VMware Site Recovery Manager con ONTAP

Enterprise applications

NetApp
February 10, 2026

Tabla de contenidos

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 ASA A, 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 conmutación 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 conmutación 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:

- conmutación por error de prueba 8x veces más rápida*
- limpieza y reprotección 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'.

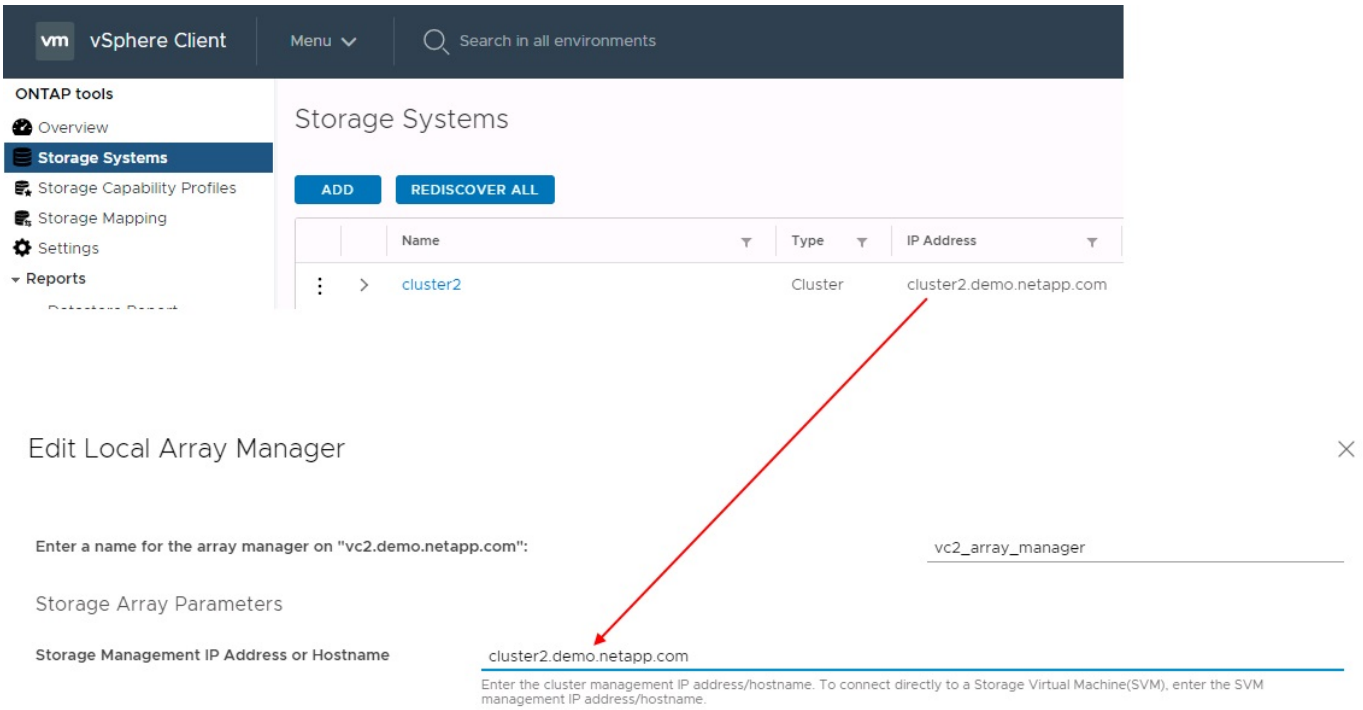
```
snap autodelete modify -volume -commitment try
```

- 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 conmutación 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.



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 site de producción en otro site 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 reprotección 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.

Conmutación 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 reprotección 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 reprotección de nuevo.

La ejecución de la reprotección 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).

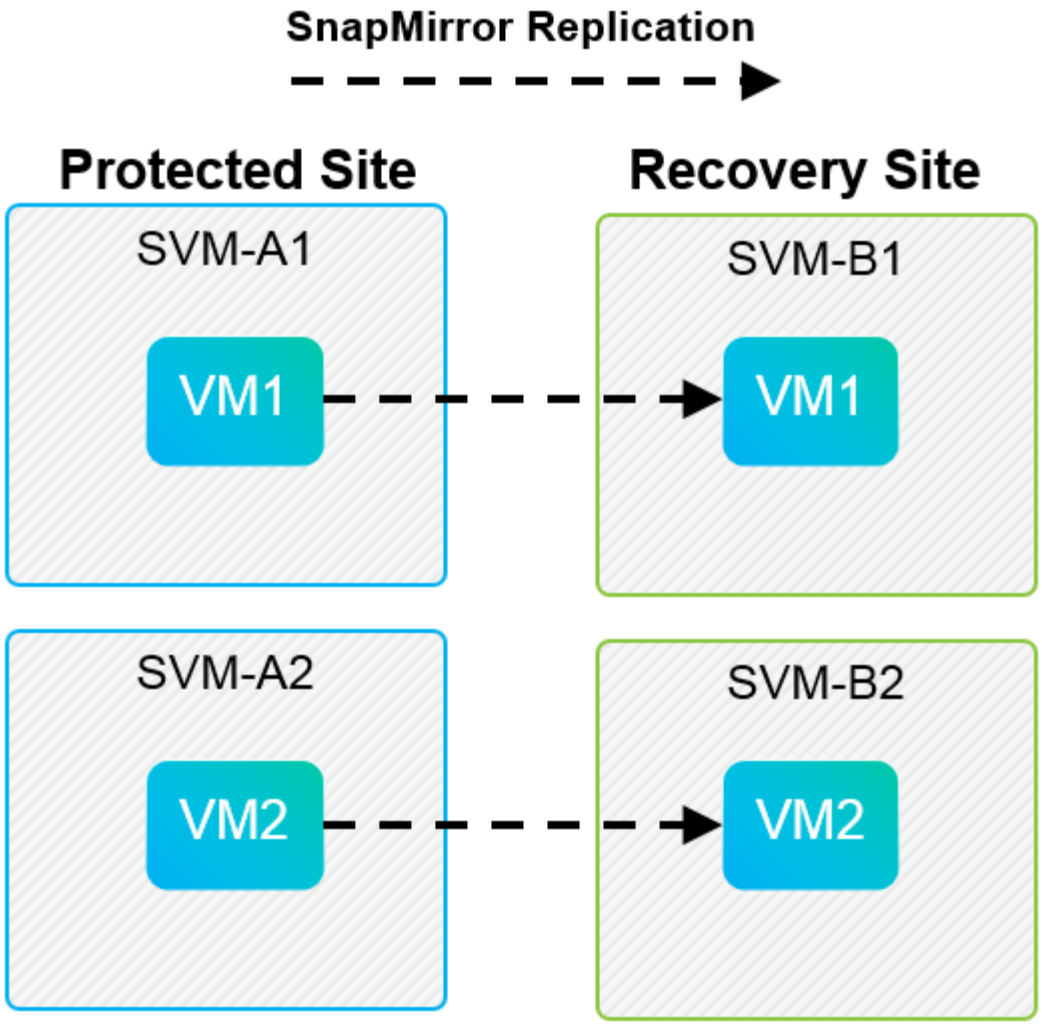
Una sola máquina virtual no puede poseer datos, Virtual Machine Disk (VMDK) o RDM, en más de una cabina de VLSR por los siguientes motivos:

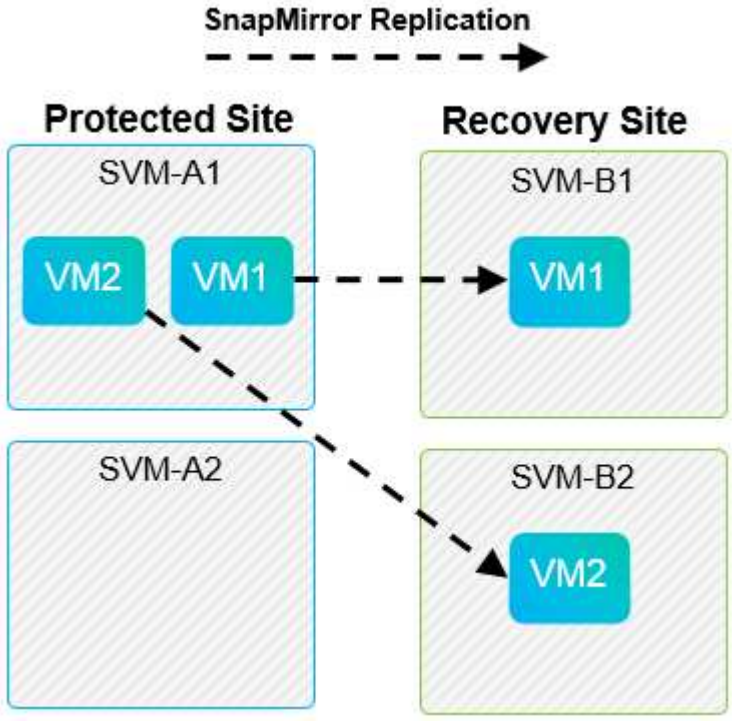
- VLSR solo ve la SVM, no una controladora física individual.
- Una SVM puede controlar los LUN y los volúmenes que abarcan varios nodos en un clúster.

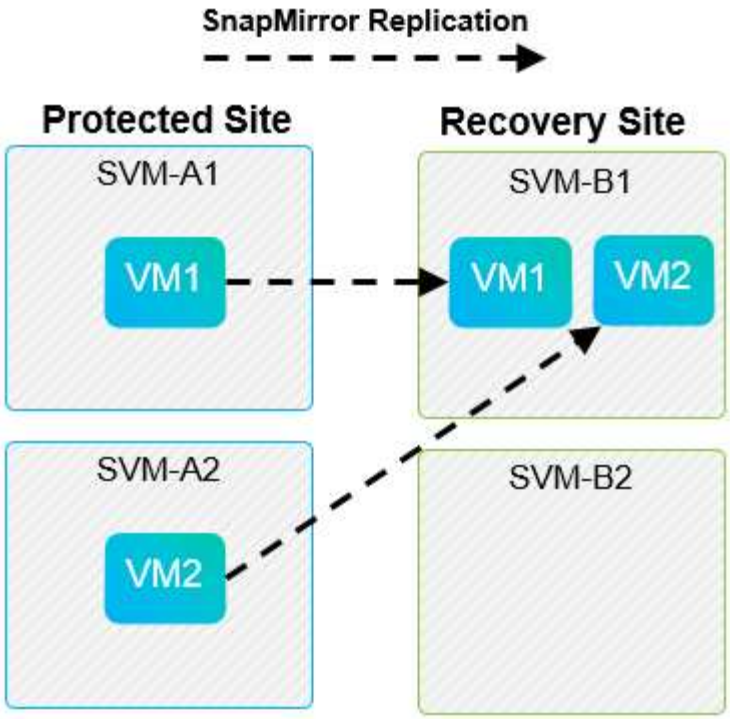
Mejor práctica
Para determinar la compatibilidad, tenga presente esta regla: Para proteger una máquina virtual con el VLSR y el SRA de NetApp, todas las partes de la máquina virtual deben existir en un solo SVM. Esta regla se aplica tanto al sitio protegido como al sitio de recuperación.

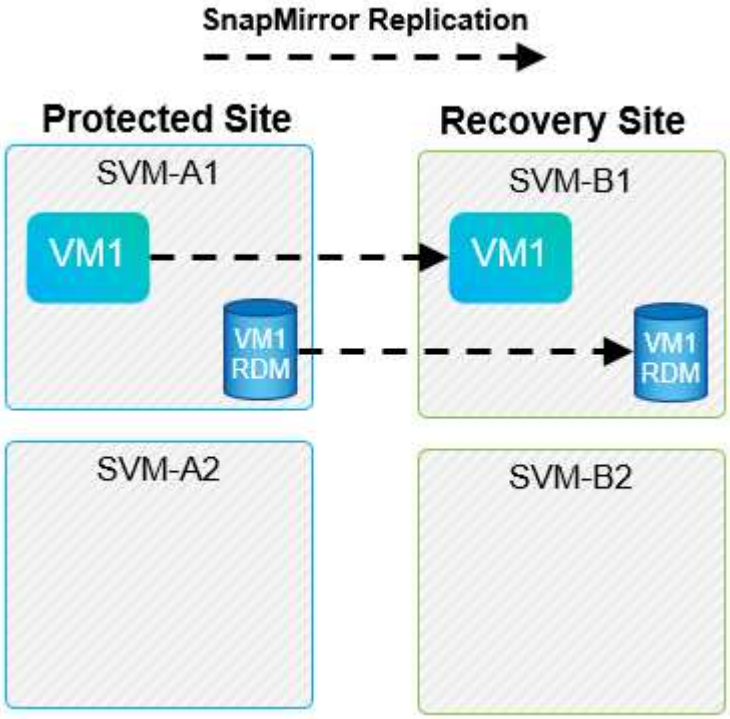
Distribuciones de SnapMirror compatibles

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
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2





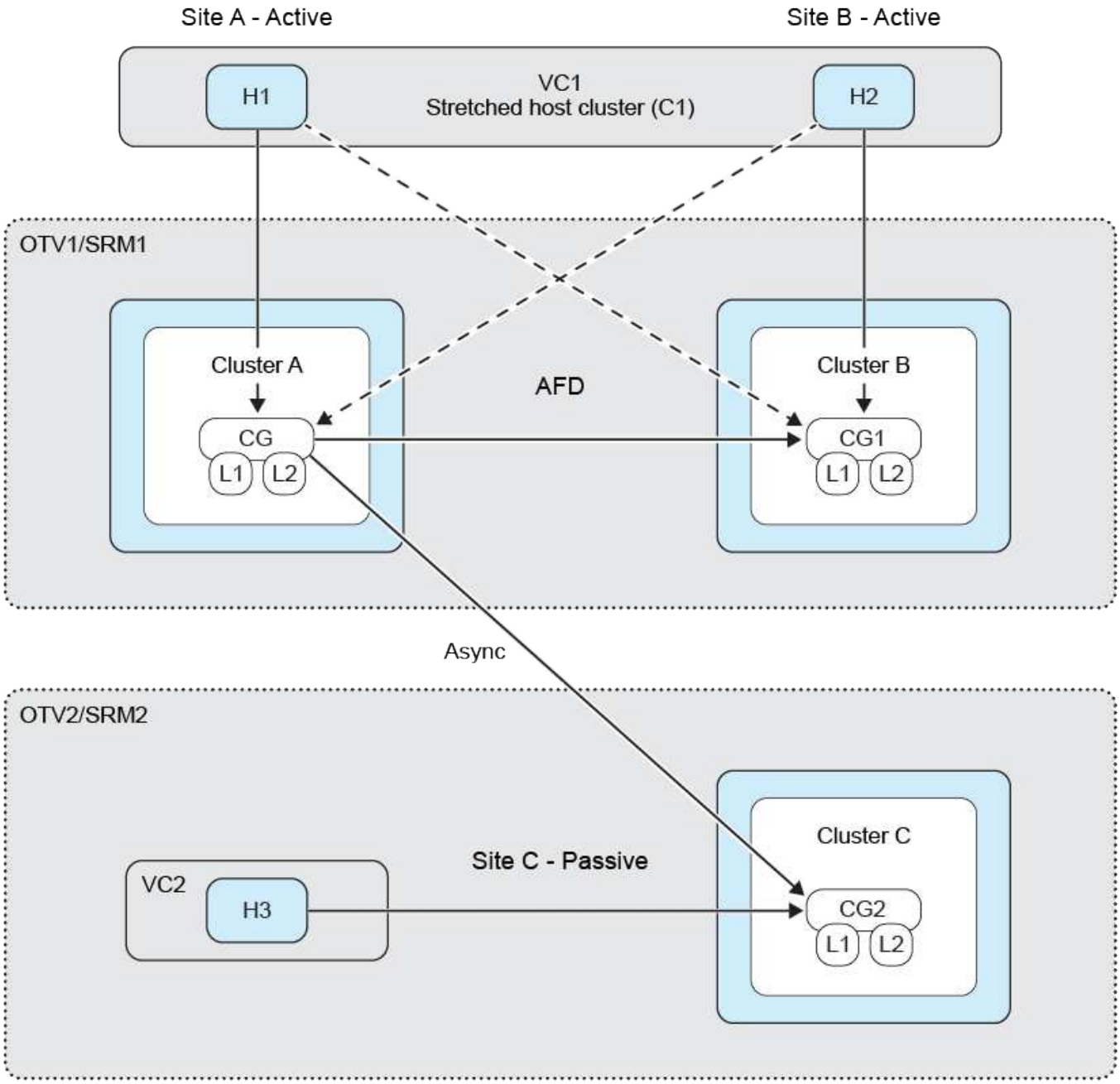
Compatibilidad de VMFS con sincronización activa de SnapMirror

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 conmutación 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.

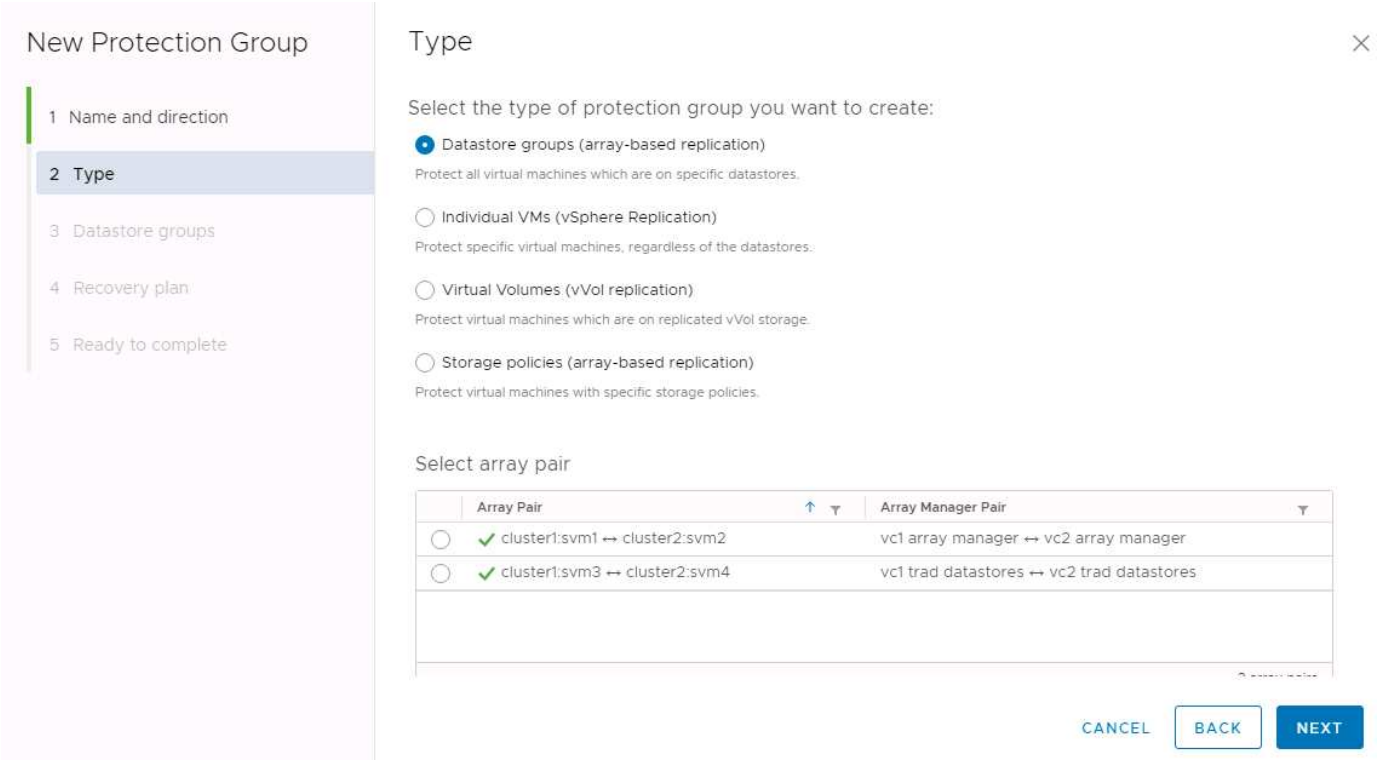
Algunos ejemplos podrían ser tener sitios en Berlín y Hamburgo protegidos por SMas y una tercera réplica del sitio utilizando SnapMirror asincrónico y protegido por VLSR. Otro ejemplo podría ser proteger sitios en Nueva York y Nueva Jersey utilizando SMas, con un tercer sitio en Chicago.



Diseños compatibles de Array Manager

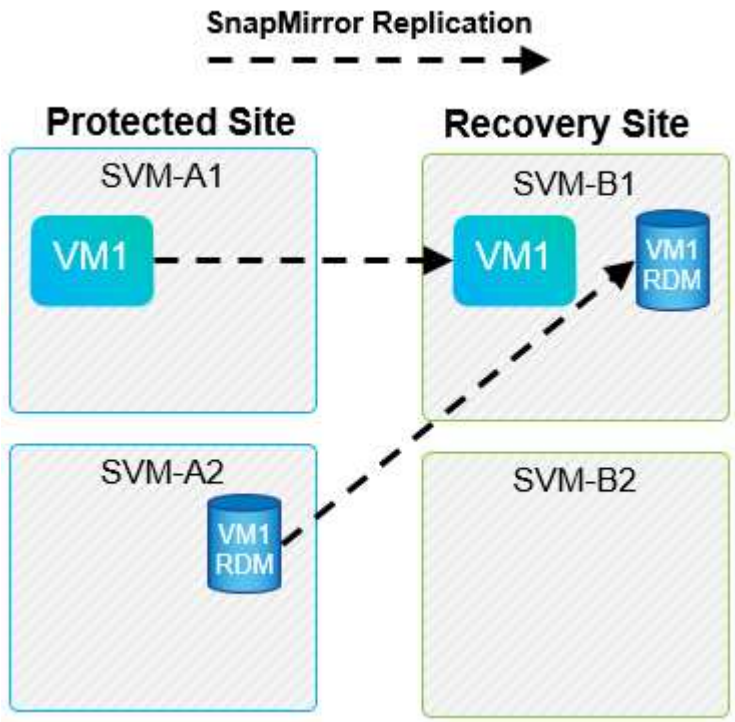
Cuando se utiliza la replicación basada en cabinas (ABR) en VLSR, los grupos de protección se aíslan en un solo par de cabina, como se muestra en la siguiente captura de pantalla. En este caso, `SVM1` y `SVM2` se relacionan con `SVM3` y `SVM4` en el sitio de recuperación. Sin embargo, es posible seleccionar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

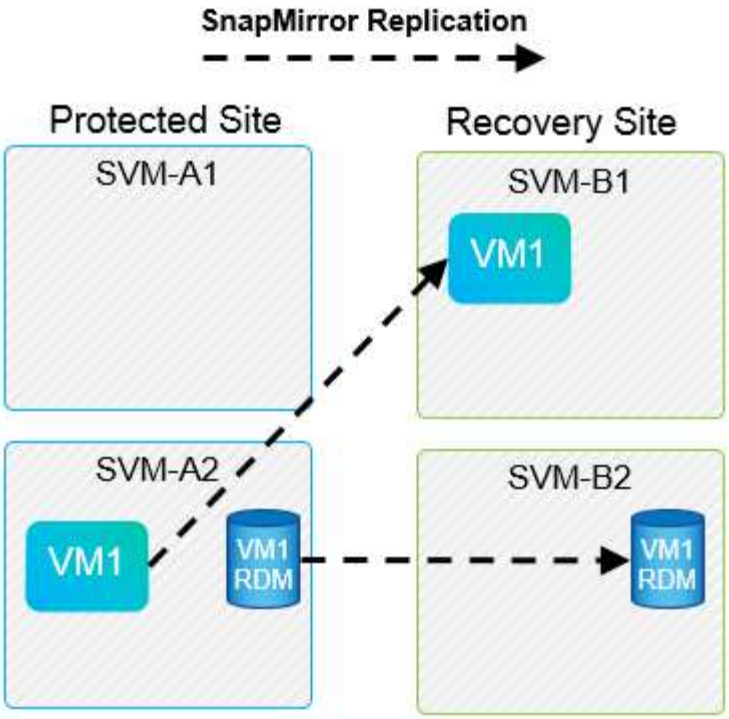
dos parejas de cabinas al crear un grupo de protección.



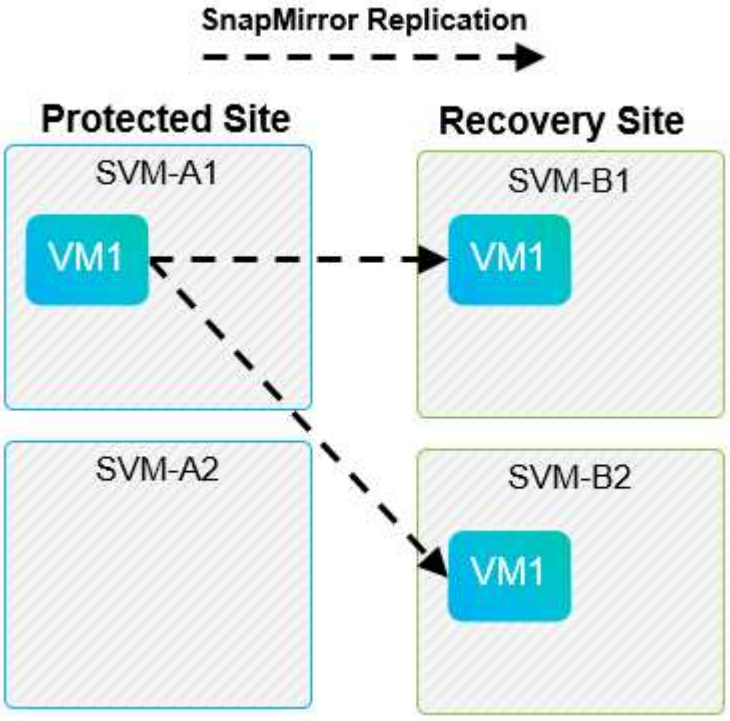
Diseños no admitidos

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.





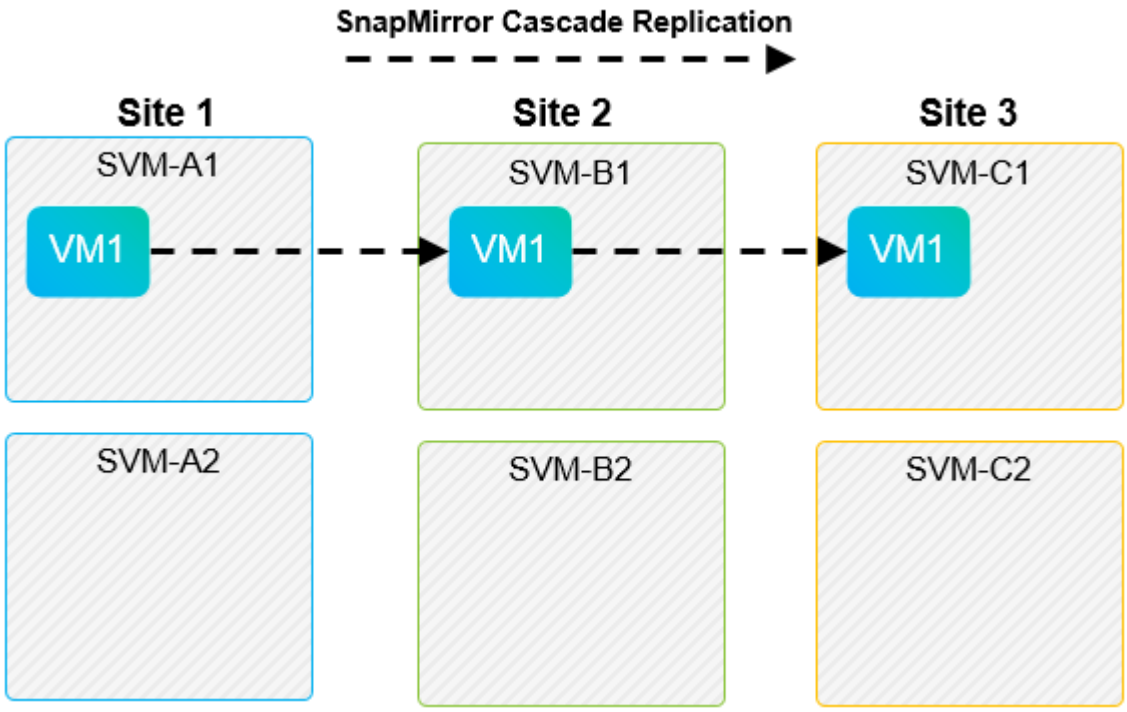
Toda relación de replicación en la que se replica un volumen individual de NetApp desde una SVM de origen a varios destinos en la misma SVM o en distintas SVM se denomina «fan-out» de SnapMirror. VLSR no es compatible con fan-out. En el ejemplo que se muestra en la siguiente figura, `VM1` no se puede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

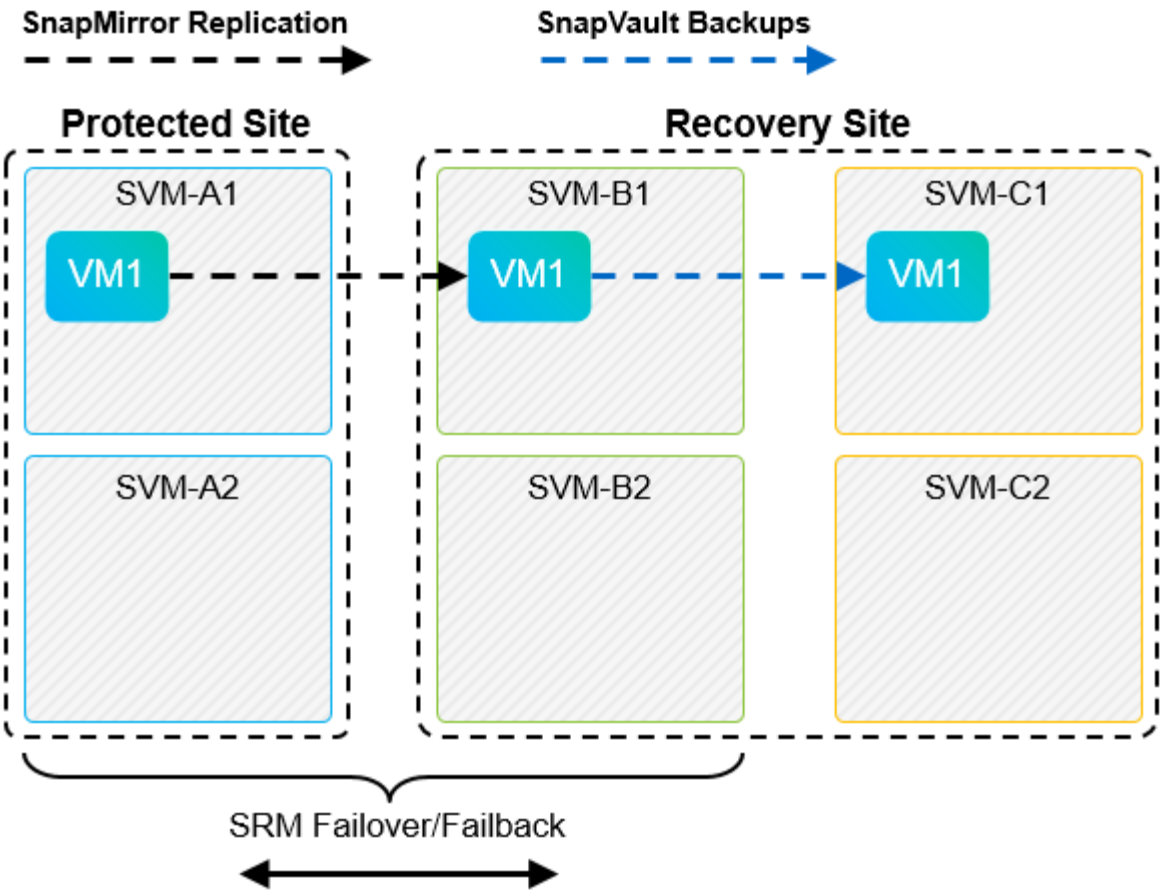
no reconfigura automáticamente la relación de SnapVault para usar el volumen de destino de SnapMirror como origen del almacén cuando se produce la conmutación por error del VLSR o la reversión de la replicación.

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."

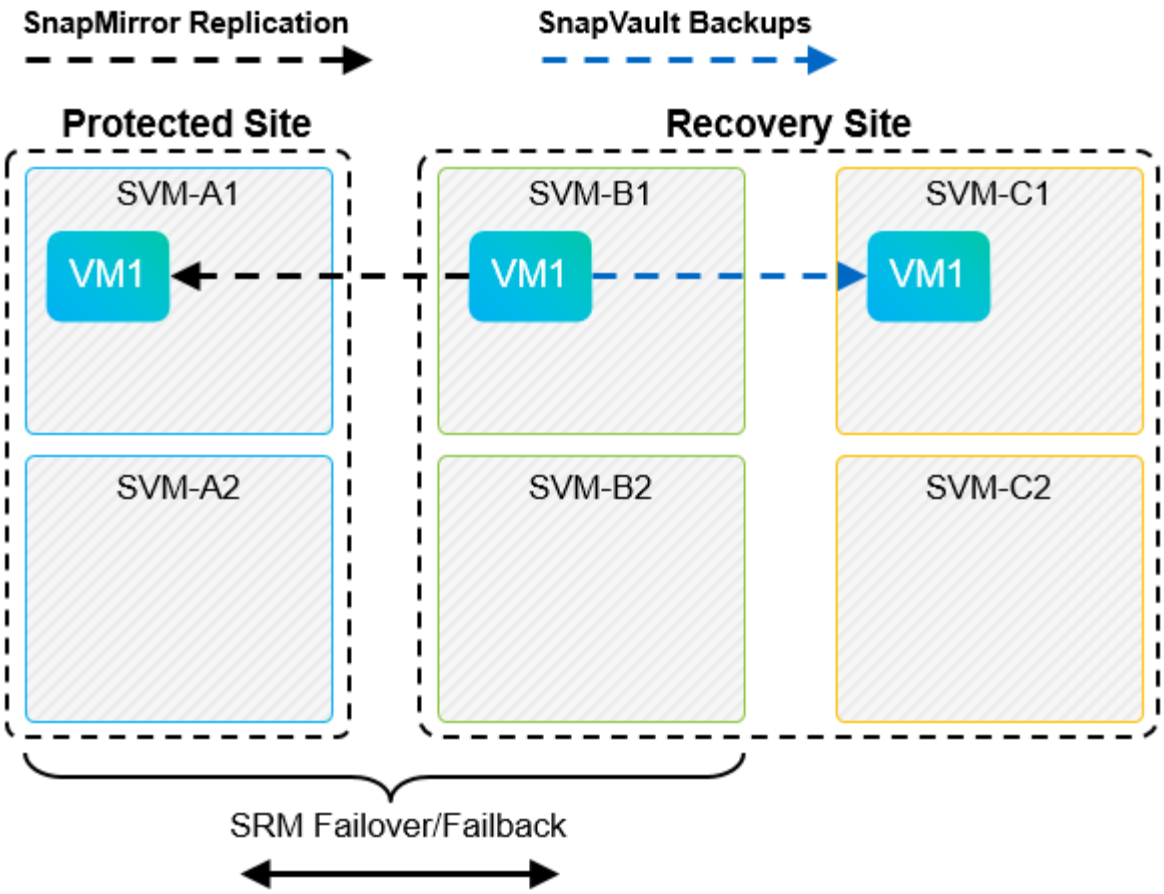
Mejor práctica
Si se emplean SnapVault y VLSR en el mismo entorno, NetApp recomienda utilizar una configuración en cascada de SnapMirror a SnapVault en la que los backups de SnapVault se realizan normalmente desde el destino de SnapMirror en el centro de recuperación ante desastres. En caso de desastre, 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 conmutación 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 conmutación 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 iSCI), 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 almacenes de datos conectados a FC y almacenes 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 almacenes 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. PapreFailoverReplicationGroup: 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"
- Herramientas de ONTAP para VMware vSphere 9.x Resources "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"
- TR-4400: VMware vSphere Virtual Volumes con ONTAP "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.