vCenter para crear el clúster de almacén de datos y, a continuación, añadir el almacén de datos. Una vez creado el clúster de almacenes de datos, es posible añadir almacenes de datos adicionales al clúster de almacenes de datos directamente desde el asistente de aprovisionamiento de la página Details.

Otras prácticas recomendadas de ONTAP para SDRS incluyen lo siguiente:

- Todos los almacenes de datos del clúster deben usar el mismo tipo de almacenamiento (como SAS, SATA o SSD), ser todos los almacenes de datos VMFS o NFS y tener la misma configuración de replicación y protección.
- Considere el uso de SDR en modo predeterminado (manual). Este enfoque permite revisar las recomendaciones y decidir si se aplican o no. Tenga en cuenta los siguientes efectos de las migraciones de VMDK:
  - Cuando SDRS mueve VMDK entre almacenes de datos, se pierde cualquier ahorro de espacio con la clonado o deduplicación de ONTAP. Puede volver a ejecutar la deduplicación para recuperar este ahorro.
  - Después de que SDRS mueva los VMDK, NetApp recomienda volver a crear las snapshots en el almacén de datos de origen porque el espacio se bloqueará por la máquina virtual que se movió.
  - Mover VMDK entre almacenes de datos en el mismo agregado tiene pocas ventajas y LOS SDRS no tienen visibilidad en otras cargas de trabajo que puedan compartir el agregado.

## Gestión basada en políticas de almacenamiento y vVols

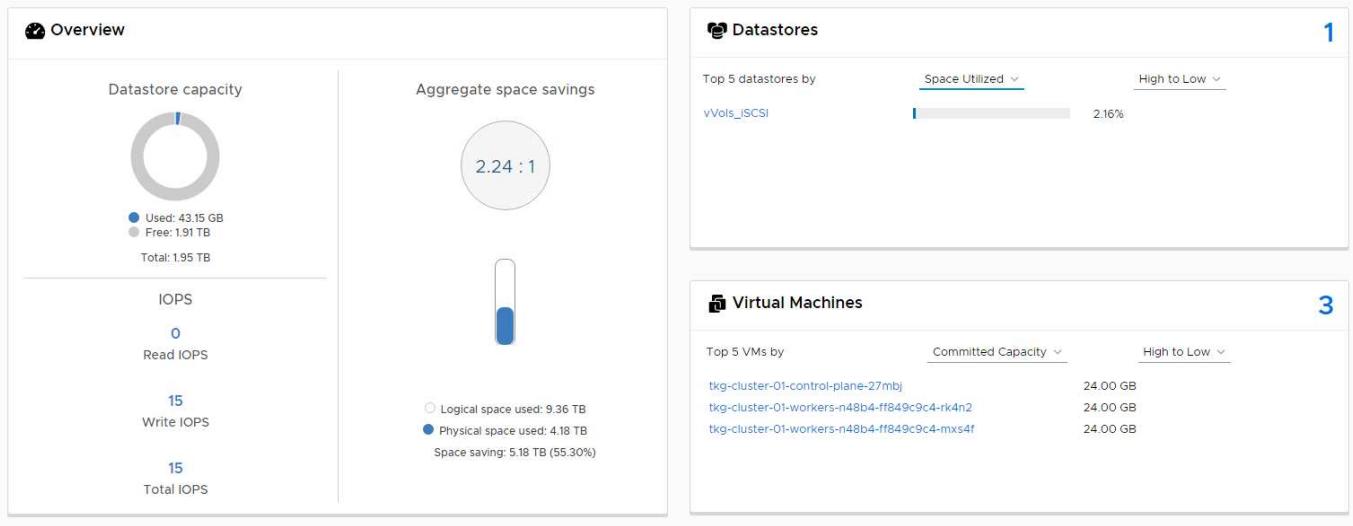
Las API de VMware vSphere para el reconocimiento del almacenamiento (VASA) facilitan que un administrador de almacenamiento configure almacenes de datos con funcionalidades bien definidas y permiten que el administrador de equipos virtuales los utilice siempre que sea necesario para aprovisionar máquinas virtuales sin tener que interactuar entre sí. Merece la pena echar un vistazo a este enfoque para ver cómo puede optimizar sus operaciones de almacenamiento de virtualización y evitar un gran trabajo trivial.

Antes de VASA, los administradores de máquinas virtuales podían definir políticas de almacenamiento de máquinas virtuales, pero tenían que trabajar con el administrador de almacenamiento para identificar los almacenes de datos adecuados, a menudo usando documentación o convenciones de nomenclatura. Con VASA, el administrador de almacenamiento puede definir una serie de capacidades de almacenamiento, como el rendimiento, la clasificación por niveles, el cifrado y la replicación. Un conjunto de funcionalidades para un volumen o un conjunto de volúmenes se denomina perfil de capacidad de almacenamiento (SCP).

El SCP admite QoS mínimo y/o máximo para los vVols de datos de una VM. La calidad de servicio mínima solo se admite en los sistemas AFF. Las herramientas de ONTAP para VMware vSphere incluyen una consola donde se muestra el rendimiento granular de máquinas virtuales y la capacidad lógica para vVols en sistemas ONTAP.

La siguiente figura muestra las herramientas de ONTAP para el panel de vVols de VMware vSphere 9.8.

ⓘ The dashboard displays IOPS, latency, throughput, and logical space values obtained from ONTAP.



Una vez definido el perfil de funcionalidad de almacenamiento, puede utilizarse para aprovisionar equipos virtuales mediante la normativa de almacenamiento que identifique sus requisitos. La asignación entre la política de almacenamiento de máquinas virtuales y el perfil de capacidad de almacenamiento de almacenes de datos permite que vCenter muestre una lista de almacenes de datos compatibles que podrá seleccionar. Este enfoque se conoce como gestión basada en políticas de almacenamiento.

VASA proporciona la tecnología para consultar el almacenamiento y devolver un conjunto de funcionalidades de almacenamiento a vCenter. Los proveedores de VASA proporcionan la traducción entre las API y construcciones del sistema de almacenamiento y las API de VMware que comprende vCenter. VASA Provider de NetApp para ONTAP se ofrece como parte de las herramientas de ONTAP para VM del dispositivo VMware vSphere. El complemento de vCenter proporciona la interfaz para aprovisionar y gestionar almacenes de datos VVOL, así como la capacidad para definir perfiles de capacidades de almacenamiento (SCPs).

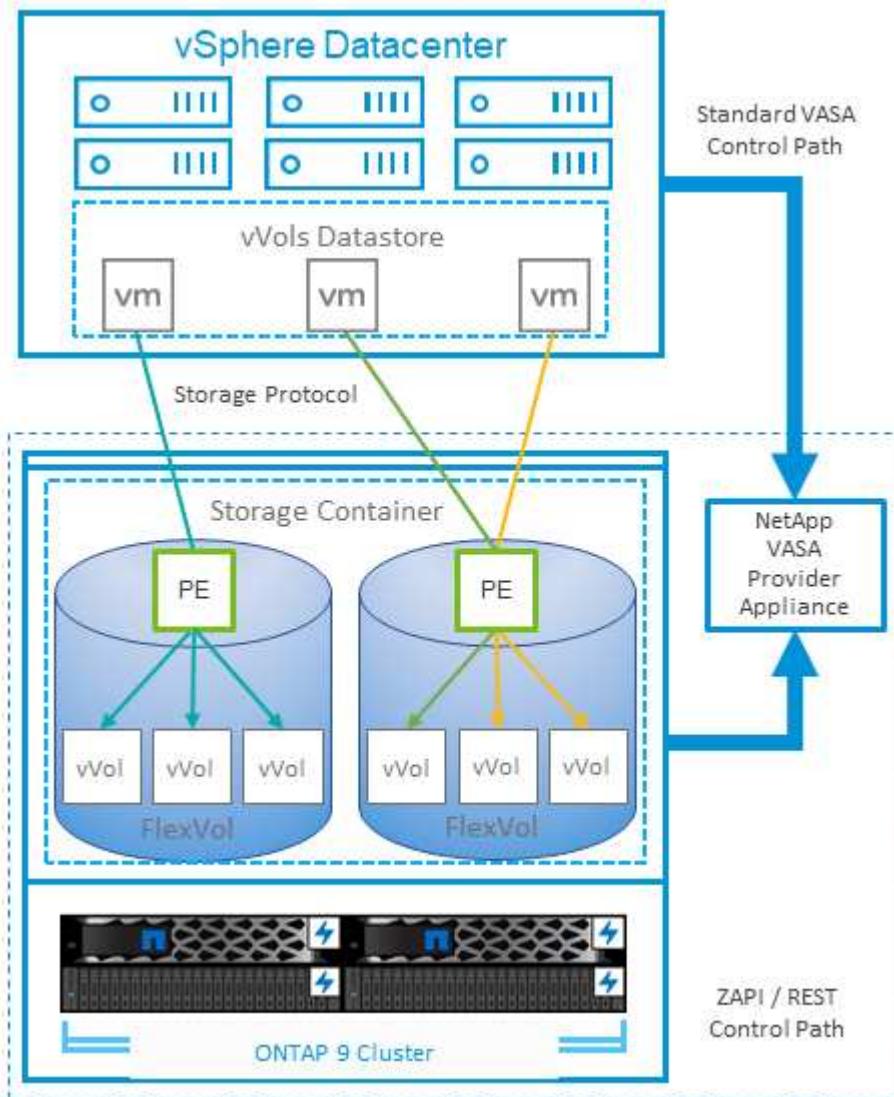
ONTAP admite almacenes de datos de VVol tanto VMFS como NFS. El uso de vVols con almacenes DE datos SAN aporta algunas de las ventajas de NFS, como la granularidad a nivel de equipo virtual. Aquí encontrará algunas prácticas recomendadas para tener en cuenta y información adicional en ["CONSULTE TR-4400"](#):

- Un almacén de datos de VVol puede consistir en varios volúmenes de FlexVol en varios nodos de clúster. El método más sencillo es un único almacén de datos, incluso cuando los volúmenes tienen diferentes funcionalidades. SPBM garantiza que se utiliza un volumen compatible para la máquina virtual. Sin embargo, todos los volúmenes deben formar parte de una única SVM de ONTAP y se debe acceder a ellos mediante un único protocolo. Un LIF por nodo para cada protocolo es suficiente. Evite el uso de varias versiones de ONTAP en un único almacén de datos de VVol, ya que las funcionalidades de almacenamiento pueden variar entre las versiones.
- Utilice las herramientas de ONTAP para el plugin de VMware vSphere para crear y gestionar almacenes de datos de VVol. Además de gestionar el almacén de datos y su perfil, crea automáticamente un extremo de protocolo para acceder a vVols, si es necesario. Si se utilizan LUN, tenga en cuenta que los extremos de protocolo de LUN se asignan mediante los ID de LUN 300 y posteriores. Compruebe que la opción de configuración del sistema avanzado del host ESXi Disk.MaxLUN Permite un número de ID de LUN que sea mayor que 300 (el valor predeterminado es 1,024). Para realizar este paso, seleccione el host ESXi en vCenter, después la pestaña Configure y busque Disk.MaxLUN En la lista Advanced System Settings.
- No instale ni migre VASA Provider, vCenter Server (basado en dispositivos o Windows) ni las herramientas

de ONTAP para VMware vSphere en un almacén de datos vVols, ya que estos dependen mutuamente, lo cual limita la capacidad de gestionarlos en caso de una interrupción del suministro eléctrico u otra interrupción del centro de datos.

- Realice un backup regular de la máquina virtual del proveedor de VASA. Como mínimo, cree copias Snapshot por hora del almacén de datos tradicional que contenga VASA Provider. Para obtener más información sobre la protección y recuperación del proveedor de VASA, consulte este tema ["Artículo de base de conocimientos"](#).

La siguiente figura muestra los componentes de vVols.



## Migración al cloud y backup

Otra ventaja de ONTAP es la amplia compatibilidad con el cloud híbrido, al fusionar sistemas en el cloud privado local con funcionalidades de cloud público. Estas son algunas de las soluciones cloud de NetApp que se pueden usar junto con vSphere:

- Ofertas de primera mano.** Amazon FSx for NetApp ONTAP, Google Cloud NetApp Volumes y Azure NetApp Files proporcionan servicios de almacenamiento administrados de múltiples protocolos y alto rendimiento en los principales entornos de nube pública. VMware Cloud on AWS (VMC on AWS), Azure VMware Solution (AVS) y Google Cloud VMware Engine (GCVE) pueden usarlos directamente como

almacenes de datos o almacenamiento para sistemas operativos invitados (GOS) e instancias de cómputo.

- **Servicios en la nube.** Utilice NetApp Backup and Recovery o SnapMirror Cloud para proteger datos de sistemas locales mediante almacenamiento en la nube pública. NetApp Copy and Sync ayuda a migrar y mantener sus datos sincronizados en NAS y almacenes de objetos. NetApp Disaster Recovery ofrece una solución rentable y eficiente para aprovechar las tecnologías de NetApp como base para una solución de recuperación ante desastres robusta y capaz para DR en la nube, DR en las instalaciones locales y de las instalaciones locales a las instalaciones locales.
- **FabricPool.** FabricPool ofrece una organización en niveles rápida y fácil para los datos de ONTAP. Los bloques inactivos se pueden migrar a un almacén de objetos en clouds públicos o en un almacén de objetos de StorageGRID privado y se recuerdan automáticamente cuando se vuelve a acceder a los datos de ONTAP. También puede usar el nivel de objeto como un tercer nivel de protección para los datos que ya está gestionado por SnapVault. Este enfoque le permite ["Almacenar más snapshots de sus máquinas virtuales"](#) En sistemas de almacenamiento ONTAP principales o secundarios
- **ONTAP Select.** Utilice el almacenamiento definido por software de NetApp para ampliar su cloud privado a través de Internet a instalaciones y oficinas remotas, donde puede utilizar ONTAP Select para ofrecer compatibilidad con servicios de bloques y archivos, así como las mismas funcionalidades de gestión de datos vSphere que tiene en su centro de datos empresarial.

Al diseñar sus aplicaciones basadas en máquinas virtuales, tenga en cuenta la movilidad futura en la nube. Por ejemplo, en lugar de colocar los archivos de aplicaciones y datos juntos, utilice una exportación LUN o NFS separada para los datos. Esto le permite migrar la máquina virtual y los datos por separado a los servicios en la nube.

Para obtener una visión más detallada de más temas de seguridad, consulte los siguientes recursos.

- ["Documentación de ONTAP Select"](#)
- ["Documentación de copia de seguridad y recuperación"](#)
- ["Documentación de recuperación ante desastres"](#)
- ["Amazon FSX para ONTAP de NetApp"](#)
- ["VMware Cloud en AWS"](#)
- ["¿Qué es Azure NetApp Files?"](#)
- ["Solución Azure VMware"](#)
- ["Motor de Google Cloud VMware"](#)
- ["¿Qué es Google Cloud NetApp Volumes?"](#)

## Cifrado para datos de vSphere

Hoy en día, hay cada vez más demandas de protección de los datos en reposo mediante el cifrado. Aunque el foco inicial era la información financiera y de atención sanitaria, existe un creciente interés en proteger toda la información, ya sea en archivos, bases de datos u otros tipos de datos.

Los sistemas que ejecutan ONTAP facilitan la protección de cualquier dato con cifrado en reposo. El cifrado de almacenamiento de NetApp (NSE) utiliza unidades de autocifrado (SED) con ONTAP para proteger los datos SAN y NAS. NetApp también ofrece el cifrado de volúmenes de NetApp y el cifrado de agregados de NetApp como un método sencillo basado en software para cifrar volúmenes en cualquier unidad de disco. Este cifrado de software no requiere unidades de disco especiales ni gestores de claves externos y está disponible para los clientes de ONTAP sin coste adicional. Puede actualizarla y empezar a utilizarla sin interrumpir la actividad

de sus clientes o aplicaciones, y están validados según el estándar FIPS 140-2 de nivel 1, incluido el gestor de claves incorporado.

Existen varios métodos para proteger los datos de las aplicaciones virtualizadas que se ejecutan en VMware vSphere. Uno de los métodos consiste en proteger los datos con software dentro de los equipos virtuales a nivel de SO «guest». Los hipervisores más recientes, como vSphere 6.5, ahora admiten el cifrado a nivel de equipo virtual como otra alternativa. Sin embargo, el cifrado del software de NetApp es simple y fácil y tiene estas ventajas:

- **Sin efecto sobre la CPU del servidor virtual.** algunos entornos de servidor virtual necesitan todos los ciclos de CPU disponibles para sus aplicaciones, aunque las pruebas han demostrado que se necesitan hasta 5 veces los recursos de CPU con cifrado a nivel de hipervisor. Incluso si el software de cifrado admite el conjunto de instrucciones AES-NI de Intel para descargar la carga de trabajo de cifrado (como lo hace el cifrado de software NetApp), este enfoque podría no ser factible debido a la necesidad de nuevas CPU que no son compatibles con servidores antiguos.
- **Onboard Key Manager incluido.** El cifrado de software de NetApp incluye un gestor de claves incorporado sin coste adicional, lo que facilita empezar sin servidores de gestión de claves de alta disponibilidad complejos de adquirir y utilizar.
- **No afecta a la eficiencia del almacenamiento.** las técnicas de eficiencia del almacenamiento como la deduplicación y la compresión se utilizan ampliamente hoy en día y son clave para utilizar medios de disco flash de forma rentable. Sin embargo, por lo general, los datos cifrados no se pueden deduplicar o comprimir. El cifrado de almacenamiento y hardware de NetApp funciona a un nivel inferior y permite el uso completo de funciones de eficiencia del almacenamiento de NetApp, líderes del sector, a diferencia de otros métodos.
- **Cifrado granular sencillo del almacén de datos.** con el cifrado de volúmenes de NetApp, cada volumen obtiene su propia clave AES de 256 bits. Si necesita cambiarlo, puede hacerlo con un solo comando. Este método es genial si tiene varios clientes o necesita probar el cifrado independiente para diferentes departamentos o aplicaciones. Este cifrado se gestiona a nivel de almacén de datos, lo cual es mucho más fácil que gestionar equipos virtuales individuales.

Es fácil empezar a utilizar el cifrado de software. Una vez instalada la licencia, solo tiene que configurar el administrador de claves incorporado especificando una clave de acceso y, a continuación, crear un volumen nuevo o mover un volumen del lado del almacenamiento para habilitar el cifrado. NetApp está trabajando para añadir compatibilidad más integrada con funcionalidades de cifrado en futuros lanzamientos de sus herramientas de VMware.

Para obtener una visión más detallada de más temas de seguridad, consulte los siguientes recursos.

- "[Informes técnicos de seguridad](#)"
- "[Guías de refuerzo de seguridad](#)"
- "[Documentación de productos de seguridad y cifrado de datos de ONTAP](#)"

## Active IQ Unified Manager

Active IQ Unified Manager proporciona visibilidad de los VM en su infraestructura virtual y permite supervisar y solucionar los problemas de almacenamiento y rendimiento en su entorno virtual.

Una infraestructura virtual típica puesta en marcha en ONTAP tiene diversos componentes que se distribuyen en las capas informática, de red y de almacenamiento. Cualquier retraso en el rendimiento de una aplicación de equipo virtual puede producirse debido a una combinación de latencias que deben afrontar los distintos componentes de las capas respectivas.

La siguiente captura de pantalla muestra la vista Máquinas virtuales de Active IQ Unified Manager.

Virtual Machines

| Name     | Status | Power State | Protocol | Capacity (Used   Allocated) | 4 IOPS | VM Latency (ms) | Host IOPS | Host Latency (ms) | Network Latency (ms) | Datastore IOPS | Datastore Latency (ms) |
|----------|--------|-------------|----------|-----------------------------|--------|-----------------|-----------|-------------------|----------------------|----------------|------------------------|
| vCenter7 | ON     | NFS         |          | 160 GB   712 GB             | 183    | 0               | 243       | 0                 | 0                    | 831            | 0.3                    |

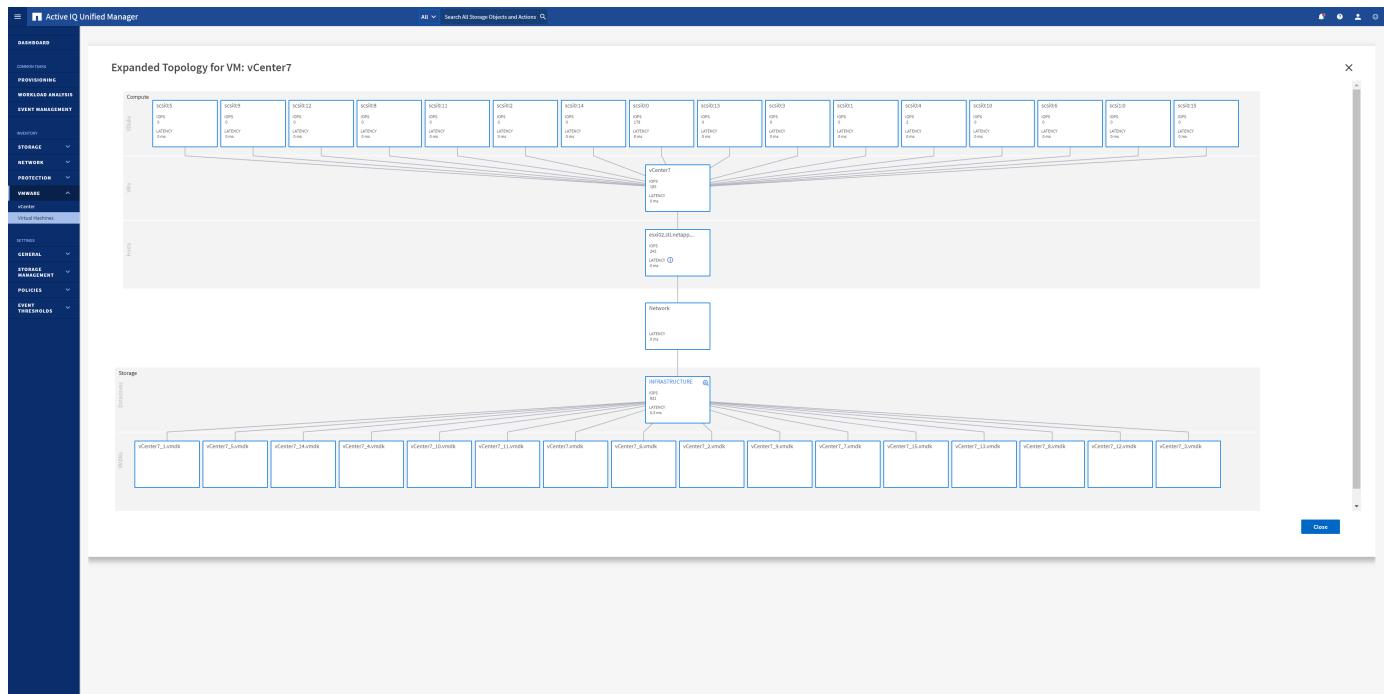
POWER: ON

TOPOLOGY VIEW

Showing all 44 Virtual Machines

Unified Manager presenta el subsistema subyacente de un entorno virtual en una vista topológica para determinar si se ha producido un problema de latencia en el nodo de computación, la red o el almacenamiento. La vista también destaca el objeto específico que provoca el desfase en el rendimiento a la hora de dar pasos correctivas y solucionar el problema subyacente.

La siguiente captura de pantalla muestra la topología ampliada de AIUM.



## Gestión basada en políticas de almacenamiento y vVols

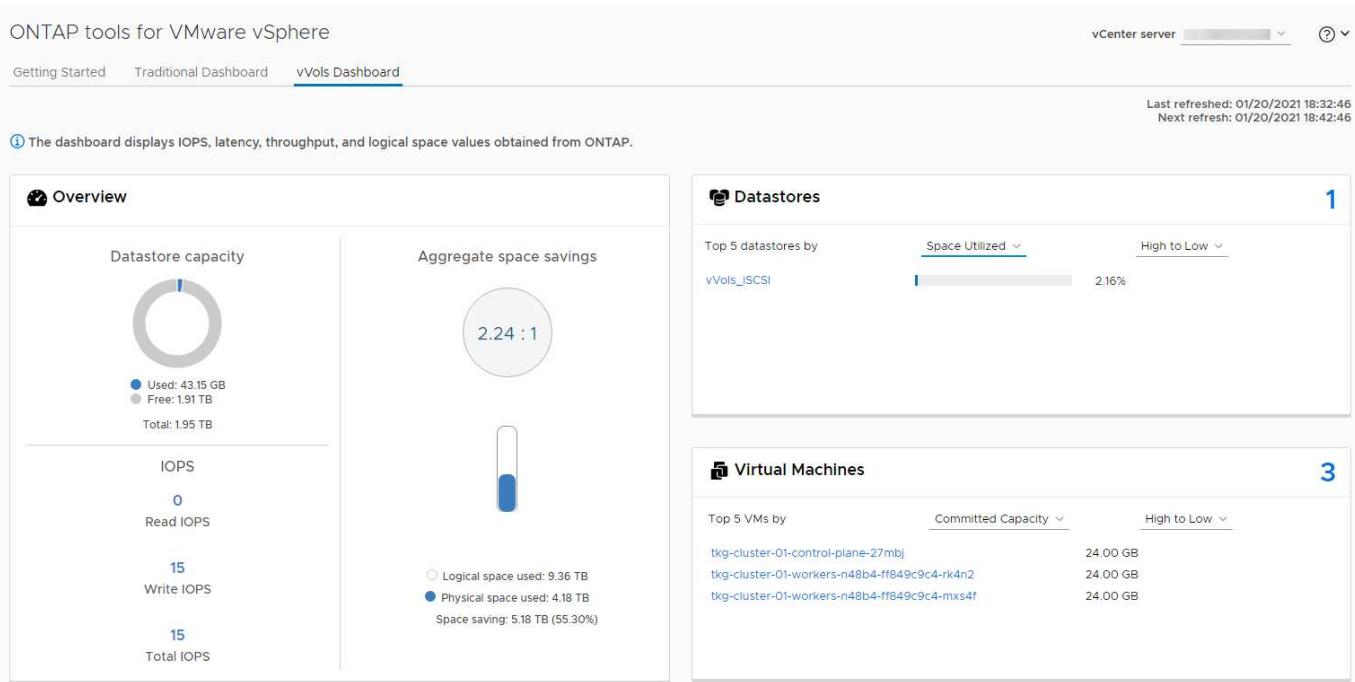
Las API de VMware vSphere para el reconocimiento del almacenamiento (VASA) facilitan que un administrador de almacenamiento configure almacenes de datos con funcionalidades bien definidas y permiten que el administrador de equipos virtuales los utilice siempre que sea necesario para aprovisionar máquinas virtuales sin tener que interactuar entre sí.

Merece la pena echar un vistazo a este enfoque para ver cómo puede optimizar sus operaciones de almacenamiento de virtualización y evitar un gran trabajo trivial.

Antes de VASA, los administradores de máquinas virtuales podían definir políticas de almacenamiento de máquinas virtuales, pero tenían que trabajar con el administrador de almacenamiento para identificar los almacenes de datos adecuados, a menudo usando documentación o convenciones de nomenclatura. Con VASA, el administrador de almacenamiento puede definir una serie de capacidades de almacenamiento, como el rendimiento, la clasificación por niveles, el cifrado y la replicación. Un conjunto de funcionalidades para un volumen o un conjunto de volúmenes se denomina perfil de capacidad de almacenamiento (SCP).

El SCP admite QoS mínimo y/o máximo para los vVols de datos de una VM. La calidad de servicio mínima solo se admite en los sistemas AFF. Las herramientas de ONTAP para VMware vSphere incluyen una consola donde se muestra el rendimiento granular de máquinas virtuales y la capacidad lógica para vVols en sistemas ONTAP.

La siguiente figura muestra las herramientas de ONTAP para el panel de vVols de VMware vSphere 9.8.



Una vez definido el perfil de funcionalidad de almacenamiento, puede utilizarse para aprovisionar equipos virtuales mediante la normativa de almacenamiento que identifique sus requisitos. La asignación entre la política de almacenamiento de máquinas virtuales y el perfil de capacidad de almacenamiento de almacenes de datos permite que vCenter muestre una lista de almacenes de datos compatibles que podrá seleccionar. Este enfoque se conoce como gestión basada en políticas de almacenamiento.

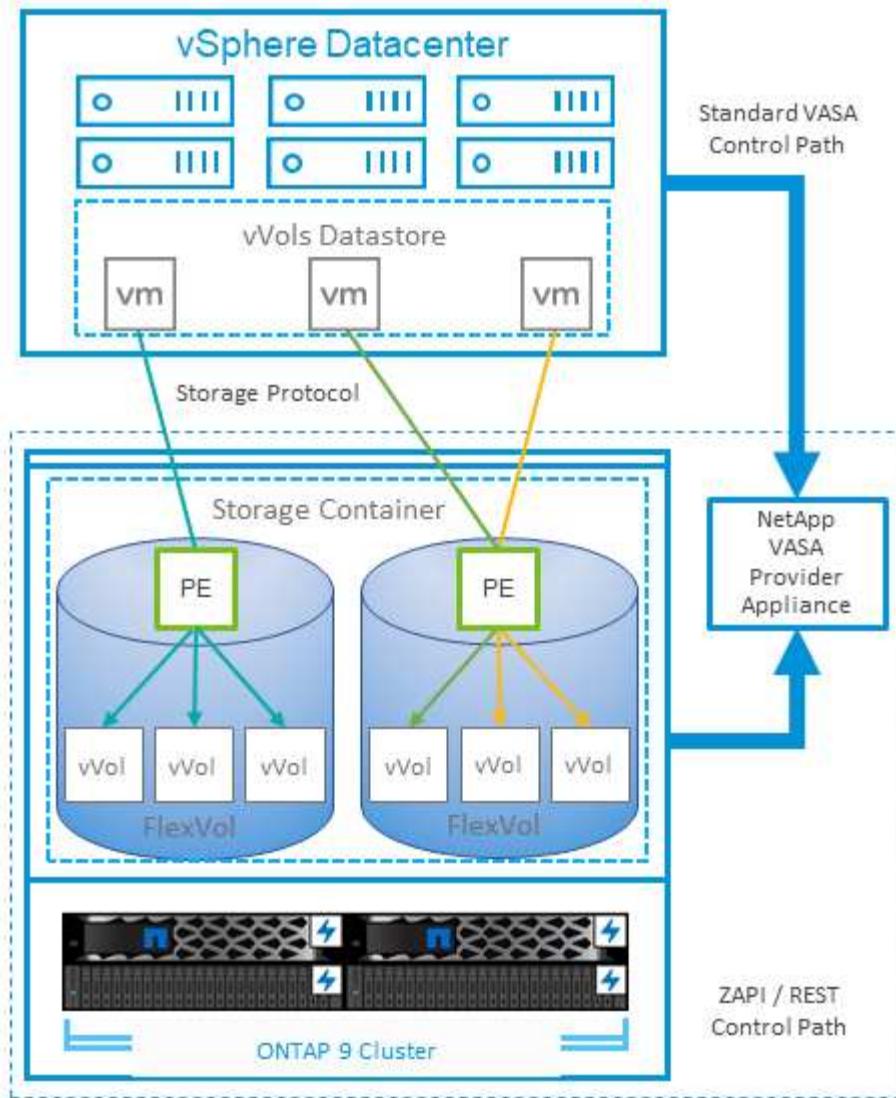
VASA proporciona la tecnología para consultar el almacenamiento y devolver un conjunto de funcionalidades

de almacenamiento a vCenter. Los proveedores de VASA proporcionan la traducción entre las API y construcciones del sistema de almacenamiento y las API de VMware que comprende vCenter. VASA Provider de NetApp para ONTAP se ofrece como parte de las herramientas de ONTAP para VM del dispositivo VMware vSphere. El complemento de vCenter proporciona la interfaz para aprovisionar y gestionar almacenes de datos VVOL, así como la capacidad para definir perfiles de capacidades de almacenamiento (SCPs).

ONTAP admite almacenes de datos de VVol tanto VMFS como NFS. El uso de vVols con almacenes DE datos SAN aporta algunas de las ventajas de NFS, como la granularidad a nivel de equipo virtual. Aquí encontrará algunas prácticas recomendadas para tener en cuenta y información adicional en "[CONSULTE TR-4400](#)":

- Un almacén de datos de VVol puede consistir en varios volúmenes de FlexVol en varios nodos de clúster. El método más sencillo es un único almacén de datos, incluso cuando los volúmenes tienen diferentes funcionalidades. SPBM garantiza que se utiliza un volumen compatible para la máquina virtual. Sin embargo, todos los volúmenes deben formar parte de una única SVM de ONTAP y se debe acceder a ellos mediante un único protocolo. Un LIF por nodo para cada protocolo es suficiente. Evite el uso de varias versiones de ONTAP en un único almacén de datos de VVol, ya que las funcionalidades de almacenamiento pueden variar entre las versiones.
- Utilice las herramientas de ONTAP para el plugin de VMware vSphere para crear y gestionar almacenes de datos de VVol. Además de gestionar el almacén de datos y su perfil, crea automáticamente un extremo de protocolo para acceder a vVols, si es necesario. Si se utilizan LUN, tenga en cuenta que los extremos de protocolo de LUN se asignan mediante los ID de LUN 300 y posteriores. Compruebe que la opción de configuración del sistema avanzado del host ESXi `Disk.MaxLUN` Permite un número de ID de LUN que sea mayor que 300 (el valor predeterminado es 1,024). Para realizar este paso, seleccione el host ESXi en vCenter, después la pestaña Configure y busque `Disk.MaxLUN` En la lista Advanced System Settings.
- No instale ni migre VASA Provider, vCenter Server (basado en dispositivos o Windows) ni las herramientas de ONTAP para VMware vSphere en un almacén de datos vVols, ya que estos dependen mutuamente, lo cual limita la capacidad de gestionarlos en caso de una interrupción del suministro eléctrico u otra interrupción del centro de datos.
- Realice un backup regular de la máquina virtual del proveedor de VASA. Como mínimo, cree copias Snapshot por hora del almacén de datos tradicional que contenga VASA Provider. Para obtener más información sobre la protección y recuperación del proveedor de VASA, consulte este tema "[Artículo de base de conocimientos](#)".

La siguiente figura muestra los componentes de vVols.



## Planificador de recursos distribuidos de almacenamiento de VMware

El planificador de recursos distribuidos (SDRS) de VMware Storage es una función de vSphere que coloca automáticamente los equipos virtuales en un clúster de almacenamiento de datos en función de la latencia de I/O y el uso del espacio actuales.

A continuación, mueve la máquina virtual o los VMDK de forma no disruptiva entre los almacenamientos de datos de un clúster de almacenamientos de datos (también conocido como "pod"), seleccionando el mejor almacenamiento de datos en el que colocar la máquina virtual o los VMDK en el clúster de almacenamientos de datos. Un clúster de almacenamientos de datos es una colección de almacenamientos de datos similares que se agregan en una única unidad de consumo desde la perspectiva del administrador de vSphere.

Cuando se usan SDRS con herramientas de ONTAP para VMware vSphere, primero debe crear un almacenamiento de datos con el plugin, utilizar vCenter para crear el clúster de almacenamiento de datos y, a continuación, añadir el almacenamiento de datos. Una vez creado el clúster de almacenamientos de datos, es posible añadir almacenamientos de datos adicionales al clúster de almacenamientos de datos directamente desde el asistente de aprovisionamiento de la página Details.

Otras prácticas recomendadas de ONTAP para SDRS incluyen lo siguiente:

- No utilice SDR a menos que tenga un requisito específico para hacerlo.
  - SDRS no es necesario cuando se utiliza ONTAP. LOS SDRS no son conscientes de las funciones de eficiencia del almacenamiento de ONTAP como la deduplicación y la compresión, por lo que puede tomar decisiones que no sean óptimas para su entorno.
  - LOS SDRS no son conscientes de las políticas de calidad de servicio de ONTAP, por lo que puede tomar decisiones que no sean óptimas para el rendimiento.
  - LOS SDRS no conocen las copias snapshot de ONTAP, por lo que se pueden tomar decisiones que hagan que las snapshots crezcan exponencialmente. Por ejemplo, al mover una máquina virtual a otro almacén de datos, se crean archivos nuevos en el nuevo almacén de datos, lo que hace que la copia Snapshot crezca. Esto se aplica sobre todo en el caso de equipos virtuales con discos de gran tamaño o gran cantidad de snapshots. En caso de que la máquina virtual vuelva a moverse al almacén de datos original, la copia Snapshot del almacén de datos original aumentará aún más.

Si utiliza SDR, tenga en cuenta las siguientes mejores prácticas:

- Todos los almacenes de datos del clúster deben usar el mismo tipo de almacenamiento (como SAS, SATA o SSD), ser todos los almacenes de datos VMFS o NFS y tener la misma configuración de replicación y protección.
- Considere el uso de SDR en modo predeterminado (manual). Este enfoque permite revisar las recomendaciones y decidir si se aplican o no. Tenga en cuenta los siguientes efectos de las migraciones de VMDK:
  - Cuando SDRS mueve VMDK entre almacenes de datos, se puede reducir el ahorro de espacio obtenido con el clonado o la deduplicación de ONTAP, en función de cómo se deduplique o comprima en el destino.
  - Después de que SDRS mueva los VMDK, NetApp recomienda volver a crear las snapshots en el almacén de datos de origen porque el espacio se bloqueará por la máquina virtual que se movió.
  - Mover VMDK entre almacenes de datos en el mismo agregado tiene pocas ventajas y LOS SDRS no tienen visibilidad en otras cargas de trabajo que puedan compartir el agregado.

Puede encontrar más información sobre LOS SDR en la documentación de VMware en "["Preguntas frecuentes sobre el DRS de almacenamiento"](#)".

## Host ESXi recomendado y otra configuración de ONTAP

NetApp ha desarrollado un conjunto de configuraciones óptimas de hosts ESXi tanto para los protocolos NFS como para los protocolos de bloques. También se proporciona orientación específica para configurar el tiempo de espera del adaptador de bus de host y la función multivía para que funcione correctamente con ONTAP basado en pruebas internas de NetApp y VMware.

Estos valores se establecen fácilmente mediante las herramientas de ONTAP para VMware vSphere: En la página de descripción general de herramientas de ONTAP, desplácese hasta la parte inferior y haga clic en **Apply Recommended Settings** en el portlet de cumplimiento de normativas de host ESXi.

Esta es la configuración de host recomendada para todas las versiones de ONTAP compatibles actualmente.

| Configuración del host                | Valor recomendado por NetApp | Se requiere reinicio |
|---------------------------------------|------------------------------|----------------------|
| <b>Configuración avanzada de ESXi</b> |                              |                      |

| Configuración del host           | Valor recomendado por NetApp   | Se requiere reinicio |
|----------------------------------|--|----------------------|
| VMFS3.HardwareAcceleratedLocking | Mantener predeterminado (1)  | No                   |
| VMFS3.EnableBlockDelete          | Mantener el valor predeterminado (0), pero se puede cambiar si es necesario. Para obtener más información, consulte <a href="#">"Recuperación de espacio para VMFS5 equipos virtuales"</a> | No                   |
| VMFS3.EnableVMFS6Unmap           | Mantener valor predeterminado (1)<br>Para obtener más información, consulte <a href="#">"API de VMware vSphere: Integración de cabinas (VAAI)"</a>   | No                   |
| <b>Ajustes NFS</b>               |  |                      |
| NewSyncInterval                  | Si no utiliza vSphere CSI para Kubernetes, establezca Por <a href="#">"VMware KB 386364"</a>   | No                   |
| NET.TcpipHeapSize                | VSphere 6.0 o posterior; establezca esta opción en 32.<br>El resto de configuraciones de NFS se establecen en 30   | Sí                   |
| NET.TcpipHeapMax                 | Configure 512 MB para la mayoría de las versiones de vSphere 6.X.<br>Establezca el valor predeterminado (1024MB) para 6.5U3, 6.7U3 y 7.0 o posterior.                                      | Sí                   |
| NFS.MaxVolumes                   | VSphere 6.0 o posterior, configurado en 256<br>Todas las demás configuraciones NFS están establecidas en 64.   | No                   |
| NFS41.MaxVolumes                 | VSphere 6.0 o posterior, configurado en 256.   | No                   |
| NFS.MaxQueueDepth                | VSphere 6.0 o posterior; establezca esta opción en 128   | Sí                   |
| NFS.HeartbeatMaxFailures         | Establezca en 10 para todas las configuraciones NFS  | No                   |
| NFS.HeartbeatFrequency           | Establezca en 12 para todas las configuraciones NFS  | No                   |
| NFS.HeartbeatTimeout             | Establezca en 5 para todas las configuraciones NFS.  | No                   |
| SunRPC.MaxConnPerIP              | vSphere 7.0 a 8.0, establecido en 128. Esta configuración se ignora en las versiones de ESXi posteriores a 8.0.  | No                   |
| <b>Configuración de FC/FCoE</b>  |  |                      |

| Configuración del host                | Valor recomendado por NetApp  | Se requiere reinicio |
|---------------------------------------|---|----------------------|
| Política de selección de rutas        | <p>Establezca el valor RR (round robin) cuando se utilicen rutas FC con ALUA. Establezca COMO FIJO para todas las demás configuraciones.</p> <p>Al establecer este valor en RR, se ayuda a proporcionar un equilibrio de carga en todas las rutas activas/optimizadas.</p> <p>El valor FIJO es para configuraciones antiguas que no pertenecen a ALUA y ayuda a evitar las operaciones de I/o del proxy. En otras palabras, ayuda a evitar que las operaciones de I/o vayan al otro nodo de una pareja de alta disponibilidad (ha) en un entorno con Data ONTAP en 7-Mode</p> | No                   |
| Disk.QFullSampleSize                  | <p>Establezca en 32 para todas las configuraciones.</p> <p>Si configura este valor, se evitan los errores de I/O.</p>   | No                   |
| Disk.QFullThreshold                   | <p>Establecer en 8 para todas las configuraciones.</p> <p>Si configura este valor, se evitan los errores de I/O.</p>  | No                   |
| Tiempos de espera de FC HBA de Emulex | Se utiliza el valor predeterminado.   | No                   |
| Tiempos de espera de HBA FC de QLogic | Se utiliza el valor predeterminado.   | No                   |
| <b>Configuración iSCSI</b>            |   |                      |
| Política de selección de rutas        | <p>Establezca el valor RR (round robin) para todas las rutas iSCSI.</p> <p>Al establecer este valor en RR, se ayuda a proporcionar un equilibrio de carga en todas las rutas activas/optimizadas.</p>   | No                   |
| Disk.QFullSampleSize                  | <p>Establezca en 32 para todas las configuraciones.</p> <p>Si configura este valor, se evitan los errores de I/O.</p>   | No                   |
| Disk.QFullThreshold                   | <p>Establecer en 8 para todas las configuraciones.</p> <p>Si configura este valor, se evitan los errores de I/O.</p>  | No                   |



La opción de configuración avanzada de NFS MaxQueueDepth puede no funcionar según lo previsto si se utiliza VMware vSphere ESXi 7.0.1 y VMware vSphere ESXi 7.0.2. Referencia ["86331 de la base de conocimientos de VMware"](#) para más información.

Las herramientas de ONTAP también especifican determinada configuración predeterminada al crear volúmenes de ONTAP FlexVol y LUN:

| Herramienta ONTAP   | Ajuste predeterminado           |
|---|---------------------------------|
| Reserva de Snapshot (-Porcentaje-espacio de instantáneas) | 0                               |
| Reserva fraccionaria (-reserva fraccionaria)              | 0                               |
| Actualización del tiempo de acceso (-atime-update)        | Falso                           |
| Lectura mínima (lectura mínima)                           | Falso                           |
| Snapshots programadas                                     | Ninguno                         |
| Eficiencia del almacenamiento                             | Activado                        |
| Garantía de volumen                                       | Ninguno (con thin provisioning) |
| Tamaño automático del volumen                             | aumentar_reducción              |
| Reserva de espacio de LUN                                 | Deshabilitado                   |
| Asignación de espacio de LUN                              | Activado                        |

## Configuración de multivía para el rendimiento

Aunque no está configurado actualmente por las herramientas de ONTAP disponibles, NetApp sugiere estas opciones de configuración:

- Al utilizar sistemas que no sean ASA en entornos de alto rendimiento o al probar el rendimiento con un único almacén de datos LUN, considere cambiar la configuración de equilibrio de carga de la política de selección de ruta (PSP) round-robin (VMW\_PSP\_RR) de la configuración de IOPS predeterminada de 1000 a un valor de 1. Ver ["VMware KB 2069356"](#) Para más información.
- En vSphere 6.7 Update 1, VMware introdujo un nuevo mecanismo de equilibrio de carga de latencia para Round Robin PSP. La opción de latencia ahora también está disponible cuando se utiliza HPP (complemento de alto rendimiento) con espacios de nombres NVMe y con vSphere 8.0u2 y versiones posteriores, LUN conectados iSCSI y FCP. La nueva opción considera el ancho de banda de E/S y la latencia de la ruta al seleccionar la ruta óptima para E/S. NetApp recomienda utilizar la opción de latencia en entornos con conectividad de ruta no equivalente, como casos con más saltos de red en una ruta que en otra, o cuando se utiliza un sistema NetApp ASA . Ver ["Cambie los parámetros predeterminados para la rotación de redondeo de latencia"](#) Para más información.

## Documentación adicional

Para FCP e iSCSI con vSphere 7, puede encontrar más información en ["Utilice VMware vSphere 7.x con ONTAP"](#) para FCP e iSCSI con vSphere 8, puede encontrar más información en ["Utilice VMware vSphere 8.x con ONTAP"](#) para NVMe-oF con vSphere 7. Para NVMe-oF con vSphere 8, puede encontrar más información en ["Para NVMe-oF, puede encontrar más información en NVMe-oF Configuración del host para ESXi 7.x con ONTAP"](#) ["Para NVMe-oF, puede encontrar más información en NVMe-oF Configuración del host para ESXi 8.x con ONTAP"](#)

# Virtual Volumes (vVols) con herramientas de ONTAP 10

## Descripción general

ONTAP ha sido una solución de almacenamiento líder para entornos VMware vSphere durante más de dos décadas y continúa añadiendo funcionalidades innovadoras para simplificar la gestión al tiempo que reduce los costes.

Este documento trata las funcionalidades de ONTAP para VMware vSphere Virtual Volumes (vVols), incluida la información más reciente sobre el producto y los casos de uso, junto con las prácticas recomendadas y otra información para optimizar la puesta en marcha y reducir los errores.



Esta documentación sustituye a los informes técnicos *TR-4400 publicados previamente: VMware vSphere Virtual Volumes (vVols) con ONTAP*

Las prácticas recomendadas complementan otros documentos, como guías y listas de compatibilidad. Se desarrollan según pruebas de laboratorio y una amplia experiencia de campo por parte de ingenieros y clientes de NetApp. Puede que no sean las únicas prácticas que funcionan o son compatibles, pero generalmente son las soluciones más simples que satisfacen las necesidades de la mayoría de los clientes.



Este documento se ha actualizado para incluir las nuevas funciones de vVols que se encuentran en vSphere 8.0 update 3, el lanzamiento de ONTAP tools 10.4 y los nuevos sistemas NetApp ASA.

## Información general sobre Virtual Volumes (vVols)

NetApp comenzó trabajando con VMware para dar soporte a las API vSphere de Storage Awareness (VASA) para vSphere 5 en 2012. Este primer proveedor de VASA permitía definir las capacidades de almacenamiento en un perfil que podía utilizarse para filtrar almacenajes de datos al aprovisionar y comprobar después el cumplimiento de la política. Con el tiempo, esta evolución evolucionó y se añadieron nuevas funcionalidades que permitían una mayor automatización en el aprovisionamiento, y nuevos volúmenes virtuales o vVols, donde se utilizan objetos de almacenamiento individuales para archivos de máquinas virtuales y discos virtuales. Estos objetos podrían ser LUN, archivos y ahora con espacios de nombres vSphere 8 - NVMe (se utiliza con las herramientas de ONTAP 9.13P2). NetApp colaboró estrechamente con VMware como partner de referencia para vVols lanzado con vSphere 6 en 2015 y de nuevo como partner de diseño para vVols utilizando NVMe over Fabrics en vSphere 8. NetApp sigue mejorando vVols para aprovechar las últimas funcionalidades de ONTAP.

Hay varios componentes a tener en cuenta:

### Proveedor de VASA

Este es el componente de software que gestiona la comunicación entre VMware vSphere y el sistema de almacenamiento. Para ONTAP, VASA Provider se ejecuta en un dispositivo conocido como herramientas de ONTAP para VMware vSphere (herramientas de ONTAP para abreviar). Las herramientas de ONTAP también incluyen un complemento para vCenter, un adaptador de replicación de almacenamiento (SRA) para el administrador de recuperación de sitio de VMware y un servidor API de REST para crear su propia automatización. Una vez que las herramientas de ONTAP se han configurado y registrado con vCenter, ya no es necesario interactuar directamente con el sistema ONTAP, ya que casi todas sus necesidades de almacenamiento pueden gestionarse desde la interfaz de usuario de vCenter o mediante la automatización de la API de REST.

## Extremo de protocolo (PE)

El extremo de protocolo es un proxy para I/O entre los hosts ESXi y el almacén de datos vVols. El proveedor VASA de ONTAP crea estos automáticamente, ya sea un LUN de extremo de protocolo (4MB TB de tamaño) por volumen FlexVol del almacén de datos vVols, o un punto de montaje de NFS por interfaz NFS (LIF) en el nodo de almacenamiento que aloja un volumen FlexVol en el almacén de datos. El host ESXi monta estos extremos de protocolo de forma directa en lugar de LUN VVol individuales y archivos de disco virtual. No es necesario gestionar los extremos de protocolo, ya que el proveedor VASA los crea, monta, desmonta y elimina automáticamente, junto con los grupos de interfaces necesarios o las políticas de exportación.

## Extremo de protocolo virtual (VPE)

Como novedad en vSphere 8, cuando se usa NVMe over Fabrics (NVMe-oF) con vVols, el concepto de extremo de protocolo ya no es relevante en ONTAP. En su lugar, el host ESXi crea una instancia de PE virtual automáticamente para cada grupo ANA en cuanto se enciende la primera máquina virtual. ONTAP crea automáticamente grupos ANA para cada volumen de FlexVol que usa el almacén de datos.

Otra ventaja de usar NVMe-oF para vVols es que no hay solicitudes de enlace requeridas del proveedor VASA. En su lugar, el host ESXi gestiona la funcionalidad de vinculación de VVol internamente según VPE. Esto reduce la posibilidad de que un enlace masivo de VVOL afecte al servicio.

Para obtener más información, consulte "[NVMe y Virtual Volumes](#)" encendido "[vmware.com](#)"

## Almacén de datos de volúmenes virtuales

El almacén de datos de volumen virtual es una representación lógica del almacén de datos de un contenedor vVols, que es creado y mantenido por un proveedor de VASA. El contenedor representa un grupo de capacidad de almacenamiento aprovisionado desde sistemas de almacenamiento administrados por el proveedor de VASA. Las herramientas ONTAP admiten la asignación de múltiples volúmenes FlexVol (denominados volúmenes de respaldo) a un único almacén de datos vVols, y estos almacenes de datos vVols pueden abarcar varios nodos en un clúster ONTAP, combinando sistemas flash e híbridos con diferentes capacidades. El administrador puede crear nuevos volúmenes FlexVol utilizando el asistente de aprovisionamiento o la API REST, o seleccionar volúmenes FlexVol creados previamente para el almacenamiento de respaldo si están disponibles.

## Volúmenes virtuales (vVols)

Los vVols son los archivos y discos de la máquina virtual reales almacenados en el almacén de datos de vVols. El uso del término vVol (singular) se refiere a un solo archivo, LUN o espacio de nombres específico. ONTAP crea espacios de nombres NVMe, LUN o archivos según el protocolo que utilice el almacén de datos. Hay varios tipos distintos de vVols; los más comunes son Config (el único con VMFS, contiene archivos de metadatos como el archivo VMX de la VM), Data (disco virtual o VMDK) y Swap (creado cuando se enciende la VM). Los vVols protegidos por el cifrado de VM de VMware serán del tipo Otro. El cifrado de máquinas virtuales de VMware no debe confundirse con el cifrado de volumen o agregado de ONTAP.

## Gestión basada en políticas

Las API de VMware vSphere para Storage Awareness (VASA) facilitan que un administrador de máquinas virtuales utilice las capacidades de almacenamiento necesarias para aprovisionar máquinas virtuales sin tener que interactuar con su equipo de almacenamiento. Antes de VASA, los administradores de VM podían definir políticas de almacenamiento de VM, pero tenían que trabajar con sus administradores de almacenamiento para identificar almacenes de datos apropiados, a menudo mediante documentación o convenciones de nomenclatura. Con VASA, los administradores de vCenter con los permisos adecuados pueden definir una variedad de capacidades de almacenamiento que los usuarios de vCenter pueden usar para aprovisionar máquinas virtuales. La asignación entre la política de almacenamiento de VM y las capacidades del almacén

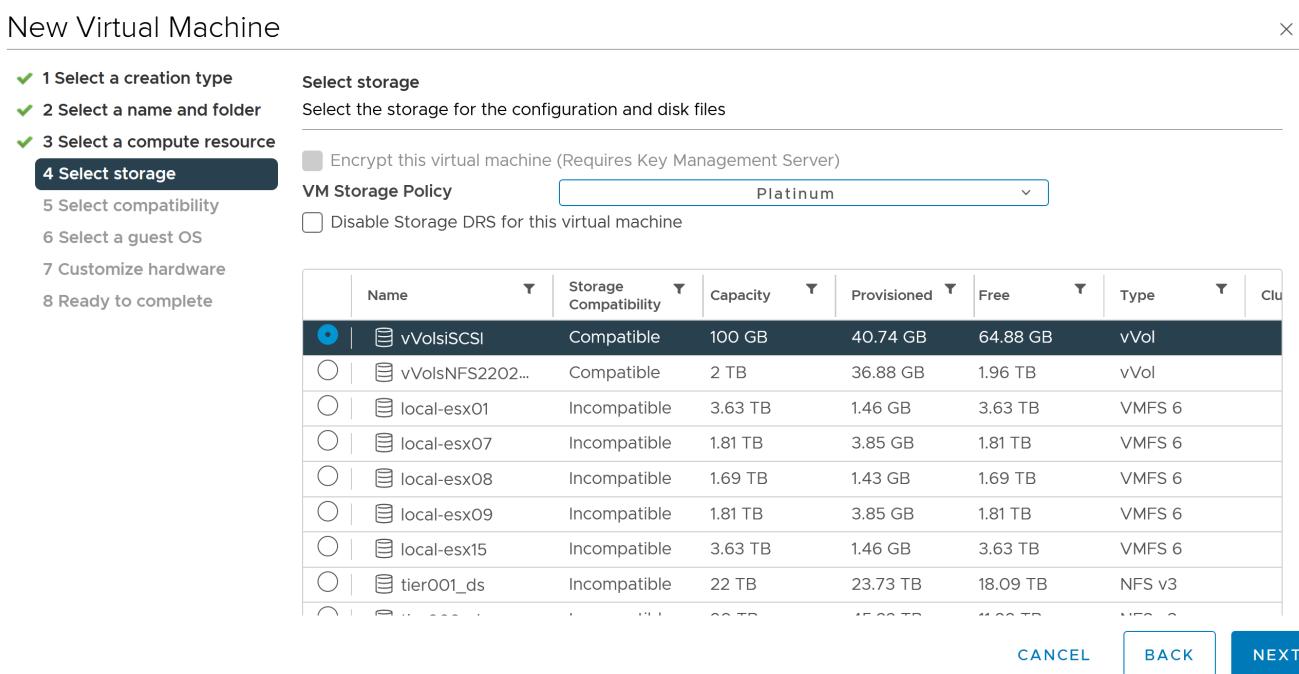
de datos permite a vCenter mostrar una lista de almacenes de datos compatibles para su selección, además de permitir que otras tecnologías como VCF (anteriormente conocido como Aria y vRealize) Automation o VMware vSphere Kubernetes Service (VKS) seleccionen automáticamente el almacenamiento de una política asignada. Este enfoque se conoce como gestión basada en políticas de almacenamiento. Si bien las reglas del proveedor VASA y las políticas de almacenamiento de VM también se pueden usar con almacenes de datos tradicionales, aquí nos centraremos en los almacenes de datos vVols .

### Políticas de almacenamiento de máquinas virtuales

Las políticas de almacenamiento de máquinas virtuales se crean en vCenter en Políticas y perfiles. Para vVols, cree un conjunto de reglas mediante reglas del proveedor de tipo de almacenamiento de NetApp vVols. Las herramientas de ONTAP 10.X ofrecen ahora un método más sencillo que las herramientas de ONTAP 9.X, ya que le permiten especificar directamente los atributos de almacenamiento en la normativa de almacenamiento de las máquinas virtuales misma.

Como se ha mencionado anteriormente, el uso de políticas puede ayudar a simplificar la tarea de aprovisionar un equipo virtual o VMDK. Solo tiene que seleccionar una política adecuada y VASA Provider mostrará los almacenes de datos de vVols compatibles con esa política y colocará el VVOL en una FlexVol volume individual que cumpla las normativas.

### Puesta en marcha de equipos virtuales mediante políticas de almacenamiento



The screenshot shows the 'New Virtual Machine' wizard in vCenter. The current step is '4 Select storage'. On the left, a sidebar lists steps 1 to 8. Step 4 is highlighted with a dark background. The main area shows a table of storage policies:

| Name            | Storage Compatibility | Capacity | Provisioned | Free     | Type   |
|-----------------|-----------------------|----------|-------------|----------|--------|
| vVolsiSCSI      | Compatible            | 100 GB   | 40.74 GB    | 64.88 GB | vVol   |
| vVolsNFS2202... | Compatible            | 2 TB     | 36.88 GB    | 1.96 TB  | vVol   |
| local-esx01     | Incompatible          | 3.63 TB  | 1.46 GB     | 3.63 TB  | VMFS 6 |
| local-esx07     | Incompatible          | 1.81 TB  | 3.85 GB     | 1.81 TB  | VMFS 6 |
| local-esx08     | Incompatible          | 1.69 TB  | 1.43 GB     | 1.69 TB  | VMFS 6 |
| local-esx09     | Incompatible          | 1.81 TB  | 3.85 GB     | 1.81 TB  | VMFS 6 |
| local-esx15     | Incompatible          | 3.63 TB  | 1.46 GB     | 3.63 TB  | VMFS 6 |
| tier001_ds      | Incompatible          | 22 TB    | 23.73 TB    | 18.09 TB | NFS v3 |

At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

Una vez que se aprovisiona una máquina virtual, el proveedor VASA continuará verificando el cumplimiento y alertará al administrador de la máquina virtual con una alarma en vCenter cuando el volumen de respaldo ya no cumpla con la política.

### Cumplimiento de políticas de almacenamiento de máquinas virtuales

# Storage Policies



## VM Storage Policies

AFF\_VASA10



## VM Storage Policy Compliance

Noncompliant

## Last Checked Date

5/20/2022, 12:59:35 PM

## VM Replication Groups



[CHECK COMPLIANCE](#)

## Compatibilidad con NetApp vVols

ONTAP ha admitido la especificación VASA desde su lanzamiento inicial en 2012. Si bien otros sistemas de almacenamiento de NetApp pueden admitir VASA, este documento se centra en las versiones actualmente compatibles de ONTAP 9.

### ONTAP

Además de ONTAP 9 en sistemas AFF, ASA y FAS, NetApp admite cargas de trabajo de VMware en ONTAP Select, Amazon FSx para NetApp con VMware Cloud en AWS, Azure NetApp Files con Azure VMware Solution, Google Cloud NetApp Volumes con Google Cloud VMware Engine y NetApp Private Storage en Equinix, pero la funcionalidad específica puede variar según el proveedor de servicios y la conectividad de red disponible.

Al momento de la publicación, los entornos de hiperescalador están limitados únicamente a almacenes de datos NFS v3 tradicionales; por lo tanto, los vVols solo están disponibles con sistemas ONTAP locales o sistemas conectados a la nube que ofrecen la funcionalidad completa de un sistema local, como aquellos alojados por socios de NetApp y proveedores de servicios en todo el mundo.

Para obtener más información sobre ONTAP, consulte ["Documentación de productos de ONTAP"](#)

Para obtener más información acerca de las prácticas recomendadas para ONTAP y VMware vSphere, consulte ["CONSULTE TR-4597"](#)

## Ventajas del uso de vVols con ONTAP

Cuando VMware introdujo el soporte de vVols con VASA 2.0 en 2015, lo describieron como "un marco de

integración y gestión que ofrece un nuevo modelo operativo para almacenamiento externo (SAN/NAS)". Este modelo operativo ofrece varios beneficios junto con el almacenamiento ONTAP .

### Gestión basada en políticas

Como se explica en la sección 1.2, la administración basada en políticas permite aprovisionar máquinas virtuales y luego administrarlas mediante políticas predefinidas. Esto puede ayudar a las operaciones de TI de varias maneras:

- **Aumentar la velocidad.** Las herramientas de ONTAP eliminan la necesidad de que el administrador de vCenter abra tickets con el equipo de almacenamiento para actividades de aprovisionamiento de almacenamiento. Sin embargo, los roles RBAC de las herramientas ONTAP en vCenter y en el sistema ONTAP aún permiten equipos independientes (como equipos de almacenamiento) o actividades independientes del mismo equipo, al restringir el acceso a funciones específicas si así se desea.
- \* Provisionamiento más inteligente. \* Las capacidades del sistema de almacenamiento se pueden exponer a través de las API de VASA, lo que permite que los flujos de trabajo de aprovisionamiento aprovechen las capacidades avanzadas sin que el administrador de VM tenga que entender cómo administrar el sistema de almacenamiento.
- \* Provisionamiento más rápido.\* Se pueden admitir diferentes capacidades de almacenamiento en un único almacén de datos y seleccionarlas automáticamente según sea apropiado para una VM basada en la política de VM.
- **Evite errores.** Las políticas de almacenamiento y VM se desarrollan con anticipación y se aplican según sea necesario sin tener que personalizar el almacenamiento cada vez que se aprovisiona una VM. Las alarmas de cumplimiento de normativas se generan cuando las funcionalidades de almacenamiento van más allá de las políticas definidas. Como se ha mencionado anteriormente, los SCPs hacen que el aprovisionamiento inicial sea predecible y repetible, mientras que basar las políticas de almacenamiento de los equipos virtuales en los SCPs garantiza una ubicación precisa.
- \* Mejor gestión de la capacidad.\* Las herramientas VASA y ONTAP permiten ver la capacidad de almacenamiento hasta el nivel de agregado individual si es necesario y proporcionar varias capas de alerta en caso de que la capacidad empiece a ser baja.

### Gestión granular de máquinas virtuales en el SAN moderno

Los sistemas de almacenamiento SAN que utilizan Fibre Channel e iSCSI fueron los primeros en recibir soporte de VMware para ESX, pero carecían de la capacidad de administrar archivos y discos de VM individuales desde el sistema de almacenamiento. En su lugar, se aprovisionan los LUN y VMFS administran los archivos individuales. Esto dificulta que el sistema de almacenamiento administre directamente el rendimiento, la clonación y la protección del almacenamiento de cada máquina virtual individual. vVols aporta una granularidad de almacenamiento que los clientes que utilizan almacenamiento NFS ya disfrutan, con las capacidades SAN robustas y de alto rendimiento de ONTAP.

Ahora, con vSphere 8 y las ONTAP tools for VMware vSphere 9.12 y versiones posteriores, esos mismos controles granulares utilizados por vVols para protocolos heredados basados en SCSI ahora están disponibles en la SAN de canal de fibra moderna que utiliza NVMe sobre Fabrics para un rendimiento aún mayor a escala. Con vSphere 8.0 update 1, ahora es posible implementar una solución NVMe completa de extremo a extremo utilizando vVols sin ninguna traducción de E/S en la pila de almacenamiento del hipervisor.

### Mayor capacidad de descarga de soluciones de almacenamiento

Si bien VAAI ofrece una variedad de operaciones que se descargan en el almacenamiento, existen algunas brechas que el proveedor VASA aborda. SAN VAAI no puede descargar instantáneas administradas por VMware al sistema de almacenamiento. NFS VAAI puede descargar instantáneas administradas por VM, pero existen limitaciones en una VM con instantáneas nativas de almacenamiento. Dado que vVols usa LUN

individuales, espacios de nombres o archivos para discos de máquinas virtuales, ONTAP puede clonar de manera rápida y eficiente los archivos o LUN para crear instantáneas granulares de VM que ya no requieren archivos delta. NFS VAAI tampoco admite la descarga de operaciones de clonación para migraciones de Storage vMotion en caliente (encendido). La máquina virtual debe estar apagada para permitir la descarga de la migración cuando se utiliza VAAI con almacenes de datos NFS tradicionales. El proveedor VASA en las herramientas ONTAP permite realizar clones casi instantáneos y con uso eficiente del almacenamiento para migraciones en caliente y en frío, y también admite copias casi instantáneas para migraciones entre volúmenes de vVols. Debido a estos importantes beneficios de eficiencia de almacenamiento, es posible que pueda aprovechar al máximo las cargas de trabajo de vVols en ["Garantía de eficiencia"](#) programa. Del mismo modo, si los clones entre volúmenes que utilizan VAAI no satisfacen sus requisitos, probablemente podrá resolver su desafío comercial gracias a las mejoras en la experiencia de copia con vVols.

### Casos de uso comunes para vVols

Además de estos beneficios, también se observan estos casos de uso comunes para el almacenamiento de VVOL:

- **Provisionamiento bajo demanda de VMs**

- Cloud privado o IaaS de proveedor de servicios.
- Aproveche la automatización y la orquestación a través del paquete Aria (anteriormente vRealize), OpenStack, etc.

- **Discos de primera clase (FCDs)**

- Volúmenes persistentes de VMware vSphere Kubernetes Service (VKS).
- Proporcione servicios similares a Amazon EBS a través de la gestión del ciclo de vida de VMDK independiente.

- **Provisionamiento bajo demanda de VMs temporales**

- Laboratorios de prueba/desarrollo
- Entornos de formación

### Beneficios comunes con vVols

Cuando se utiliza a su máximo beneficio, como en los casos de uso anteriores, vVols proporciona las siguientes mejoras específicas:

- Los clones se crean rápidamente dentro de un solo volumen o en varios volúmenes en un clúster ONTAP, lo que constituye una ventaja en comparación con los clones tradicionales habilitados para VAAI. También son eficientes en cuanto al almacenamiento. Los clones dentro de un volumen utilizan la clonación de archivos ONTAP, que son como los volúmenes FlexClone y solo almacenan los cambios del archivo/LUN/espacio de nombres vVol de origen. De este modo, las máquinas virtuales a largo plazo para producción u otros fines de aplicación se crean rápidamente, ocupan un espacio mínimo y pueden beneficiarse de la protección a nivel de máquina virtual (utilizando el complemento NetApp SnapCenter para VMware vSphere, instantáneas administradas por VMware o respaldo VADP) y la administración del rendimiento (con ONTAP QoS). Los clones entre volúmenes son mucho más rápidos con vVols que con VAAI porque con VASA podemos crear el clon y permitir el acceso a él en el destino antes de que se complete la copia. Los bloques de datos se copian como un proceso en segundo plano para completar el vVol de destino. Esto es similar a la forma en que funciona el movimiento de LUN no disruptivo de ONTAP para los LUN tradicionales.
- Los vVols son la tecnología de almacenamiento ideal cuando se utiliza TKG con vSphere CSI, lo que proporciona capacidades y clases de almacenamiento discretas gestionadas por el administrador de vCenter.

- Los servicios similares a Amazon EBS se pueden entregar a través de FCD porque un FCD VMDK, como sugiere el nombre, es un ciudadano de primera clase en vSphere y tiene un ciclo de vida que se puede administrar de forma independiente, separado de las máquinas virtuales a las que puede estar conectado.

## Lista de comprobación

Utilice esta lista de comprobación para la instalación para garantizar una puesta en marcha correcta (actualizada para 10,3 y versiones posteriores).

1

## Planificación inicial

- Antes de comenzar la instalación, debe comprobar el ["Herramienta de matriz de interoperabilidad \(IMT\)"](#) para asegurarse de que la implementación ha sido certificada.
  - Determine el tamaño y el tipo de configuración de las herramientas de ONTAP que necesita su entorno. Consulte el documento ["Límites de configuración para poner en marcha herramientas de ONTAP para VMware vSphere"](#) si desea obtener más información.
  - Determine si utilizará SVM multitenant o permitir el acceso completo al clúster. Si utiliza SVM multitenant, deberá tener un LIF de gestión de SVM en cada SVM para usar. Las herramientas de ONTAP deben poder acceder a este LIF a través del puerto 443.
  - Determine si utilizará Fibre Channel (FC) para la conectividad de almacenamiento. Si es así, ["configurar la división en zonas"](#) debe en sus switches FC para habilitar la conectividad entre los hosts ESXi y los LIF FC de la SVM.
  - Determinar si va a usar el adaptador de replicación de almacenamiento (SRA) de herramientas de ONTAP para el administrador de recuperación de sitio (SRM) de VMware o la recuperación de sitios activos (VLSR). Si es así, necesitará acceder a la interfaz de gestión del servidor SRM/VLSR para instalar el SRA.
  - Si va a utilizar la replicación de SnapMirror gestionada por las herramientas de ONTAP (incluidas, entre otras, la sincronización activa de SnapMirror), el administrador de ONTAP debe ["Cree una relación de paridad entre clústeres en ONTAP"](#) y ["Cree una relación entre iguales de SVM entre clústeres en ONTAP"](#) antes de poder utilizar las herramientas de ONTAP con SnapMirror.
  - ["Descargue"](#) Las herramientas de ONTAP OVA y, si es necesario, el archivo SRA tar.gz.

2

## Provisión de direcciones IP y registros DNS

- Solicite la siguiente información IP a su equipo de red. Se requieren las primeras tres direcciones IP, y los nodos dos y tres se utilizan para puestas en marcha de escalado horizontal de alta disponibilidad. Los registros de host DNS son necesarios y todos los nombres de nodo y todas las direcciones deben estar en la misma VLAN y subred.
  - Dirección de la aplicación de herramientas de ONTAP \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
  - Dirección de Servicios Internos \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
  - Nombre de host DNS del nodo uno \_\_\_\_
  - Dirección IP del nodo uno \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
  - Máscara de subred \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
  - Puerta de enlace predeterminada \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
  - Servidor DNS 1 \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
  - Servidor DNS 2 \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_

- Dominio de búsqueda DNS \_\_\_\_\_
  - Nombre de host DNS del nodo dos (opcional) \_\_\_\_\_
  - Dirección IP del nodo dos (opcional) \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_
  - Nombre de host DNS del nodo tres (opcional) \_\_\_\_\_
  - Dirección IP del nodo tres (opcional) \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_
  - Cree registros DNS para todas las direcciones IP anteriores.

3

## Configuración del firewall de red

- Abra los puertos necesarios para las direcciones IP anteriores en el firewall de red. Consulte la ["Requisitos de puertos"](#) para obtener la última actualización.

4

## Reducida

- Se requiere un almacén de datos en un dispositivo de almacenamiento compartido. Opcionalmente, puede utilizar una biblioteca de contenidos en el mismo almacén de datos que el nodo uno para facilitar la clonación rápida de la plantilla con VAAI.
  - Biblioteca de contenido (solo necesaria para HA) \_\_\_\_\_
  - Nodo 1 almacén de datos \_\_\_\_\_
  - Almacén de datos de nodo dos (opcional, pero recomendado para HA) \_\_\_\_\_
  - Almacén de datos de nodo tres (opcional, pero recomendado para HA) \_\_\_\_\_

5

## Implemente el OVA

- Tenga en cuenta que este paso puede tardar hasta 45 minutos en completarse
  - ["Implemente el OVA"](#) Con el cliente vSphere.
  - En el paso 3 de la implementación de OVA, seleccione la opción para personalizar el hardware de esta máquina virtual y configure lo siguiente en el paso 10:
    - Activación de Hot Add de CPU
    - Conexión en caliente de memoria

6

## Agregar yCenters a herramientas de ONTAP

- "Añada instancias de vCenter Server" En el gestor de herramientas de ONTAP.

7

## Añadir back-ends de almacenamiento a herramientas de QNAP

- ["Configure los roles y privilegios de usuario de ONTAP"](#) Usando el archivo JSON incluido si no utiliza admin.
  - Si desea asignar SVM específicos a vCenters mediante multitenencia de almacenamiento en lugar de usar credenciales de clúster ONTAP en vCenter, siga estos pasos:
  - ["clústeres incorporados"](#) En el administrador de herramientas de ONTAP y asócielo con vCenter.

- "[SVM integradas](#)" En ONTAP tools vCenter UI.
- Si **no** se utilizan SVM multiinquilino dentro de vCenter:
- "[clústeres incorporados](#)" Directamente en la interfaz de usuario de ONTAP Tools vCenter. Como alternativa, en esta situación, es posible añadir SVM directamente cuando no se utilizan vVols.

**8**

### Configurar servicios de dispositivos (opcional)

- Para utilizar vVols, primero debe "[Edite la configuración del dispositivo y habilite el servicio VASA](#)". Al mismo tiempo, revise los dos elementos siguientes.
- Si tiene pensado utilizar vVols en producción, "[alta disponibilidad](#)" con las dos direcciones IP opcionales anteriores.
- Si tiene pensado utilizar las herramientas de ONTAP Storage Replication Adapter (SRA) para el administrador de recuperación de sitio de VMware o la recuperación de sitios activos, "[Habilite los servicios de SRA](#)".

**9**

### Certificados (opcional)

- Según VMware, se requieren certificados firmados por CA si se utilizan vVols con varios vCenter.
- Servicios VASA \_\_\_\_\_
- Servicios ADMINISTRATIVOS \_\_\_\_\_

**10**

### Otras tareas posteriores al despliegue

- Cree reglas de antiafinidad para equipos virtuales en una puesta en marcha de alta disponibilidad.
- Si se utiliza alta disponibilidad, los nodos de vMotion de almacenamiento dos y tres para separar almacenes de datos (opcional, pero recomendado).
- "[usar administrar certificados](#)" En el administrador de herramientas de ONTAP, para instalar los certificados requeridos firmados por CA.
- Si habilitó SRA para SRM/VLSR para proteger almacenes de datos tradicionales, "[Configurar el SRA en el dispositivo VMware Live Site Recovery](#)".
- Configurar copias de seguridad nativas para "[RPO casi cero](#)".
- Configurar copias de seguridad regulares en otros medios de almacenamiento.

## Usar vVols con ONTAP

La clave para usar vVols con NetApp es las herramientas de ONTAP para VMware vSphere, que son servidores como la interfaz VASA (vSphere API for Storage Awareness) Provider para sistemas ONTAP 9 de NetApp.

Las herramientas de ONTAP también incluyen extensiones de interfaz de usuario de vCenter, servicios API de REST, adaptadores de replicación de almacenamiento para VMware Site Recovery Manager / Live Site Recovery, herramientas de supervisión y configuración de host, y una serie de informes que le ayudan a gestionar mejor su entorno de VMware.

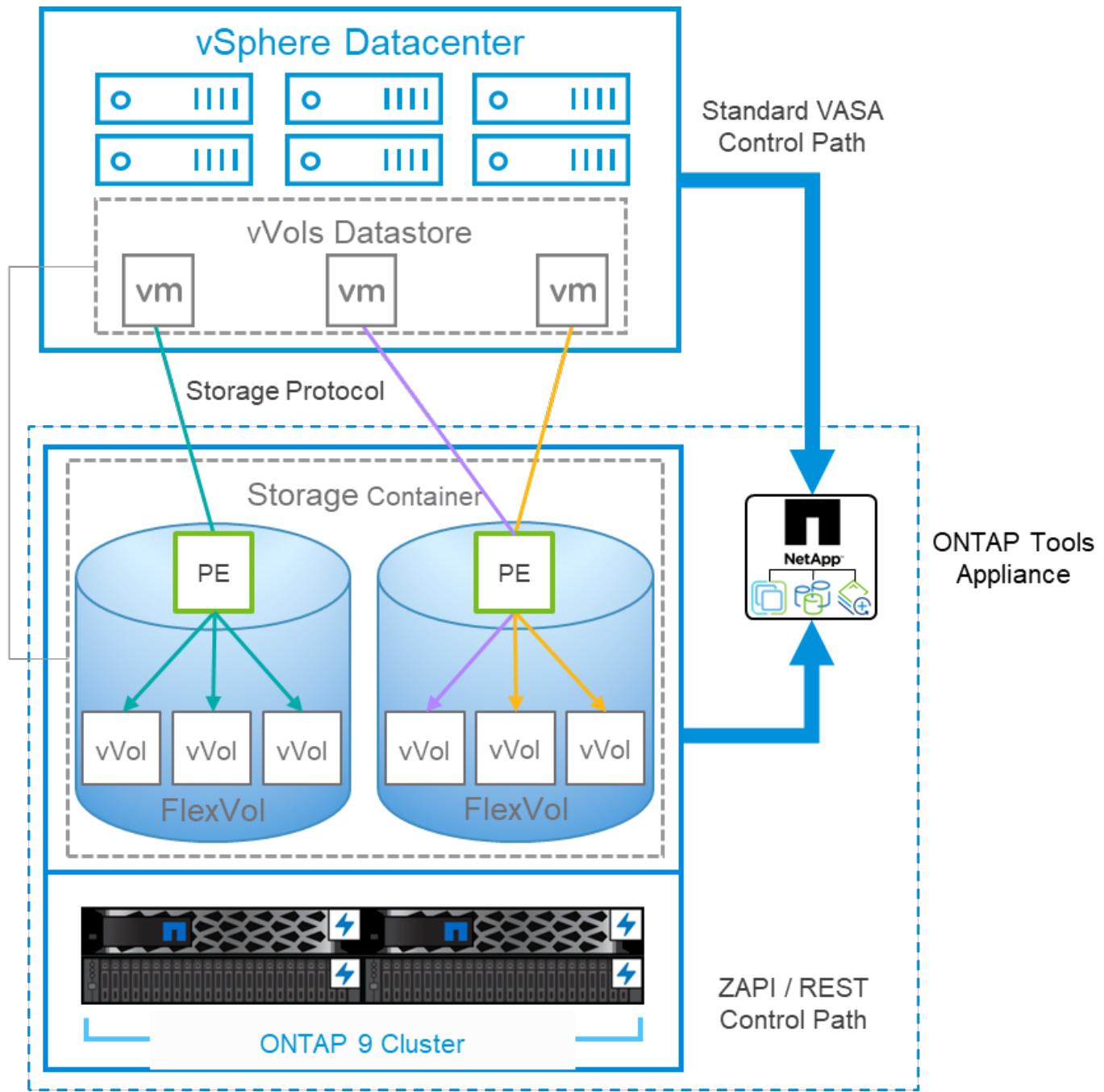
## Productos y Documentación

La licencia ONTAP One incluye todas las licencias necesarias para utilizar vVols con sistemas ONTAP. El único requisito adicional es el OVA gratuito con herramientas de ONTAP, que actúa como proveedor VASA. En un entorno vVols, el software VASA Provider traduce las funcionalidades de cabinas en atributos basados en políticas que se pueden aprovechar a través de las API VASA sin que el administrador de vSphere tenga que saber cómo se gestionan las funcionalidades en segundo plano. Esto permite un consumo dinámico de la capacidad de almacenamiento asignada según políticas, lo que elimina la necesidad de crear manualmente almacenes de datos tradicionales y gestionar sus tasas de consumo de almacenamiento individuales. En resumen, vVols elimina toda la complejidad de la gestión del almacenamiento empresarial y la abstrae del administrador de vSphere para que puedan centrarse en la capa de virtualización.

Para los clientes que usan VMware Cloud Foundation con vSAN, vVols se puede agregar a cualquier dominio de gestión o carga de trabajo como almacenamiento complementario. VVols se integra perfectamente con vSAN a través de un marco de administración común basado en políticas de almacenamiento.

La familia de herramientas 10 de ONTAP de última generación moderniza las funcionalidades anteriores con una arquitectura escalable, en contenedores y basada en microservicio que se puede poner en marcha mediante un sencillo dispositivo de formato OVA en ESXi. ONTAP TOOLS 10 combina todas las funcionalidades de tres antiguos dispositivos y productos en una única implementación. Para la gestión de vVols, usará las intuitivas extensiones de interfaz de usuario de vCenter o las API de REST para las herramientas de ONTAP VASA Provider. Tenga en cuenta que el componente SRA es para almacenes de datos tradicionales; Site Recovery Manager de VMware no utiliza SRA para vVols.

**ONTAP herramientas de la arquitectura VASA Provider cuando se utiliza iSCSI o FCP con sistemas unificados**



#### Instalación del producto

En el caso de nuevas instalaciones, implemente el dispositivo virtual en el entorno de vSphere. Una vez puesta en marcha, puede iniciar sesión en la interfaz de usuario de administrador o utilizar las API REST para escalar vertical o horizontalmente la puesta en marcha, vCenters (esto registra el complemento con vCenter), sistemas de almacenamiento incorporados y asociar los sistemas de almacenamiento con sus vCenters. Solo es necesario incorporar sistemas de almacenamiento en la interfaz de usuario del administrador de herramientas de ONTAP y asociar clústeres con vCenters si planea utilizar multi-tenancy seguro con SVM dedicadas; de lo contrario, solo puede incorporar los clústeres de almacenamiento deseados en las extensiones de interfaz de usuario de ONTAP tools vCenter o mediante las API de REST.

Consulte "[Despliegue de vVols Storage](#)" en este documento, o "[Documentación de las herramientas de ONTAP para VMware vSphere](#)".



La práctica recomendada es almacenar las herramientas de ONTAP y los dispositivos vCenter en almacenes de datos NFS o VMFS tradicionales para evitar cualquier conflicto de interdependencia. Puesto que tanto las herramientas vCenter como ONTAP deben comunicarse entre sí durante las operaciones de vVols, no instale ni mueva los dispositivos de herramientas ONTAP ni los dispositivos vCenter Server (VCSA) al almacenamiento vVols que gestionen. Si esto sucede, reiniciar los dispositivos de las herramientas vCenter o ONTAP puede provocar la interrupción del acceso al plano de control y la imposibilidad de arrancar el dispositivo.

Las actualizaciones in situ de las herramientas de ONTAP son compatibles con el archivo ISO de actualización disponible para descargar en "[Herramientas de ONTAP para VMware vSphere 10: Descargas](#)" el sitio de soporte de NetApp (se requiere iniciar sesión). Siga "[Actualice desde ONTAP tools para VMware vSphere 10.x a 10,3](#)" las instrucciones de la guía para actualizar el aparato. También es posible realizar una actualización en paralelo de las herramientas de ONTAP 9,13 a 10,3. Consulte el "[Migre desde ONTAP Tools para VMware vSphere 9.x a 10,3](#)" para obtener información más detallada sobre ese tema.

Para obtener información sobre el ajuste de tamaño del dispositivo virtual y cuáles son los límites de configuración, consulte "[Límites de configuración para poner en marcha herramientas de ONTAP para VMware vSphere](#)"

#### **Documentación de producto**

La siguiente documentación puede ayudarle a poner en marcha las herramientas de ONTAP.

["Documentación de las herramientas de ONTAP para VMware vSphere"](#)

#### **Manos a la obra**

- "[Notas de la versión](#)"
- "[Información general de las herramientas de ONTAP para VMware vSphere](#)"
- "[Ponga en funcionamiento las herramientas de ONTAP](#)"
- "[Actualice las herramientas de ONTAP](#)"

#### **Utilice las herramientas de ONTAP**

- "[Aprovisione los almacenes de datos](#)"
- "[Configure el control de acceso basado en roles](#)"
- "[Configuración de la alta disponibilidad](#)"
- "[Modifique la configuración del host ESXi](#)"

#### **Proteja y gestione almacenes de datos**

- "[Configure vSphere Metro Storage Cluster \(VMSC\) con las herramientas ONTAP y la sincronización activa de SnapMirror](#)"
- "[Proteja las máquinas virtuales](#)" Con SRM
- "[Supervisar clústeres, almacenes de datos y máquinas virtuales](#)"

#### **Consola del proveedor de VASA**

VASA Provider incluye una consola con información de rendimiento y capacidad para máquinas virtuales de vVols individuales. Esta información proviene directamente de ONTAP para los archivos y LUN VVOL,

incluidos la latencia, IOPS, rendimiento y más. Está habilitada de forma predeterminada cuando se utilizan todas las versiones compatibles actualmente de ONTAP 9. Tenga en cuenta que, tras la configuración inicial, los datos pueden tardar hasta 30 minutos en rellenar el panel de control.

## Otras prácticas recomendadas

El uso de vVols de ONTAP con vSphere es sencillo y sigue los métodos de vSphere publicados (consulte Trabajar con volúmenes virtuales en la documentación de vSphere Storage en VMware para su versión de ESXi). A continuación, se muestran algunas prácticas adicionales que se deben tener en cuenta junto con ONTAP.

### Límites

En general, ONTAP admite los límites de vVols definidos por VMware (ver Publicado ["Valores máximos de configuración"](#)). Compruebe siempre los ["Hardware Universe de NetApp"](#) límites actualizados sobre números y tamaños de LUN, espacios de nombres y archivos.

**Utilice las herramientas de ONTAP para las extensiones de interfaz de usuario de VMware vSphere o API REST para aprovisionar almacenes de datos vVols y puntos finales de protocolo.**

Aunque es posible crear almacenes de datos vVols con la interfaz general de vSphere, mediante las herramientas de ONTAP se crearán automáticamente extremos de protocolo según sea necesario y se crearán volúmenes de FlexVol (no es necesario con ASA R2) mediante las prácticas recomendadas de ONTAP. Solo tiene que hacer clic con el botón derecho en el host/clúster/centro de datos y, a continuación, seleccionar *ONTAP TOOLS* y *PROVISION datastore*. A partir de ahí, simplemente elija las opciones de vVols deseadas en el asistente.

**Nunca almacene el dispositivo de herramientas ONTAP o el dispositivo vCenter Server (VCSA) en un almacén de datos vVols que estén administrando.**

Esto puede resultar en una “situación de pollo y huevo” si necesita reiniciar los aparatos porque no serán capaces de volver a ensamblar sus propios vVols mientras se reinician. Puede almacenarlos en un almacén de datos de vVols que se gestiona con otras herramientas de ONTAP y en una puesta en marcha de vCenter.

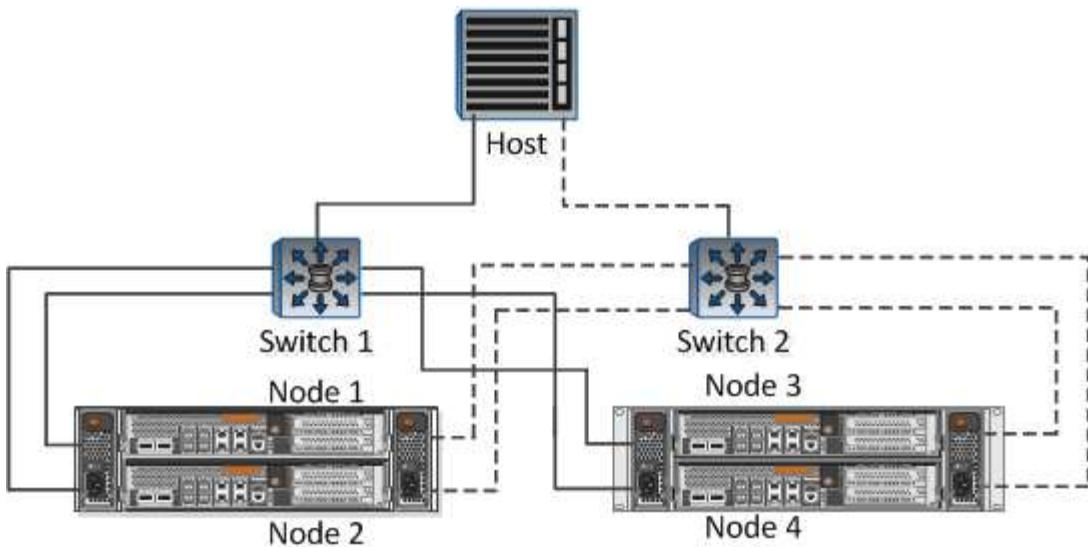
**Evite las operaciones vVols a través de diferentes versiones de ONTAP.**

Las funcionalidades de almacenamiento compatibles como calidad de servicio, personalidad y otras han cambiado en varias versiones del proveedor VASA; algunas dependen de la versión de ONTAP. El uso de diferentes versiones de un clúster de ONTAP o el movimiento de vVols entre clústeres con diferentes versiones puede provocar un comportamiento inesperado o alarmas de cumplimiento de normativas.

**Zone su estructura Fibre Channel antes de usar FCP para vVols.**

El proveedor de VASA de herramientas de ONTAP se encarga de gestionar iGroups FCP e iSCSI, así como subsistemas NVMe en ONTAP basado en iniciadores detectados de hosts ESXi gestionados. Sin embargo, no se integra con switches Fibre Channel para gestionar la división en zonas. La división en zonas debe realizarse siguiendo las mejores prácticas antes de realizar ningún aprovisionamiento. A continuación se muestra un ejemplo de división en zonas de un solo iniciador en cuatro sistemas ONTAP:

División en zonas de un solo iniciador:



Consulte los siguientes documentos para obtener más prácticas recomendadas:

["TR-4080 Mejores prácticas para ONTAP SAN moderno 9"](#)

["TR-4684 Implementación y configuración de SAN modernas con NVMe-oF"](#)

#### **Planifica tus volúmenes de respaldo de FlexVol de acuerdo a tus necesidades.**

En el caso de los sistemas R2 que no sean de ASA, puede ser conveniente añadir diversos volúmenes de backup al almacén de datos vVols para distribuir la carga de trabajo por el clúster de ONTAP, admitir distintas opciones de normativas o aumentar el número de LUN o archivos permitidos. Sin embargo, si se requiere una eficiencia del almacenamiento máxima, coloque todos los volúmenes de backup en un único agregado. O, si es necesario un rendimiento de clonación máximo, considere la posibilidad de usar un único volumen de FlexVol y mantener sus plantillas o biblioteca de contenido en el mismo volumen. El proveedor VASA libera muchas operaciones de almacenamiento de vVols en ONTAP, incluidas la migración, el clonado y las copias Snapshot. Cuando esta operación se realiza en un único volumen FlexVol, se usan clones de archivos con gestión eficiente del espacio y están disponibles casi al instante. Cuando esto se realiza en volúmenes de FlexVol, las copias se encuentran disponibles rápidamente y utilizan deduplicación y compresión en línea, pero es posible que no se recupere la máxima eficiencia del almacenamiento hasta que se ejecuten trabajos en segundo plano en volúmenes con deduplicación y compresión en segundo plano. En función del origen y el destino, se puede degradar cierta eficiencia.

Con los sistemas R2 de ASA, esta complejidad se elimina cuando el concepto de un volumen o agregado es abstracto del usuario. La ubicación dinámica se gestiona automáticamente y los extremos de protocolo se crean según sea necesario. Si se requiere un escalado adicional, se pueden crear automáticamente extremos de protocolo adicionales sobre la marcha.

#### **Considera usar Max IOPS para controlar VMs desconocidas o de prueba.**

Por primera vez, disponible en VASA Provider 7.1, Max IOPS puede usarse para limitar las IOPS a un VVol específico para una carga de trabajo desconocida y así evitar el impacto en otras cargas de trabajo más críticas. Consulte la Tabla 4 para obtener más información sobre gestión del rendimiento.

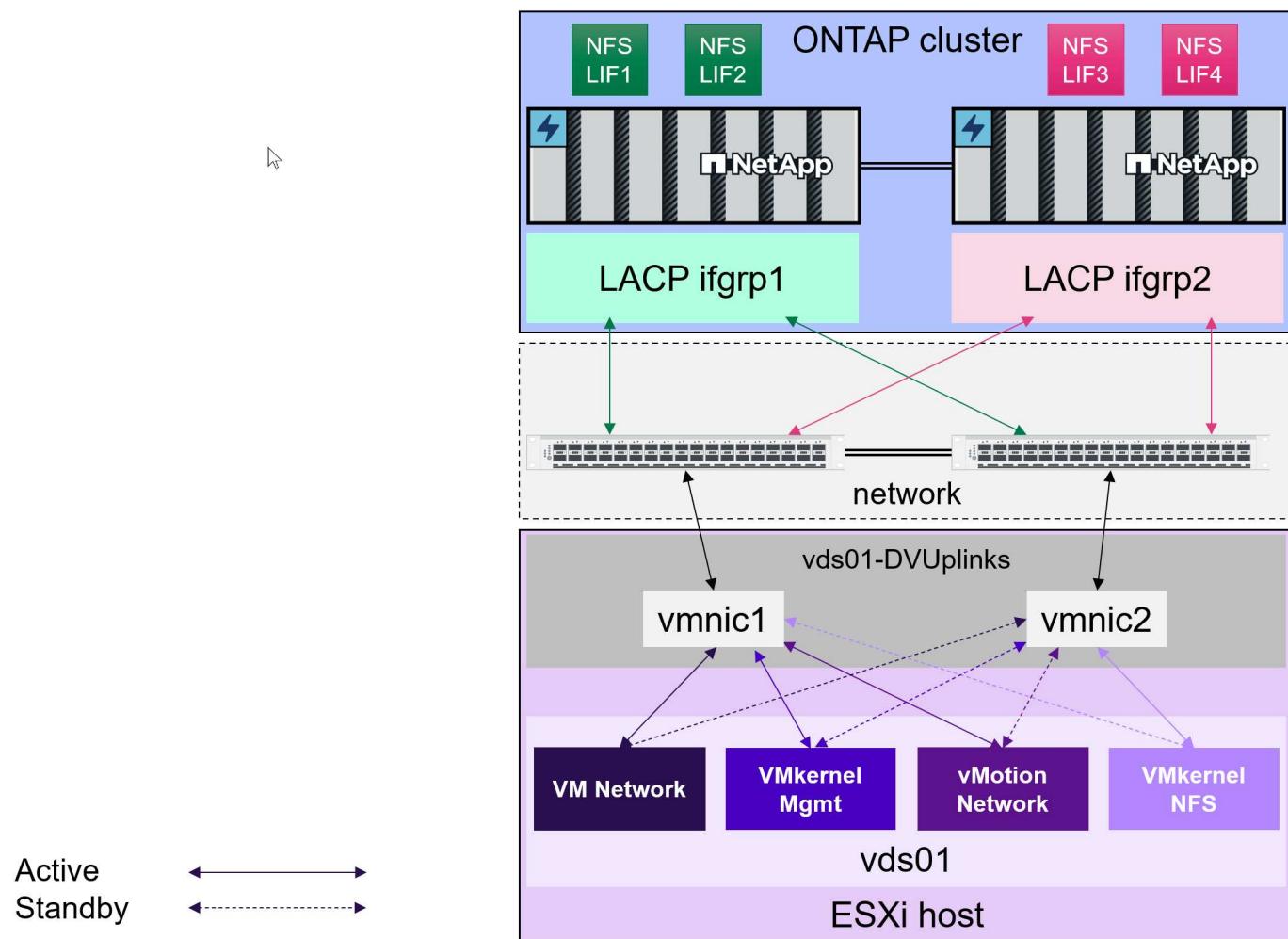
**Asegúrese de tener suficientes LIF de datos.** Consulte ["Despliegue de vVols Storage"](#).

#### **Siga todas las mejores prácticas del protocolo.**

Consulte las otras guías de prácticas recomendadas de NetApp y VMware específicas del protocolo que ha

seleccionado. En general, no hay ningún cambio aparte de los ya mencionados.

### Ejemplo de configuración de red usando vVols sobre NFS v3



### Puesta en marcha de vVols en sistemas AFF, ASA, ASA R2 y FAS

Siga estas mejores prácticas para crear almacenamiento de vVols para los equipos virtuales.

El aprovisionamiento de almacenes de datos vVols implica varios pasos. Los sistemas ASA R2 de NetApp están diseñados para cargas de trabajo de VMware y proporcionan una experiencia de usuario diferente a la de los sistemas ONTAP tradicionales. Al utilizar los sistemas ASA R2, las versiones 10,3 o posteriores de las herramientas de ONTAP requieren menos pasos para configurar e incluir extensiones de interfaz de usuario y soporte de API DE REST optimizado para la nueva arquitectura de almacenamiento.

#### Preparar la creación de vVols datastores con herramientas ONTAP

Puede omitir los dos primeros pasos del proceso de puesta en marcha si ya utiliza las herramientas de ONTAP para gestionar, automatizar e informar sobre el almacenamiento existente VMFS o el tradicional basado en NFS. También puede consultar este completo ["lista de comprobación"](#) para implementar y configurar las herramientas de ONTAP.

1. Cree la máquina virtual de almacenamiento (SVM) y su configuración de protocolo. Tenga en cuenta que esto puede no ser necesario para los sistemas ASA r2, ya que normalmente ya tendrán una única SVM

para los servicios de datos. Seleccionará NVMe/FC (solo herramientas ONTAP 9.13), NFSv3, NFSv4.1, iSCSI, FCP o una combinación de esas opciones. NVMe/TCP y NVMe/FC también se pueden usar para almacenes de datos VMFS tradicionales con herramientas ONTAP 10.3 y posteriores. Puede utilizar los asistentes del Administrador del sistema ONTAP o la línea de comandos del shell del clúster.

- ["Asigne niveles locales \(agregados\) a SVM"](#) Para todos los sistemas R2 que no son de ASA.
- Al menos un LIF por nodo para cada conexión de switch/estructura. Como práctica recomendada, cree dos o más por nodo para los protocolos basados en FCP, iSCSI o NVMe. Un LIF por nodo es suficiente para vVols basados en NFS, pero este LIF debería estar protegido por un ifgroup de LACP. Consulte ["Descripción general de la configuración de LIF"](#) y ["Combine puertos físicos para crear grupos de interfaces"](#) para obtener más información.
- Al menos un LIF de administración por SVM si pretende utilizar credenciales con alcance de SVM para sus vCenters de inquilino.
- Si planea usar SnapMirror, asegúrese de que su origen y destino ["Los clústeres de ONTAP y las SVM tienen una relación entre iguales"](#).
- Para los sistemas que no sean ASA r2, se pueden crear volúmenes en este momento, pero se recomienda dejar que el asistente *Provision Datastore* en las herramientas de ONTAP los cree. La única excepción a esta regla es si planea utilizar la replicación vVols con VMware Site Recovery Manager y las herramientas ONTAP 9.13. Esto es más fácil de configurar con volúmenes FlexVol preexistentes con relaciones SnapMirror existentes. Tenga en cuenta que no debe habilitar QoS en ningún volumen que se vaya a utilizar para vVols, ya que esto debe ser administrado por las herramientas SPBM y ONTAP .

## 2. ["Ponga en marcha herramientas de ONTAP para VMware vSphere"](#) Utilice el OVA descargado del sitio de soporte de NetApp.

- Las herramientas ONTAP 10.0 y posteriores admiten varios servidores vCenter por dispositivo; ya no es necesario implementar un dispositivo de herramientas ONTAP por vCenter.
  - Si planea conectar varios vCenters a una única instancia de herramientas ONTAP , debe crear e instalar certificados firmados por CA. Referirse a ["Gestionar certificados"](#) para los pasos.
- A partir de la versión 10.3, las herramientas de ONTAP ahora se implementan como un dispositivo pequeño de un solo nodo adecuado para la mayoría de las cargas de trabajo que no son vVols.
  - La mejor práctica recomendada es ["Herramientas de ONTAP de escalado horizontal"](#) 10.3 y posteriores a la configuración de alta disponibilidad (HA) de 3 nodos para todas las cargas de trabajo de producción. Para fines de laboratorio o de prueba, es posible utilizar una implementación de nodo único.
  - La mejor práctica recomendada para el uso de vVols de producción es eliminar cualquier punto único de falla. Cree reglas antiafinidad para evitar que las máquinas virtuales de las herramientas ONTAP se ejecuten juntas en el mismo host. Despues de la implementación inicial, también se recomienda utilizar Storage vMotion para colocar las máquinas virtuales de las herramientas ONTAP en diferentes almacenes de datos. Leer más sobre ["Uso de reglas de afinidad sin vSphere DRS"](#) o ["Cree una regla de afinidad de VM-VM"](#). También debe programar copias de seguridad frecuentes y/o ["utilice la utilidad de copia de seguridad de configuración incorporada"](#).

### 1. Configure las herramientas de ONTAP 10,3 para su entorno.

- ["Añada instancias de vCenter Server"](#) En la IU del administrador de herramientas de ONTAP.
- ONTAP tools 10,3 admite multi-tenancy seguro. Si no necesita multi-tenancy seguro, puede simplemente ["Añada los clústeres de ONTAP"](#) ir al menú de herramientas de ONTAP en vCenter, hacer clic en *Storage backends* y hacer clic en el botón *add*.

- En un entorno multi-tenant seguro en el que desee delegar máquinas virtuales de almacenamiento (SVM) específicas en vCenter específicos, debe hacer lo siguiente.
  - Inicie sesión en la IU del administrador de herramientas de ONTAP
  - "Cree el clúster de almacenamiento"
  - "Asocie un back-end de almacenamiento a una instancia de vCenter Server"
  - Proporcione las credenciales SVM específicas al administrador de vCenter, quien luego agregará el SVM como un back-end de almacenamiento en el menú de back-ends de almacenamiento de las herramientas ONTAP en vCenter.



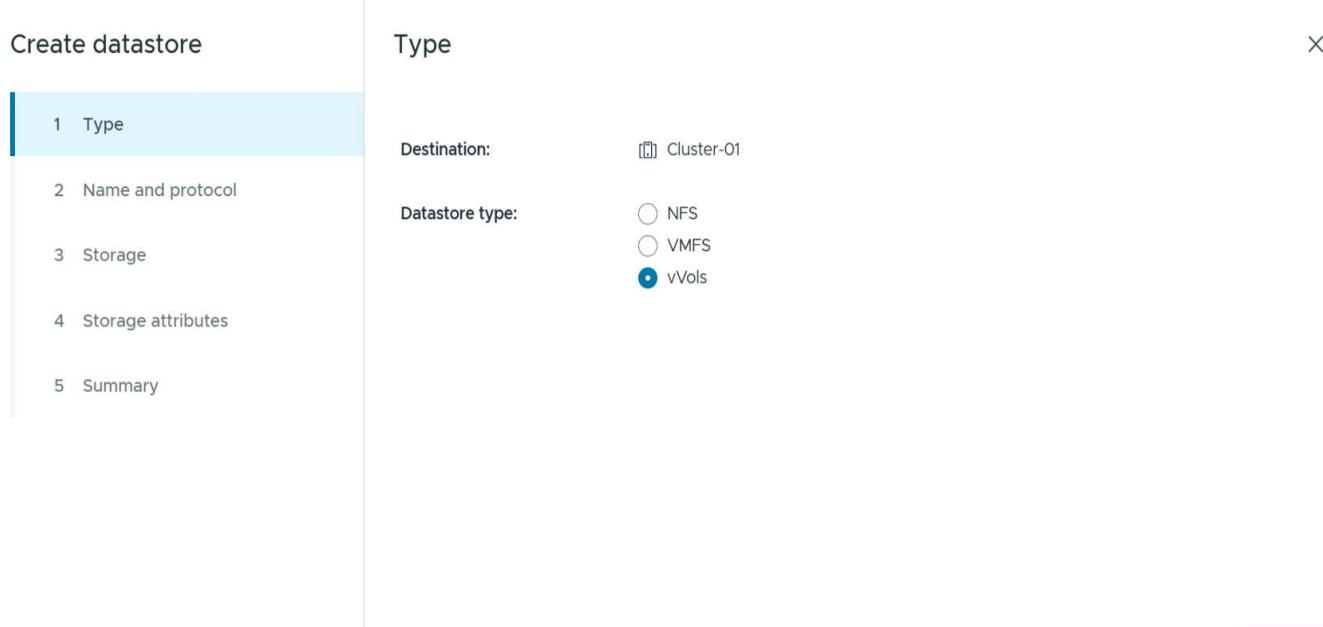
- Crear roles de RBAC para sus cuentas de almacenamiento es una práctica recomendada.
- Las herramientas de ONTAP incluyen un archivo JSON que contiene los permisos de rol necesarios para las cuentas de almacenamiento de las herramientas de ONTAP. Puede cargar el archivo JSON en ONTAP System Manager para simplificar la creación de roles y usuarios RBAC.
- Puede obtener más información acerca de los roles de RBAC de ONTAP en "["Configure los roles y privilegios de usuario de ONTAP"](#)".



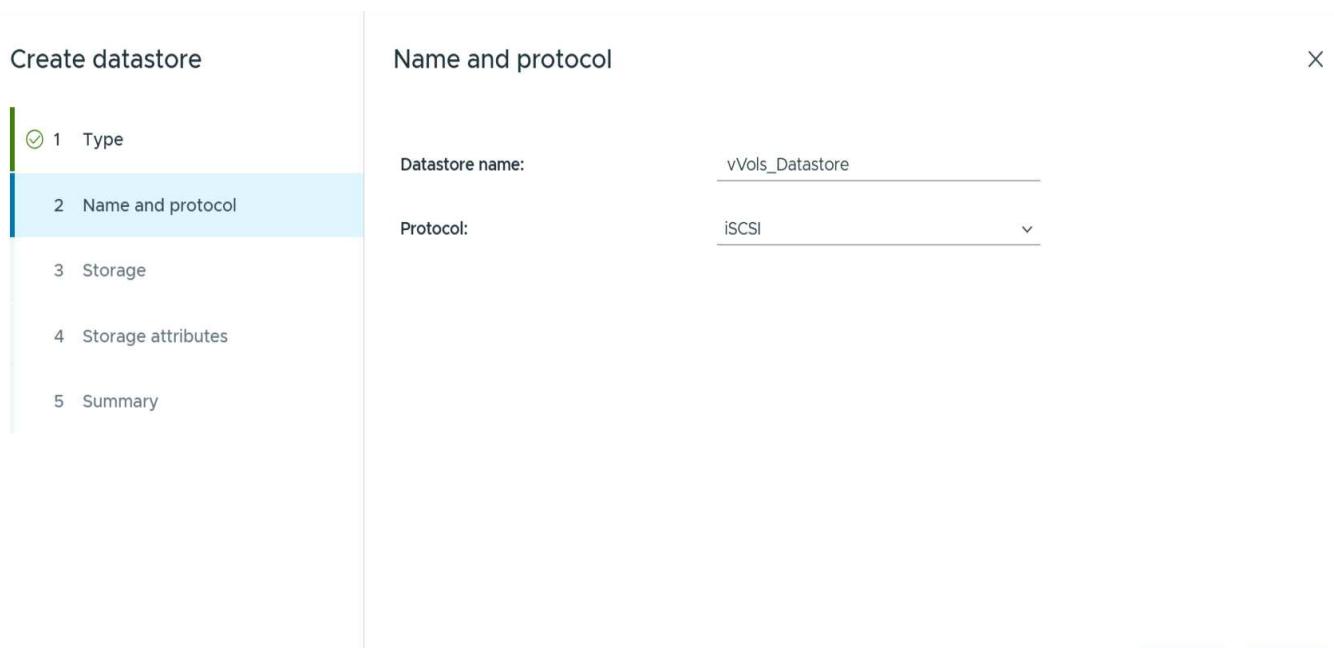
El motivo por el cual todo el clúster debe estar incorporado en la interfaz de usuario del administrador de herramientas de ONTAP es que muchas de las API utilizadas para vVols solo están disponibles en el nivel del clúster.

## Crear almacenes de datos vVols con herramientas de ONTAP

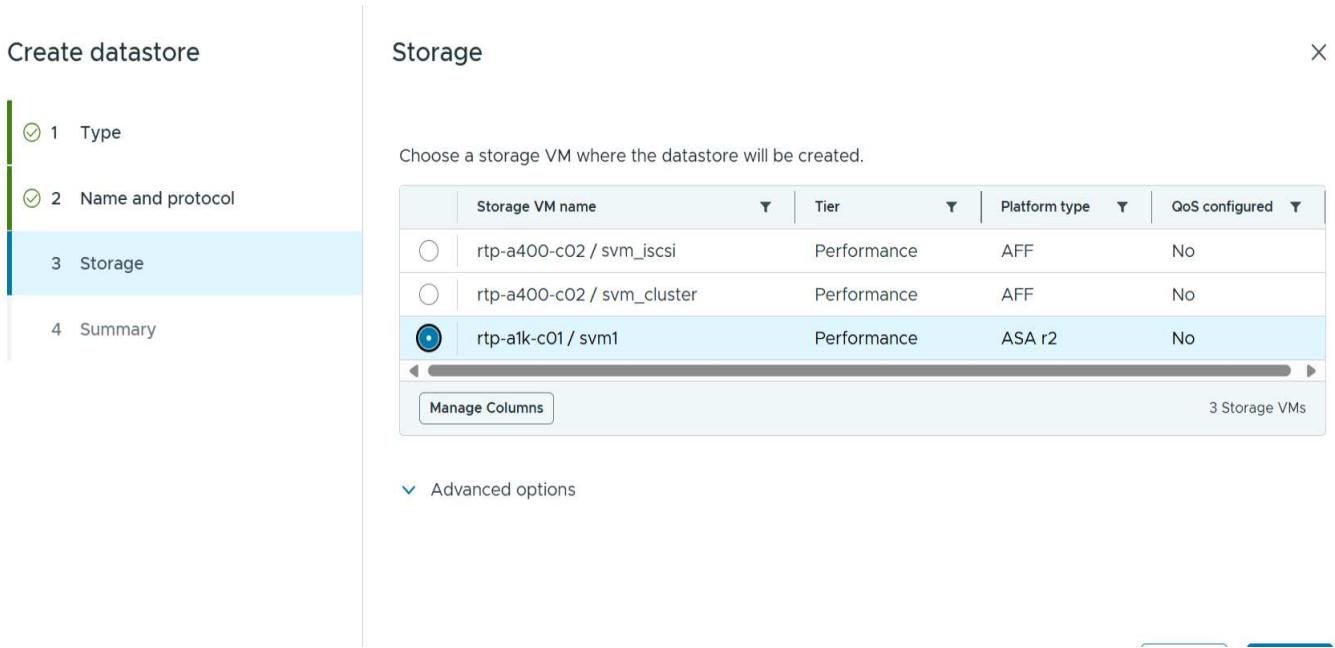
Haga clic con el botón derecho en el host, clúster o centro de datos en el que desea crear el almacén de datos vVols y, a continuación, seleccione *ONTAP tools > Provision Datastore*.



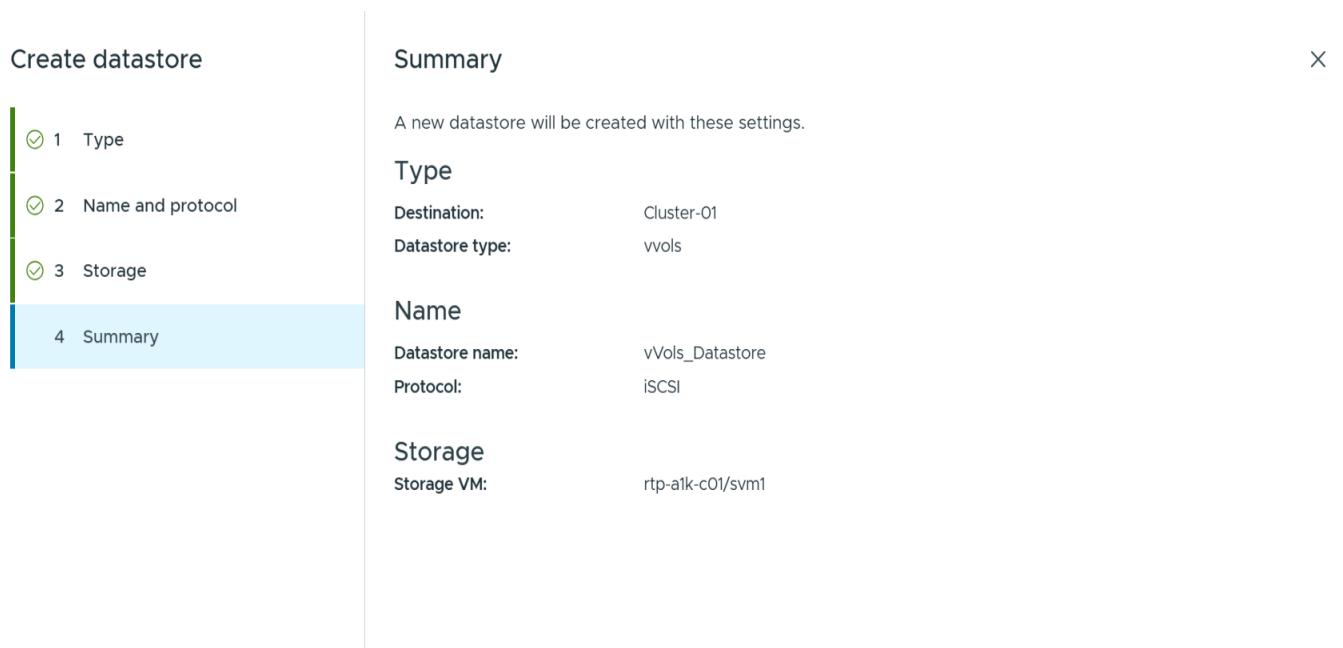
- Elija vVols y proporcione un nombre significativo y seleccione el protocolo deseado. También puede proporcionar una descripción del almacén de datos.
  - ONTAP tools 10,3 con ASA R2.



- Seleccione la SVM del sistema ASA R2 y haga clic en *next*.



- Haga clic en *FINALIZAR*



Create datastore

Summary

A new datastore will be created with these settings.

Type

Destination: Cluster-01  
Datastore type: vVols

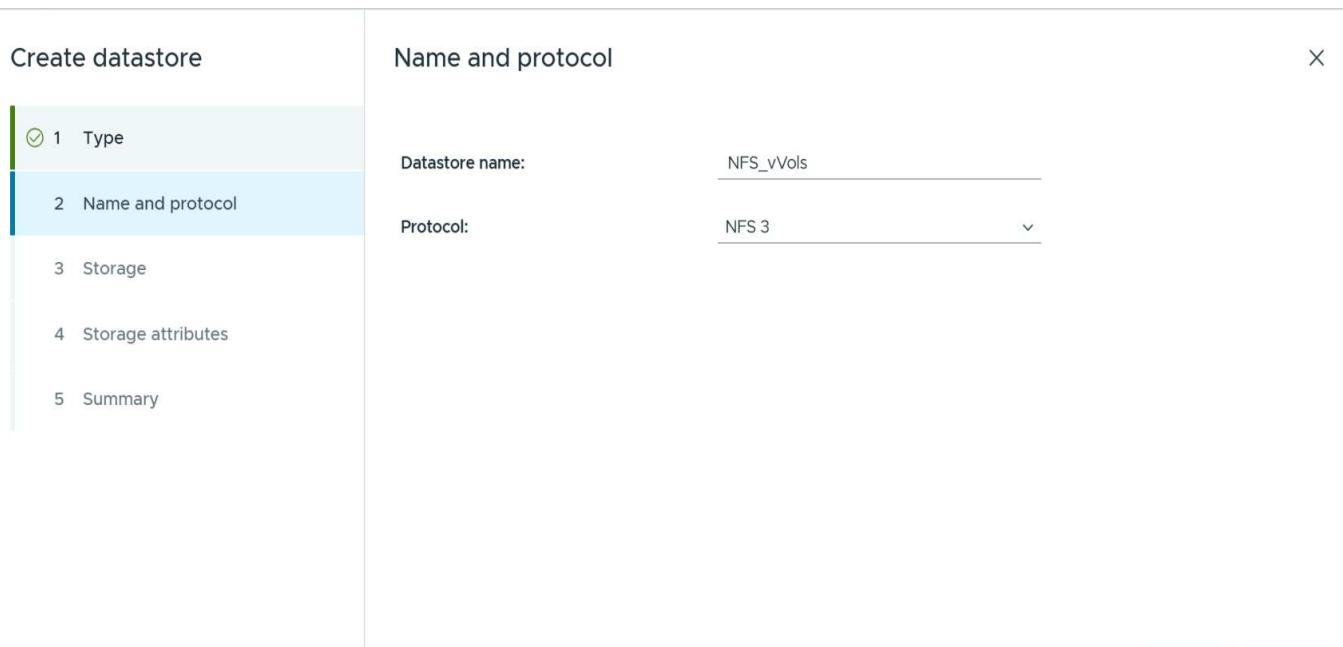
Name

Datastore name: vVols\_Datastore  
Protocol: iSCSI

Storage

Storage VM: rtp-alk-c01/svm1

- ¡Así de fácil!
  - Herramientas ONTAP 10.3 con ONTAP FAS, AFF y ASA anteriores a ASA r2.
- Seleccione el protocolo



Create datastore

Name and protocol

Datastore name: NFS\_vVols

Protocol: NFS 3

- Seleccione la SVM y haga clic en *next*.

**Create datastore**

- 1 Type
- 2 Name and protocol
- 3 Storage
- 4 Storage attributes
- 5 Summary

**Storage**

Choose a storage VM where the datastore will be created.

| Storage VM name                 | Tier        | Platform type | QoS configured |
|---------------------------------|-------------|---------------|----------------|
| rtp-a400-c02 / alpha_new        | Performance | AFF           | No             |
| <b>rtp-a400-c02 / gpvs2</b>     | Performance | AFF           | No             |
| rtp-a400-c02 / alpha2           | Performance | AFF           | No             |
| rtp-a400-c02 / cifs_depot_alpha | Performance | AFF           | No             |

Manage Columns

8 Storage VMs

**Advanced options**

- Haga clic en *agregar nuevos volúmenes o usar volumen existente* y especifique los atributos. Tenga en cuenta que en las herramientas ONTAP 10.3, puede solicitar que se creen varios volúmenes al mismo tiempo. También puede agregar manualmente varios volúmenes para equilibrarlos en el clúster ONTAP . Haga clic en *siguiente*

**Create datastore**

- 1 Type
- 2 Name and protocol
- 3 Storage
- 4 Storage attributes
- 5 Summary

**Add new volume**

Single volume  Multiple volumes

**Volume Name:** \* NFS\_vVols\_Volumes

Volume name will be appended with sequential numbers. For example, <volume\_name>\_01, <volume\_name>\_02 and so on.

**Count:** \* 4

**Size (GB):** \* 1024

**Space reserve:** \* Thin

**Local tier:** \* aggr1\_alpha\_01 ( 22.86 TB Free)

**Advanced options**

**Create datastore**

- 1 Type
- 2 Name and protocol
- 3 Storage
- 4 Storage attributes**
- 5 Summary

**Storage attributes**

Create new volumes or use the existing FlexVol volumes with free size equal to or greater than 5 GB to add storage to the datastore.

**Volumes:**  Create new volumes  Use existing volumes

**ADD NEW VOLUME**

| Name                  | Size | Space reserve | QoS configured | Local tier      |
|-----------------------|------|---------------|----------------|-----------------|
| : NFS_vVols_Volume... | 1 TB | Thin          | No             | aggr1_alpha_... |
| : NFS_vVols_Volume... | 1 TB | Thin          | No             | aggr1_alpha_... |
| : NFS_vVols_Volume... | 1 TB | Thin          | No             | aggr1_alpha_... |
| : NFS_vVols_Volume... | 1 TB | Thin          | No             | aggr1_alpha_... |

4 Volumes

- Haga clic en *FINALIZAR*

**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: Cluster-01  
Datastore type: vvol

**Name**

Datastore name: NFS\_vVols  
Protocol: NFS 3

**Storage**

Storage VM: rtp-a400-c02/gpvs2

**Storage attributes**

Create volumes

- Es posible ver los volúmenes asignados en el menú de herramientas ONTAP de la pestaña de configuración del almacén de datos.

- Ahora puede crear políticas de almacenamiento de máquinas virtuales desde el menú *Policies and Profiles* en la interfaz de usuario de vCenter.

## Migración de máquinas virtuales desde almacenes de datos tradicionales a vVols

La migración de máquinas virtuales de almacenes de datos tradicionales a un almacén de datos vVols es tan sencilla como mover máquinas virtuales entre almacenes de datos tradicionales. Solo tiene que seleccionar las máquinas virtuales y, a continuación, seleccionar *Migrate* en la lista *Actions* y seleccionar un tipo de migración *change storage only*. Cuando se le solicite, seleccione una política de almacenamiento de máquinas virtuales que coincida con su almacén de datos de vVols. Las operaciones de copia de migración se pueden descargar con vSphere 6,0 y versiones posteriores para las migraciones de SAN VMFS a vVols, pero no de VMDK de NAS a vVols.

## Gestionar máquinas virtuales con políticas

Para automatizar el aprovisionamiento de almacenamiento con administración basada en políticas, debe crear políticas de almacenamiento de VM que se correspondan con las capacidades de almacenamiento deseadas.

**Información:** Las herramientas de ONTAP 10,0 y versiones posteriores ya no utilizan los perfiles de capacidades de almacenamiento como las versiones anteriores. Las capacidades de almacenamiento se definen directamente en la propia política de almacenamiento de máquinas virtuales.

## Creación de políticas de almacenamiento de equipos virtuales

Las políticas de almacenamiento de VM se utilizan en vSphere para administrar funciones opcionales como el control de E/S de almacenamiento o el cifrado de vSphere. También se utilizan con vVols para aplicar capacidades de almacenamiento específicas a la VM. Utilice el tipo de almacenamiento "NetApp.clustered.Data. ONTAP.VP.vvol". Consulte el enlace: [vmware-vvols-ontap.html#Best Practices](#) [ejemplo de configuración de red usando vVols sobre NFS v3] para ver un ejemplo de esto con el proveedor VASA de herramientas ONTAP. Las reglas para el almacenamiento "NetApp.clustered.Data. ONTAP.VP.VASA10" deben usarse con almacenes de datos que no estén basados en vVols.

Una vez creada la política de almacenamiento, esta se puede utilizar para aprovisionar nuevos equipos virtuales.

Policies and Profiles

- VM Storage Policies
- VM Customization Specifications
- Host Profiles
- Compute Policies
- Storage Policy Components

VM Storage Policies

CREATE

Quick Filter

|                          | Name                                       | VC                                       |
|--------------------------|--|--|
| <input type="checkbox"/> | VM Encryption Policy                       | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | vSAN Default Storage Policy                | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | vVol No Requirements Policy                | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Management Storage Policy - Regular        | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Management Storage policy - Thin           | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Management Storage Policy - Large          | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Management Storage Policy - Stretched      | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Management Storage Policy - Stretched Lite | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Management Storage Policy - Single Node    | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Management Storage policy - Encryption     | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | Host-local PMem Default Storage Policy     | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | vsAN ESA Default Policy - RAID5            | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | vsAN ESA Default Policy - RAID10           | vcf-vc01.onappmtme.openenglab.netapp.com |
| <input type="checkbox"/> | vsAN ESA Default Policy - RAID1            | vcf-vc01.onappmtme.openenglab.netapp.com |

## Create VM Storage Policy

- 1 Name and description
  - 2 Policy structure
  - 3 Storage compatibility
  - 4 Review and finish

## Create VM Storage Policy

- 1 Name and description
  - 2 Policy structure**
  - 3 NetApp.clustered.Data.ONTAP.VI  
vvol rules
  - 4 Storage compatibility
  - 5 Review and finish

### Name and description

### vCenter Server:

VCE-VC01 ONTAPPMTME OPENENGLAB NETAPP.COM

Name: \_\_\_\_\_

## NetApp VM Storage Policy

**Description:**

## Policy structure

## Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.

Enable host based rules

### Datastore specific rules

Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

Enable rules for "vSAN" storage

Enable rules for "vSANDirect" storage

Enable rules for "VB.NET" (MEF)

Enable rules for "VMFS" storage

Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage

Enable tag based placement rules

## Tanzu on vSphere Storage topology

Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.

Enable Zonal topology for multi-zone Supervisor

## Create VM Storage Policy

1 Name and description

2 Policy structure

### 3 NetApp.clustered.Data.ONTAP.VP.vvol rules

4 Storage compatibility

5 Review and finish

## NetApp.clustered.Data.ONTAP.VP.vvol rules

Placement Tags

Platform Type ①

AFF

Tier ①

Performance

Space Efficiency ①

Thin

ADD RULE ▼

QoS IOPS

## Create VM Storage Policy

1 Name and description

2 Policy structure

### 3 NetApp.clustered.Data.ONTAP.VP.vvol rules

4 Storage compatibility

5 Review and finish

## NetApp.clustered.Data.ONTAP.VP.vvol rules

Placement Tags

Platform Type ①

AFF

Tier ①

Performance

Space Efficiency ①

Thin

QoS IOPS ①

REMOVE

MaxThroughput IOPS ①

10000

MinThroughput IOPS ①

1000

## Create VM Storage Policy

1 Name and description

2 Policy structure

### 3 NetApp.clustered.Data.ONTAP.VP.vvol rules

4 Storage compatibility

5 Review and finish

## Storage compatibility

COMPATIBLE INCOMPATIBLE

Expand datastore clusters

Compatible storage 4 TB (3.8 TB free)

Quick Filter

| Name      | Datacenter | Type | Free Space | Capacity | Warnings |
|-----------|------------|------|------------|----------|----------|
| NFS_vVols | Raleigh    | vVol | 3.80 TB    | 4.00 TB  |          |



**Create VM Storage Policy**

- 1 Name and description
- 2 Policy structure
- 3 NetApp.clustered.Data.ONTAP.VP.vvol rules
- 4 Storage compatibility
- 5 Review and finish**

**Review and finish**

**General**

|             |   |
|-------------|---|
| Name        | NetApp VM Storage Policy                  |
| Description | vcf-vc01.ontappmtme.openenglab.netapp.com |

**NetApp.clustered.Data.ONTAP.VP.vvol rules**

**Placement**

|                    |             |
|--------------------|-------------|
| Platform Type      | AFF         |
| Tier               | Performance |
| Space Efficiency   | Thin        |
| QoS IOPS           |             |
| MaxThroughput IOPS | 10,000      |
| MinThroughput IOPS | 1,000       |

CANCEL
BACK
FINISH

## Gestión del rendimiento con herramientas de ONTAP

Las herramientas de ONTAP utilizan su propio algoritmo de colocación equilibrada para colocar un nuevo VVOL en el mejor FlexVol volume con sistemas ASA unificados o clásicos, o zona de disponibilidad de almacenamiento (SAZ) con sistemas ASA R2, dentro de un almacén de datos vVols. La colocación se basa en asociar el almacenamiento de respaldo con la normativa de almacenamiento de las máquinas virtuales. Esto garantiza que el almacén de datos y el almacenamiento de respaldo puedan cumplir con los requisitos de rendimiento especificados.

Cambiar las capacidades de rendimiento, como IOPS mínimo y máximo, requiere cierta atención a la configuración específica.

- **IOPS mín. Y máx.** se pueden especificar en una Política de VM.
  - Cambiar las IOPS en la política no cambiará la calidad de servicio en los vVols hasta que la política de VM se vuelva a aplicar a las VM que la utilizan. O puede crear una nueva política con las IOPS deseadas y aplicarla a las máquinas virtuales de destino. En general, se recomienda simplemente definir políticas de almacenamiento de VM independientes para diferentes niveles de servicio y simplemente cambiar la política de almacenamiento de VM en la VM.
  - Las personalidades ASA, ASA r2, AFF y FAS tienen diferentes configuraciones de IOP. Tanto Min como Max están disponibles en todos los sistemas flash; sin embargo, los sistemas que no son AFF solo pueden usar configuraciones de IOP Max.
- Las herramientas de ONTAP crean políticas de calidad de servicio individuales no compartidas con las versiones actuales compatibles de ONTAP. Por lo tanto, cada VMDK individual recibirá su propia asignación de IOPS.

## Nueva aplicación de la normativa de almacenamiento de equipos virtuales

## VM Storage Policies

|                                     | Name                                       | VC                              |
|-------------------------------------|--|---------------------------------|
| <input type="checkbox"/>            | Management Storage Policy - Large          | vm-is-vcenter01.vtme.netapp.com |
| <input type="checkbox"/>            | VVol No Requirements Policy                | vm-is-vcenter01.vtme.netapp.com |
| <input type="checkbox"/>            | Management Storage Policy - Stretched Lite | vm-is-vcenter01.vtme.netapp.com |
| <input type="checkbox"/>            | VM Encryption Policy                       | vm-is-vcenter01.vtme.netapp.com |
| <input type="checkbox"/>            | Management Storage policy - Encryption     | vm-is-vcenter01.vtme.netapp.com |
| <input type="checkbox"/>            | Management Storage Policy - Single Node    | vm-is-vcenter01.vtme.netapp.com |
| <input type="checkbox"/>            | Management Storage policy - Thin           | vm-is-vcenter01.vtme.netapp.com |
| <input checked="" type="checkbox"/> | AFF_iSCSI_VMSP                             | vm-is-vcenter01.vtme.netapp.com |
| <input type="checkbox"/>            | Host-local PMem Default Storage Policy     | vm-is-vcenter01.vtme.netapp.com |
| <input checked="" type="checkbox"/> | 1  | 14 items                        |

## Protección de vVols

Las siguientes secciones describen los procedimientos y las mejores prácticas para usar vVols de VMware con almacenamiento de ONTAP.

### Alta disponibilidad del proveedor de VASA

El proveedor VASA de NetApp se ejecuta como parte del dispositivo virtual junto con el complemento para vCenter y el servidor de la API de REST (anteriormente conocido como Virtual Storage Console [VSC]) y Storage Replication Adapter. Si el proveedor VASA no está disponible, se seguirán ejecutando las máquinas virtuales que utilizan vVols. Sin embargo, no se pueden crear nuevos almacenes de datos vVols y no se puede crear ni enlazar vVols mediante vSphere. Esto significa que las máquinas virtuales que usan vVols no se pueden encender ya que vCenter no podrá solicitar la creación del VVol de intercambio. Y las máquinas virtuales en ejecución no pueden usar vMotion para migrar a otro host porque vVols no puede vincularse al nuevo host.

VASA Provider 7.1 y versiones posteriores admiten nuevas funcionalidades para garantizar que los servicios estén disponibles cuando se necesiten. Incluye nuevos procesos de vigilancia que supervisan el proveedor VASA y los servicios integrados de base de datos. Si detecta un fallo, actualiza los archivos de registro y, a continuación, reinicia los servicios automáticamente.

El administrador de vSphere debe configurar una mayor protección con las mismas funciones de disponibilidad utilizadas para proteger otras máquinas virtuales críticas para el negocio de fallos en software, hardware de host y red. No se requiere configuración adicional en el dispositivo virtual para utilizar estas funciones; simplemente configúrelas mediante enfoques de vSphere estándar. Han sido probados y cuentan con soporte de NetApp.

vSphere High Availability se puede configurar fácilmente para reiniciar un equipo virtual en otro host del clúster de hosts en caso de fallo. La tolerancia a fallos de vSphere proporciona una mayor disponibilidad al crear un equipo virtual secundario que se replica continuamente y que puede asumir el control en cualquier punto. La información adicional sobre estas funciones está disponible en la ["Documentación de las herramientas de ONTAP para VMware vSphere \(Configurar alta disponibilidad para herramientas de ONTAP\)"](#). Además de la documentación de VMware vSphere (busque vSphere Availability en ESXi y vCenter Server).

Las herramientas de ONTAP VASA Provider realiza automáticamente backups de la configuración de vVols en tiempo real en sistemas ONTAP gestionados donde la información de vVols se almacena en metadatos de volumen de FlexVol. En el caso de que el dispositivo de herramientas de ONTAP deje de estar disponible por cualquier motivo, puede implementar uno nuevo de forma fácil y rápida e importar la configuración. Consulte este artículo de la base de conocimientos para obtener más información sobre los pasos de recuperación del proveedor VASA:

["Cómo realizar una recuperación de desastres de un proveedor VASA: Guía de resolución"](#)

## Replicación de vVols

Muchos clientes de ONTAP replican sus almacenes de datos tradicionales en sistemas de almacenamiento secundario mediante SnapMirror de NetApp y, a continuación, utilizan el sistema secundario para recuperar máquinas virtuales individuales o todo un sitio en caso de desastre. En la mayoría de los casos, los clientes utilizan una herramienta de software para gestionarlo, por ejemplo, un producto de software de backup como el complemento de NetApp SnapCenter para VMware vSphere o una solución de recuperación ante desastres como Site Recovery Manager de VMware (junto con el adaptador de replicación de almacenamiento en herramientas de ONTAP).

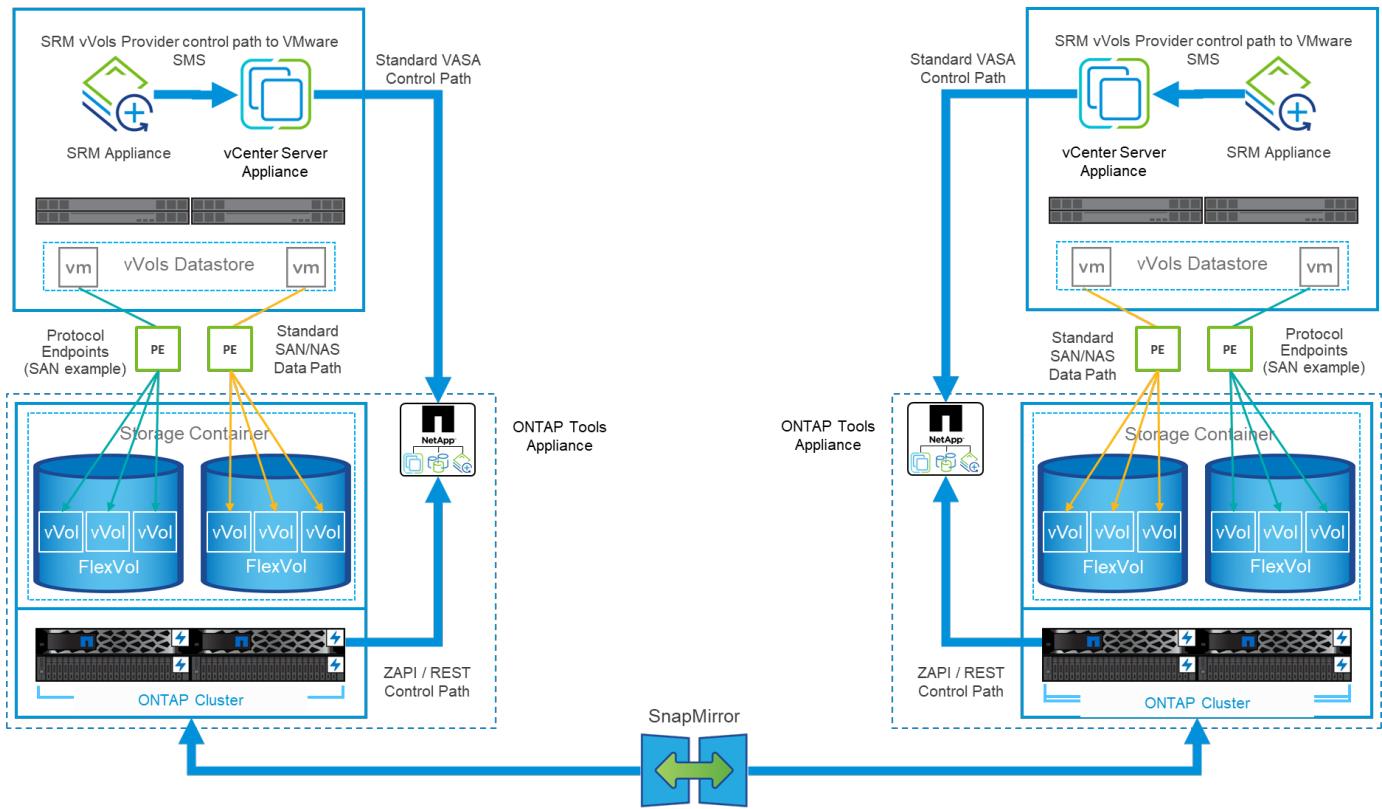
Este requisito de una herramienta de software es aún más importante para gestionar la replicación vVols. A pesar de que algunos aspectos pueden gestionarse mediante funcionalidades nativas (por ejemplo, las copias Snapshot de vVols gestionadas por VMware se descargan a ONTAP, que utiliza clones de archivos o LUN rápidos y eficientes), se necesita una orquestación general para gestionar la replicación y la recuperación. Los metadatos acerca de vVols están protegidos tanto por ONTAP como por el proveedor VASA, pero es necesario procesar más para usarlos en un sitio secundario.

Las herramientas de ONTAP 9.7.1, junto con la versión VMware Site Recovery Manager (SRM) 8.3, añadieron compatibilidad para la recuperación ante desastres y la orquestación del flujo de trabajo de migración aprovechando la tecnología SnapMirror de NetApp.

En la versión inicial de la compatibilidad de SRM con las herramientas de ONTAP 9.7.1, era necesario crear previamente volúmenes de FlexVol y habilitar la protección SnapMirror antes de usarlos como backups de volúmenes para un almacén de datos vVols. A partir de ONTAP TOOLS 9.10, ese proceso ya no es necesario. Ahora puede añadir protección de SnapMirror a los volúmenes de respaldo existentes y actualizar sus políticas de almacenamiento de máquinas virtuales para aprovechar la gestión basada en políticas con recuperación ante desastres y orquestación de migración, y automatización integrada con SRM.

Actualmente, VMware SRM es la única solución de recuperación ante desastres y automatización de la migración para vVols compatible con NetApp, y las herramientas de ONTAP comprobarán la existencia de un servidor SRM 8.3 o posterior registrado en su vCenter antes de permitir habilitar la replicación de vVols. Aunque es posible aprovechar las API de REST DE herramientas de ONTAP para crear sus propios servicios.

## Replicación de vVols con SRM



## Soporte de MetroCluster

Aunque las herramientas de ONTAP no pueden activar una conmutación por error de MetroCluster, sí son compatibles con los sistemas MetroCluster de NetApp para vVols que realizan el backup de volúmenes en una configuración uniforme de vSphere Metro Storage Cluster (VMSC). La conmutación de un sistema MetroCluster se efectúa de la forma normal.

Aunque SnapMirror Business Continuity (SM-BC) de NetApp también puede utilizarse como base para una configuración VMSC, actualmente no es compatible con vVols.

Consulte estas guías para obtener más información sobre MetroCluster de NetApp:

["TR-4689 Arquitectura y diseño de la solución MetroCluster IP"](#)

["TR-4705 Arquitectura y diseño de la solución MetroCluster de NetApp"](#)

["VMware KB 2031038 Soporte de VMware vSphere con NetApp MetroCluster"](#)

## Descripción general de vVols Backup

Existen varios enfoques para proteger las máquinas virtuales, como el uso de agentes de backup internos, la asociación de archivos de datos de máquinas virtuales a un proxy de backup o el uso de API definidas como VMware VADP. Es posible que vVols esté protegido usando los mismos mecanismos, y muchos partners de NetApp admiten backups de VM, incluidos vVols.

Como se ha mencionado anteriormente, las snapshots gestionadas por VMware vCenter se descargan en clones rápidos de archivos o LUN de ONTAP con gestión eficiente del espacio. Se pueden utilizar para realizar backups manuales rápidos, pero el vCenter limita a un máximo de 32 copias Snapshot. Puede utilizar vCenter para tomar Snapshot y revertir según sea necesario.

Comenzando con el complemento SnapCenter para VMware vSphere (SCV) 4,6 cuando se usa junto con

ONTAP Tools 9,10 y versiones posteriores añade soporte para el backup y la recuperación consistentes con los fallos de máquinas virtuales basadas en vVols aprovechando snapshots de volúmenes de ONTAP FlexVol con compatibilidad con replicación de SnapMirror y SnapVault. Se admiten hasta 1023 copias Snapshot por volumen. SCV también puede almacenar más copias Snapshot con una retención más prolongada en volúmenes secundarios mediante SnapMirror con una política de reflejo de almacenamiento.

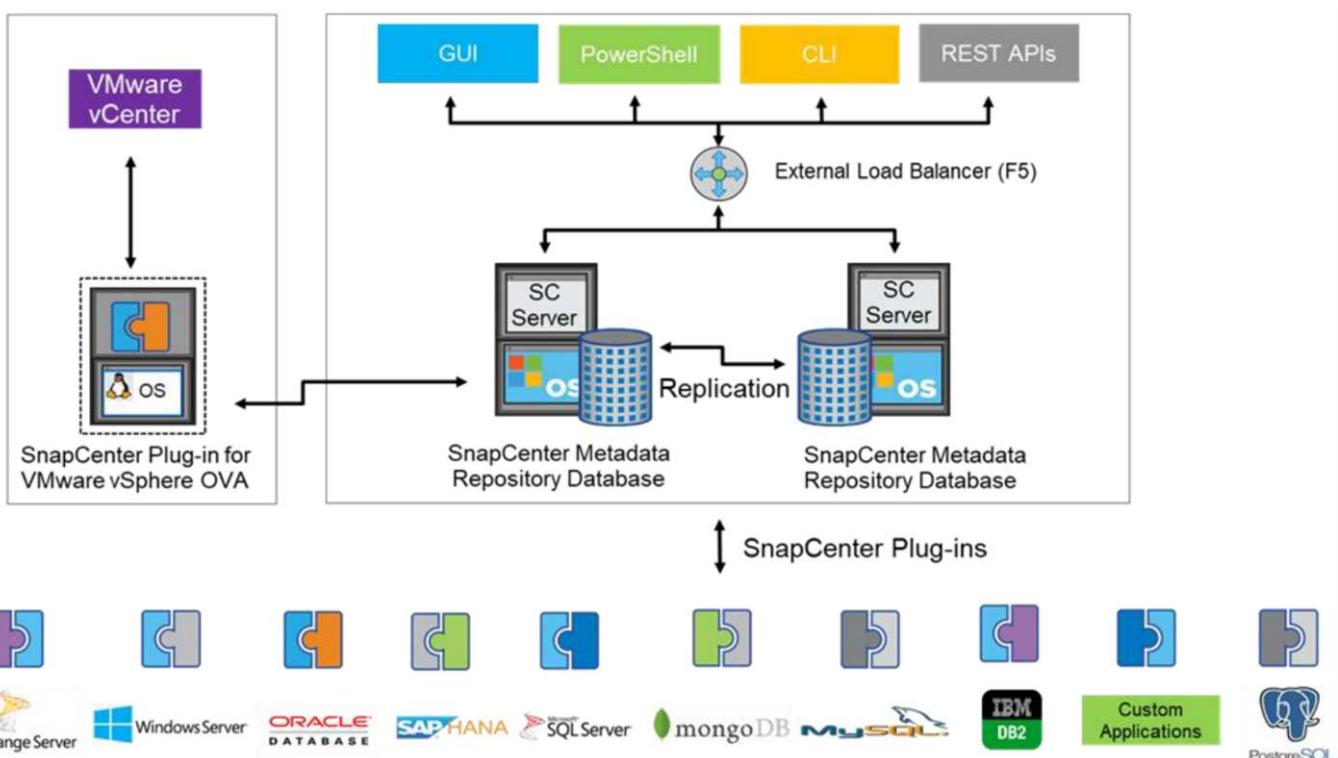
Se introdujo la compatibilidad con vSphere 8,0 con SCV 4,7, que utilizó una arquitectura de complemento local aislada. Se agregó compatibilidad con vSphere 8.0U1 a SCV 4,8, que realizó la transición completa a la nueva arquitectura de complementos remotos.

## VVols Backup con el complemento de SnapCenter para VMware vSphere

Con NetApp SnapCenter, ahora puede crear grupos de recursos para vVols basados en etiquetas y/o carpetas para aprovechar automáticamente las snapshots basadas en FlexVol de ONTAP para máquinas virtuales basadas en vVols. De este modo, podrá definir servicios de backup y recuperación de datos que protegerán automáticamente las máquinas virtuales cuando se aprovisionen dinámicamente en su entorno.

El complemento de SnapCenter para VMware vSphere se pone en marcha como dispositivo independiente registrado como extensión de vCenter, gestionado a través de la interfaz de usuario de vCenter o a través de API de REST para la automatización de servicios de backup y recuperación de datos.

### Arquitectura SnapCenter



Como los otros complementos de SnapCenter aún no admiten vVols en el momento de escribir este documento, nos centraremos en el modelo de implementación independiente de este documento.

Como SnapCenter utiliza copias Snapshot de ONTAP FlexVol, no se genera ninguna sobrecarga en vSphere ni el rendimiento se ve afectado por las máquinas virtuales tradicionales utilizando copias Snapshot gestionadas de vCenter. Además, dado que la funcionalidad de SCV se expone a través de las API DE REST, es más fácil crear flujos de trabajo automatizados mediante herramientas como Aria Automation de VMware, Ansible, Terraform y prácticamente cualquier otra herramienta de automatización capaz de usar API DE REST estándar.

Para obtener más información sobre las API de REST de SnapCenter, consulte "["Información general de las API de REST"](#)"

Para obtener información sobre las API de REST del plugin de SnapCenter para VMware vSphere, consulte "["API de REST del plugin de SnapCenter para VMware vSphere"](#)"

### Mejores prácticas

Las siguientes mejores prácticas pueden ayudarle a sacar el máximo partido de la puesta en marcha de SnapCenter.

- SCV es compatible con el control de acceso basado en roles de vCenter Server y de ONTAP, e incluye roles predefinidos de vCenter que se crean automáticamente para usted cuando se registra el plugin. Es posible obtener más información sobre los tipos de RBAC admitidos "["aquí"](#)".
  - Use la interfaz de usuario de vCenter para asignar acceso a cuentas con menos privilegios mediante los roles predefinidos descritos "["aquí"](#)".
  - Si utiliza SCV con SnapCenter Server, debe asignar el rol *SnapCenterAdmin*.
  - El control de acceso basado en roles de ONTAP hace referencia a la cuenta de usuario que se utiliza para añadir y gestionar los sistemas de almacenamiento que utiliza SCV. El control de acceso basado en roles de ONTAP no se aplica a los backups basados en vVols. Obtenga más información sobre el control de acceso basado en roles de ONTAP y SCV "["aquí"](#)".
- Replique sus conjuntos de datos de backups en un segundo sistema mediante SnapMirror para obtener réplicas completas de volúmenes de origen. Como ya se ha mencionado anteriormente, también puede utilizar políticas de mirror-vault para la retención a largo plazo de los datos de backup con independencia de la configuración de retención de copias Snapshot del volumen de origen. Ambos mecanismos son compatibles con vVols.
- Dado que SCV también requiere las herramientas de ONTAP para la funcionalidad de VMware vSphere para vVols, compruebe siempre la compatibilidad de versiones específica de la Herramienta de Matriz de Interoperabilidad (IMT) de NetApp
- Si usa la replicación de vVols con VMware SRM, tenga en cuenta el objetivo de punto de recuperación y la programación de backups de su política
- Diseñe sus políticas de backup con ajustes de retención que cumplan los objetivos de punto de recuperación (RPO) definidos de su organización
- Configure los ajustes de notificación en los grupos de recursos para que se notifique el estado cuando se ejecuten los backups (consulte la figura 10 a continuación).

### Opciones de notificación para el grupo de recursos

## Edit Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

✓ 5. Schedules

✓ 6. Summary

|                         |   |
|-------------------------|---|
| vCenter Server:         | vm-is-vcenter01.vtme.netapp.com   |
| Name:                   | vVols_VMs   |
| Description:            | Description   |
| Notification:           | Never   |
| Email send from:        | Error or Warnings   |
| Email send to:          | Errors  |
| Email subject:          | Always  |
| Latest Snapshot name    | Never   |
| Custom snapshot format: | <input checked="" type="checkbox"/> Enable _recent suffix for latest Snapshot Copy <small>i</small> |
|                         | <input type="checkbox"/> Use custom name format for Snapshot copy                                   |

Note that the Plug-in for VMware vSphere cannot do the following:

**BACK** **NEXT** **FINISH** **CANCEL**

### Comience a usar SCV usando estos documentos

["Obtenga información sobre el plugin de SnapCenter para VMware vSphere"](#)

["Ponga en marcha el plugin de SnapCenter para VMware vSphere"](#)

### Resolución de problemas

Existen varios recursos de solución de problemas disponibles con información adicional.

#### Sitio de soporte de NetApp

Además de una variedad de artículos de la base de conocimientos para los productos de virtualización de NetApp, el sitio de soporte de NetApp también ofrece una página de inicio práctica para el ["Herramientas de ONTAP para VMware vSphere"](#) producto. Este portal proporciona enlaces a artículos, descargas, informes técnicos y debates sobre soluciones de VMware sobre la comunidad de NetApp. Está disponible en:

["Sitio de soporte de NetApp"](#)

Aquí se encuentra disponible documentación adicional sobre la solución:

["Soluciones de NetApp para la virtualización con VMware de Broadcom"](#)

#### Solución de problemas del producto

Los distintos componentes de las herramientas de ONTAP, como el complemento vCenter, el proveedor VASA y el adaptador de replicación de almacenamiento, se documentan juntos en el repositorio de documentos de NetApp. Sin embargo, cada uno tiene una subsección independiente de la base de conocimientos y puede tener procedimientos específicos de solución de problemas. Estos solucionan los problemas más comunes

que se pueden encontrar con el proveedor VASA.

#### Problemas de interfaz de usuario del proveedor de VASA

Ocasionalmente, vCenter vSphere Web Client encuentra problemas con los componentes de Serenity, lo que hace que no se muestren los elementos de menú VASA Provider for ONTAP. Consulte Resolver problemas de registro del proveedor VASA en la guía de puesta en marcha o esta base de conocimientos "[artículo](#)".

#### Error de aprovisionamiento del almacén de datos de vVols

En ocasiones, es posible que se agote el tiempo de espera de los servicios de vCenter al crear el almacén de datos vVols. Para corregirlo, reinicie el servicio vmware-sps y vuelva a montar el almacén de datos vVols mediante los menús de vCenter (Storage > New Datastore). Esto se trata en el error del aprovisionamiento de almacenes de datos de vVols con vCenter Server 6,5 en la guía de administración.

#### La actualización de Unified Appliance no puede montar ISO

Debido a un error en vCenter, es posible que el ISO utilizado para actualizar Unified Appliance de una versión a la siguiente no se pueda montar. Si la ISO se puede conectar al dispositivo en vCenter, siga el proceso en esta base de conocimientos "[artículo](#)" para solucionar.

## VMware Site Recovery Manager con ONTAP

### Recuperación de sitios en vivo de VMware con ONTAP

ONTAP ha sido una solución de almacenamiento líder para VMware vSphere y, más recientemente, Cloud Foundation, desde que ESX se introdujo en los centros de datos modernos hace más de dos décadas. NetApp continúa introduciendo sistemas innovadores, como la última generación de la serie ASAA, junto con funciones como la sincronización activa SnapMirror. Estos avances simplifican la gestión, mejoran la resiliencia y reducen el costo total de propiedad (TCO) de su infraestructura de TI.

Este documento presenta la solución ONTAP para VMware Live Site Recovery (VLSR), anteriormente conocido como Site Recovery Manager (SRM), el software de recuperación ante desastres (DR) líder en la industria de VMware, que incluye la información más reciente del producto y las mejores prácticas para optimizar la implementación, reducir el riesgo y simplificar la gestión continua.



Esta documentación reemplaza el informe técnico publicado anteriormente *TR-4900: VMware Site Recovery Manager con ONTAP*

Las prácticas recomendadas complementan otros documentos como guías y herramientas de compatibilidad. Se desarrollan según pruebas de laboratorio y una amplia experiencia de campo por parte de ingenieros y clientes de NetApp. En algunos casos, las prácticas recomendadas pueden no ser la opción adecuada para su entorno; sin embargo, generalmente son las soluciones más sencillas que satisfacen las necesidades del mayor número de clientes.

Este documento se centra en las funcionalidades de los últimos lanzamientos de ONTAP 9 cuando se utiliza junto con las herramientas de ONTAP para VMware vSphere 10,4 (que incluye el adaptador de replicación del almacenamiento de NetApp [SRA] y el proveedor VASA [VP]), así como la recuperación de sitio en activo de VMware 9.

## ¿Por qué usar ONTAP con VLSR o SRM?

Las plataformas de gestión de datos de NetApp impulsadas por ONTAP son algunas de las soluciones de almacenamiento más adoptadas para VLSR. Las razones son abundantes: una plataforma de gestión de datos segura, de alto rendimiento y con protocolo unificado (NAS y SAN juntos) que proporciona eficiencia de almacenamiento que define la industria, multitenencia, controles de calidad de servicio, protección de datos con instantáneas que ahorran espacio y replicación con SnapMirror. Todo ello aprovechando la integración nativa de múltiples nubes híbridas para la protección de las cargas de trabajo de VMware y una gran cantidad de herramientas de automatización y orquestación a su alcance.

Cuando utiliza SnapMirror para la replicación basada en matrices, aprovecha una de las tecnologías más probadas y maduras de ONTAP. SnapMirror le ofrece la ventaja de realizar transferencias de datos seguras y altamente eficientes, copiando únicamente bloques del sistema de archivos modificados, no máquinas virtuales o almacenes de datos completos. Incluso esos bloques aprovechan los ahorros de espacio, como la deduplicación, la compresión y la compactación. Los sistemas ONTAP modernos ahora utilizan SnapMirror independiente de la versión, lo que le permite flexibilidad al seleccionar sus clústeres de origen y destino. SnapMirror se ha convertido verdaderamente en una de las herramientas más poderosas disponibles para la recuperación ante desastres.

Ya sea que utilice almacenes de datos tradicionales conectados a NFS, iSCSI o Fibre Channel (ahora con soporte para almacenes de datos vVols), VLSR proporciona una oferta sólida de primera mano que aprovecha lo mejor de las capacidades de ONTAP para la recuperación ante desastres o la planificación y orquestación de la migración del centro de datos.

## Aprovechamiento de VLSR ONTAP 9

VLSR aprovecha las tecnologías avanzadas de gestión de datos de los sistemas de ONTAP al integrarse con herramientas de ONTAP para VMware vSphere, un dispositivo virtual que incluye tres componentes principales:

- El complemento de herramientas de ONTAP para vCenter, anteriormente conocido como consola de almacenamiento virtual (VSC), simplifica 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 obtener todos estos beneficios, NetApp recomienda este plugin cuando se utiliza vSphere con sistemas que ejecutan ONTAP.
- Las herramientas de ONTAP VASA Provider admiten las API de VMware vStorage para el marco de conocimiento del almacenamiento (VASA). El proveedor DE VASA conecta vCenter Server con ONTAP para ayudar en el aprovisionamiento y la supervisión del almacenamiento de máquinas virtuales. Esto ha permitido el soporte de VMware Virtual Volumes (vVols) y la gestión de políticas de almacenamiento de VM y el rendimiento de vVols individuales de VM. También proporciona alarmas para controlar la capacidad y el cumplimiento de los perfiles.
- El SRA se usa junto con el VLSR 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. Incluye tanto un dispositivo de servidor SRA como adaptadores SRA para el servidor SRM de Windows y el dispositivo VLSR.

Después de haber instalado y configurado los adaptadores SRA en el servidor VLSR para proteger almacenes de datos que no sean vVols, puede comenzar la tarea de configurar su entorno vSphere para la recuperación ante desastres.

El SRA proporciona una interfaz de comando y control para que el servidor VLSR gestione los volúmenes de

ONTAP FlexVol que contienen las máquinas virtuales de VMware (VM), además de la replicación de SnapMirror que las protege.

VLSR puede probar su plan de recuperación ante desastres de forma no disruptiva utilizando la tecnología FlexClone, propiedad de NetApp, para realizar clones casi instantáneos de sus almacenes de datos protegidos en su sitio de recuperación ante desastres. VLSR crea un entorno sandbox para realizar pruebas de forma segura para que su organización y sus clientes estén protegidos en caso de un verdadero desastre, lo que le brinda confianza en la capacidad de su organización para ejecutar una comutación por error durante un desastre.

En caso de verdadero desastre o incluso de una migración planificada, VLSR permite enviar cualquier cambio de última hora al conjunto de datos mediante una actualización final de SnapMirror (si lo decide). A continuación, interrumpe el reflejo y monta el almacén de datos en los hosts de recuperación ante desastres. En ese momento, las máquinas virtuales pueden encenderse automáticamente en cualquier orden de acuerdo con la estrategia planificada previamente.



Aunque los sistemas ONTAP le permitirán emparejar SVM en el mismo clúster para la replicación de SnapMirror, ese escenario no se ha probado ni certificado con VLSR. Por lo tanto, se recomienda usar solo SVM de diferentes clústeres cuando se utilice VLSR.

## **VLSR con ONTAP y otros casos de uso: Cloud híbrido y migración**

La integración de su implementación de VLSR con las capacidades de gestión de datos avanzadas de ONTAP permite una escala y un rendimiento enormemente mejorados en comparación con las opciones de almacenamiento local. Pero más que eso, aporta la flexibilidad de la nube híbrida. La nube híbrida le permite ahorrar dinero al organizar en niveles los bloques de datos no utilizados desde su matriz de alto rendimiento hasta su hiperescalador preferido usando FabricPool, que podría ser un almacén S3 local como NetApp StorageGRID. También puede usar SnapMirror para sistemas basados en el borde con ONTAP Select definido por software o DR basado en la nube usando "[Almacenamiento de NetApp en Equinix Metal](#)", u otros servicios ONTAP alojados.

Podría entonces hacer una comutación por error de prueba dentro del centro de datos de un proveedor de servicios en cloud con un espacio de almacenamiento prácticamente nulo gracias a FlexClone. La protección de su empresa ahora puede costar menos que nunca.

VLSR también puede utilizarse para ejecutar migraciones planificadas aprovechando SnapMirror para transferir de forma eficiente sus máquinas virtuales desde un centro de datos a otro o incluso dentro del mismo centro de datos, ya sea el suyo o mediante cualquier otro proveedor de servicios para partners de NetApp.

## **Mejores prácticas de puesta en marcha**

Las siguientes secciones describen las mejores prácticas para la puesta en marcha con ONTAP y VMware SRM.

### **Utilice la versión más reciente de las herramientas de ONTAP 10**

ONTAP TOOLS 10 proporciona mejoras significativas con respecto a versiones anteriores, como las siguientes:

- comutación por error de prueba 8x veces más rápida\*
- limpieza y reprotectación 2x veces más rápidas\*

- 32% más rápido de failover\*
- Mayor escala
- Compatibilidad nativa para diseños de sitios compartidos

\*Estas mejoras se basan en pruebas internas y pueden variar en función de su entorno.

## Distribución y segmentación de SVM para SMT

Con ONTAP, el concepto de las máquinas virtuales de almacenamiento (SVM) proporciona una segmentación estricta en entornos multi-tenant seguros. Los usuarios de SVM en una SVM no pueden acceder a los recursos ni gestionarlos desde otra. De este modo, puede aprovechar la tecnología ONTAP creando SVM independientes para diferentes unidades de negocio que gestionan sus propios flujos de trabajo de SRM en el mismo clúster para mejorar la eficiencia general del almacenamiento.

Considere la posibilidad de gestionar ONTAP mediante cuentas de ámbito SVM y LIF de administración de SVM para no solo mejorar los controles de seguridad, sino también mejorar el rendimiento. El rendimiento es inherentemente mayor cuando se usan conexiones de ámbito SVM porque el SRA no es necesario para procesar todos los recursos de todo un clúster, incluidos los recursos físicos. En su lugar, solo debe comprender los activos lógicos que se abstraen a una SVM en particular.

## Prácticas recomendadas para gestionar sistemas ONTAP 9

Como se ha mencionado anteriormente, puede gestionar clústeres de ONTAP utilizando credenciales de ámbito de clúster o de SVM y LIF de gestión. Para obtener un rendimiento óptimo, es posible que desee considerar el uso de las credenciales del ámbito SVM siempre que no utilice vVols. Sin embargo, al hacerlo, debe conocer algunos requisitos y perder algunas funciones.

- La cuenta de SVM predeterminada de vsadmin no tiene el nivel de acceso requerido para realizar tareas de las herramientas de ONTAP. Por lo tanto, debe crear una cuenta de SVM nueva. ["Configure los roles y privilegios de usuario de ONTAP"](#) Usando el archivo JSON incluido. Puede utilizarse para cuentas de SVM o de ámbito de clúster.
- Dado que el complemento de interfaz de usuario de vCenter, VASA Provider y el servidor SRA son microservicios totalmente integrados, debe añadir almacenamiento al adaptador de SRA en SRM de la misma manera que añade almacenamiento en la interfaz de usuario de vCenter para las herramientas de ONTAP. De lo contrario, es posible que el servidor SRA no reconozca las solicitudes que se envían desde el SRM a través del adaptador SRA.
- La comprobación de rutas de NFS no se realiza con credenciales de ámbito SVM, a menos que primero ["clústeres incorporados"](#) en el administrador de herramientas de ONTAP y las asocie a vCenter. Esto se debe a que la ubicación física se abstrae de forma lógica de la SVM. Sin embargo, este no es un motivo de preocupación, ya que los sistemas ONTAP modernos ya no sufren una disminución notable del rendimiento cuando se utilizan rutas indirectas.
- Es posible que no se informe del ahorro de espacio agregado debido a la eficiencia del almacenamiento.
- Si es compatible, los duplicados de uso compartido de carga no se pueden actualizar.
- Es posible que no se realicen registros de EMS en sistemas ONTAP gestionados con credenciales de ámbito de SVM.

## Mejores prácticas operativas

Las siguientes secciones describen las mejores prácticas operativas para el almacenamiento de VMware SRM y ONTAP.

## Almacenes de datos y protocolos

- Si es posible, utilice siempre herramientas ONTAP para aprovisionar almacenes de datos y volúmenes. De este modo se garantiza que los volúmenes, rutas de unión, LUN, iGroups, políticas de exportación, y otros ajustes se configuran de forma compatible.
- El SRM admite iSCSI, Fibre Channel y NFS versión 3 con ONTAP 9 al usar la replicación basada en cabinas a través de SRA. SRM no admite la replicación basada en cabinas para NFS versión 4.1 con almacenes de datos tradicionales o vVols.
- Para confirmar la conectividad, siempre compruebe que puede montar y desmontar un almacén de datos de prueba nuevo en el sitio de recuperación ante desastres del clúster de ONTAP de destino. Pruebe cada protocolo que pretenda utilizar para la conectividad de almacenes de datos. Una práctica recomendada es usar las herramientas de ONTAP para crear su almacén de datos de prueba, ya que está haciendo toda la automatización del almacén de datos según las indicaciones del SRM.
- Los protocolos SAN deben ser homogéneos para cada sitio. Puede mezclar NFS y SAN, pero los protocolos SAN no deben mezclarse dentro de un sitio. Por ejemplo, puede utilizar FCP en el sitio A e iSCSI en el sitio B. No debería utilizar FCP e iSCSI en el sitio A.
- Las guías anteriores aconsejan crear LIF para la localidad de datos. Es decir, monte siempre un almacén de datos con una LIF ubicada en el nodo que posee físicamente el volumen. Aunque sigue siendo la mejor práctica, ya no es un requisito en las versiones modernas de ONTAP 9. Siempre que sea posible y si se dan credenciales de ámbito de clúster determinadas, las herramientas de ONTAP seguirán optando por equilibrar la carga entre las LIF locales de los datos, pero no es un requisito de alta disponibilidad ni rendimiento.
- ONTAP 9 se puede configurar para eliminar automáticamente instantáneas para mantener el tiempo de actividad en caso de una condición de falta de espacio cuando autosize no puede suministrar suficiente capacidad de emergencia. La configuración predeterminada para esta funcionalidad no elimina automáticamente las copias Snapshot que crea SnapMirror. Si se eliminan las snapshots de SnapMirror, el SRA de NetApp no puede revertir ni resincronizar la replicación del volumen afectado. Para evitar que ONTAP elimine snapshots de SnapMirror, configure la funcionalidad de eliminación automática de snapshots como 'Probar'.

```
snap autodelete modify -volume -commitment try
```

- el tamaño automático del volumen debe establecerse en `grow` para los volúmenes que contienen almacenes de datos SAN y `grow_shrink` para almacenes de datos NFS. Obtenga más información sobre este tema en ["Configure los volúmenes para que aumenten y reduzcan su tamaño automáticamente"](#).
- SRM tiene un mejor rendimiento cuando el número de almacenes de datos y, por lo tanto, grupos de protección se minimizan en sus planes de recuperación. Por tanto, debería considerar la optimización para la densidad de las máquinas virtuales en entornos protegidos por SRM, donde el objetivo de tiempo de recuperación es de una importancia clave.
- Use el planificador de recursos distribuido (DRS) para equilibrar la carga en los clústeres ESXi protegidos y de recuperación. Recuerde que si tiene previsto realizar una commutación tras recuperación, al ejecutar una nueva protección, los clústeres protegidos anteriormente se convertirán en los nuevos clústeres de recuperación. DRS ayudará a equilibrar la colocación en ambas direcciones.
- Siempre que sea posible, evite usar la personalización de IP con SRM, ya que esto puede aumentar su RTO.

## Acerca de parejas de cabinas

Se crea un gestor de cabinas para cada pareja de cabinas. Con las herramientas SRM y ONTAP, el emparejamiento de cabinas se realiza con el ámbito de una SVM, incluso si utiliza credenciales de clúster. Esto le permite segmentar los flujos de trabajo de recuperación ante desastres entre inquilinos en función de los cuales se hayan asignado a gestionar las SVM. Puede crear varios administradores de cabina para un clúster determinado y pueden ser asimétricos. Es posible fan out o fan in entre diferentes clústeres de ONTAP 9. Por ejemplo, puede tener SVM-A y SVM-B en el clúster-1 que replica en SVM-C en el clúster-2, SVM-D en el clúster-3 o viceversa.

Al configurar parejas de cabinas en SRM, siempre debe añadirlas a SRM de la misma forma que las añadió a las herramientas de ONTAP, lo que significa que deben usar el mismo nombre de usuario, contraseña y LIF de gestión. Este requisito garantiza que el SRA se comunique correctamente con la matriz. La siguiente captura de pantalla ilustra cómo puede aparecer un clúster en las herramientas de ONTAP y cómo se puede añadir a un administrador de cabinas.

The screenshot shows the vSphere Client interface. On the left, a sidebar titled 'ONTAP tools' includes 'Storage Systems' (which is selected and highlighted in blue). The main pane is titled 'Storage Systems' and shows a table with one entry: 'cluster2' (Type: Cluster, IP Address: cluster2.demo.netapp.com). Below this, there are 'ADD' and 'REDISCOVER ALL' buttons. A red arrow points from the 'cluster2' entry in the table to the 'Storage Management IP Address or Hostname' field in the 'Edit Local Array Manager' dialog. The dialog has a header 'Edit Local Array Manager' and a sub-header 'Enter a name for the array manager on "vc2.demo.netapp.com":'. It contains a text input field with the value 'vc2\_array\_manager' and a note below it: 'cluster2.demo.netapp.com'. The note also specifies: 'Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.'

## Acerca de los grupos de replicación

Los grupos de replicación contienen colecciones lógicas de máquinas virtuales que se recuperan juntas. Dado que la replicación de SnapMirror de ONTAP se produce en el nivel de volumen, todas las máquinas virtuales de un volumen se encuentran en el mismo grupo de replicación.

La consideración de los grupos de replicación es diversa y cómo se distribuyen los equipos virtuales entre los volúmenes de FlexVol. Agrupar equipos virtuales similares en el mismo volumen puede aumentar la eficiencia del almacenamiento con sistemas ONTAP anteriores que carecen de deduplicación a nivel de agregado, pero la agrupación aumenta el tamaño del volumen y reduce la concurrencia de I/O de volúmenes. El mejor equilibrio entre rendimiento y eficiencia del almacenamiento se puede lograr en los sistemas ONTAP modernos mediante la distribución de máquinas virtuales entre volúmenes de FlexVol en el mismo agregado, aprovechando así la deduplicación a nivel de agregado y ganando una mayor paralelización de I/O en múltiples volúmenes. Puede recuperar las máquinas virtuales en los volúmenes juntos porque un grupo de protección (tratado a continuación) puede contener varios grupos de replicación. La desventaja de esta distribución es que es posible que los bloques se transmitan a través de la conexión varias veces, ya que SnapMirror no tiene en cuenta la deduplicación de agregados.

Un aspecto final que se debe tener en cuenta para los grupos de replicación es que cada uno de ellos es, por su naturaleza, un grupo de consistencia lógico (que no se debe confundir con los grupos de consistencia SRM). Esto se debe a que todas las máquinas virtuales del volumen se transfieren juntas con la misma copia de Snapshot. Si tiene equipos virtuales que deben ser coherentes entre sí, considere almacenarlos en el mismo FlexVol.

## Acerca de los grupos de protección

Los grupos de protección definen las máquinas virtuales y los almacenes de datos en grupos que se recuperan conjuntamente del sitio protegido. El sitio protegido es donde existen las máquinas virtuales configuradas en un grupo de protección durante las operaciones normales de estado constante. Es importante tener en cuenta que, aunque SRM puede mostrar varios administradores de cabinas para un grupo de protección, un grupo de protección no puede abarcar varios administradores de cabinas. Por este motivo, no debe abarcar los archivos de equipos virtuales entre almacenes de datos en diferentes SVM.

## Acerca de los planes de recuperación

Los planes de recuperación definen qué grupos de protección se recuperan en el mismo proceso. Se pueden configurar varios grupos de protección en el mismo plan de recuperación. Además, para ofrecer más opciones para la ejecución de planes de recuperación, se puede incluir un solo grupo de protección en varios planes de recuperación.

Los planes de recuperación permiten a los administradores de SRM definir flujos de trabajo de recuperación asignando las máquinas virtuales a un grupo de prioridad de 1 (más alta) a 5 (más baja), siendo 3 (medio) el valor predeterminado. Dentro de un grupo de prioridad, las máquinas virtuales pueden configurarse para las dependencias.

Por ejemplo, su empresa podría tener una aplicación empresarial crítica de nivel 1 que dependa de un servidor Microsoft SQL para su base de datos. Por lo tanto, se deciden colocar las máquinas virtuales en el grupo de prioridad 1. Dentro del grupo de prioridad 1, comienza a planificar el pedido para que se traigan los servicios. Es probable que desee que el controlador de dominio de Microsoft Windows se inicie antes que el servidor Microsoft SQL, que tendría que estar en línea antes del servidor de aplicaciones, y así sucesivamente. Debe agregar todas estas máquinas virtuales al grupo de prioridades y, después, establecer las dependencias, dado que las dependencias solo se aplican dentro de un determinado grupo de prioridad.

NetApp recomienda encarecidamente trabajar con sus equipos de aplicaciones para comprender el orden de las operaciones necesarias en un escenario de conmutación por error y construir sus planes de recuperación según corresponda.

## Probar la recuperación tras fallos

Como práctica recomendada, siempre realice una conmutación por error de prueba cada vez que se realice un cambio en la configuración del almacenamiento de VM protegido. Esto garantiza que, en caso de desastre, pueda confiar en que Site Recovery Manager pueda restaurar los servicios dentro del objetivo de RTO esperado.

NetApp también recomienda confirmar la funcionalidad de aplicaciones «en invitado» ocasionalmente, especialmente tras reconfigurar el almacenamiento de máquinas virtuales.

Cuando se realiza una operación de recuperación de pruebas, se crea una red privada de burbuja de pruebas en el host ESXi para los equipos virtuales. Sin embargo, esta red no está conectada automáticamente a ningún adaptador de red físico y, por lo tanto, no proporciona conectividad entre los hosts ESXi. Para permitir la comunicación entre máquinas virtuales que se ejecutan en diferentes hosts ESXi durante las pruebas de recuperación ante desastres, se crea una red privada física entre los hosts ESXi en el sitio de recuperación ante desastres. Para verificar que la red de prueba es privada, la red de burbuja de prueba se puede separar

físicamente o mediante VLAN o etiquetado VLAN. Esta red debe separarse de la red de producción porque, a medida que se recuperan los equipos virtuales, no se pueden colocar en la red de producción con direcciones IP que puedan entrar en conflicto con los sistemas de producción reales. Cuando se crea un plan de recuperación en SRM, es posible seleccionar la red de pruebas creada como la red privada para conectar los equipos virtuales a durante la prueba.

Una vez que la prueba se ha validado y ya no es necesaria, realice una operación de limpieza. La ejecución de la limpieza devuelve las máquinas virtuales protegidas a su estado inicial y restablece el plan de recuperación al estado Ready.

### **Consideraciones sobre la conmutación por error**

Hay otros factores que se deben tener en cuenta a la hora de conmutar por error un sitio además del orden de las operaciones mencionado en esta guía.

Un problema que puede tener que lidiar es las diferencias de redes entre sitios. Es posible que algunos entornos puedan usar las mismas direcciones IP de red en el sitio primario y en el sitio de recuperación tras desastres. Esta capacidad se conoce como una configuración de red LAN virtual (VLAN) ampliada o extendida. Es posible que otros entornos tengan que utilizar diferentes direcciones IP de red (por ejemplo, diferentes VLAN) en el sitio principal con respecto al sitio de recuperación ante desastres.

VMware ofrece varias formas de resolver este problema. En primer lugar, las tecnologías de virtualización de redes como el centro de datos NSX-T de VMware abstraen toda la pila de redes de las capas 2 a 7 del entorno operativo, permitiendo soluciones más portátiles. Más información acerca de "["Opciones de NSX-T con SRM"](#)".

SRM también le permite cambiar la configuración de red de un equipo virtual mientras se recupera. Esta reconfiguración incluye ajustes como las direcciones IP, las direcciones de puerta de enlace y la configuración del servidor DNS. Los diferentes ajustes de red, que se aplican a las VM individuales a medida que se recuperan, se pueden especificar en la configuración de la propiedad de una VM en el plan de recuperación.

Para configurar SRM de modo que aplique diferentes ajustes de red a varios equipos virtuales sin tener que editar las propiedades de cada uno del plan de recuperación, VMware ofrece una herramienta llamada DR-ip-customizer. Aprenda a usar esta utilidad, consulte "["Documentación de VMware"](#)".

### **Vuelva a proteger**

Después de una recuperación, el sitio de recuperación se convierte en el nuevo sitio de producción. Dado que la operación de recuperación rompió la replicación de SnapMirror, el nuevo sitio de producción no está protegido contra ningún desastre futuro. Una mejor práctica es proteger el nuevo sitio de producción en otro sitio inmediatamente después de una recuperación. Si el sitio de producción original está operativo, el administrador de VMware puede utilizar el sitio de producción original como un nuevo sitio de recuperación para proteger el nuevo sitio de producción, invirtiendo efectivamente la dirección de la protección. La reprotectación solo está disponible en fallos no catastróficos. Por lo tanto, en algún momento deben recuperarse los servidores vCenter Server, los servidores ESXi, los servidores SRM y las bases de datos correspondientes originales. Si no están disponibles, deben crearse un nuevo grupo de protección y un nuevo plan de recuperación.

### **Comutación tras recuperación**

Una operación de conmutación tras recuperación es fundamentalmente una conmutación por error en una dirección diferente a la anterior. Como práctica recomendada, compruebe que el sitio original vuelve a los niveles aceptables de funcionalidad antes de intentar realizar la conmutación tras recuperación o, en otras palabras, la conmutación por error al sitio original. Si la instalación original sigue en peligro, deberá retrasar la conmutación tras recuperación hasta que se solucione el fallo lo suficiente.

Otra práctica recomendada para la conmutación tras recuperación es siempre realizar una conmutación al nodo de respaldo de prueba después de completar la reprotectación y antes de llevar a cabo la conmutación tras recuperación final. Esto verifica que los sistemas en el sitio original pueden completar la operación.

### **Volver a proteger el sitio original**

Después de la conmutación por recuperación, debe confirmar con todas las partes interesadas que sus servicios se han vuelto a la normalidad antes de ejecutar la reprotectación de nuevo.

La ejecución de la reprotectación después de la conmutación tras recuperación hace que el entorno vuelva a estar en el estado que estaba al principio, cuando la replicación de SnapMirror se ejecuta de nuevo desde el centro de producción al centro de recuperación.

### **Topologías de replicación**

En ONTAP 9, los componentes físicos de un clúster son visibles para los administradores del clúster, pero no pueden ver directamente las aplicaciones y los hosts que utilizan el clúster. Los componentes físicos proporcionan un conjunto de recursos compartidos desde los cuales se construyen los recursos del clúster lógicos. Las aplicaciones y los hosts solo acceden a los datos a través de SVM que contienen volúmenes y LIF.

Cada SVM de NetApp se trata como una matriz única en Site Recovery Manager. VLSR admite ciertos diseños de replicación de matriz a matriz (o de SVM a SVM).

Una sola máquina virtual no puede poseer datos, Virtual Machine Disk (VMDK) o RDM, en más de una cabina de VLSR por los siguientes motivos:

- VLSR solo ve la SVM, no una controladora física individual.
- Una SVM puede controlar los LUN y los volúmenes que abarcan varios nodos en un clúster.

#### **Mejor práctica**

Para determinar la compatibilidad, tenga presente esta regla: Para proteger una máquina virtual con el VLSR y el SRA de NetApp, todas las partes de la máquina virtual deben existir en un solo SVM. Esta regla se aplica tanto al sitio protegido como al sitio de recuperación.

### **Distribuciones de SnapMirror compatibles**

Las siguientes figuras muestran los escenarios de diseño de la relación de SnapMirror compatibles con VLSR y SRA. Cada equipo virtual de los volúmenes replicados posee datos en una sola cabina de VLSR (SVM) en cada sitio.

### SnapMirror Replication



#### Protected Site

SVM-A1

VM1

#### Recovery Site

SVM-B1

VM1

SVM-A2

VM2

SVM-B2

VM2

### SnapMirror Replication



#### Protected Site

SVM-A1

VM2

VM1

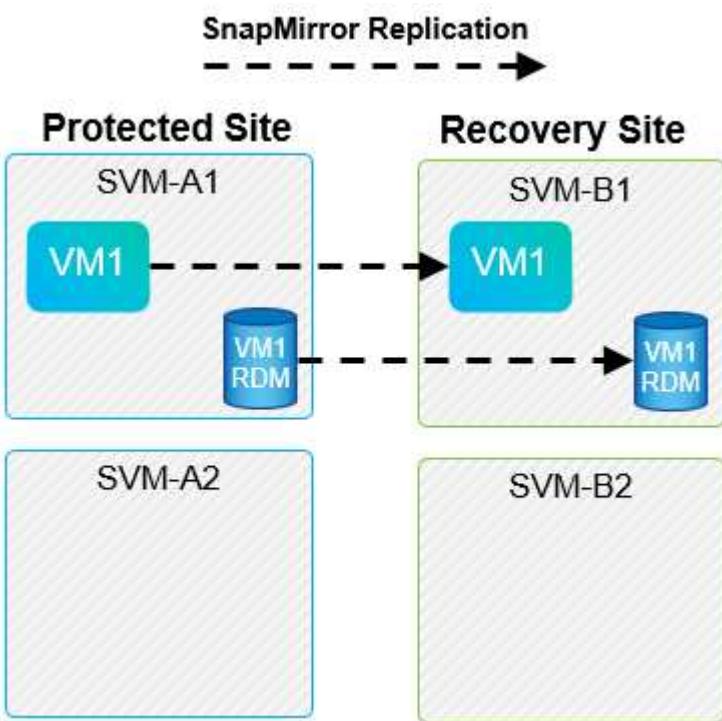
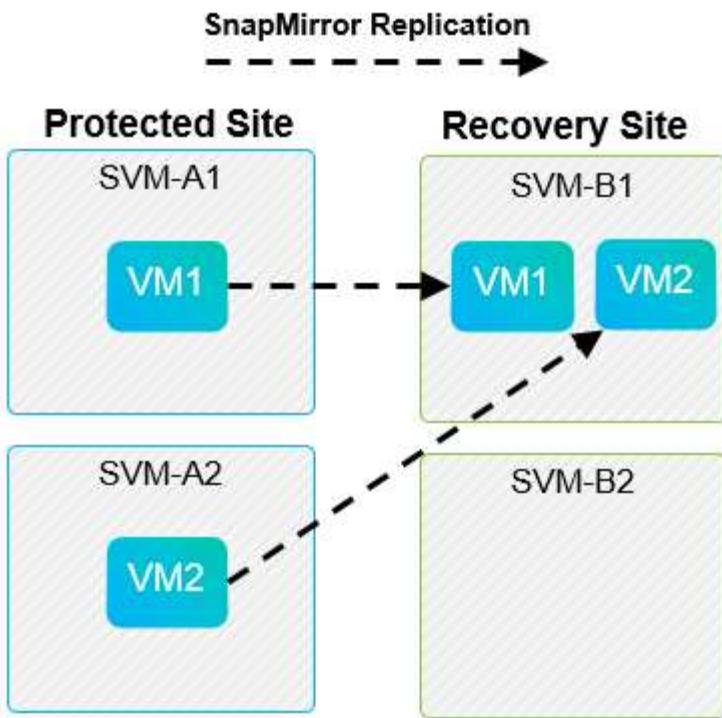
#### Recovery Site

SVM-B1

VM1

SVM-B2

VM2



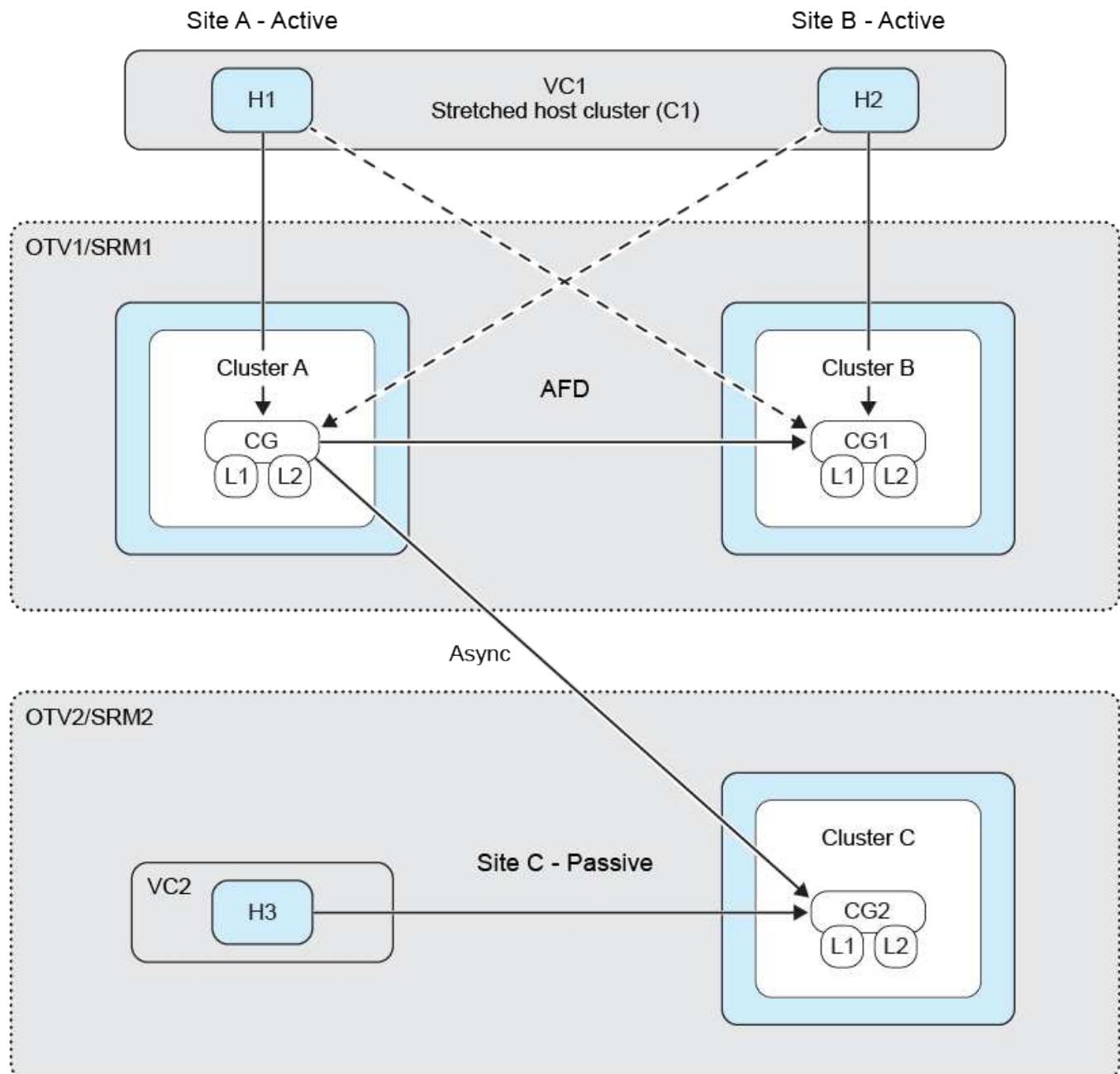
#### Compatibilidad de VMFS con sincronización activa de SnapMirror

Las herramientas ONTAP 10.3 y posteriores también admiten la protección de sus almacenes de datos VMFS con SnapMirror Active Sync (SMas). Esto permite una comutación por error transparente para la continuidad del negocio entre dos centros de datos (denominados dominios de falla) que están relativamente cerca uno del otro. La recuperación ante desastres a larga distancia se puede orquestar utilizando SnapMirror de forma asincrónica a través de las herramientas ONTAP SRA con VLSR.

["Obtenga más información sobre la sincronización activa de ONTAP SnapMirror"](#)

Los almacenes de datos se recopilan juntos en un grupo de consistencia (CG) y las máquinas virtuales en todos los almacenes de datos permanecerán consistentes en el orden de escritura como miembros del mismo CG.

Algunos ejemplos podrían ser tener sitios en Berlín y Hamburgo protegidos por SMas y una tercera réplica del sitio utilizando SnapMirror asincrónico y protegido por VLSR. Otro ejemplo podría ser proteger sitios en Nueva York y Nueva Jersey utilizando SMas, con un tercer sitio en Chicago.



### Diseños compatibles de Array Manager

Cuando se utiliza la replicación basada en cabinas (ABR) en VLSR, los grupos de protección se aíslan en un solo par de cabinas, como se muestra en la siguiente captura de pantalla. En este caso, SVM1 y SVM2 se relacionan con SVM3 y SVM4 en el sitio de recuperación. Sin embargo, es posible seleccionar solo una de las

dos parejas de cabinas al crear un grupo de protección.

New Protection Group

Type

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

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.

Storage policies (array-based replication)  
Protect virtual machines with specific storage policies.

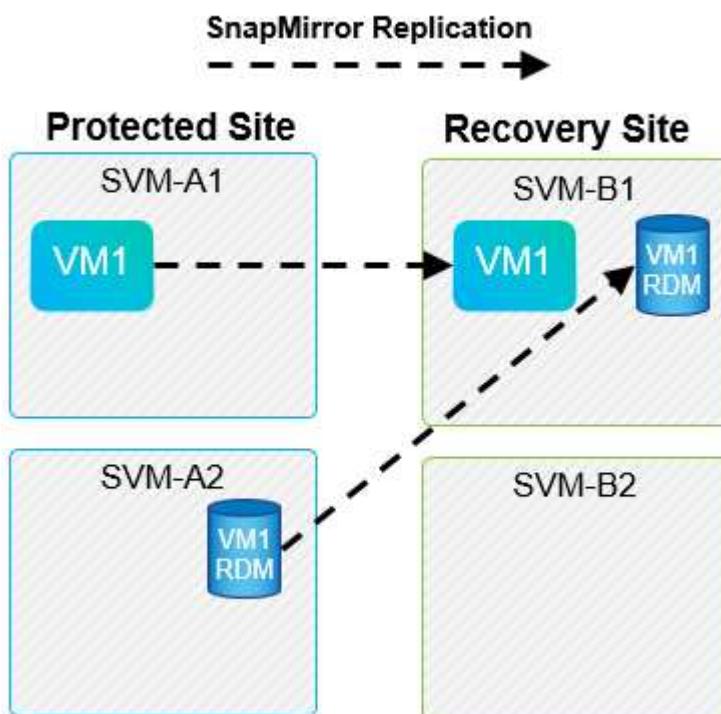
Select array pair

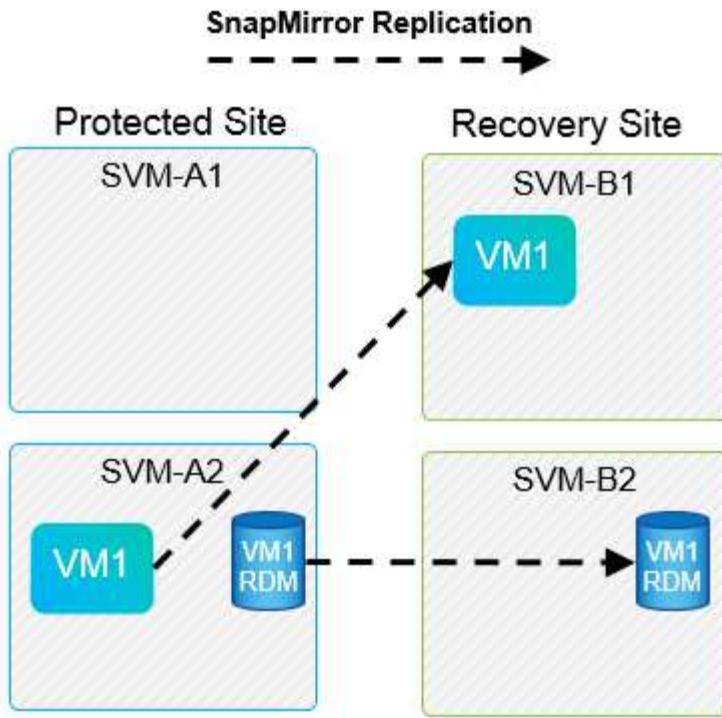
| Array Pair  | Array Manager Pair                        |
|---|---|
| <input type="radio"/> ✓ cluster1:svm1 ↔ cluster2:svm2 | vc1 array manager ↔ vc2 array manager     |
| <input type="radio"/> ✓ cluster1:svm3 ↔ cluster2:svm4 | vc1 trad datastores ↔ vc2 trad datastores |

CANCEL BACK NEXT

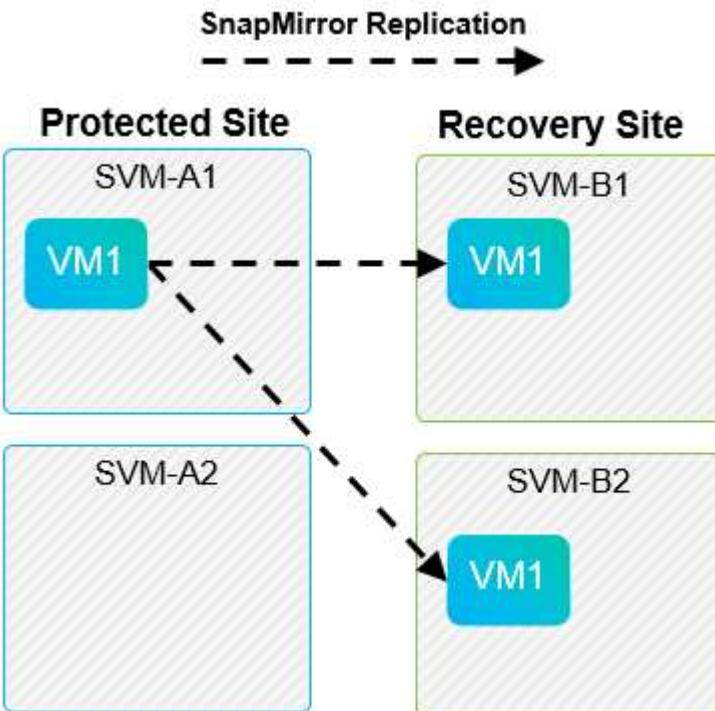
## Diseños no admitidos

Las configuraciones no compatibles tienen datos (VMDK o RDM) en varias SVM que son propiedad de una máquina virtual individual. En los ejemplos que se muestran en las siguientes figuras, VM1 no se puede configurar para protección con VLSR porque VM1 tiene datos en dos SVM.





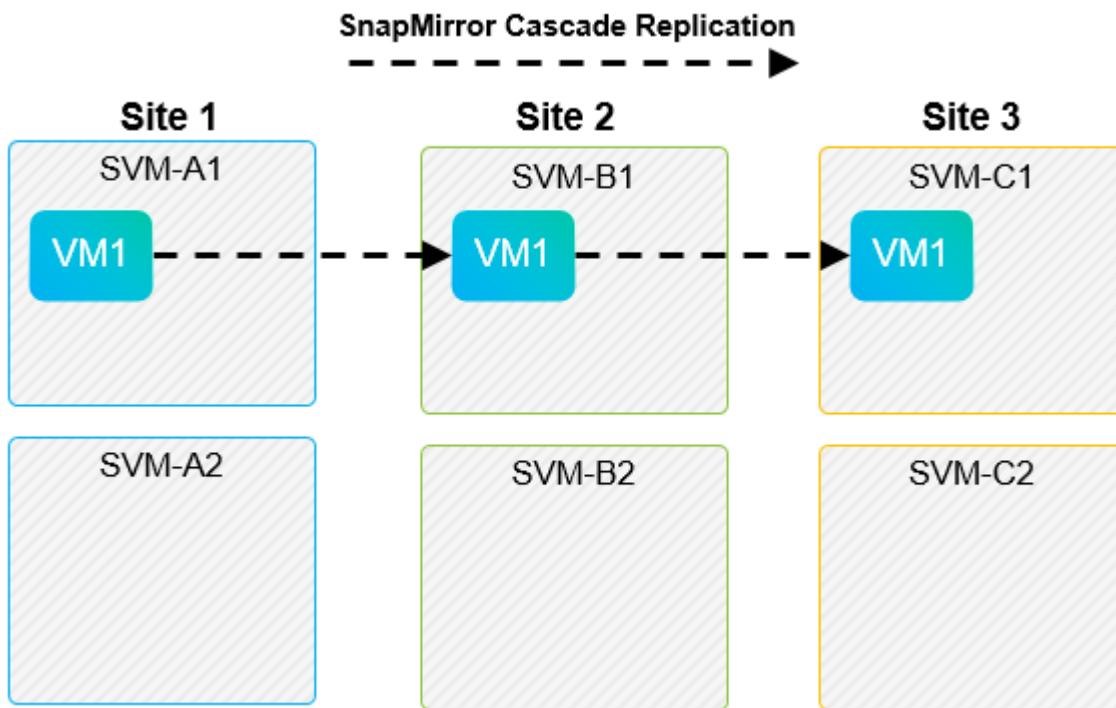
Toda relación de replicación en la que se replica un volumen individual de NetApp desde una SVM de origen a varios destinos en la misma SVM o en distintas SVM se denomina «fan-out» de SnapMirror. VLSR no es compatible con fan-out. En el ejemplo que se muestra en la siguiente figura, VM1 no se puede configurar para protección en VLSR porque se replica con SnapMirror en dos ubicaciones diferentes.



### Cascada de SnapMirror

VLSR no admite la configuración en cascada de relaciones de SnapMirror, en las que un volumen de origen se replica en un volumen de destino, y ese volumen de destino también se replica con SnapMirror en otro volumen de destino. En el caso que se muestra en la siguiente figura, VLSR no se puede utilizar para la

comutación por error entre sitios.



### SnapMirror y SnapVault

El software SnapVault de NetApp permite el backup a disco de datos empresariales entre sistemas de almacenamiento de NetApp. SnapVault y SnapMirror pueden coexistir en el mismo entorno. Sin embargo, VLSR admite la comutación por error únicamente de las relaciones de SnapMirror.



El SRA de NetApp admite el `mirror-vault` tipo de política.

SnapVault fue reconstruido desde sus cimientos para ONTAP 8.2. Aunque los antiguos usuarios de Data ONTAP 7-Mode deberían encontrar similitudes, se han mejoras importantes en esta versión de SnapVault. Un avance importante es la capacidad de preservar las eficiencias del almacenamiento en los datos primarios durante las transferencias de SnapVault.

Un cambio de arquitectura importante es que SnapVault en ONTAP 9 se replica a nivel de volumen, frente a en el nivel de qtree, como es el caso de SnapVault en 7-Mode. Esta configuración significa que el origen de una relación de SnapVault debe ser un volumen y dicho volumen debe replicar en su propio volumen en el sistema secundario SnapVault.

En un entorno en el que se utiliza SnapVault, se crean específicamente copias Snapshot con nombre en el sistema de almacenamiento primario. En función de la configuración implementada, las instantáneas con nombre se pueden crear en el sistema primario mediante una programación de SnapVault o mediante una aplicación como NetApp Active IQ Unified Manager. Las copias Snapshot con nombre que se crean en el sistema primario se replican a continuación en el destino de SnapMirror y, desde allí, se almacenan en el destino de SnapVault.

Un volumen de origen se puede crear en una configuración en cascada en la que se replica un volumen a un destino de SnapMirror en el centro de recuperación ante desastres; a partir de ese punto, se realiza la copia en un destino de SnapVault. Un volumen de origen también puede crearse en una relación de dispersión en la que un destino es un destino de SnapMirror y el otro destino es un destino de SnapVault. Sin embargo, el SRA no reconfigura automáticamente la relación de SnapVault para usar el volumen de destino de SnapMirror.

como origen del almacén cuando se produce la conmutación por error del VLSR o la reversión de la replicación.

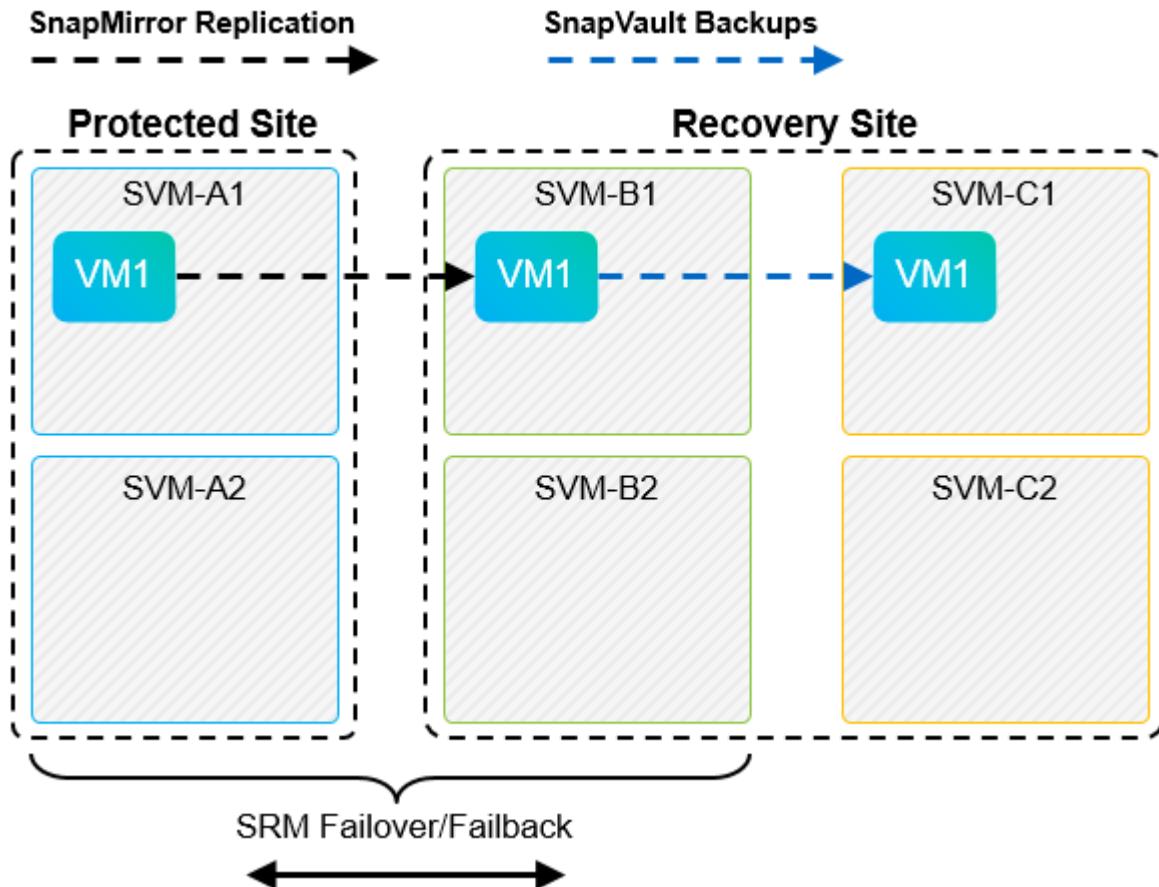
Para obtener la información más reciente sobre SnapMirror y SnapVault para ONTAP 9, consulte ["TR-4015 Guía de mejores prácticas para la configuración de SnapMirror para ONTAP 9."](#)

#### Mejor práctica

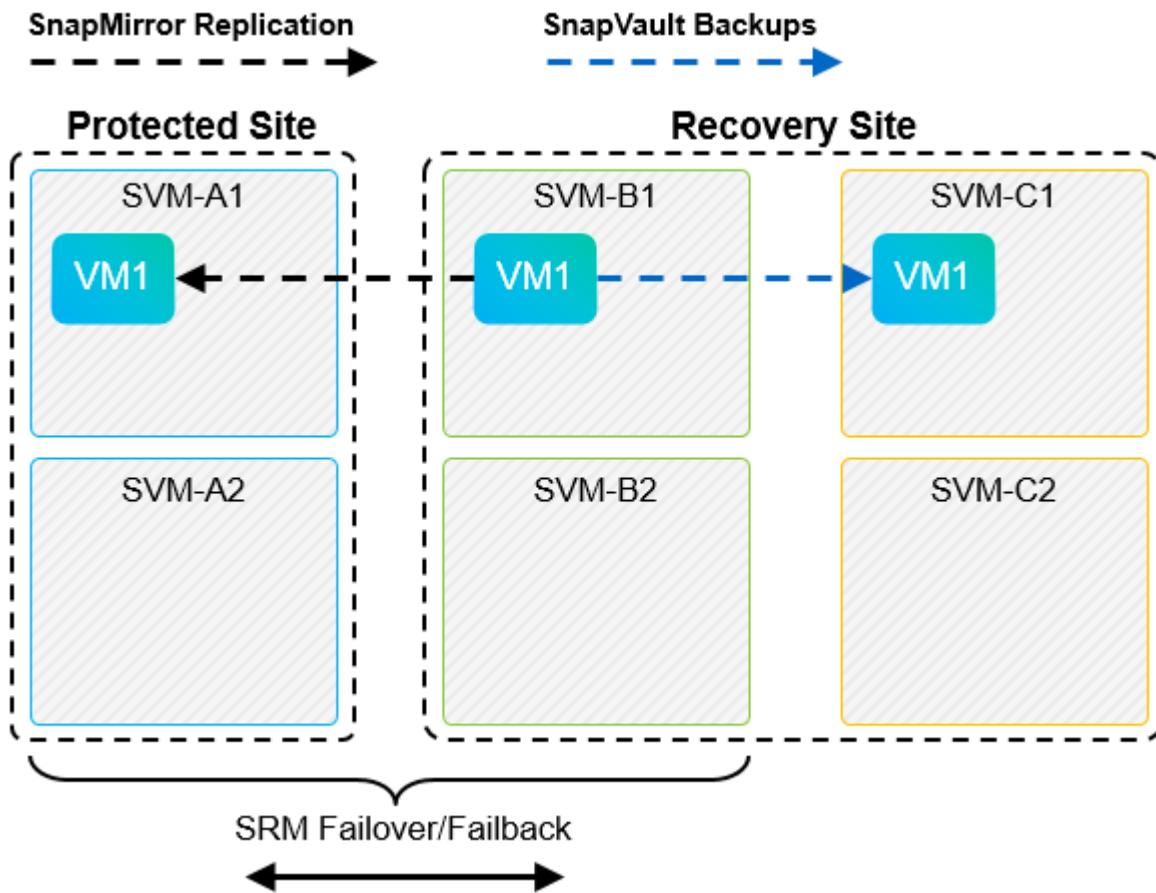
Si se emplean SnapVault y VLSR en el mismo entorno, NetApp recomienda utilizar una configuración en cascada de SnapMirror a SnapVault en la que los backups de SnapVault se realizan normalmente desde el destino de SnapMirror en el centro de recuperación ante desastres. En caso de desastre, esta configuración hace que el sitio primario sea inaccesible. Si se mantiene el destino de SnapVault en el centro de recuperación, los backups de SnapVault se pueden volver a configurar tras la conmutación por error para que los backups de SnapVault puedan continuar mientras estén en el centro de recuperación.

En un entorno VMware, cada almacén de datos tiene un identificador único universal (UUID) y cada máquina virtual tiene un ID de objeto gestionado único (MOID). VLSR no mantiene estos ID durante la conmutación por error o la conmutación tras recuperación. Dado que los UUID de almacenes de datos y los MOIDs de máquinas virtuales no se mantienen durante la conmutación por error por parte de VLSR, cualquier aplicación que dependa de estos identificadores se debe volver a configurar tras la conmutación por error de VLSR. Una aplicación de ejemplo es Active IQ Unified Manager de NetApp, que coordina la replicación de SnapVault con el entorno vSphere.

La siguiente figura muestra la configuración en cascada de SnapMirror a SnapVault. Si el destino de SnapVault se encuentra en el centro de recuperación ante desastres o en un sitio terciario que no se ve afectado por una interrupción en el centro principal, es posible volver a configurar el entorno para que los backups continúen tras la conmutación por error.



En la siguiente figura, se muestra la configuración una vez que se ha utilizado VLSR para revertir la replicación de SnapMirror al centro principal. También se ha reconfigurado el entorno para que los backups SnapVault se realicen desde el origen de SnapMirror. Esta configuración es una configuración de dispersión de SnapMirror SnapVault.



Cuando vsrm realiza una comutación de retorno tras recuperación y una segunda reversión de las relaciones de SnapMirror, los datos de producción vuelven a estar en el sitio principal. Estos datos ahora están protegidos del mismo modo que antes la comutación al centro de recuperación ante desastres, mediante backups de SnapMirror y SnapVault.

### Uso de Qtrees en entornos de Site Recovery Manager

Los qtrees son directorios especiales que permiten aplicar cuotas del sistema de archivos para NAS. ONTAP 9 permite la creación de qtrees y pueden existir qtrees en los volúmenes replicados con SnapMirror. Sin embargo, SnapMirror no permite la replicación de qtrees individuales o a nivel de qtree. Toda la replicación de SnapMirror se realiza únicamente a nivel de volumen. Por este motivo, NetApp no recomienda el uso de qtrees con VLSR.

### Entornos FC e iSCSI mixtos

Con los protocolos SAN compatibles (Fibre Channel, FCoE e iSCSI), ONTAP 9 ofrece servicios LUN, esto es, la capacidad de crear y asignar LUN a los hosts conectados. Dado que el clúster se compone de varias controladoras, existen varias rutas lógicas que se gestionan mediante I/o multivía con cualquier LUN individual. En los hosts se utiliza ALUA (Asymmetric LUN Access) para que se seleccione la ruta optimizada a cada LUN. Si la ruta optimizada a cualquier LUN cambia (por ejemplo, debido a que se mueve el volumen que lo contiene), ONTAP 9 reconoce automáticamente y se ajusta de forma no disruptiva para este cambio. Si la ruta optimizada deja de estar disponible, ONTAP puede cambiar a otra ruta disponible sin interrupciones.

El VLSR de VMware y el SRA de NetApp admiten el uso del protocolo FC en un sitio y el protocolo iSCSI en el otro sitio. Sin embargo, no admite el hecho de haber una combinación de almacenamiento de datos conectados a FC y almacenamiento de datos conectados a iSCSI en el mismo host ESXi o en hosts diferentes en el mismo clúster. Esta configuración no es compatible con VLSR porque, durante la conmutación por error de VLSR o la conmutación por error de prueba, VLSR incluye todos los iniciadores de FC e iSCSI de los hosts ESXi que están en la solicitud.

#### Mejor práctica

El VLSR y el SRA admiten protocolos mixtos de FC e iSCSI entre los sitios protegidos y de recuperación. Sin embargo, cada sitio debe configurarse con un solo protocolo, ya sea FC o iSCSI, y no con ambos protocolos en el mismo sitio. Si existe un requisito de tener configurados tanto los protocolos FC como iSCSI en el mismo sitio, NetApp recomienda que algunos hosts utilicen iSCSI y otros hosts utilicen FC. En este caso, NetApp también recomienda configurar las asignaciones de recursos de VLSR para que las máquinas virtuales se configuren para conmutar al nodo de respaldo en un grupo de hosts u otro.

### Solución de problemas de VLSRM/ SRM cuando se usa la replicación de vVols

Cuando se utilizan las herramientas de ONTAP 9.13P2, el flujo de trabajo que hay en VLSR y SRM es muy diferente cuando se usa la replicación vVols de lo que se utiliza con el SRA y los almacenamientos de datos tradicionales. Por ejemplo, no hay ningún concepto de administrador de cabinas. Como tal, `discoverarrays` y `discoverdevices` los comandos nunca se ven.

Para la solución de problemas, resulta beneficioso comprender los nuevos flujos de trabajo, que se enumeran a continuación:

1. `QueryReplicationPeer`: Descubre los acuerdos de replicación entre dos dominios de fallo.
2. `QueryFaultDomain`: Detecta la jerarquía de dominios de fallo.
3. `QueryReplicationGroup`: Detecta los grupos de replicación presentes en los dominios de origen o destino.
4. `SyncReplicationGroup`: Sincroniza los datos entre el origen y el destino.
5. `QueryPointInTimeReplica`: Detecta las réplicas de punto en tiempo en un destino.
6. `TestFailoverReplicationGroupStart`: Inicia la conmutación por error de prueba.
7. `TestFailoverReplicationGroupStop`: Finaliza la conmutación por error de prueba.
8. `PromoteReplicationGroup`: Promueve un grupo actualmente en pruebas a la producción.
9. `PrepareFailoverReplicationGroup`: Prepara para una recuperación ante desastres.
10. `FailoverReplicationGroup`: Ejecuta la recuperación ante desastres.
11. `ReverseReplicateGroup`: Inicia la replicación inversa.
12. `QueryMatchingContainer`: Busca contenedores (junto con hosts o grupos de replicación) que puedan satisfacer una solicitud de aprovisionamiento con una directiva determinada.
13. `QueryResourceMetadata`: Descubre los metadatos de todos los recursos del proveedor VASA, la utilización de recursos puede devolverse como respuesta a la función `queryMatchingContainer`.

El error más común que se produce al configurar la replicación de vVols es no descubrir las relaciones de SnapMirror. Esto ocurre porque los volúmenes y las relaciones de SnapMirror se crean fuera del alcance de las herramientas de ONTAP. Por lo tanto, una práctica recomendada es asegurarse de que su relación con SnapMirror esté completamente inicializada y de que ha ejecutado una nueva detección en las herramientas

de ONTAP en ambos sitios antes de intentar crear un almacén de datos vVols replicado.

## Información adicional

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

- Herramientas de ONTAP para VMware vSphere 10.x Resources  
["https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"](https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab)
- Herramientas de ONTAP para VMware vSphere 9.x Resources  
["https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"](https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab)
- TR-4597: VMware vSphere para ONTAP  
["https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"](https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html)
- TR-4400: VMware vSphere Virtual Volumes con ONTAP  
["https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"](https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html)
- Guía de prácticas recomendadas para la configuración de SnapMirror TR-4015 para ONTAP 9  
<https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf>
- Documentación de VMware Live Site Recovery "<https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html>"

Consulte el "[Herramienta de matriz de interoperabilidad \(IMT\)](#)" sitio de soporte de NetApp para confirmar que las versiones exactas del producto y las funciones descritas en este documento son compatibles con su entorno concreto. La cabina IMT de NetApp define los componentes y las versiones del producto que pueden utilizarse para crear configuraciones que sean compatibles con NetApp. Los resultados específicos dependen de la instalación que realice cada cliente de acuerdo con las especificaciones publicadas.

## Clúster de almacenamiento vSphere Metro con ONTAP

### Clúster de almacenamiento vSphere Metro con ONTAP

El hipervisor vSphere líder del sector de VMware se puede poner en marcha como un clúster ampliado conocido como vSphere Metro Storage Cluster (VMSC).

Las soluciones VMSC son compatibles con NetApp® MetroCluster™ y SnapMirror Active Sync (anteriormente conocido como continuidad empresarial de SnapMirror o SMBC) y proporcionan continuidad empresarial avanzada si uno o más dominios de fallo sufren una interrupción total. La resistencia a los diferentes modos de fallo depende de las opciones de configuración que elija.



Esta documentación sustituye a los informes técnicos publicados anteriormente *TR-4128: VSphere en NetApp MetroCluster*

### Soluciones de disponibilidad continua para entornos vSphere

La arquitectura ONTAP es una plataforma de almacenamiento flexible y escalable que proporciona servicios SAN (FCP, iSCSI y NVMe-oF) y NAS (NFS v3 y v4.1) para almacenes de datos. Los sistemas de almacenamiento AFF, ASA y FAS de NetApp utilizan el sistema operativo ONTAP para ofrecer protocolos adicionales para el acceso al almacenamiento invitado, como S3 y SMB/CIFS.

NetApp MetroCluster utiliza la función de alta disponibilidad (comutación por error de controladora o director financiero) de NetApp para proteger frente a fallos de controladora. También incluye tecnología SyncMirror

local, recuperación tras fallos en clúster en caso de desastre (comutación por error en cluster en caso de desastre o CFOD), redundancia de hardware y separación geográfica para alcanzar altos niveles de disponibilidad. SyncMirror refleja de forma síncrona los datos en las dos mitades de la configuración de MetroCluster mediante la escritura de los datos en dos plexes: El plex local (en la bandeja local) que sirve los datos de forma activa y el plex remoto (en la bandeja remota) normalmente no ofrece datos. La redundancia de hardware se pone en marcha para todos los componentes de MetroCluster, como las controladoras, el almacenamiento, los cables, los switches (utilizados con Fabric MetroCluster) y los adaptadores.

La sincronización activa de NetApp SnapMirror, disponible en sistemas que no sean MetroCluster y en sistemas ASA R2, ofrece protección granular en almacenes de datos con protocolos FCP e iSCSI SAN. Le permite proteger todo el VMSC o proteger de forma selectiva las cargas de trabajo de alta prioridad. Ofrece acceso activo-activo tanto a sitios locales como remotos, a diferencia de NetApp MetroCluster, que es una solución activa-en espera. A partir de ONTAP 9.15.1, la sincronización activa de SnapMirror admite una funcionalidad activo-activo simétrica, lo que permite operaciones de I/O de lectura y escritura desde ambas copias de una LUN protegida con replicación síncrona bidireccional, lo que permite que ambas copias LUN sirvan operaciones de I/O localmente. Antes de ONTAP 9.15.1, la sincronización activa de SnapMirror solo admite configuraciones activo-activo asimétricas, en las que los datos del sitio secundario están proxy a la copia principal de una LUN.

Para crear un clúster HA/DRS de VMware en dos sitios, los hosts ESXi se usan y gestionan mediante una instancia de vCenter Server Appliance (VCSA). Las redes de gestión de vSphere, vMotion® y máquinas virtuales están conectadas a través de una red redundante entre los dos sitios. El servidor vCenter que gestiona el clúster HA/DRS puede conectarse a los hosts ESXi en ambos sitios y se debe configurar mediante vCenter HA.

Consulte "[¿Cómo se crean y configuran clústeres en vSphere Client](#)" Para configurar una alta disponibilidad de vCenter.

También debe consultar "[Prácticas recomendadas para VMware vSphere Metro Storage Cluster](#)" .

### **¿Qué es vSphere Metro Storage Cluster?**

vSphere Metro Storage Cluster (vMSC) es una configuración certificada que protege las máquinas virtuales (VM) y los contenedores contra fallas. Esto se logra mediante el uso de conceptos de almacenamiento extendido junto con clústeres de hosts ESXi, que se distribuyen en diferentes dominios de falla, como racks, edificios, campus o incluso ciudades. Las tecnologías de almacenamiento de sincronización activa NetApp MetroCluster y SnapMirror se utilizan para proporcionar una protección de objetivo de punto de recuperación cero (RPO=0) a los clústeres de host. La configuración de vMSC está diseñada para garantizar que los datos estén siempre disponibles incluso si falla un "sitio" físico o lógico completo. Un dispositivo de almacenamiento que forma parte de la configuración de vMSC debe certificarse después de someterse a un proceso de certificación de vMSC exitoso. Todos los dispositivos de almacenamiento compatibles se pueden encontrar en "[Guía de compatibilidad de almacenamiento de VMware](#)".

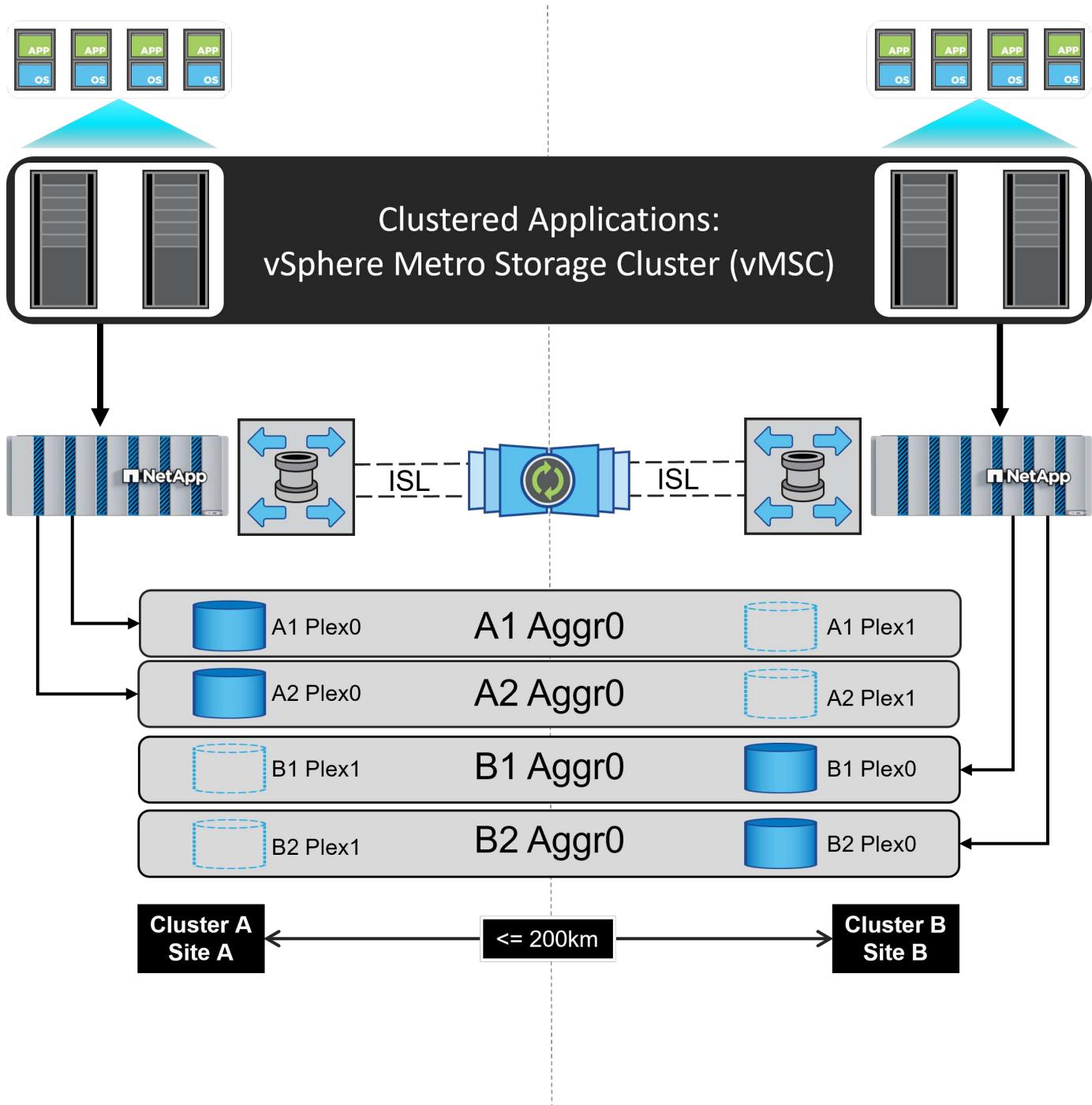
Si desea obtener más información sobre las directrices de diseño para vSphere Metro Storage Cluster, consulte la siguiente documentación:

- "[Compatibilidad de VMware vSphere con NetApp MetroCluster](#)"
- "[Compatibilidad de VMware vSphere con Continuidad del negocio de SnapMirror de NetApp](#)" (Ahora conocido como SnapMirror active sync)

NetApp MetroCluster se puede poner en marcha en dos configuraciones diferentes para usarlas con vSphere:

- Stretch MetroCluster
- Fabric MetroCluster

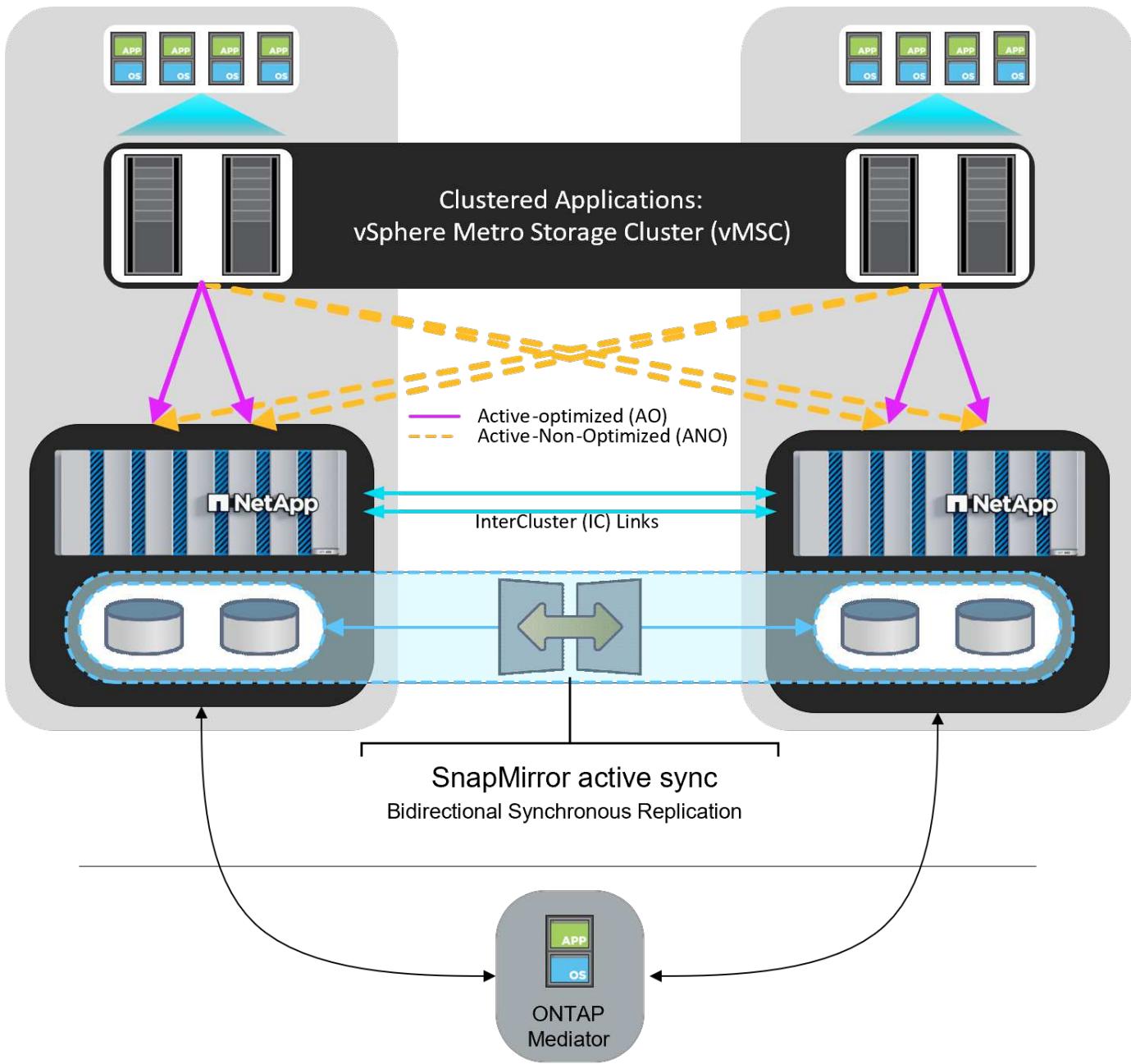
A continuación se muestra un diagrama topológico de alto nivel de MetroCluster de ampliación.



Consulte ["Documentación de MetroCluster"](#) Para obtener información específica sobre diseño e implementación para MetroCluster.

SnapMirror Active Sync también se puede poner en marcha de dos formas distintas.

- Asimétrico
- Sincronización activa simétrica (ONTAP 9.15.1)



Consulte ["Documentos de NetApp"](#) para obtener información específica sobre el diseño y la puesta en marcha de la sincronización activa de SnapMirror.

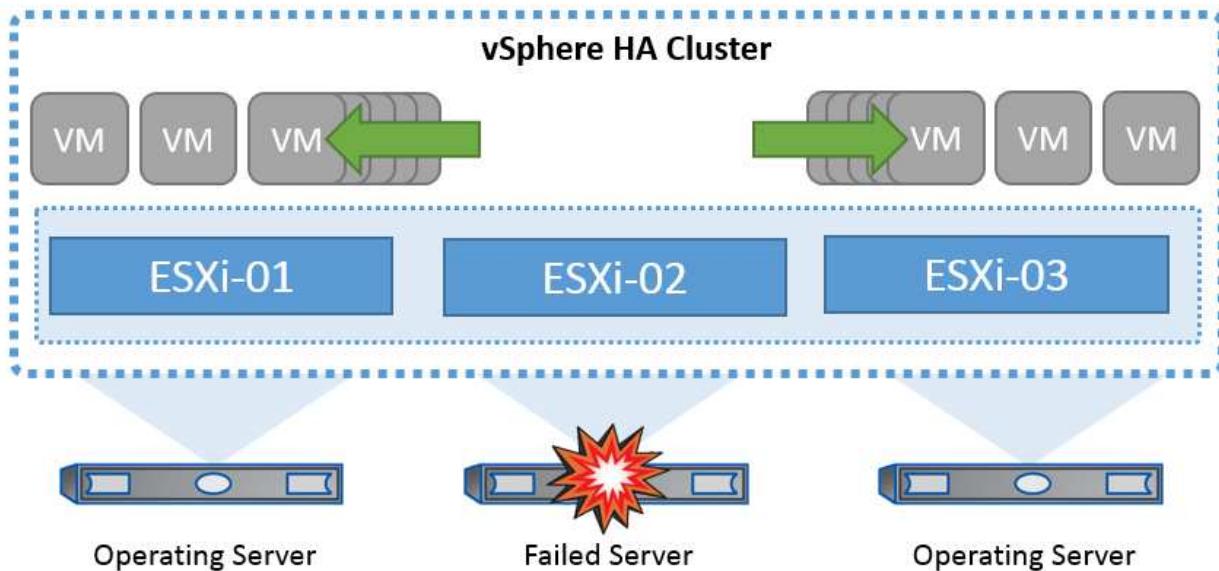
## Descripción general de la solución de VMware vSphere

vCenter Server Appliance (VCSA) es un potente sistema de administración centralizada y un panel único para vSphere que permite a los administradores operar de manera eficaz los clústeres ESXi. Facilita funciones clave como el aprovisionamiento de máquinas virtuales, la operación de vMotion, alta disponibilidad (HA), programador de recursos distribuidos (DRS), VMware vSphere Kubernetes Service (VKS) y más. Es un componente esencial en los entornos de nube de VMware y debe diseñarse teniendo en cuenta la disponibilidad del servicio.

## Alta disponibilidad de vSphere

La tecnología de clúster de VMware agrupa los servidores ESXi en pools de recursos compartidos para máquinas virtuales y proporciona vSphere High Availability (HA). vSphere HA proporciona alta disponibilidad fácil de usar para aplicaciones que se ejecutan en máquinas virtuales. Cuando se habilita la función HA en el clúster, cada servidor ESXi mantiene la comunicación con otros hosts de modo que si algún host ESXi deja de responder o aísla, el clúster de alta disponibilidad puede negociar la recuperación de las máquinas virtuales que se estaban ejecutando en ese host ESXi entre los hosts supervivientes del clúster. En caso de fallo del sistema operativo invitado, la alta disponibilidad de vSphere puede reiniciar la máquina virtual afectada en el mismo servidor físico. vSphere HA permite reducir los tiempos de inactividad planificados, evitar tiempos de inactividad no planificados y recuperarse rápidamente de las interrupciones.

Clúster vSphere HA que recupera máquinas virtuales de un servidor fallido.



Es importante entender que VMware vSphere no tiene conocimientos de la sincronización activa de NetApp MetroCluster o SnapMirror y ve todos los hosts ESXi del clúster de vSphere como hosts elegibles para las operaciones en clúster de alta disponibilidad en función de las configuraciones de afinidad de hosts y grupos de máquinas virtuales.

## Detección de fallo de host

Tan pronto como se crea el clúster HA, todos los hosts del clúster participan en la elección y uno de los hosts se convierte en maestro. Cada esclavo realiza un latido de red al maestro, y el maestro, a su vez, realiza un latido de red en todos los hosts esclavos. El host maestro de un clúster vSphere HA es responsable de detectar la falla de los hosts esclavos.

Según el tipo de error detectado, es posible que las máquinas virtuales que se ejecutan en los hosts deban conmutar al nodo de respaldo.

En un clúster de alta disponibilidad de vSphere se detectan tres tipos de fallos de host:

- Fallo: Un host deja de funcionar.
  - Aislamiento: Un host se convierte en una red aislada.
  - Partición: Un host pierde la conectividad de red con el host maestro.

El host maestro supervisa los hosts esclavos del cluster. Esta comunicación se realiza a través del intercambio

de latidos de la red cada segundo. Cuando el host maestro deja de recibir estos latidos de un host esclavo, comprueba si hay vida activa del host antes de declarar que el host ha fallado. La comprobación de vida que realiza el host maestro es determinar si el host esclavo está intercambiando latidos con uno de los almacenes de datos. Además, el host maestro comprueba si el host responde a los ping ICMP enviados a sus direcciones IP de gestión para detectar si simplemente está aislado de su nodo maestro o completamente aislado de la red. Para ello, haga ping en la puerta de enlace predeterminada. Se pueden especificar manualmente una o varias direcciones de aislamiento para mejorar la fiabilidad de la validación de aislamiento.

 NetApp recomienda especificar un mínimo de dos direcciones de aislamiento adicionales, y que cada una de estas direcciones sea local de sitio. Esto mejorará la fiabilidad de la validación del aislamiento.

## Respuesta de aislamiento del host

La respuesta de aislamiento es una configuración en vSphere HA que determina la acción que se activa en las máquinas virtuales cuando un host en un clúster de vSphere HA pierde sus conexiones de red de administración pero continúa ejecutándose. Hay tres opciones para esta configuración: "Deshabilitado", "Apagar y reiniciar máquinas virtuales" y "Apagar y reiniciar máquinas virtuales".

"Apagar" es mejor que "Apagar", que no borra los cambios más recientes en el disco ni confirma las transacciones. Si las máquinas virtuales no se apagan en 300 segundos, se apagan. Para cambiar el tiempo de espera, utilice la opción avanzada `das.isolationshutdowntimeout`.

Antes de que HA inicie la respuesta de aislamiento, primero comprueba si el agente maestro HA de vSphere posee el almacén de datos que contiene los archivos de configuración de la máquina virtual. Si no es así, el host no activará la respuesta de aislamiento, porque no hay ningún maestro para reiniciar las máquinas virtuales. El host comprobará periódicamente el estado del almacén de datos para determinar si un agente de alta disponibilidad de vSphere que posee el rol maestro.

 NetApp recomienda establecer la respuesta de aislamiento del host en Desactivada.

Se puede producir una condición de cerebro dividido si un host se aísla o partitiona desde el host maestro HA de vSphere y el maestro no puede comunicarse a través de los almacenes de datos de latido o mediante ping. El maestro declara que el host aislado está muerto y reinicia los equipos virtuales en otros hosts del cluster. Ahora existe una condición de cerebro dividido porque hay dos instancias de la máquina virtual en ejecución, solo una de las cuales puede leer o escribir los discos virtuales. Ahora se pueden evitar las condiciones del cerebro dividido configurando VM Component Protection (VMCP).

## Protección de componentes de máquina virtual (VMCP)

Una de las mejoras de funciones de vSphere 6, relevante para la alta disponibilidad, es VMCP. VMCP proporciona protección mejorada contra todas las condiciones de pérdida permanente de dispositivos (APD) y de pérdida permanente de dispositivos (PDL) para bloques (FC, iSCSI, FCoE) y almacenamiento de archivos (NFS).

### Pérdida permanente de dispositivo (PDL)

PDL es una condición que ocurre cuando un dispositivo de almacenamiento falla permanentemente o se elimina administrativamente y no se espera que regrese. La matriz de almacenamiento NetApp emite un código SCSI Sense a ESXi, declarando que el dispositivo se perdió de forma permanente. En la sección Condiciones de falla y respuesta de VM de vSphere HA, puede configurar cuál debe ser la respuesta después de que se detecta una condición PDL.



NetApp recomienda configurar la "Respuesta para almacén de datos con PDL" en "**Apagar y reiniciar las máquinas virtuales**". Cuando se detecta esta condición, una máquina virtual se reiniciará instantáneamente en un host en buen estado dentro del clúster vSphere HA.

#### Todas las rutas hacia abajo (APD)

APD es una condición que ocurre cuando un dispositivo de almacenamiento se vuelve inaccesible para el host y no hay rutas disponibles a la matriz. ESXi considera que se trata de un problema temporal con el dispositivo y espera que vuelva a estar disponible.

Cuando se detecta una condición de APD, se inicia un temporizador. Después de 140 segundos, la condición APD se declara oficialmente, y el dispositivo se marca como APD Time Out. Una vez transcurridos los 140 segundos, HA comenzará a contar el número de minutos especificado en el APD de retraso para failover de VM. Cuando transcurra el tiempo especificado, HA reiniciará los equipos virtuales afectados. Puede configurar VMCP para que responda de manera diferente si lo desea (Desactivado, Incidir eventos o Apagar y reiniciar VM).



- NetApp recomienda configurar la respuesta para el almacén de datos con APD en «**Apagar y reiniciar VM (conservador)**».
- Conservador se refiere a la probabilidad de que HA pueda reiniciar las máquinas virtuales. Cuando se configura en Conservador, HA solo reiniciará la VM afectada por el APD si sabe que otro host puede reiniciarla. En el caso de Agresivo, HA intentará reiniciar la VM incluso si no conoce el estado de los otros hosts. Esto puede provocar que las máquinas virtuales no se reinicien si no hay ningún host con acceso al almacén de datos donde se encuentran.
- Si se resuelve el estado de APD y se restaura el acceso al almacenamiento antes de que haya pasado el tiempo de espera, HA no reiniciará innecesariamente la máquina virtual a menos que lo configure explícitamente para hacerlo. Si se desea una respuesta, incluso cuando el entorno se ha recuperado de la condición APD, la respuesta para la recuperación APD después del tiempo de espera APD debe configurarse para restablecer las máquinas virtuales.
- NetApp recomienda configurar la respuesta para la recuperación de APD después del tiempo de espera de APD en Desactivado.

#### Implementación de VMware DRS para NetApp SnapMirror Active Sync

VMware DRS es una función que agrega los recursos de host en un clúster y se usa principalmente para equilibrar cargas dentro de un clúster de una infraestructura virtual. VMware DRS calcula principalmente los recursos de la CPU y la memoria para realizar el equilibrio de carga en un clúster. Como vSphere no es consciente de la agrupación en cluster ampliada, considera todos los hosts en ambos sitios al equilibrar la carga.

#### Implementación de VMware DRS para NetApp MetroCluster

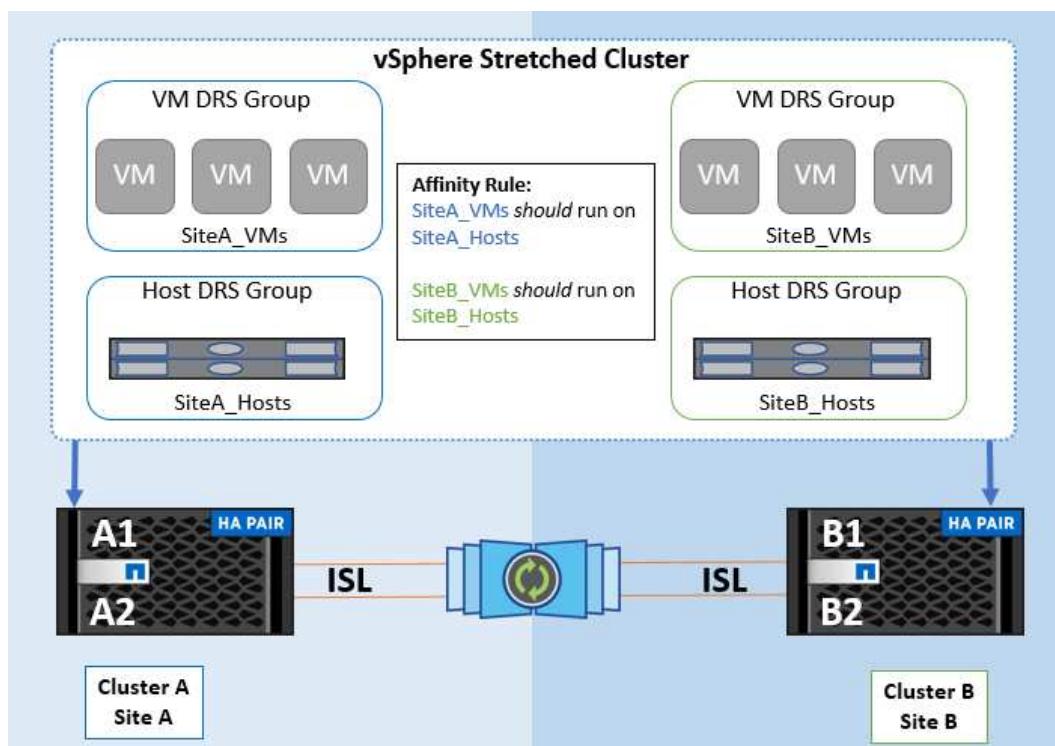
To avoid cross-site traffic, NetApp recommends configuring DRS affinity rules to manage a logical separation of VMs. This will ensure that, unless there is a complete site failure, HA and DRS will only use local hosts. Si crea una regla de afinidad de DRS para su clúster, puede especificar cómo aplica vSphere esa regla durante una conmutación al respaldo de una máquina virtual.

Hay dos tipos de reglas que puede especificar para el comportamiento de conmutación por error de vSphere HA:

- Las reglas de anti-afinidad de equipos virtuales obligan a los equipos virtuales especificados a permanecer separados durante las acciones de recuperación tras fallos.
- Las reglas de afinidad de host de VM colocan las máquinas virtuales especificadas en un host particular o un miembro de un grupo definido de hosts durante las acciones de conmutación por error.

Mediante el uso de reglas de afinidad de host de VM en VMware DRS, se puede tener una separación lógica entre el sitio A y el sitio B, de modo que la VM se ejecute en el host en el mismo sitio que la cabina que está configurada como la controladora de lectura/escritura primaria para un almacenamiento de datos determinado. Además, las reglas de afinidad de host de VM permiten que las máquinas virtuales permanezcan locales en el almacenamiento, lo que, a su vez, verifica la conexión a la máquina virtual en caso de fallos de red entre los sitios.

A continuación se muestra un ejemplo de los grupos de hosts y las reglas de afinidad de las máquinas virtuales.



#### Best Practice

NetApp recomienda implementar reglas de «debería» en lugar de reglas de «obligación» porque vSphere HA las infringe en caso de fallo. El uso de reglas «imprescindibles» podría provocar interrupciones del servicio.

La disponibilidad de los servicios debe prevalecer siempre sobre el rendimiento. En el escenario en el que falla un centro de datos completo, las reglas "obligatorias" deben elegir hosts del grupo de afinidad de host de VM y, cuando el centro de datos no está disponible, las máquinas virtuales no se reiniciarán.

#### Implementación de VMware Storage DRS con NetApp MetroCluster

La función VMware Storage DRS permite agregar almacenes de datos en una sola unidad y equilibra los discos de máquina virtual cuando se superan los umbrales de control de I/O de almacenamiento (SIOC).

El control de la I/O de almacenamiento se habilita de forma predeterminada en los clústeres DRS habilitados para Storage DRS. El control de las operaciones de I/O de almacenamiento permite a un administrador controlar la cantidad de I/O de almacenamiento que se asigna a máquinas virtuales durante períodos de congestión de I/O, lo que permite que las máquinas virtuales más importantes tengan preferencia por máquinas virtuales menos importantes para la asignación de recursos de E/S.

Storage DRS utiliza Storage vMotion para migrar los equipos virtuales a diferentes almacenes de datos dentro de un clúster de almacén de datos. En un entorno NetApp MetroCluster, una migración de máquinas virtuales debe controlarse dentro de los almacenes de datos de ese sitio. Por ejemplo, en condiciones ideales, la máquina virtual A, que se ejecuta en un host en el sitio A, debería migrar dentro de los almacenes de datos de la SVM en el sitio A. Si no lo hace, la máquina virtual continuará funcionando pero con un rendimiento degradado, ya que la lectura/escritura del disco virtual será desde la ubicación B a través de enlaces entre sitios.

\*Cuando se utiliza el almacenamiento ONTAP, se recomienda desactivar el DRS de Almacenamiento.

- Por lo general, los DRS de almacenamiento no son necesarios ni se recomiendan para su uso con sistemas de almacenamiento de ONTAP.
- ONTAP proporciona sus propias funciones de eficiencia del almacenamiento, como la deduplicación, la compresión y la compactación, que pueden verse afectadas por Storage DRS.
- Si está usando instantáneas de ONTAP, Storage vMotion dejaría atrás la copia de la VM en la instantánea, lo que podría aumentar la utilización del almacenamiento y afectar aplicaciones de respaldo como NetApp SnapCenter, que rastrean las VM y sus instantáneas de ONTAP.



## Directrices de implementación y diseño de VMSC

Este documento describe las guías de diseño e implementación para VMSC con sistemas de almacenamiento ONTAP.

### Configuración de almacenamiento de NetApp

Las instrucciones de configuración para NetApp MetroCluster están disponibles en "[Documentación de MetroCluster](#)". Las instrucciones para SnapMirror Active Sync (SMAS) también están disponibles en "[Información general sobre la continuidad del negocio de SnapMirror](#)".

Después de configurar MetroCluster, administrarlo es como administrar un entorno ONTAP tradicional. Puede configurar máquinas virtuales de almacenamiento (SVM) con diferentes herramientas, como la interfaz de línea de comandos (CLI), System Manager o Ansible. Una vez que se han configurado las SVM, cree interfaces lógicas (LIF), volúmenes y números de unidad lógica (LUN) en el clúster que se utilizarán para operaciones normales. Estos objetos se replicarán automáticamente en el otro clúster mediante la red de conexión de clústeres.

Si no utiliza MetroCluster o tiene sistemas ONTAP que no son compatibles con MetroCluster, como los sistemas ASA R2, puede usar la sincronización activa de SnapMirror que proporciona protección granular de almacenes de datos y acceso activo-activo en varios clústeres de ONTAP de diferentes dominios de fallo. SMAS utiliza grupos de coherencia (CG) para garantizar la coherencia en orden de escritura entre uno o varios almacenes de datos y puede crear varios CG en función de los requisitos de su aplicación y de su almacén de datos. Los grupos de coherencia son especialmente útiles para aplicaciones que requieren sincronización de datos entre varios almacenes de datos. Por ejemplo, LVM invitados distribuidos entre almacenes de datos. SMAS también admite asignaciones de dispositivos sin procesar (RDM) y

almacenamiento conectado mediante invitado con iniciadores iSCSI en los invitados. Puede obtener más información sobre los grupos de consistencia en "["Información general sobre los grupos de consistencia"](#)".

Hay alguna diferencia en la gestión de una configuración VMSC con sincronización activa de SnapMirror en comparación con una MetroCluster. En primer lugar, SMAS es una configuración solo SAN, no se puede proteger ningún almacén de datos NFS con sincronización activa de SnapMirror. Segundo, debe asignar ambas copias de las LUN a los hosts ESXi para que accedan a los almacenes de datos replicados en ambos dominios de fallo. Tercero, debe crear uno o varios grupos de coherencia para los almacenes de datos que desea proteger con la sincronización activa de SnapMirror. Por último, debe crear una política de SnapMirror para los grupos de consistencia que creó. Todo esto puede realizarse fácilmente usando el asistente para proteger clúster del complemento vCenter de herramientas de ONTAP, o bien manualmente usando la CLI de ONTAP o System Manager.

### **Uso del complemento de herramientas de ONTAP para vCenter para SnapMirror**

El complemento para vCenter para herramientas de ONTAP proporciona un método sencillo e intuitivo de configurar la sincronización activa de SnapMirror para VMSC. Es posible usar el complemento de herramientas de ONTAP para crear y gestionar relaciones de sincronización activa de SnapMirror entre dos clústeres de ONTAP. Este plugin proporciona una interfaz fácil de usar para establecer y gestionar estas relaciones de manera eficiente. Puede obtener más información sobre el complemento para vCenter de herramientas de ONTAP en "["Herramientas de ONTAP para VMware vSphere"](#)", o ir directamente a "["Proteja mediante la protección del clúster de hosts"](#)".

### **Configuración de VMware vSphere**

#### **Cree un clúster de vSphere HA**

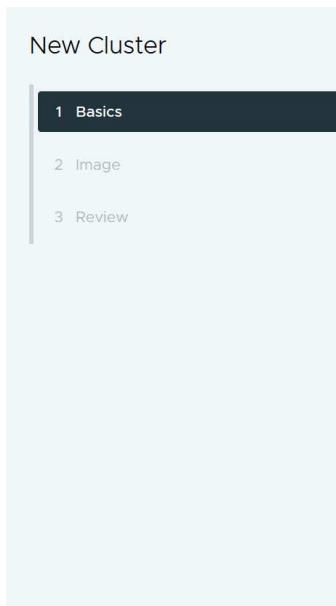
La creación de un clúster de vSphere HA es un proceso de varios pasos que se documenta completamente en "["Cómo se crean y configuran clústeres en vSphere Client en docs.vmware.com"](#)". En resumen, primero debe crear un clúster vacío y, después, utilizando vCenter, debe añadir hosts y especificar la alta disponibilidad de vSphere y otros ajustes del clúster.



Nada en este documento sustituye "["Prácticas recomendadas para VMware vSphere Metro Storage Cluster"](#)". Este contenido se ofrece para facilitar la referencia y no sustituye la documentación oficial de VMware.

Para configurar un clúster de alta disponibilidad, realice los siguientes pasos:

1. Conéctese a la interfaz de usuario de vCenter.
2. En Hosts and Clusters, vaya al centro de datos donde desea crear su clúster de alta disponibilidad.
3. Haga clic con el botón derecho en el objeto del centro de datos y seleccione New Cluster. En los conceptos básicos, asegúrese de haber habilitado vSphere DRS y vSphere HA. Complete el asistente.



Basics

Name: MCC Cluster

Location: Raleigh

vSphere DRS:

vSphere HA:

vSAN:  Enable vSAN ESA (i)

Manage all hosts in the cluster with a single image (i)

Choose how to set up the cluster's image

- Compose a new image
- Import image from an existing host in the vCenter inventory
- Import image from a new host

Manage configuration at a cluster level (i)

1. Seleccione el clúster y vaya a la pestaña Configure. Seleccione vSphere HA y haga clic en Edit.
2. En Supervisión de host, seleccione la opción Habilitar supervisión de host.

Edit Cluster Settings | MCC Cluster

vSphere HA:

Failures and responses    Admission Control    Heartbeat Datastores    Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring (i)

|                               |   |
|-------------------------------|---|
| > Host Failure Response       | Restart VMs   |
| > Response for Host Isolation | Disabled  |
| > Datastore with PDL          | Power off and restart VMs                               |
| > Datastore with APD          | Power off and restart VMs - Conservative restart policy |
| > VM Monitoring               | Disabled  |

1. Mientras todavía está en la pestaña Fallos y Respuestas, en VM Monitoring, seleccione la opción VM Monitoring Only o VM and Application Monitoring.

## Edit Cluster Settings | MCC Cluster

X

> Response for Host Isolation      Disabled

> Datastore with PDL      Power off and restart VMs

> Datastore with APD      Power off and restart VMs - Conservative restart policy

▼ VM Monitoring

Enable heartbeat monitoring

VM monitoring resets individual VMs if their VMware tools heartbeats are not received within a set time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.

Disabled

VM Monitoring Only

Turns on VMware tools heartbeats. When heartbeats are not received within a set time, the VM is reset.

VM and Application Monitoring

Turns on application heartbeats. When heartbeats are not received within a set time, the VM is reset.

CANCEL OK

1. En Control de admisión, establezca la opción de control de admisión de HA en Reserva de recursos de cluster; utilice 50% CPU/MEM.

## Edit Cluster Settings | MCC Cluster

X

vSphere HA

Failures and responses

Admission Control

Heartbeat Datastores

Advanced Options

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

Host failures cluster tolerates

1



Maximum is one less than number of hosts in cluster.

Define host failover capacity by

Cluster resource Percentage

Override calculated failover capacity.

Reserved failover CPU capacity:  50 % CPU

Reserved failover Memory capacity:  50 % Memory

Reserve Persistent Memory failover capacity

Override calculated Persistent Memory failover capacity

CANCEL

OK

1. Haga clic en OK.

2. Seleccione DRS y haga clic en EDIT.

3. Establezca el nivel de automatización en manual a menos que las aplicaciones lo requieran.

## Edit Cluster Settings | MCC Cluster

X

vSphere DRS

Automation

Additional Options

Power Management

Advanced Options

Automation Level

Manual

DRS generates both power-on placement recommendations, and migration recommendations for virtual machines. Recommendations need to be manually applied or ignored.

Migration Threshold

Conservative



(Less  
Frequent  
vMotions)

(3) DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads. (Default)

Aggressive  
(More  
Frequent  
vMotions)

Predictive DRS

Enable

Virtual Machine Automation

Enable

1. Habilite VM Component Protection, consulte "[docs.vmware.com](https://docs.vmware.com)".
2. Se recomiendan las siguientes configuraciones adicionales de alta disponibilidad de vSphere para VMSC con MetroCluster:

| Fallo  | Respuesta  |
|--|--|
| Error del host   | Reiniciar las máquinas virtuales                   |
| Aislamiento de hosts   | Deshabilitado                                      |
| Almacén de datos con pérdida permanente de dispositivo (PDL)     | Apagar y reiniciar los equipos virtuales           |
| Almacén de datos con todas las rutas inactivas (APD)             | Apagar y reiniciar los equipos virtuales           |
| El huésped no es molesto   | Restablecer las máquinas virtuales                 |
| Política de reinicio de máquinas virtuales                       | Determinado por la importancia del equipo virtual  |
| Respuesta para el aislamiento del host                           | Apagar y reiniciar equipos virtuales               |
| Respuesta para datastore con PDL                                 | Apagar y reiniciar los equipos virtuales           |
| Respuesta del almacén de datos con APD                           | Apagar y reiniciar equipos virtuales (conservador) |
| Demora en recuperación tras fallos de equipos virtuales para APD | 3 minutos  |
| Respuesta para la recuperación de APD con tiempo de espera APD   | Deshabilitado                                      |
| Supervisión de la sensibilidad de los equipos virtuales          | Preajuste ALTO                                     |

#### Configurar almacenes de datos para Heartbeat

La alta disponibilidad de vSphere utiliza almacenes de datos para supervisar hosts y máquinas virtuales cuando se produce un error en la red de gestión. Es posible configurar la forma en la que vCenter selecciona los almacenes de datos de latido. Para configurar los almacenes de datos para latir, lleve a cabo los siguientes pasos:

1. En la sección Datastore Heartbeat, seleccione Use datastores from the Specified List y complemente automáticamente si es necesario.
2. Seleccione los almacenes de datos que desee utilizar vCenter en ambos sitios y pulse OK.

vSphere HA 
[Failures and responses](#) [Admission Control](#) [Heartbeat Datastores](#) [Advanced Options](#)

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 4 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

- Automatically select datastores accessible from the hosts
- Use datastores only from the specified list
- Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

|                                     | Name ↑ | Datastore Cluster | Hosts Mounting Datastore |
|-------------------------------------|--------|-------------------|--------------------------|
| <input checked="" type="checkbox"/> | d11    | N/A               | 2                        |
| <input checked="" type="checkbox"/> | d12    | N/A               | 2                        |
| <input checked="" type="checkbox"/> | d21    | N/A               | 2                        |
| <input checked="" type="checkbox"/> | d22    | N/A               | 2                        |
| <input type="checkbox"/>            | d31    | N/A               | 2                        |
| <input type="checkbox"/>            | d32    | N/A               | 2                        |
| <input type="checkbox"/>            | d41    | N/A               | 2                        |
| <input type="checkbox"/>            | d42    | N/A               | 2                        |

11 items

CANCEL

OK

### Configurar opciones avanzadas

Los eventos de aislamiento se producen cuando los hosts dentro de un clúster de alta disponibilidad pierden la conectividad a la red u otros hosts del clúster. De forma predeterminada, vSphere HA utilizará la puerta de enlace predeterminada para su red de gestión como dirección de aislamiento predeterminada. Sin embargo, puede especificar direcciones de aislamiento adicionales para que el host haga ping para determinar si se debe activar una respuesta de aislamiento. Agregue dos IP de aislamiento que puedan hacer ping, una por sitio. No utilice la IP de la puerta de enlace. La configuración avanzada de HA de vSphere utilizada es `das.isolationaddress`. Puede utilizar las direcciones IP de ONTAP o Mediator para este fin.

Consulte ["Prácticas recomendadas para VMware vSphere Metro Storage Cluster"](#) para obtener más información.

vSphere HA

Failures and responses   Admission Control   Heartbeat Datastores   Advanced Options

You can set advanced options that affect the behavior of your vSphere HA cluster.

**Add** **Delete**

| Option                        | Value        |
|-------------------------------|--------------|
| das.IgnoreRedundantNetWarning | true         |
| das.Isolationaddress0         | 10.61.99.100 |
| das.Isolationaddress1         | 10.61.99.110 |
| das.heartbeatDsPerHost        | 4            |

4 items

**CANCEL** **OK**

Agregar una configuración avanzada llamada das.heartbeatDsPerHost puede aumentar el número de almacenes de datos de latido. Utilice cuatro almacenes de datos para el corazón (HB DSS): Dos por sitio. Utilice la opción Seleccionar de la lista pero complementar. Esto es necesario porque si un sitio falla, usted todavía necesita dos HB DSS. Sin embargo, dichas aplicaciones no tienen por qué estar protegidas con MetroCluster o SnapMirror con sincronización activa.

Consulte "[Prácticas recomendadas para VMware vSphere Metro Storage Cluster](#)" para obtener más información.

#### Afinidad de VMware DRS para NetApp MetroCluster

En esta sección creamos grupos DRS para equipos virtuales y hosts para cada sitio\clúster del entorno MetroCluster. A continuación, configuraremos las reglas de VM\Host para alinear la afinidad de host de VM con los recursos de almacenamiento local. Por ejemplo, las máquinas virtuales de la dirección A pertenecen al grupo de máquinas virtuales sitea\_vms y la ubicación A pertenecen al grupo de hosts sitea\_hosts. A continuación, en VM\Host Rules, indicamos que sitea\_vms debe ejecutarse en hosts en sitea\_Hosts.

- NetApp recomienda encarecidamente la especificación **Debe ejecutarse en hosts del grupo** en lugar de la especificación **Debe ejecutarse en hosts del grupo**. En caso de que se produzca un fallo del host del sitio A, es necesario reiniciar las máquinas virtuales del sitio A en los hosts del sitio B a través de vSphere HA, pero la última especificación no permite a HA reiniciar los equipos virtuales en el sitio B, ya que es una regla estricta. La especificación anterior es una regla flexible y se infringirá en caso de alta disponibilidad, lo que permitirá la disponibilidad en lugar de rendimiento.
- Puede crear una alarma basada en eventos que se dispara cuando una máquina virtual viola una regla de afinidad VM-Host. En vSphere Client, agregue una nueva alarma para la máquina virtual y seleccione VM is Violating VM-Host Affinity Rule como activador de evento. Para obtener más información sobre la creación y edición de alarmas, consulte "[Supervisión y rendimiento de vSphere](#)" la documentación.

### Crear grupos de hosts DRS

Para crear grupos de hosts DRS específicos del sitio A y del sitio B, realice los siguientes pasos:

1. En vSphere Web Client, haga clic con el botón derecho en el clúster en el inventario y seleccione Settings.
2. Haga clic en VM\Host Groups.
3. Haga clic en Añadir.
4. Escriba el nombre del grupo (por ejemplo, sitea\_hosts).
5. En el menú Tipo, seleccione Grupo de hosts.
6. Haga clic en Agregar y seleccione los hosts deseados del sitio A y haga clic en Aceptar.
7. Repita estos pasos para agregar otro grupo de hosts para el sitio B.
8. Haga clic en Aceptar.

### Crear grupos de máquinas virtuales DRS

Para crear grupos de máquinas virtuales DRS específicos del sitio A y del sitio B, realice los siguientes pasos:

1. En vSphere Web Client, haga clic con el botón derecho en el clúster en el inventario y seleccione Settings.
2. Haga clic en VM\Host Groups.
3. Haga clic en Añadir.
4. Escriba el nombre del grupo (por ejemplo, sitea\_vms).
5. En el menú Type, seleccione VM Group.
6. Haga clic en Add y seleccione las máquinas virtuales deseadas en el sitio A y, a continuación, haga clic en OK.
7. Repita estos pasos para agregar otro grupo de hosts para el sitio B.
8. Haga clic en Aceptar.

### Crear reglas de host de VM

Para crear reglas de afinidad de DRS específicas para el sitio A y el sitio B, realice los siguientes pasos:

1. En vSphere Web Client, haga clic con el botón derecho en el clúster en el inventario y seleccione Settings.
2. Haga clic en VM\Host Rules.

3. Haga clic en Añadir.
4. Escriba el nombre de la regla (por ejemplo, sitea\_affinity).
5. Compruebe que la opción Activar regla está activada.
6. En el menú Type, seleccione Virtual Machines to Hosts.
7. Seleccione el grupo de VM (por ejemplo, sitea\_vms).
8. Seleccione el grupo Host (por ejemplo, sitea\_Hosts).
9. Repita estos pasos para añadir otra regla VM\Host para el sitio B.
10. Haga clic en Aceptar.

Create VM/Host Rule | Cluster-01 X

|      |                           |  |
|------|---------------------------|--|
| Name | sitea_affinity            | <input checked="" type="checkbox"/> Enable rule. |
| Type | Virtual Machines to Hosts |  |

Virtual machines that are members of the Cluster VM Group sitea\_vms should run on host group sitea\_hosts.

VM Group:

sitea\_vms

Should run on hosts in group

Host Group:

sitea\_hosts

CANCEL
OK

### Cree clústeres de almacenes de datos si es necesario

Para configurar un clúster de almacén de datos para cada sitio, complete los siguientes pasos:

1. Use el cliente web de vSphere, vaya al centro de datos donde reside el clúster de alta disponibilidad en Storage.
2. Haga clic con el botón derecho en el objeto del centro de datos y seleccione Storage > New Datastore Cluster.

\*Cuando se utiliza el almacenamiento ONTAP, se recomienda desactivar el DRS de Almacenamiento.

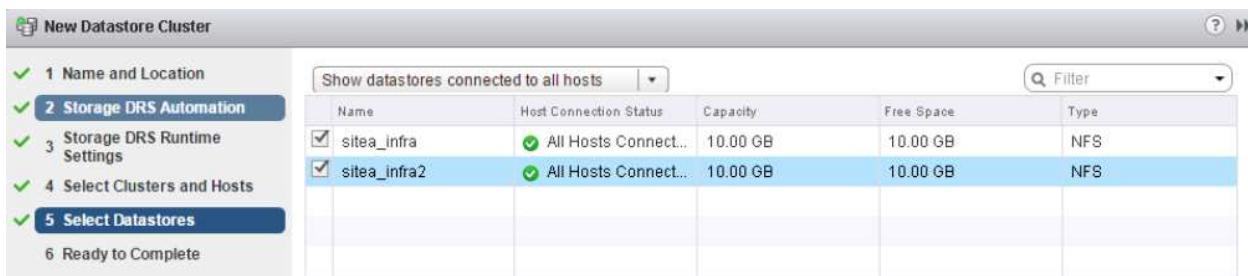
- Por lo general, los DRS de almacenamiento no son necesarios ni se recomiendan para su uso con sistemas de almacenamiento de ONTAP.
- ONTAP proporciona sus propias funciones de eficiencia del almacenamiento, como la deduplicación, la compresión y la compactación, que pueden verse afectadas por Storage DRS.
- Si utiliza copias Snapshot de ONTAP, Storage vMotion dejaría detrás de la copia del equipo virtual en la copia Snapshot, lo que puede aumentar el uso del almacenamiento y puede afectar a las aplicaciones de backup como NetApp SnapCenter, que registran las máquinas virtuales y sus copias Snapshot de ONTAP.



1. Seleccione el clúster de alta disponibilidad y haga clic en Next.



1. Seleccione los almacenes de datos que pertenecen al sitio A y haga clic en Next.



1. Revise las opciones y haga clic en Finish.
2. Repita estos pasos para crear el clúster de almacenes de datos del sitio B y verifique que solo estén seleccionados los almacenes de datos del sitio B.

## Disponibilidad del vCenter Server

Los dispositivos vCenter Server Appliances (VCSA) deben estar protegidos con alta disponibilidad de vCenter. La alta disponibilidad de vCenter le permite implementar dos VCSA en un par de alta disponibilidad activo-pasivo. Uno en cada dominio de fallo. Puede obtener más información sobre la alta disponibilidad de vCenter en ["docs.vmware.com"](https://docs.vmware.com).

## Resiliencia para eventos planificados y no planificados

NetApp MetroCluster y SnapMirror Active Sync son potentes herramientas que mejoran la alta disponibilidad y las operaciones no disruptivas del hardware de NetApp y del software ONTAP®.

Estas herramientas proporcionan protección en todo el sitio para todo el entorno de almacenamiento, lo que garantiza que los datos están siempre disponibles. Ya sea que utilice servidores independientes, clústeres de servidores de alta disponibilidad, contenedores o servidores virtualizados, la tecnología NetApp mantiene fácilmente la disponibilidad de almacenamiento en caso de interrupción total por pérdida de alimentación, refrigeración o conectividad de red, apagado del array de almacenamiento o error de funcionamiento.

MetroCluster y SnapMirror de sincronización activa proporcionan tres métodos básicos de continuidad de datos en caso de eventos previstos o no planificados:

- Componentes redundantes para protección contra fallos de un solo componente
- Toma de control local de alta disponibilidad para eventos que afectan a una única controladora
- Protección completa del sitio: Reanudación rápida del servicio al mover el almacenamiento y el acceso de clientes del clúster de origen al clúster de destino

Esto significa que las operaciones continúan sin problemas en caso de fallo de un único componente y vuelven automáticamente al funcionamiento redundante cuando se reemplaza el componente fallido.

Todos los clústeres de ONTAP, excepto los clústeres de un solo nodo (normalmente las versiones definidas por software, como ONTAP Select, por ejemplo), tienen funciones de alta disponibilidad incorporadas denominadas toma de control y retorno al nodo primario. Cada controladora del clúster se empareja con otra controladora, lo que forma una pareja de alta disponibilidad. Estos pares garantizan que cada nodo esté conectado localmente al almacenamiento.

La toma de control es un proceso automatizado en el que un nodo asume el almacenamiento del otro para mantener los servicios de datos. Giveback es el proceso inverso que restaura el funcionamiento normal. La toma de control puede planificarse, por ejemplo, al realizar tareas de mantenimiento del hardware o actualizaciones de ONTAP, o no planificadas, resultantes de un error de hardware o de alarma en el nodo.

Durante una toma de control, los LIF NAS en configuraciones de MetroCluster comutan automáticamente al respaldo. Sin embargo, los LIF de SAN no comutan al nodo de respaldo; seguirán utilizando la ruta directa a los números de unidad lógica (LUN).

Si quiere más información sobre la toma de control y el retorno al nodo primario de alta disponibilidad, consulte el ["Información general sobre la gestión de parejas de HA"](#). Vale la pena señalar que esta funcionalidad no es específica de la sincronización activa de MetroCluster o SnapMirror.

El cambio de sitio con MetroCluster se produce cuando un sitio está sin conexión o como una actividad planificada para el mantenimiento de todo el sitio. El sitio restante asume la propiedad de los recursos de almacenamiento (discos y agregados) del clúster sin conexión y las SVM del sitio con el que se ha producido el fallo se conectan y se reinician en el sitio de desastre, conservando su identidad completa para el acceso de clientes y host.

Con la sincronización activa de SnapMirror, dado que ambas copias se usan de forma activa a la vez, los hosts existentes seguirán funcionando. El Mediador de ONTAP es necesario para garantizar que la comutación por error del sitio se produce correctamente.

## Situaciones de fallo para VMSC con MetroCluster

En las siguientes secciones se resumen los resultados esperados de varios escenarios de fallo con sistemas VMSC y NetApp MetroCluster.

### Fallo de ruta de almacenamiento única

En esta situación, si se produce un error en componentes como el puerto HBA, el puerto de red, el puerto del switch de datos de interfaz de usuario o un cable FC o Ethernet, esa ruta particular al dispositivo de almacenamiento se marca como muerta por el host ESXi. Si se configuran varias rutas para el dispositivo de almacenamiento proporcionando resiliencia en el puerto de HBA/red/switch, ESXi idealmente ejecuta una conmutación de rutas. Durante este periodo, las máquinas virtuales permanecen en ejecución sin que se vean afectadas, porque se cuida de la disponibilidad del almacenamiento mediante varias rutas al dispositivo de almacenamiento.



No hay ningún cambio en el comportamiento de MetroCluster en este escenario, y todos los almacenes de datos siguen estando intactos en sus sitios respectivos.

#### *Best Practice*

En entornos en los que se utilizan volúmenes NFS/iSCSI, NetApp recomienda tener al menos dos vínculos superiores de red configurados para el puerto NFS vmkernel en el vSwitch estándar y lo mismo en el grupo de puertos en el que se asigna la interfaz de NFS vmkernel para el vSwitch distribuido. La agrupación de NIC se puede configurar en activo-activo o activo-en espera.

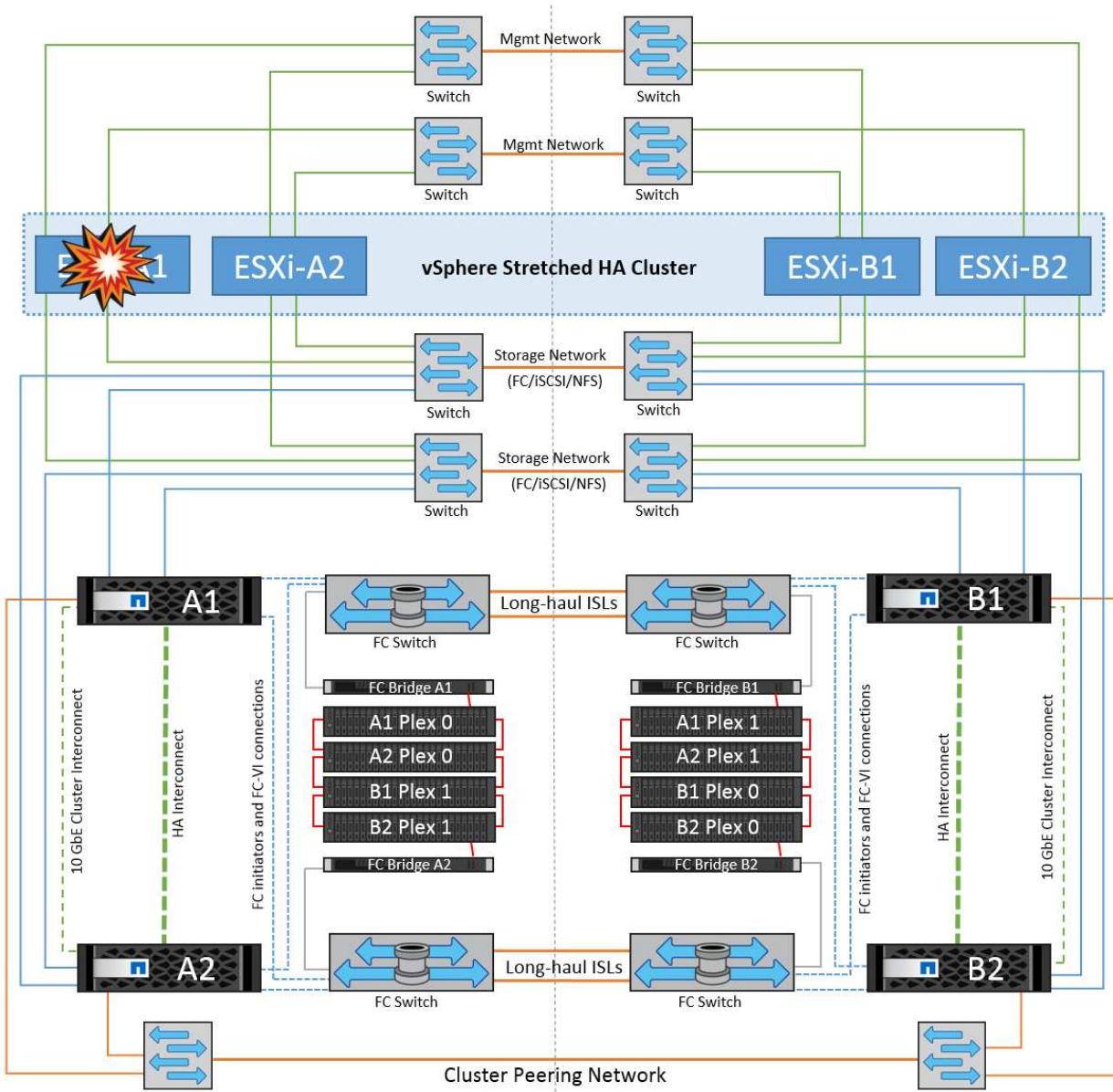
Además, para las LUN iSCSI, la multivía debe configurarse vinculando las interfaces de vmkernel con los adaptadores de red iSCSI. Si quiere más información, consulte la documentación de almacenamiento de vSphere.

#### *Best Practice*

En entornos en los que se usan LUN de Fibre Channel, NetApp recomienda tener al menos dos HBA, lo que garantiza la resistencia a nivel de HBA/puerto. NetApp también recomienda la división en zonas de un solo iniciador a un único destino como práctica recomendada para configurar la división en zonas.

Debe utilizarse Virtual Storage Console (VSC) para establecer normativas de accesos múltiples, porque establece normativas para todos los dispositivos de almacenamiento de NetApp nuevos y existentes.

### Fallo de un host ESXi único



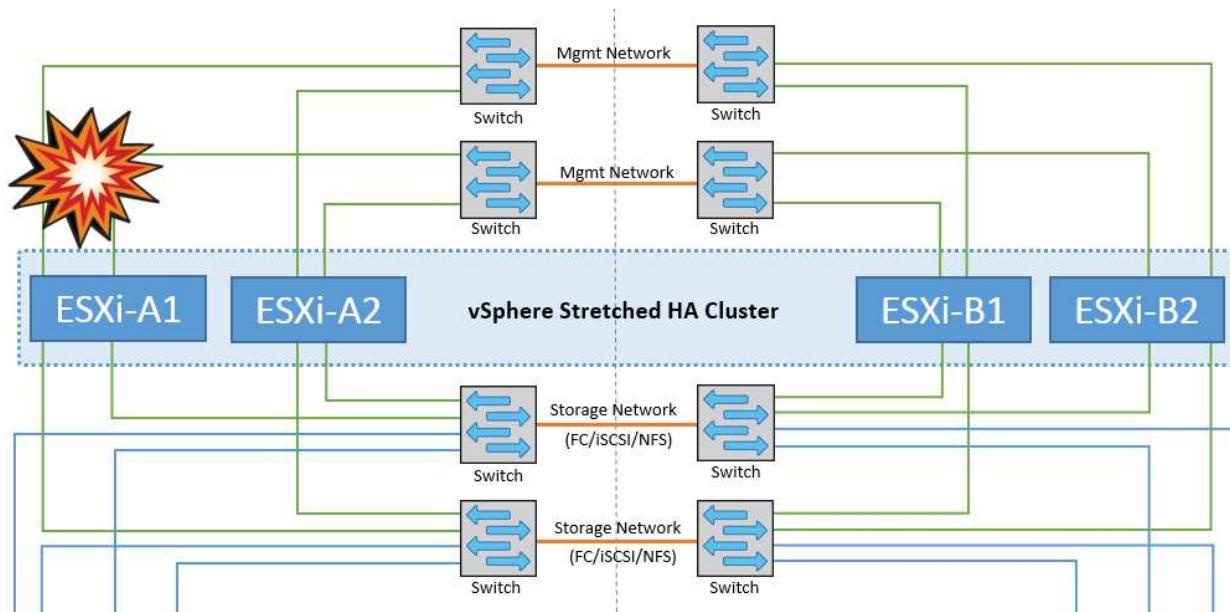
En esta situación, si hay un fallo de host ESXi, el nodo maestro del clúster de alta disponibilidad de VMware detecta el fallo del host porque ya no recibe los latidos de red. Para determinar si el host está realmente inactivo o sólo una partición de red, el nodo maestro supervisa los latidos del almacenamiento y, si están ausentes, realiza una comprobación final haciendo ping en las direcciones IP de gestión del host fallido. Si todas estas comprobaciones son negativas, el nodo maestro declara a este host un host fallido y todas las máquinas virtuales que se estaban ejecutando en este host fallido se reinician en el host superviviente del clúster.

Si se han configurado las reglas de afinidad de host y VM de DRS (las VM del grupo de VM sitea\_vms deben ejecutar hosts en el grupo de hosts sitea\_Hosts), el maestro de HA primero comprueba los recursos disponibles en el sitio A. Si no hay hosts disponibles en el sitio A, el maestro intenta reiniciar las máquinas virtuales en los hosts del sitio B.

Es posible que las máquinas virtuales se inicien en los hosts ESXi en el otro sitio si hay una restricción de recursos en el sitio local. Sin embargo, las reglas de afinidad de host y máquina virtual de DRS definidas corregirán si se viola alguna regla migrando las máquinas virtuales de nuevo a cualquier host ESXi sobreviviente en el sitio local. En los casos en que DRS se defina en manual, NetApp recomienda invocar DRS y aplicar las recomendaciones para corregir la ubicación de la máquina virtual.

No hay ningún cambio en el comportamiento de MetroCluster en este escenario y todos los almacenes de datos siguen estando intactos en sus sitios respectivos.

### Aislamiento de hosts ESXi

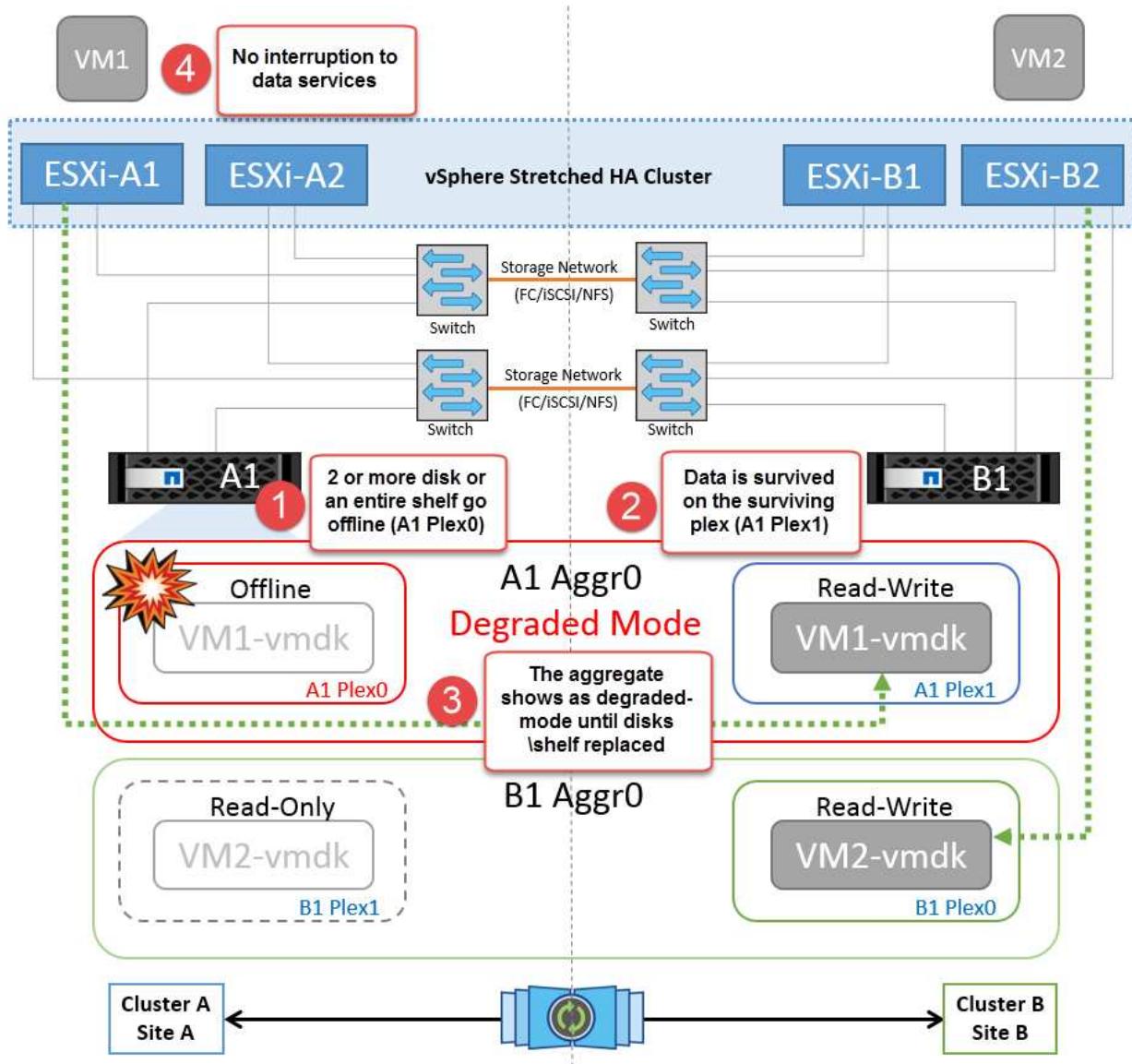


En esta situación, si la red de gestión del host ESXi está inactiva, el nodo principal del clúster de alta disponibilidad no recibirá ningún latido y, por lo tanto, este host se aísla en la red. Para determinar si ha fallado o solo está aislado, el nodo maestro comienza a supervisar el latido del almacén de datos. Si está presente, el nodo maestro declara que el host está aislado. Dependiendo de la respuesta de aislamiento configurada, el host puede optar por apagarse, apagar las máquinas virtuales o incluso dejar encendidas las máquinas virtuales. El intervalo predeterminado para la respuesta de aislamiento es de 30 segundos.

No hay ningún cambio en el comportamiento de MetroCluster en este escenario y todos los almacenes de datos siguen estando intactos en sus sitios respectivos.

### Fallo de la bandeja de discos

En esta situación, se produce un fallo de más de dos discos o una bandeja entera. Los datos se sirven desde el plex superviviente sin interrupción de los servicios de datos. El fallo del disco puede afectar a un plex local o remoto. Los agregados se mostrarán como degradado porque solo está activo un plex. Una vez sustituidos los discos que han fallado, los agregados afectados se sincronizarán automáticamente para volver a compilar los datos. Tras realizar la resincronización, los agregados volverán automáticamente al modo reflejado normal. Si falla más de dos discos dentro de un mismo grupo RAID, es necesario reconstruir el plex.

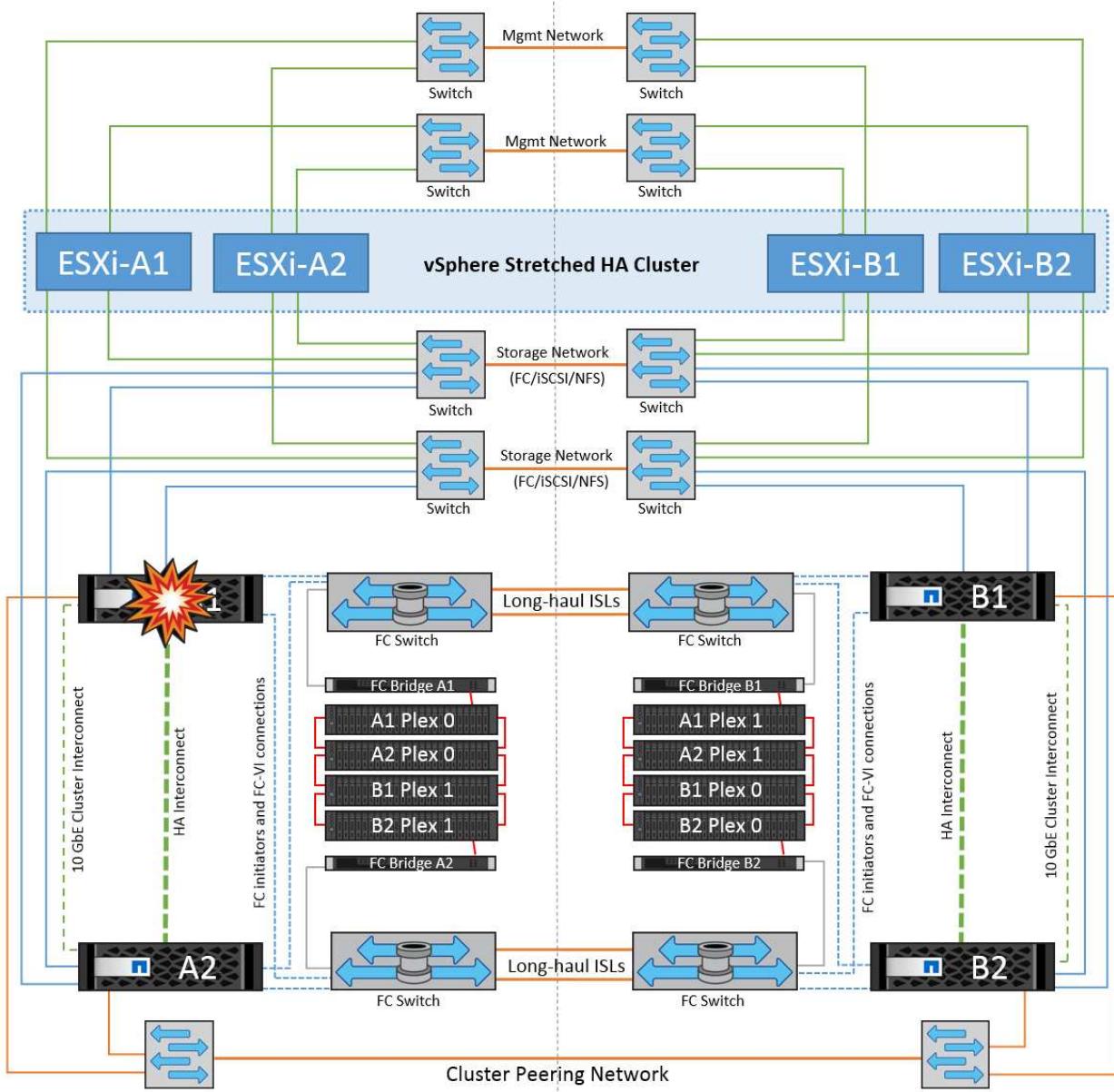


\*[NOTA]

- Durante este periodo, no se ven afectadas las operaciones de I/O de las máquinas virtuales, pero el rendimiento está degradado porque se accede a los datos desde la bandeja de discos remota a través de enlaces ISL.

### Fallo de una controladora de almacenamiento única

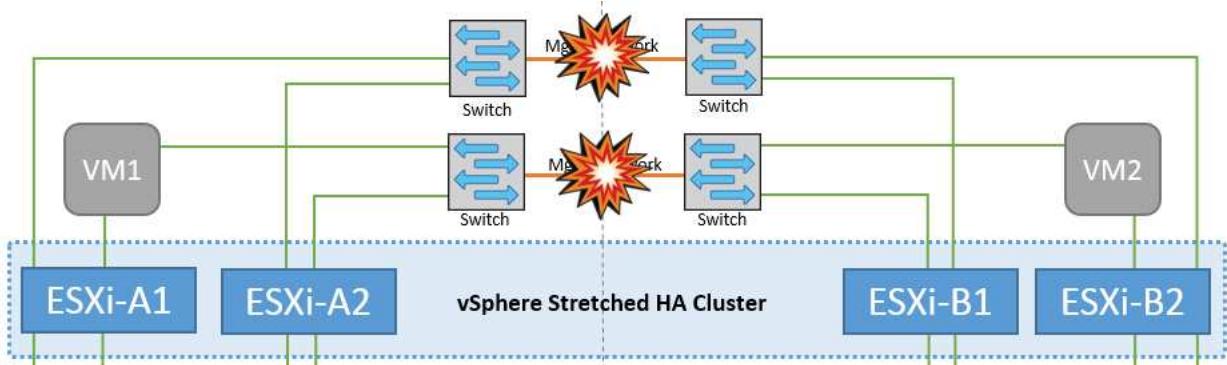
En este escenario, una de las dos controladoras de almacenamiento falla en un sitio. Dado que hay un par de alta disponibilidad en cada sitio, el fallo de un nodo de forma transparente activa automáticamente la conmutación al otro nodo. Por ejemplo, si falla el nodo A1, su almacenamiento y sus cargas de trabajo se transfieren automáticamente al nodo A2. Las máquinas virtuales no se verán afectadas porque todos los plexes permanecen disponibles. Los nodos del segundo sitio (B1 y B2) no se ven afectados. Además, vSphere HA no realizará ninguna acción porque el nodo principal del clúster seguirá recibiendo los latidos de red.



Si la conmutación al respaldo forma parte de un desastre gradual (el nodo A1 comuta al nodo A2) y hay un fallo posterior de A2 o el fallo completo del sitio A, el cambio tras un desastre puede ocurrir en el sitio B.

## Fallos de enlace de interinterruptor

### Fallo de enlace de interswitch en la red de gestión

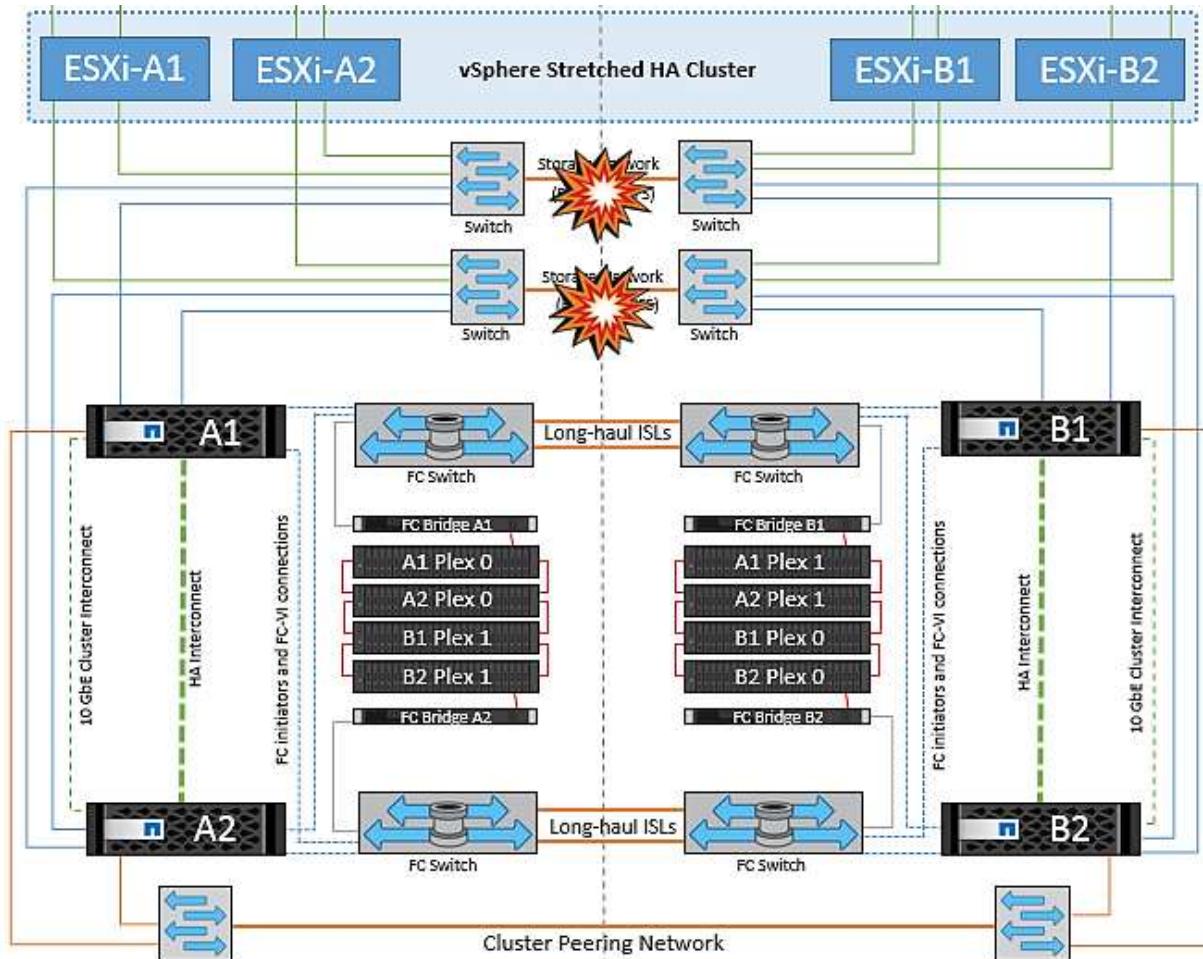


En este escenario, si los enlaces ISL en la red de gestión de host de interfaz de usuario producen un error, los hosts ESXi del sitio A no podrán comunicarse con los hosts ESXi del sitio B. Esto dará lugar a una partición de red porque los hosts ESXi de un sitio concreto no podrán enviar los latidos de red al nodo maestro del clúster HA. Como tal, habrá dos segmentos de red debido a la partición y habrá un nodo maestro en cada segmento que protegerá las VM de fallos de host dentro del sitio en particular.



Durante este período, las máquinas virtuales permanecen en ejecución y no hay cambios en el comportamiento de MetroCluster en este escenario. Todos los almacenes de datos siguen estando intactos en sus respectivos sitios.

#### Fallo de enlace interswitch en la red de almacenamiento

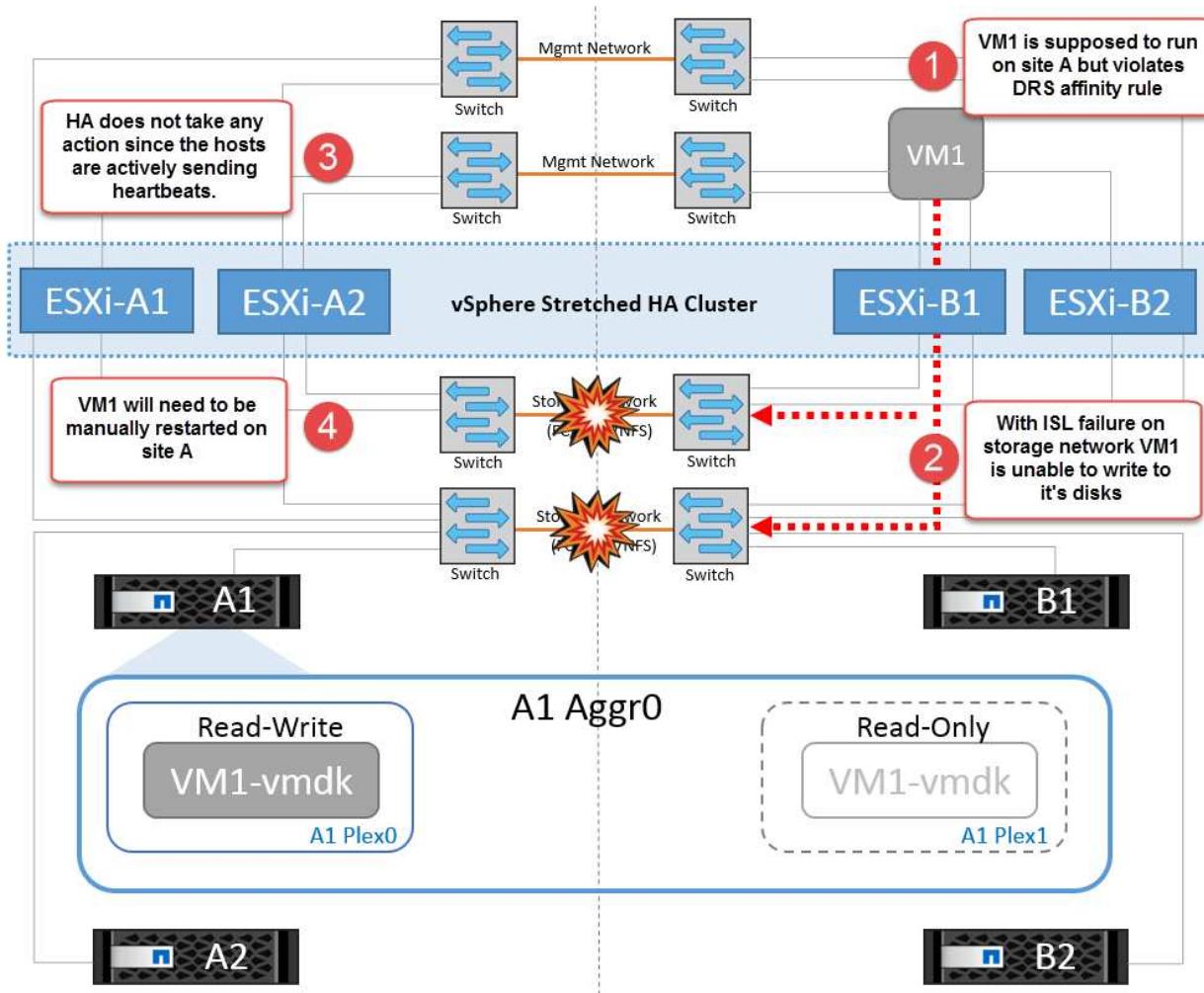


En este escenario, si los enlaces ISL en la red de almacenamiento de back-end fallan, los hosts del sitio A perderán acceso a los volúmenes de almacenamiento o las LUN del clúster B en el sitio B y viceversa. Las reglas de VMware DRS se definen de modo que la afinidad de sitios de almacenamiento host facilita que los equipos virtuales funcionen sin que el sitio se vea afectado.

Durante este período, las máquinas virtuales permanecen en ejecución en sus respectivos sitios y no hay cambios en el comportamiento de MetroCluster en este escenario. Todos los almacenes de datos siguen estando intactos en sus respectivos sitios.

Si por algún motivo se violó la regla de afinidad (por ejemplo, VM1, que se suponía que se ejecutaba desde la ubicación A donde sus discos residen en nodos del clúster local A, se está ejecutando en un host del sitio B), se accederá al disco de la máquina virtual de forma remota a través de enlaces ISL. Debido a un fallo de enlace ISL, VM1 ejecutándose en la instalación B no podría escribir en sus discos porque las rutas al volumen

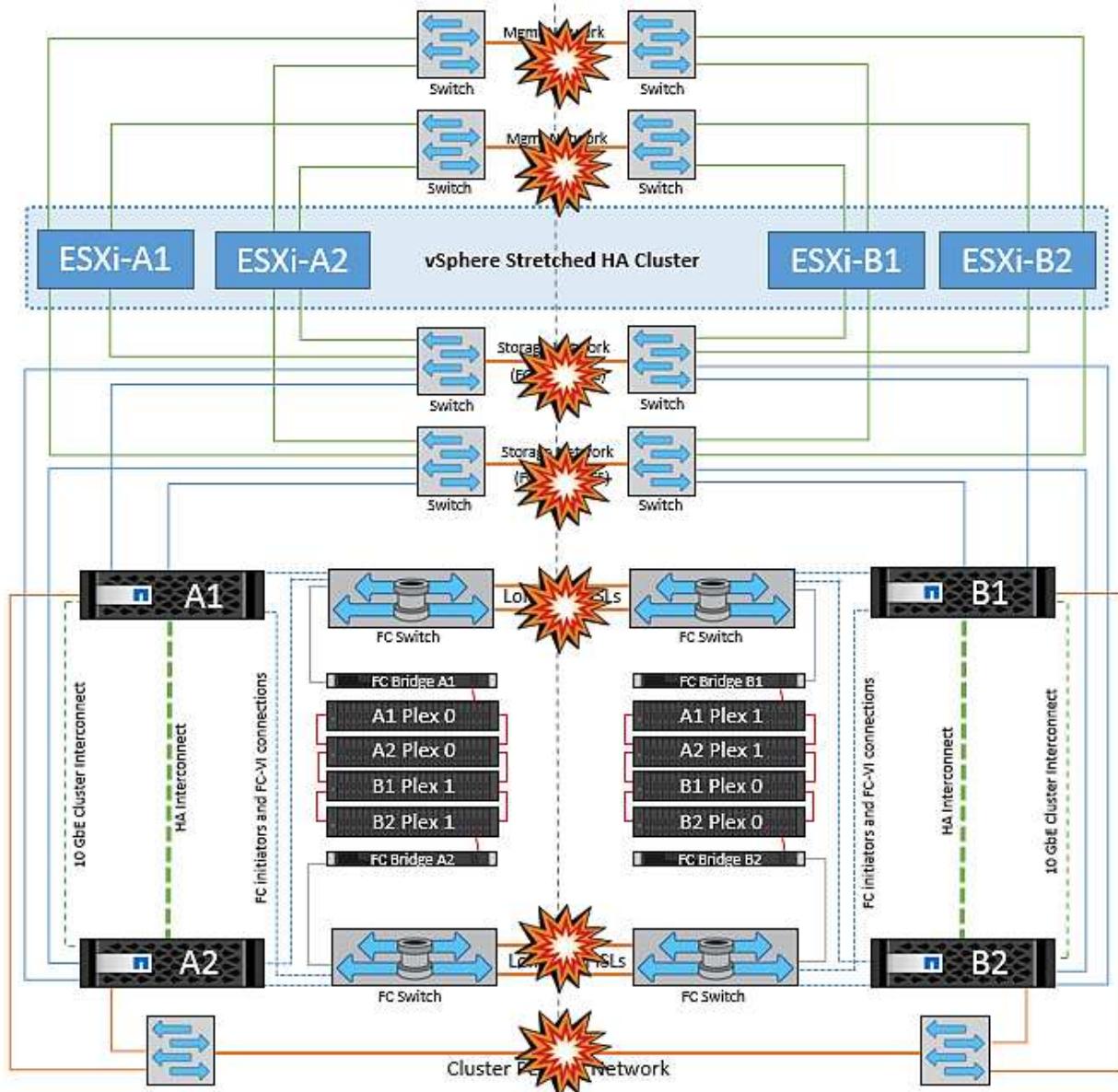
de almacenamiento están inactivas y la máquina virtual determinada está inactiva. En estos casos, VMware HA no realiza ninguna acción puesto que los hosts envían latidos de forma activa. Esas máquinas virtuales deben apagarse y encenderse manualmente en sus respectivos sitios. La siguiente figura ilustra una VM que viola una regla de afinidad DRS.



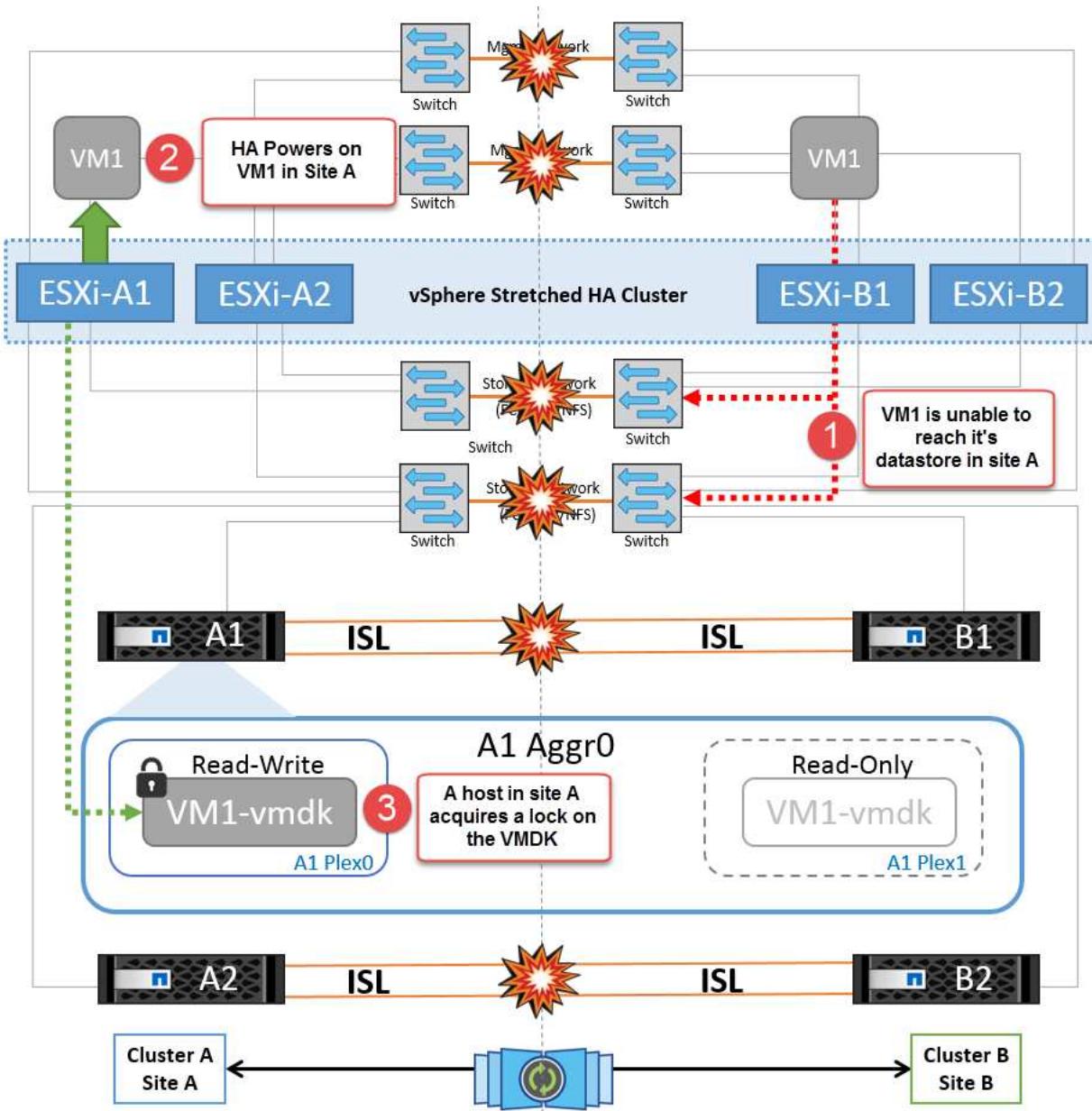
#### Todos los fallos de interswitch o la partición completa del centro de datos

En este escenario, todos los enlaces ISL entre los sitios están inactivos y los dos sitios están aislados uno de otro. Como se explicó en escenarios anteriores, como el fallo ISL en la red de gestión y en la red de almacenamiento, las máquinas virtuales no se ven afectadas por un fallo de ISL completo.

Una vez que los hosts ESXi hayan particionado entre sitios, el agente de alta disponibilidad de vSphere comprobará si hay latidos del almacén de datos y, en cada sitio, los hosts ESXi locales podrán actualizar los latidos del almacén de datos a sus respectivos volúmenes/LUN de lectura/escritura. Los hosts del sitio A asumirán que los otros hosts ESXi del sitio B han fallado porque no hay ningún latido de red/almacén de datos. VSphere HA en el sitio A intentará reiniciar las máquinas virtuales del sitio B, lo cual eventualmente fallará porque no se podrá acceder a los almacenes de datos del sitio B debido a un fallo del ISL del almacenamiento. Una situación similar se repite en el sitio B.



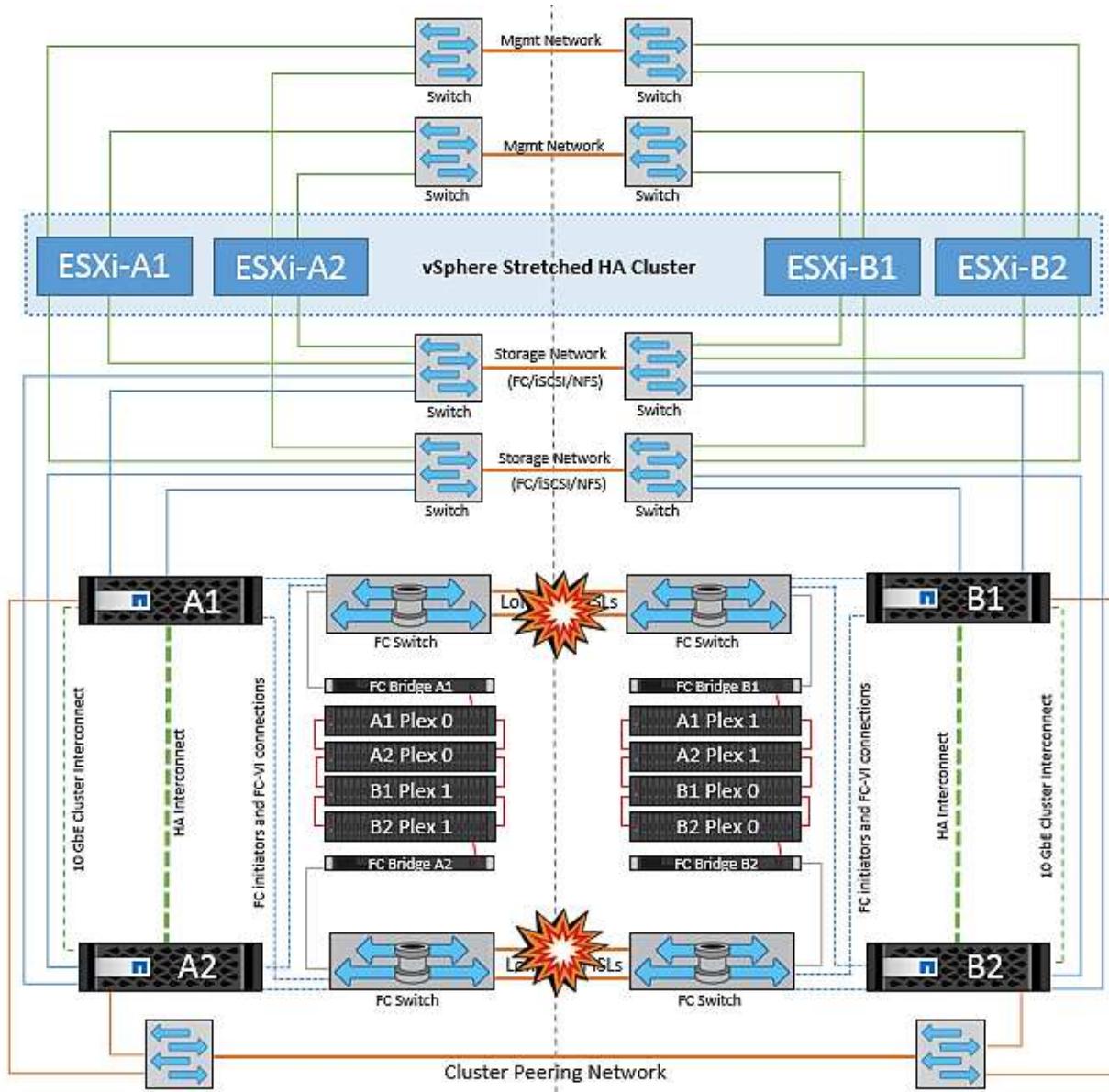
NetApp recomienda determinar si alguna máquina virtual ha infringido las reglas de DRS. Los equipos virtuales que se ejecuten desde un sitio remoto estarán inactivos ya que no podrán acceder al almacenamiento de datos y vSphere HA reiniciará esa máquina virtual en el sitio local. Una vez que los enlaces ISL vuelvan a estar en línea, la máquina virtual que se estaba ejecutando en el sitio remoto se desactivará, ya que no puede haber dos instancias de máquinas virtuales ejecutándose con las mismas direcciones MAC.



## Fallo de interswitch Link en ambas estructuras en NetApp MetroCluster

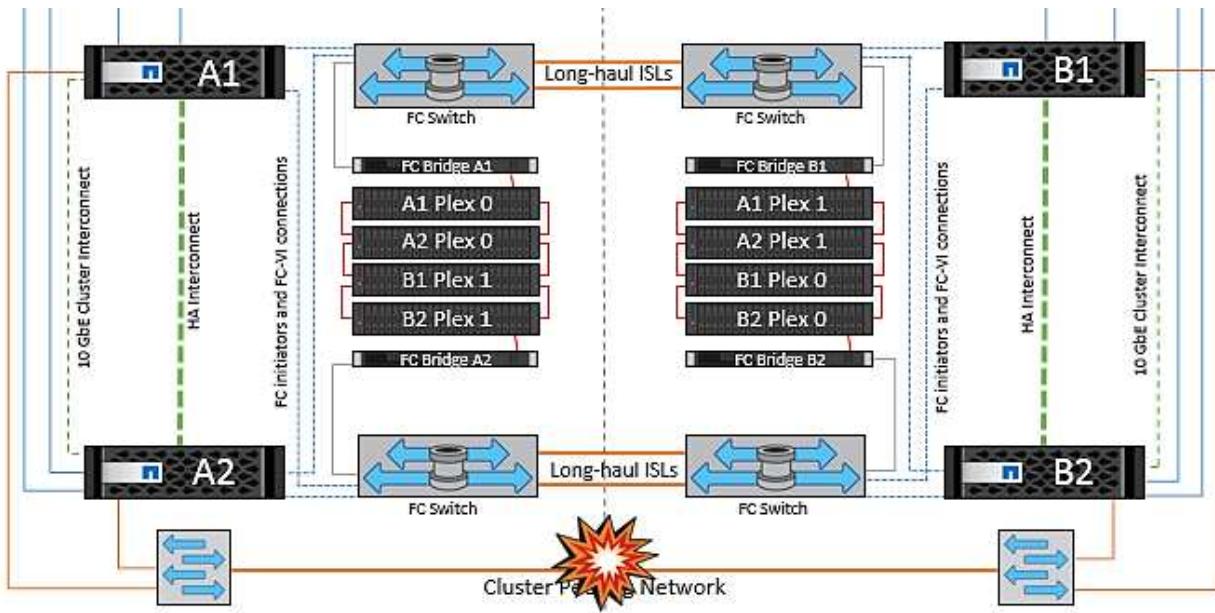
En un escenario en el que uno o varios ISL fallan, el tráfico continúa por los enlaces restantes. Si todos los ISL de ambas estructuras fallan, de modo que no hay ningún enlace entre los sitios para el almacenamiento y la replicación de NVRAM, cada controladora seguirá proporcionando sus datos locales. Cuando se restaura al menos un ISL, la resincronización de todos los complejos se realiza de forma automática.

Las escrituras que se produzcan después de que todos los ISL estén inactivos no se reflejarán en el otro sitio. Una commutación de sitios en caso de desastre, mientras la configuración se encuentra en este estado, por lo tanto, incurría en la pérdida de los datos que no se habían sincronizado. En este caso, se requiere intervención manual para la recuperación después del cambio. Si es probable que no haya ISL disponibles durante un largo período de tiempo, un administrador puede optar por cerrar todos los servicios de datos para evitar el riesgo de pérdida de datos si es necesario una commutación por desastre. La realización de esta acción debe evaluarse para la probabilidad de que se produzca un desastre que requiera la commutación del servicio antes de que esté disponible al menos un ISL. Como alternativa, si los ISL fallan en un escenario en cascada, un administrador podría activar una commutación de sitios planificada a uno de los sitios antes de que todos los enlaces hayan fallado.



#### Fallo de enlace de clúster con conexión entre iguales

En un supuesto de fallo de enlace de clústeres con conexión entre iguales, dado que los ISL de estructura aún están activos, los servicios de datos (lecturas y escrituras) continúan en ambos sitios en ambos complejos. No se puede propagar ningún cambio de configuración del clúster (por ejemplo, añadir una nueva SVM o aprovisionar un volumen o un LUN en una SVM existente) al otro sitio. Estos se mantienen en los volúmenes de metadatos de CRS locales y se propagan automáticamente al otro cluster tras la recuperación del enlace de cluster entre iguales. Si se necesita una comutación por error forzada antes de poder restaurar el enlace de clúster entre iguales, se volverán a reproducir automáticamente los cambios pendientes de configuración de clúster desde la copia replicada remota de los volúmenes de metadatos del sitio superviviente como parte del proceso de comutación por error.



#### Fallo completo del sitio

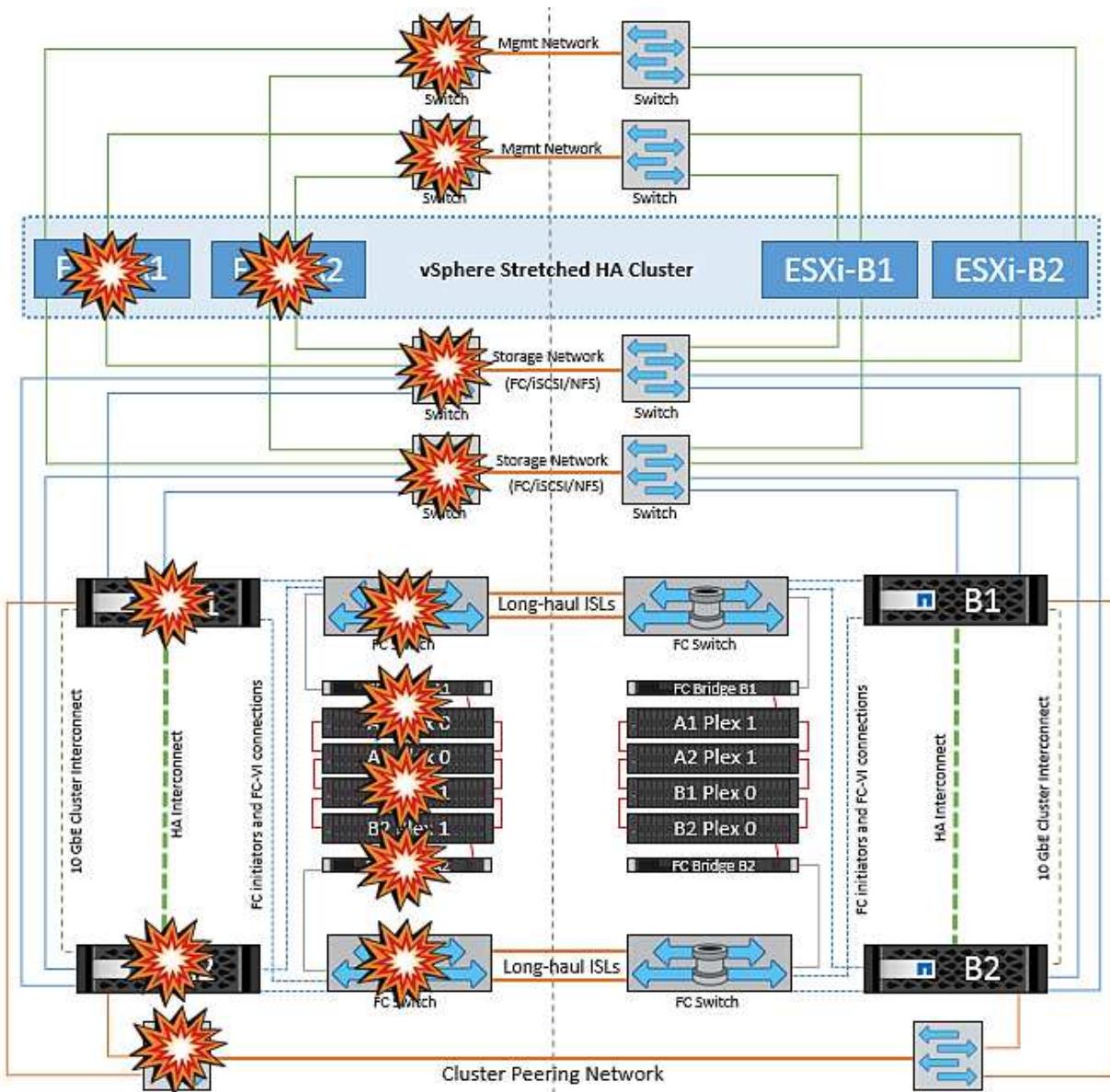
En un supuesto de fallo del sitio A completo, los hosts ESXi del sitio B no obtendrán el latido de red de los hosts ESXi del sitio A porque están inactivos. El maestro de alta disponibilidad en el sitio B verificará que los latidos del almacén de datos no están presentes, declarará que los hosts del sitio A han fallado e intentará reiniciar el sitio A de los equipos virtuales en el sitio B. Durante este periodo, el administrador de almacenamiento realiza una conmutación de sitios para reanudar los servicios de los nodos fallidos en el sitio superviviente. Esto restaura todos los servicios de almacenamiento del sitio A en el sitio B. Después de que el sitio haya volúmenes o LUN disponibles en el sitio B, el agente maestro de alta disponibilidad intentará reiniciar el sitio A, máquinas virtuales del sitio B.

Si el intento del agente maestro HA de vSphere de reiniciar una máquina virtual (lo que implica registrarla y encenderla) falla, el reinicio se vuelve a intentar después de un retraso. El retardo entre reinicios se puede configurar hasta un máximo de 30 minutos. VSphere HA intenta estos reinicios durante un número máximo de intentos (seis intentos de forma predeterminada).



El maestro de alta disponibilidad no inicia los intentos de reinicio hasta que el administrador de ubicación encuentra el almacenamiento adecuado, por lo que en caso de un fallo completo del sitio, sería después de que se haya realizado el cambio.

Si el sitio A se ha cambiado, un fallo posterior de uno de los nodos del sitio B superviviente se puede gestionar sin problemas mediante la conmutación al nodo superviviente. En este caso, solo un nodo realiza el trabajo de cuatro nodos. En este caso, la recuperación consistiría en realizar un retorno al nodo local. A continuación, cuando se restaura el sitio A, se realiza una operación de conmutación para restaurar el funcionamiento en estado constante de la configuración.



## Seguridad de los productos

### Herramientas de ONTAP para VMware vSphere

La ingeniería de software con Herramientas de ONTAP para VMware vSphere emplea las siguientes actividades de desarrollo seguro:

- **Modelado de amenazas.** el propósito del modelado de amenazas es descubrir defectos de seguridad en una característica, componente o producto al principio del ciclo de vida del desarrollo del software. Un modelo de amenaza es una representación estructurada de toda la información que afecta la seguridad de una aplicación. En esencia, es una visión de la aplicación y su entorno a través del objetivo de la seguridad.
- **Pruebas de seguridad de aplicaciones dinámicas (DAST).** esta tecnología está diseñada para detectar condiciones vulnerables en aplicaciones en su estado de funcionamiento. DAST prueba las interfaces HTTP y HTML expuestas de las aplicaciones web.
- **Moneda de código de terceros.** como parte del desarrollo de software con software de código abierto (OSS), debe tratar las vulnerabilidades de seguridad que pueden estar asociadas con cualquier OSS

incorporado en su producto. Esto es un esfuerzo continuo porque una nueva versión de OSS podría tener una vulnerabilidad recién descubierta reportada en cualquier momento.

- **Análisis de vulnerabilidades.** el propósito del análisis de vulnerabilidades es detectar vulnerabilidades de seguridad comunes y conocidas en los productos de NetApp antes de que se lancen a los clientes.
- \* Pruebas de penetración.\* la prueba de penetración es el proceso de evaluar un sistema, una aplicación web o una red para encontrar vulnerabilidades de seguridad que podrían ser explotadas por un atacante. Las pruebas de penetración (pruebas de Pen) en NetApp las realiza un grupo de empresas de terceros aprobadas y fiables. Su alcance de prueba incluye el lanzamiento de ataques contra una aplicación o software similar a intrusos hostiles o piratas informáticos que utilizan métodos o herramientas de explotación sofisticados.

## Funciones de seguridad de los productos

Las herramientas de ONTAP para VMware vSphere incluyen las siguientes funciones de seguridad en cada versión.

- **Banner de inicio de sesión.** SSH está desactivado de forma predeterminada y sólo permite inicios de sesión de una vez si está activado desde la consola de VM. Se muestra el siguiente banner de inicio de sesión una vez que el usuario introduce un nombre de usuario en la solicitud de inicio de sesión:

**ADVERTENCIA:** el acceso no autorizado a este sistema está prohibido y será procesado por ley. Al acceder a este sistema, acepta que sus acciones pueden supervisarse si se sospecha un uso no autorizado.

Una vez que el usuario complete el inicio de sesión a través del canal SSH, se muestra el siguiente texto:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Control de acceso basado en roles (RBAC).** dos tipos de controles RBAC están asociados con las herramientas ONTAP:
  - Privilegios nativos de vCenter Server
  - Privilegios específicos del plugin de vCenter. Para obtener más información, consulte "[este enlace](#)".
- **Canales de comunicaciones cifrados.** toda comunicación externa ocurre a través de HTTPS utilizando la versión 1.2 de TLS.
- **Exposición mínima del puerto.** sólo los puertos necesarios están abiertos en el firewall.

En la siguiente tabla se describen los detalles de los puertos abiertos.

| Puerto TCP v4/v6 # | Dirección | Función                              |
|--------------------|-----------|--------------------------------------|
| 8143               | entrante  | Conexiones HTTPS para la API de REST |
| 8043               | entrante  | Conexiones HTTPS                     |

| Puerto TCP v4/v6 # | Dirección                       | Función  |
|--------------------|---------------------------------|--|
| 9060               | entrante                        | Conexiones HTTPS<br>Se utiliza para conexiones SOAP a través de https<br>Este puerto se debe abrir para permitir que un cliente se conecte al servidor API de herramientas de ONTAP. |
| 22                 | entrante                        | SSH (deshabilitado de forma predeterminada)  |
| 9080               | entrante                        | Conexiones HTTPS - VP y SRA - conexiones internas sólo del bucle invertido   |
| 9083               | entrante                        | Conexiones HTTPS: VP y SRA<br>Se utiliza para conexiones SOAP a través de https  |
| 1162               | entrante                        | VP paquetes de captura SNMP  |
| 1527               | exclusivamente para uso interno | Puerto de base de datos Derby, sólo entre este equipo y él mismo, no se aceptan conexiones externas — sólo conexiones internas   |
| 443                | bidireccional                   | Se utiliza para las conexiones a clústeres de ONTAP  |

- **Compatibilidad con certificados firmados por la entidad de certificación (CA).** las herramientas de ONTAP para VMware vSphere admiten certificados firmados por CA. Vea esto ["artículo de base de conocimientos"](#) si quiere más información.
- **Registro de auditoría.** los paquetes de soporte se pueden descargar y son extremadamente detallados. Las herramientas de ONTAP registran toda la actividad de inicio de sesión y cierre de sesión de los usuarios en un archivo de registro independiente. Las llamadas de API VASA se registran en un registro de auditoría de VASA dedicado (cxf.log local).
- **Políticas de contraseña.** se siguen las siguientes directivas de contraseñas:
  - Las contraseñas no han iniciado sesión en ningún archivo de registro.
  - Las contraseñas no se comunican en texto sin formato.
  - Las contraseñas se configuran durante el propio proceso de instalación.
  - El historial de contraseñas es un parámetro configurable.
  - La antigüedad mínima de la contraseña se establece en 24 horas.
  - El proceso de finalización automática de los campos de contraseña está desactivado.
  - Las herramientas de ONTAP cifran toda la información de credenciales almacenada mediante el hash SHA256.

## Complemento de SnapCenter, VMware vSphere

La ingeniería de software del complemento SnapCenter de NetApp para VMware

vSphere utiliza las siguientes actividades de desarrollo seguro:

- **Modelado de amenazas.** el propósito del modelado de amenazas es descubrir defectos de seguridad en una característica, componente o producto al principio del ciclo de vida del desarrollo del software. Un modelo de amenaza es una representación estructurada de toda la información que afecta la seguridad de una aplicación. En esencia, es una visión de la aplicación y su entorno a través del objetivo de la seguridad.
- **Pruebas de seguridad de aplicaciones dinámicas (DAST).** Tecnologías diseñadas para detectar condiciones vulnerables en aplicaciones en estado en ejecución. DAST prueba las interfaces HTTP y HTML expuestas de las aplicaciones web.
- **Moneda de código de terceros.** como parte del desarrollo de software y el uso de software de código abierto (OSS), es importante abordar las vulnerabilidades de seguridad que pueden estar asociadas con OSS que se han incorporado a su producto. Se trata de un esfuerzo continuo, ya que la versión del componente OSS puede tener una vulnerabilidad recién descubierta reportada en cualquier momento.
- **Ánálisis de vulnerabilidades.** el propósito del análisis de vulnerabilidades es detectar vulnerabilidades de seguridad comunes y conocidas en los productos de NetApp antes de que se lancen a los clientes.
- \* Pruebas de penetración.\* la prueba de penetración es el proceso de evaluar un sistema, una aplicación web o una red para encontrar vulnerabilidades de seguridad que podrían ser explotadas por un atacante. Las pruebas de penetración (pruebas de Pen) en NetApp las realiza un grupo de empresas de terceros aprobadas y fiables. El alcance de su prueba incluye el lanzamiento de ataques contra una aplicación o software como intrusos hostiles o hackers que utilizan métodos o herramientas de explotación sofisticados.
- \* Actividad de respuesta a incidentes de seguridad de los productos.\* Las vulnerabilidades de seguridad se detectan tanto interna como externamente en la empresa y pueden representar un riesgo grave para la reputación de NetApp si no se tratan de manera puntual. Para facilitar este proceso, un equipo de respuesta a incidentes de seguridad de productos (PSIRT) informa y realiza un seguimiento de las vulnerabilidades.

## Funciones de seguridad de los productos

El plugin de SnapCenter de NetApp para VMware vSphere incluye las siguientes funciones de seguridad en cada versión:

- **Acceso restringido al shell.** SSH está desactivado de forma predeterminada, y sólo se permiten inicios de sesión una vez si están habilitados desde la consola de VM.
- **Advertencia de acceso en el banner de inicio de sesión.** se muestra el siguiente banner de inicio de sesión después de que el usuario introduzca un nombre de usuario en el indicador de inicio de sesión:

**ADVERTENCIA:** el acceso no autorizado a este sistema está prohibido y será procesado por ley. Al acceder a este sistema, acepta que sus acciones pueden supervisarse si se sospecha un uso no autorizado.

Una vez que el usuario completa el inicio de sesión a través del canal SSH, se muestra la siguiente salida:

```

Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

```

- **Control de acceso basado en roles (RBAC).** dos tipos de controles RBAC están asociados con las herramientas ONTAP:
  - Privilegios nativos de vCenter Server.
  - Privilegios específicos del complemento de VMware vCenter. Para obtener más información, consulte "[Control de acceso basado en roles \(RBAC\)](#)".
- **Canales de comunicaciones cifrados.** toda comunicación externa ocurre a través de HTTPS utilizando TLS.
- **Exposición mínima del puerto.** sólo los puertos necesarios están abiertos en el firewall.

En la siguiente tabla se proporcionan los detalles de los puertos abiertos.

| Número de puerto TCP v4/v6 | Función  |
|----------------------------|--|
| 8144                       | Conexiones HTTPS para la API de REST   |
| 8080                       | Conexiones HTTPS para interfaz gráfica de usuario de OVA   |
| 22                         | SSH (deshabilitado de forma predeterminada)  |
| 3306                       | MySQL (sólo conexiones internas; las conexiones externas están deshabilitadas de forma predeterminada) |
| 443                        | Nginx (servicios de protección de datos)   |

- **Compatibilidad con certificados firmados por entidad de certificación (CA).** el plugin de SnapCenter para VMware vSphere es compatible con la función de certificados firmados por CA. Consulte "["Cómo crear o importar un certificado SSL al plugin de SnapCenter para VMware vSphere \(SCV\)"](#)".
- **Políticas de contraseña.** las siguientes directivas de contraseñas están en vigor:
  - Las contraseñas no han iniciado sesión en ningún archivo de registro.
  - Las contraseñas no se comunican en texto sin formato.
  - Las contraseñas se configuran durante el propio proceso de instalación.
  - Toda la información de credenciales se almacena mediante el hash SHA256.
- **Imagen del sistema operativo base.** el producto se entrega con el SO base Debian para OVA con acceso restringido y acceso al shell desactivado. Esto reduce el espacio necesario para los ataques. Todos los sistemas operativos base de la versión SnapCenter se actualizan con los parches de seguridad más recientes disponibles para obtener la máxima cobertura de seguridad.

NetApp desarrolla funciones de software y parches de seguridad con respecto al dispositivo del plugin de SnapCenter para VMware vSphere y, a continuación, se los libera a los clientes como una plataforma de software integrada. Dado que estos dispositivos incluyen dependencias específicas de sistemas suboperativos

de Linux y nuestro software exclusivo, NetApp recomienda no realizar cambios en el sistema operativo de subsistema, ya que esto tiene un gran potencial para afectar al dispositivo de NetApp. Esto podría afectar a la capacidad de NetApp para dar soporte al dispositivo. NetApp recomienda probar e implementar nuestra última versión de código para los dispositivos, ya que se los publica para resolver cualquier problema relacionado con la seguridad.

## Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere

### Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere 9,13

La guía de refuerzo de la seguridad para herramientas de ONTAP para VMware vSphere proporciona un conjunto completo de instrucciones para configurar los ajustes más seguros.

Estas guías se aplican tanto a las aplicaciones como al sistema operativo «guest» del propio dispositivo.

### Verificación de la integridad de las herramientas de ONTAP para los paquetes de instalación de VMware vSphere 9,13

Existen dos métodos disponibles para que los clientes verifiquen la integridad de sus paquetes de instalación de herramientas de ONTAP.

1. Verificando las sumas de comprobación
2. Verificando la firma

Las sumas de comprobación se proporcionan en las páginas de descarga de los paquetes de instalación de OTV. Los usuarios deben verificar las sumas de comprobación de los paquetes descargados con la suma de comprobación proporcionada en la página de descarga.

### Verificación de la firma del OVA de herramientas de ONTAP

El paquete de instalación de vApp se entrega en forma de tarball. Este tarball contiene certificados intermedios y raíz para el dispositivo virtual junto con un archivo README y un paquete OVA. El archivo README guía a los usuarios sobre cómo verificar la integridad del paquete OVA vApp.

Los clientes también deben cargar el certificado raíz e intermedio proporcionado en la versión 7.0U3E de vCenter y versiones posteriores. Para versiones de vCenter entre 7.0.1 y 7.0.U3E, la funcionalidad de verificación del certificado no es compatible con VMware. Los clientes no deberán cargar ningún certificado para las versiones de vCenter 6.x.

#### Cargar el certificado raíz de confianza en vCenter

1. Inicie sesión con VMware vSphere Client en vCenter Server.
2. Especifique el nombre de usuario y la contraseña de [administrator@vsphere.local](mailto:administrator@vsphere.local) u otro miembro del grupo Administradores de inicio de sesión único de vCenter. Si especificó un dominio diferente durante la instalación, inicie sesión como [administrator@mydomain](mailto:administrator@mydomain).
3. Desplácese hasta la IU de gestión de certificados: a. En el menú Inicio, seleccione Administración. b. En Certificados, haga clic en Gestión de certificados.

4. Si el sistema le solicita, introduzca las credenciales de vCenter Server.
5. En Certificados raíz de confianza, haga clic en Agregar.
6. Haga clic en Examinar y seleccione la ubicación del archivo .pem del certificado (OTV\_OVA\_INTER\_ROOT\_CERT\_CHAIN.pem).
7. Haga clic en Añadir. El certificado se agrega a la tienda.

Consulte ["Agregue un certificado raíz de confianza al almacén de certificados"](#) si quiere más información. Al implementar una vApp (mediante el archivo OVA), la firma digital del paquete vApp se puede verificar en la página 'Detalles de revisión'. Si el paquete vApp descargado es genuino, la columna 'Publisher' muestra 'Trusted Certificate' (Certificado de confianza) (como en la siguiente captura de pantalla).

### Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

**4 Review details**

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Review details

Verify the template details.

|               |   |
|---------------|---|
| Publisher     | Entrust Code Signing CA - OVCS2 (Trusted certificate)   |
| Product       | Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere  |
| Version       | See appliance for version   |
| Vendor        | NetApp Inc.   |
| Description   | Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere for netapp storage systems. For more information or support please visit <a href="https://www.netapp.com/">https://www.netapp.com/</a> |
| Download size | 2.2 GB  |
| Size on disk  | 3.9 GB (thin provisioned)   |
|               | 53.0 GB (thick provisioned)   |

Activate
Go to System

CANCEL
BACK
NEXT

### Verificación de la firma de las herramientas de ONTAP ISO y SRA tar.gz

NetApp comparte su certificado de firma de código con los clientes en la página de descarga del producto, junto con los archivos zip del producto para OTV-iso y sra.tgz.

Del certificado de firma de código, los usuarios pueden extraer la clave pública de la siguiente manera:

```
#> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-key name>
```

A continuación, se debe utilizar la clave pública para verificar la firma para iso y el zip del producto tgz como se muestra a continuación:

```
#> openssl dgst -sha256 -verify <public-key> -signature <signature-file> <binary-name>
```

Ejemplo:

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-vsphere-9.12-upgrade.iso
Verified OK => response
```

## Puertos y protocolos para las herramientas de ONTAP 9.13

A continuación se muestran los puertos y protocolos necesarios que permiten la comunicación entre herramientas de ONTAP para el servidor VMware vSphere y otras entidades como sistemas de almacenamiento gestionados, servidores y otros componentes.

### Puertos de entrada y salida necesarios para OTV

Observe la siguiente tabla en la que se enumeran los puertos de entrada y salida necesarios para el correcto funcionamiento de las herramientas de ONTAP. Es importante asegurarse de que solo los puertos mencionados en la tabla estén abiertos para las conexiones de máquinas remotas, mientras que todos los demás puertos deben estar bloqueados para las conexiones de máquinas remotas. Esto ayudará a garantizar la seguridad de su sistema.

En la siguiente tabla se describen los detalles de los puertos abiertos.

| Puerto TCP v4/v6 # | Dirección | Función  |
|--------------------|-----------|--|
| 8143               | entrante  | Conexiones HTTPS para la API de REST   |
| 8043               | entrante  | Conexiones HTTPS   |
| 9060               | entrante  | Conexiones HTTPS<br>Se utiliza para conexiones SOAP a través de HTTPS<br>Este puerto se debe abrir para permitir que un cliente se conecte al servidor API de herramientas de ONTAP. |
| 22                 | entrante  | SSH (deshabilitado de forma predeterminada)  |

| Puerto TCP v4/v6 # | Dirección                       | Función   |
|--------------------|---------------------------------|---|
| 9080               | entrante                        | Conexiones HTTPS - VP y SRA - conexiones internas sólo del bucle invertido  |
| 9083               | entrante                        | Conexiones HTTPS - VP y SRA<br>Se utiliza para conexiones SOAP a través de HTTPS  |
| 1162               | entrante                        | VP paquetes de captura SNMP   |
| 8443               | entrante                        | Complemento remoto  |
| 1527               | exclusivamente para uso interno | Puerto de base de datos Derby, solo entre este equipo y él mismo, conexiones externas no aceptadas — Solo conexiones internas |
| 8150               | exclusivamente para uso interno | El servicio de integridad de log se ejecuta en el puerto  |
| 443                | bidireccional                   | Se utiliza para las conexiones a clústeres de ONTAP   |

### Control del acceso remoto a la base de datos Derby

Los administradores pueden acceder a la base de datos derby con los siguientes comandos. Se puede acceder a él a través de las herramientas de ONTAP VM local, así como a un servidor remoto con los siguientes pasos:

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

#### Ejemplo:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=' ;
ij> show tables;
TABLE_SCHEM | TABLE_NAME | REMARKS
-----
SYS | SYSALIASES
SYS | SYSCHECKS
SYS | SYSCOLPERMS
SYS | SYSCOLUMNNS
SYS | SYSCONGLOMERATES
SYS | SYSCONSTRAINTS
SYS | SYSDEPENDS
SYS | SYSFILES
SYS | SYSFOREIGNKEYS
SYS | SYSKEYS
SYS | SYSPERMS
```

### Herramientas de ONTAP para puntos de acceso de VMware vSphere 9,13 (usuarios)

La instalación de ONTAP Tools para VMware vSphere crea y utiliza tres tipos de usuarios:

1. Usuario del sistema: La cuenta de usuario raíz

2. Usuario de la aplicación: El usuario administrador, el usuario de mantenimiento y las cuentas de usuario de base de datos
3. Usuario de soporte: La cuenta de usuario diag

## 1. Usuario del sistema

El usuario System(root) se crea mediante la instalación de herramientas de ONTAP en el sistema operativo subyacente (Debian).

- Un usuario predeterminado del sistema “root” se crea en Debian mediante la instalación de herramientas de ONTAP. Su valor predeterminado está desactivado y se puede activar de forma ad hoc a través de la consola 'antigua'.

## 2. Usuario de la aplicación

El usuario de la aplicación se denomina usuario local en las herramientas de ONTAP. Se trata de usuarios creados en la aplicación de herramientas de ONTAP. La siguiente tabla muestra los tipos de usuarios de la aplicación:

| Usuario                  | Descripción  |
|--------------------------|--|
| Usuario administrador    | Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. La contraseña caducará en 90 días y se espera que los usuarios cambien la misma.                                |
| Usuario de mantenimiento | Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. Se trata de un usuario de mantenimiento y se crea para ejecutar las operaciones de la consola de mantenimiento. |
| Usuario de base de datos | Se crea durante la instalación de las herramientas de ONTAP y el usuario proporciona las credenciales al implementar las herramientas de ONTAP. Los usuarios tienen la opción de cambiar la 'contraseña' en 'consola antigua'. La contraseña caducará en 90 días y se espera que los usuarios cambien la misma.                                |

## 3. Usuario de apoyo (usuario diag)

Durante la instalación de las herramientas de ONTAP, se crea un usuario de soporte. Este usuario se puede utilizar para acceder a las herramientas de ONTAP en caso de cualquier problema o interrupción en el servidor y para recopilar registros. De forma predeterminada, este usuario está desactivado, pero se puede activar de forma específica a través de la consola 'antigua'. Es importante tener en cuenta que este usuario se desactivará automáticamente después de un período de tiempo determinado.

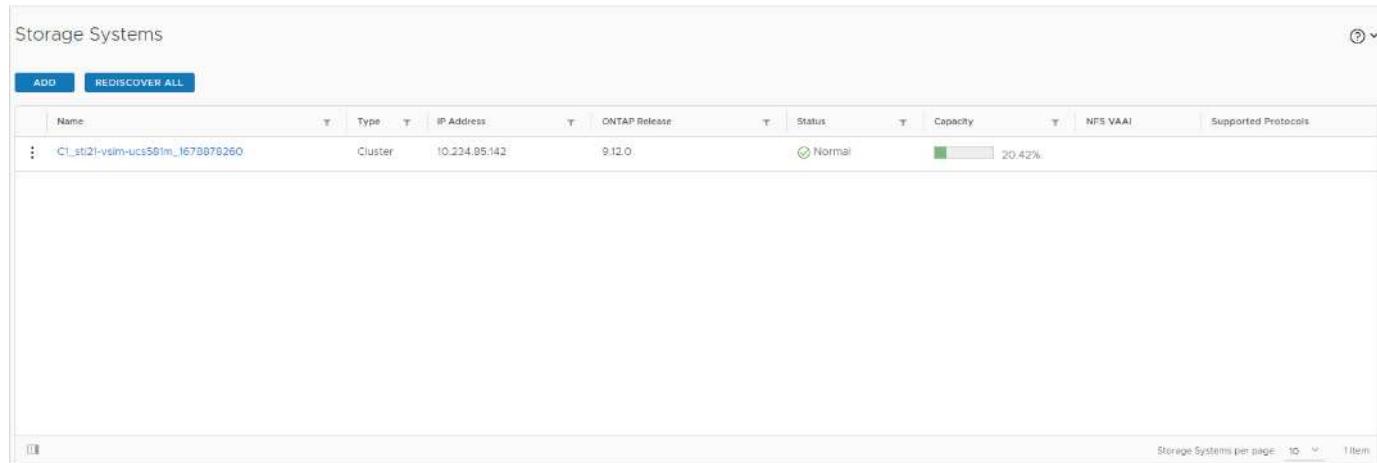
## ONTAP TOOLS 9,13 TLS mutuo (autenticación basada en certificados)

Las versiones 9,7 y posteriores de ONTAP admiten la comunicación TLS mutua. A partir de ONTAP Tools para VMware y vSphere 9,12, el TLS mutuo se utiliza para la comunicación con clústeres recién añadidos (según la versión de ONTAP).

## ONTAP

Para todos los sistemas de almacenamiento añadidos anteriormente: Durante una actualización, todos los sistemas de almacenamiento añadidos se volverán de confianza automáticamente y se configurarán los mecanismos de autenticación basados en certificados.

Como en la siguiente captura de pantalla, la página de configuración del clúster mostrará el estado de TLS mutuo (autenticación basada en certificado), configurado para cada clúster.



The screenshot shows a table titled 'Storage Systems' with a single row of data. The columns are: Name, Type, IP Address, ONTAP Release, Status, Capacity, NFS VAAI, and Supported Protocols. The data row is: C1\_sti21-vsim-ucs501m\_1670078260, Cluster, 10.224.85.142, 9.12.0, Normal, 20.42%, and a green bar indicating 20.42% capacity. There are buttons for 'ADD' and 'REDISCOVER ALL' at the top left, and a dropdown menu at the top right. At the bottom right, there are buttons for 'Storage Systems per page' (set to 10) and '1 item'.

| Name                             | Type    | IP Address    | ONTAP Release | Status | Capacity | NFS VAAI | Supported Protocols |
|----------------------------------|---------|---------------|---------------|--------|----------|----------|---------------------|
| C1_sti21-vsim-ucs501m_1670078260 | Cluster | 10.224.85.142 | 9.12.0        | Normal | 20.42%   |          |                     |

## Cluster Add

Durante el flujo de trabajo de agregación de clústeres, si el clúster que se agrega admite MTLS, MTLS se configurará de forma predeterminada. El usuario no necesita realizar ninguna configuración para esto. La siguiente captura de pantalla muestra la pantalla presentada al usuario durante la adición del clúster.

## Add Storage System

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

vCenter server

10.224.58.52



Name or IP address:

Username:

Password:

Port:

443

Advanced options 

ONTAP Cluster



Automatically fetch



Manually upload

Certificate:

CANCEL

ADD

## Add Storage System

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

vCenter server

10.224.58.52

Name or IP address:

10.234.85.142

Username:

admin

Password:

.....

Port:

443

[Advanced options >](#)

CANCEL

ADD

## Add Storage System

- ① Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server:

10.234.58.52 ▾

### Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES

CANCEL

ADD

## Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Hide certificate](#)

### Certificate Information

This certificate identifies the 10.234.85.142 host.

#### Issued By

**Name (CN or DN):** C1\_sti21-vsim-ucs581m\_1678878260

#### Issued To

**Name (CN or DN):** C1\_sti21-vsim-ucs581m\_1678878260

#### Validity

**Issued On:** 03/15/2023 11:16:06

**Expires On:** 03/14/2024 11:16:06

### Fingerprint Information

**SHA-1 Fingerprint:** 2C:38:E3:5C:4B:F3:5D:3F:39:C8:CE:4A:82:C1:A6:EE:34:53:A0:F3

**SHA-256 Fingerprint:** 05:0F:FE:CD:B0:C6:FC:6F:EB:8A:FC:86:F7:E3:EF:D4:8D:CA:02:92:9B:E1:A4:70:84:52:F8:76:98:64:FA:23

Do you want to trust this certificate?

[NO](#)

[YES](#)

## Edición de clúster

Durante la operación de edición del clúster, existen dos situaciones:

- Si el certificado ONTAP caduca, el usuario tendrá que obtener el nuevo certificado y cargarlo.
- Si el certificado OTV caduca, el usuario puede regenerarlo marcando la casilla de verificación.
  - *Generar un nuevo certificado de cliente para ONTAP.*

## Modify Storage System

Settings      Provisioning Options

IP address or hostname:

Port:

Username:

Password:

Upload Certificate  
(Optional)  [BROWSE](#)

Skip monitoring of this storage system

Generate a new client certificate for ONTAP

[CANCEL](#)

[OK](#)



## Certificado HTTPS de ONTAP TOOLS 9,13

De manera predeterminada, las herramientas de ONTAP utilizan un certificado autofirmado que se crea automáticamente durante la instalación para proteger el acceso HTTPS a la interfaz de usuario web. Las herramientas de ONTAP ofrecen las siguientes funciones:

1. Regenerar certificado HTTPS

Durante la instalación de las herramientas de ONTAP, se instala un certificado de CA HTTPS y el certificado se almacena en el almacén de claves. El usuario tiene la opción de regenerar el certificado HTTPS a través de la consola de mantenimiento.

Se puede acceder a las opciones anteriores en la consola *maint* navegando a '*Configuración de la aplicación*' → '*Volver a generar certificados*'.

## Banner de inicio de sesión de ONTAP tools 9,13

Se muestra el siguiente banner de inicio de sesión después de que el usuario introduce un nombre de usuario en la pantalla de inicio de sesión. Tenga en cuenta que SSH está deshabilitado de forma predeterminada y solo permite inicios de sesión de una vez cuando se habilita desde la consola de VM.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

Una vez que el usuario completa el inicio de sesión a través del canal SSH, se muestra el siguiente texto:

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

## Tiempo de espera de inactividad para las herramientas de ONTAP 9,13

Para evitar el acceso no autorizado, se configura un tiempo de espera de inactividad, que cierra automáticamente la sesión de los usuarios inactivos durante un cierto período mientras se utilizan los recursos autorizados. Esto garantiza que solo los usuarios autorizados puedan acceder a los recursos y ayuda a mantener la seguridad.

- De forma predeterminada, las sesiones de vSphere Client se cierran tras 120 minutos de tiempo inactivo, lo cual requiere que el usuario inicie sesión nuevamente para reanudarse usando el cliente. Puede cambiar el valor de tiempo de espera editando el archivo `webclient.properties`. Puede configurar el tiempo de espera de vSphere Client "[Configure el valor de tiempo de espera del cliente de vSphere](#)"
- Las herramientas de ONTAP tienen un tiempo de cierre de sesión de la cli web de 30 minutos.

## Número máximo de solicitudes simultáneas por usuario (protección de seguridad de red/ataque DOS) herramientas de ONTAP para VMware vSphere 9,13

Por defecto, el Núm. Máximo de solicitudes simultáneas por usuario es 48. El usuario root en las herramientas de ONTAP puede cambiar este valor en función de los requisitos de su entorno. **Este valor no debe establecerse en un valor muy alto, ya**

## que proporciona un mecanismo contra ataques de denegación de servicio (DoS).

Los usuarios pueden modificar el número máximo de sesiones simultáneas y otros parámetros admitidos en el archivo `/opt/netapp/vscserver/etc/dosfilterParams.json`.

Podemos configurar el filtro con los siguientes parámetros:

- **`delayMs`**: El retraso en milisegundos dado a todas las solicitudes por encima del límite de tasa antes de que sean consideradas. Dar -1 para rechazar la solicitud.
- **`throttleMs`**: Cuánto tiempo esperar el semáforo de forma asíncrona.
- **`maxRequestMs`**: Cuánto tiempo se debe permitir que se ejecute esta solicitud.
- **`ipWhitelist`**: Una lista separada por comas de direcciones IP que no se limitará la tasa. (Pueden ser IP de vCenter, ESXi y SRA)
- **`maxRequestsPerSec`**: El número máximo de solicitudes de una conexión por segundo.

### Valores predeterminados en el archivo `dosfilterParams`:

```
{"delayMs": "-1",
"throttleMs": "1800000",
"maxRequestMs": "300000",
"ipWhitelist": "10.224.58.52",
"maxRequestsPerSec": "48"}
```

## Configuración del Protocolo de hora de red (NTP) para las herramientas ONTAP 9,13

A veces, pueden producirse problemas de seguridad debido a discrepancias en las configuraciones de tiempo de red. Es importante asegurarse de que todos los dispositivos dentro de una red tengan una configuración de tiempo precisa para evitar tales problemas.

### Dispositivo virtual

Puede configurar los servidores NTP desde la consola de mantenimiento del dispositivo virtual. Los usuarios pueden agregar los detalles del servidor NTP en *Configuración del sistema* ⇒ *Agregar nuevo servidor NTP* opción

De forma predeterminada, el servicio para NTP es `ntpd`. Este es un servicio heredado y no funciona bien para máquinas virtuales en ciertos casos.

### Debian

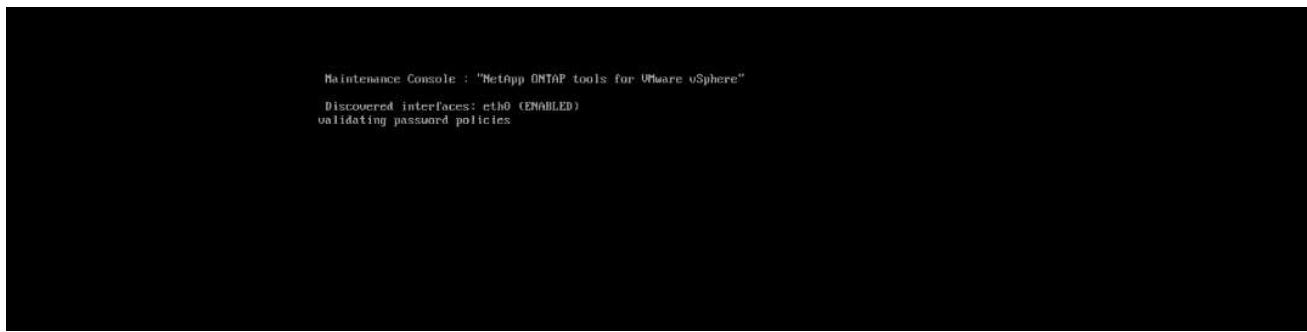
En Debian, el usuario puede acceder al archivo `/etc/ntp.conf` para obtener los detalles del servidor `ntp`.

## Políticas de contraseñas para las herramientas de ONTAP 9,13

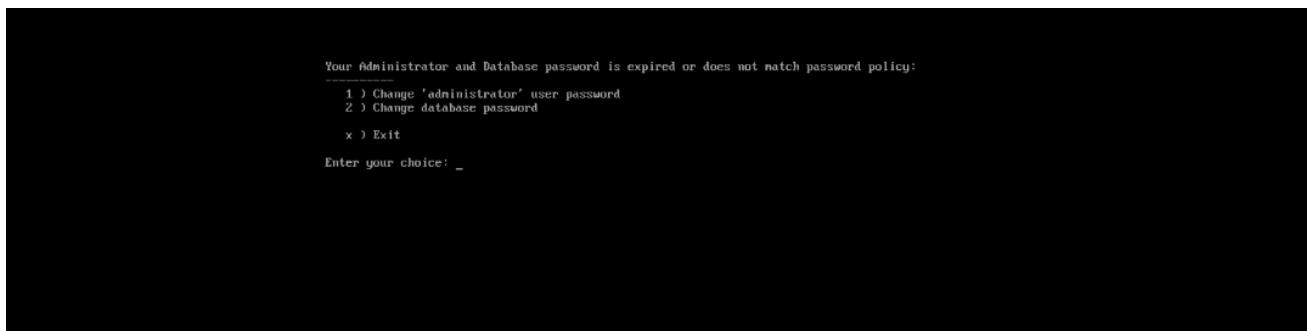
Los usuarios que implementen las herramientas de ONTAP por primera vez o que actualicen a la versión 9,12 o posterior deberán seguir la política de contraseñas seguras

tanto para el administrador como para los usuarios de la base de datos. Durante el proceso de implementación, se solicitará a los nuevos usuarios que introduzcan sus contraseñas. Para los usuarios de brownfield que actualicen a la versión 9,12 o posterior, la opción de seguir la política de contraseñas seguras estará disponible en la consola de mantenimiento.

- Una vez que el usuario inicia sesión en la consola de mantenimiento, las contraseñas se verificarán con respecto al conjunto de reglas complejo y, si se detecta que no se siguen, se solicitará al usuario que restablezca la misma.
- La validez predeterminada de la contraseña es de 90 días y después de 75 días el usuario comenzará a recibir la notificación para cambiar la contraseña.
- Es necesario establecer una nueva contraseña en cada ciclo, el sistema no tomará la última contraseña como nueva contraseña.
- Cada vez que un usuario inicia sesión en la consola de mantenimiento, comprobará las políticas de contraseñas como las siguientes capturas de pantalla antes de cargar el menú principal:



- Si no sigue la política de contraseñas o su configuración de actualización desde las herramientas de ONTAP 9,11 o anteriores. A continuación, el usuario verá la siguiente pantalla para restablecer la contraseña:



- Si el usuario intenta establecer una contraseña débil o da la última contraseña de nuevo, el usuario verá el siguiente error:

Changing password for administrator.

User: administrator  
Enter new password:  
Retype new password:

Password doesn't matches the password policy.  
For security reasons, it is recommended to use a password that is of eight to thirty characters and  
contains a minimum of one upper, one lower, one digit, and one special character.

Enter new password:  
Retype new password:  
Check if new decoder works ?  
New decoder worked successfully  
00-02-23 13:36:53 Your new password must be different

Error updating sra credential file

Press ENTER to continue...

## Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

**LEYENDA DE DERECHOS LIMITADOS:** el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.