



Protege los almacenes de datos y las máquinas virtuales

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Tabla de contenidos

- Protege los almacenes de datos y las máquinas virtuales 1
 - Protege un clúster de hosts en ONTAP tools 1
 - Proteger usando la protección SRA 2
 - Configura SRA en ONTAP tools para proteger los datastores 2
 - Configura SRA en ONTAP tools para entornos SAN y NAS 3
 - Configura SRA en ONTAP tools para entornos altamente escalados 4
 - Configura SRA en el dispositivo VMware Live Site Recovery usando ONTAP tools 5
 - Actualiza las credenciales de SRA en ONTAP tools 6
 - Configura sitios protegidos y de recuperación en ONTAP tools 7
 - Configura los recursos del sitio protegido y del sitio de recuperación 9
 - Verifica los sistemas de almacenamiento replicados en ONTAP tools 13
 - Protección fan-out en las herramientas ONTAP 13

Protege los almacenes de datos y las máquinas virtuales

Protege un clúster de hosts en ONTAP tools

ONTAP tools for VMware vSphere gestiona la protección de los clústeres de hosts. Todos los almacenes de datos pertenecientes a la SVM seleccionada y montados en uno o varios hosts del clúster están protegidos bajo un clúster de hosts.

Antes de empezar

Asegúrate de cumplir estos requisitos antes de proteger un clúster de hosts:

- El clúster de host contiene almacenes de datos de una sola SVM.
- Los almacenes de datos del clúster de hosts no están montados en hosts fuera del clúster.
- Los almacenes de datos montados en el clúster de hosts son almacenes de datos VMFS con protocolo iSCSI o FC. No puedes usar almacenes de datos vVols, NFS ni VMFS con los protocolos NVMe/FC y NVMe/TCP.
- Los almacenes de datos basados en volúmenes FlexVol/LUN montados en un host no forman parte de ningún grupo de consistencia.
- Los almacenes de datos basados en volúmenes FlexVol/LUN montados en un host no forman parte de ninguna relación SnapMirror.
- El clúster de host contiene al menos un almacén de datos.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Haz clic con el botón derecho en un clúster de hosts y selecciona **NetApp ONTAP tools > Protect Cluster**.
3. En la ventana protect cluster, el sistema rellena automáticamente el tipo de almacén de datos y los detalles de la máquina virtual (VM) de origen. Selecciona el enlace de datastores para ver los almacenes de datos protegidos.
4. Selecciona **Add Relationship**.
5. En la ventana **Add SnapMirror Relationship**, selecciona la **máquina virtual de almacenamiento de destino** y el tipo de **política**.

El tipo de política puede ser Asynchronous o AutomatedFailOverDuplex.

Cuando añadas la relación SnapMirror como una política de tipo AutomatedFailOverDuplex, debes añadir la VM de almacenamiento de destino como backend de almacenamiento al mismo vCenter donde está desplegado ONTAP tools for VMware vSphere.

En el tipo de política AutomatedFailOverDuplex, existen configuraciones de host uniformes y no uniformes. Cuando seleccionas el botón de alternancia **Configuración de host uniforme**, la configuración del grupo iniciador de host se replica implícitamente en el sitio de destino. Para más información, consulta ["Conceptos y términos clave"](#).

6. Si decides utilizar una configuración de hosts no uniforme, selecciona el acceso al host (origen/destino) para cada host dentro de ese clúster.

7. Selecciona **Add**.
8. Puedes editar la protección del clúster de hosts usando la operación **Modify host cluster protection**. Puedes editar o eliminar las relaciones usando las opciones del menú de puntos suspensivos.
9. Selecciona el botón **Proteger**.

El sistema crea una tarea de vCenter con los detalles del ID de trabajo y muestra su progreso en el panel de tareas recientes. Esta es una tarea asíncrona; la interfaz de usuario solo muestra el estado de envío de la solicitud y no espera a que la tarea termine.

10. Para ver los clústeres de hosts protegidos, ve a **NetApp ONTAP tools > Protection > Host cluster relationships**. Selecciona un grupo de consistencia para ver su capacidad, los almacenes de datos asociados y los grupos de consistencia secundarios.



Si necesitas desactivar la protección en el plazo de una hora desde su creación, ejecuta primero la detección de almacenamiento.

Información relacionada

["VMware vSphere Metro Storage Cluster \(vMSC\)"](#)

Proteger usando la protección SRA

Configura SRA en ONTAP tools para proteger los datastores

Las herramientas de ONTAP para VMware vSphere ofrecen la opción de habilitar la función SRA para configurar la recuperación ante desastres.

Antes de empezar

- Deberías haber configurado tu instancia de vCenter Server y haber configurado los hosts ESXi.
- Deberías haber implementado ONTAP tools for VMware vSphere.
- Deberías haber descargado el archivo del SRA Adapter `.tar.gz` desde la ["Sitio de soporte de NetApp"](#).
- Debes tener las mismas programaciones personalizadas de SnapMirror tanto en el clúster ONTAP de origen como en el de destino antes de ejecutar los flujos de trabajo de SRA.
- ["Habilita ONTAP tools for VMware vSphere services"](#) para activar la función SRA.

Pasos

1. Inicia sesión en la interfaz de gestión del appliance VMware Live Site Recovery usando la URL: `https://<srm_ip>:5480`, y luego ve a Adaptadores de replicación de almacenamiento en la interfaz de gestión del appliance VMware Live Site Recovery.
2. Selecciona **Nuevo adaptador**.
3. Sube el instalador `.tar.gz` del complemento SRA a VMware Live Site Recovery.
4. Vuelve a escanear los adaptadores para comprobar que los detalles estén actualizados en la página Adaptadores de replicación de almacenamiento de VMware Live Site Recovery.



Después de una conmutación por error, acciones como expandir, montar y eliminar podrían no estar disponibles para los datastores. Realiza un descubrimiento de datastores para actualizar y mostrar las acciones adecuadas del menú contextual.



Después de cada operación de reprotección, debes realizar una detección de almacenamiento en ambos sitios.

En una nueva configuración con protección SRA, siempre ejecuta una prueba de conmutación por error. Omitir la prueba de conmutación por error puede hacer que la operación de reprotección falle.

En una configuración en abanico, después de una conmutación por error de Active Sync de SnapMirror donde el origen de SnapMirror cambia al sitio B para Automated Failover Duplex y SnapMirror asíncrono, ejecuta una prueba de conmutación por error entre los sitios B y C. Si omites este paso, la operación de reprotección puede fallar.

Información relacionada

["Configura la recuperación ante desastres para los almacenes de datos NFS usando VMware Site Recovery Manager"](#)

Configura SRA en ONTAP tools para entornos SAN y NAS

Debes configurar los sistemas de almacenamiento antes de ejecutar Storage Replication Adapter (SRA) para VMware Live Site Recovery.

Configurar SRA para entornos SAN



Los grupos de consistencia en flujos de trabajo SRA solo son compatibles con protocolos SAN (iSCSI y Fibre Channel) en sistemas de almacenamiento Unified y ASA r2.

Antes de empezar

Debes tener instalados los siguientes programas tanto en el sitio protegido como en el sitio de recuperación:

- VMware Live Site Recovery: La página web de VMware ofrece documentación sobre la instalación de VMware Live Site Recovery.

["Acerca de VMware Live Site Recovery"](#)

- SRA: instala el adaptador en VMware Live Site Recovery.

Para las configuraciones de protocolo iSCSI, ten en cuenta lo siguiente antes de ejecutar los flujos de trabajo de SRA:

- **Sitio protegido:** los adaptadores de almacenamiento iSCSI y los detalles LIF de datos se configuran automáticamente cuando aprovisionas los almacenes de datos. No se requiere configuración manual.
- **Sitio de recuperación:** los adaptadores de almacenamiento iSCSI deben configurarse manualmente en cada host ESXi que se incluya en la asignación de recursos para la recuperación de desastres. Para evitar configurar los adaptadores individualmente en cada host, crea un almacén de datos de marcador de posición de tipo iSCSI en el sitio de recuperación usando la SVM en la que se configuran los flujos de trabajo de SRA. Esto agrega automáticamente el adaptador iSCSI y las direcciones IP de LIF de datos necesarias a todos los hosts ESXi asignados. Consulta ["Configura los almacenes de datos de marcadores de posición en ONTAP tools"](#) para más detalles.

Pasos

1. Comprueba que los hosts ESXi principales estén conectados a las LUN en el sistema de almacenamiento principal en el sitio protegido.

2. Verifica que los LUN estén en igroups que tienen la opción `ostype` establecida en *VMware* en el sistema de almacenamiento principal.
3. Comprueba que los hosts ESXi del sitio de recuperación dispongan de la conectividad iSCSI y Fibre Channel adecuada con la máquina virtual de almacenamiento (SVM). Los hosts ESXi del sitio secundario deben tener acceso al almacenamiento del sitio secundario, y los hosts ESXi del sitio primario deben tener acceso al almacenamiento del sitio primario.

Puedes hacer esto comprobando que los hosts ESXi tengan LUN locales conectados en el SVM o el comando `iscsi show initiators` en los SVM. Comprueba el acceso a los LUN asignados en el host ESXi para verificar la conectividad iSCSI.

Configura SRA para entornos NAS



Los grupos de consistencia no son compatibles con NFS en los flujos de trabajo de SRA. Si los volúmenes de los almacenes de datos NFS se colocan bajo un grupo de consistencia y se protegen, la operación Descubrir dispositivos fallará. No uses grupos de consistencia al proteger almacenes de datos NFS con SRA.

Antes de empezar

Debes tener instalados los siguientes programas tanto en el sitio protegido como en el sitio de recuperación:

- VMware Live Site Recovery: Puedes encontrar la documentación de instalación de VMware Live Site Recovery en la página web de VMware - ["Acerca de VMware Live Site Recovery"](#)
- SRA: Instala el adaptador en VMware Live Site Recovery y en el servidor SRA.

Pasos

1. Comprueba que los almacenes de datos del sitio protegido contengan máquinas virtuales registradas en vCenter Server.
2. Verifica que los hosts ESXi del sitio protegido hayan montado los volúmenes de exportación NFS de la máquina virtual de almacenamiento (SVM).
3. Verifica que se especifiquen direcciones IP válidas en las que estén presentes las exportaciones NFS en el campo **NFS Addresses** cuando uses el asistente de Array Manager para añadir arrays a VMware Live Site Recovery. No uses el nombre de host NFS ni el FQDN en el campo **NFS Addresses**.
4. Utiliza el comando `ping` en cada host ESXi del sitio de recuperación para comprobar que el host tiene un puerto VMkernel que puede acceder a las direcciones IP que se usan para servir exportaciones NFS desde el SVM.

Configura SRA en ONTAP tools para entornos altamente escalados

Debes configurar los intervalos de tiempo de espera de almacenamiento según los ajustes recomendados para que el Storage Replication Adapter (SRA) funcione de forma óptima en entornos altamente escalados.

Configuración del proveedor de almacenamiento

Debes configurar los siguientes valores de tiempo de espera en VMware Live Site Recovery para entornos escalados:

Configuración avanzada	Valores de tiempo de espera
------------------------	-----------------------------

<code>StorageProvider.resignatureTimeout</code>	Aumenta el valor del parámetro de 900 segundos a 12000 segundos.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Establece un valor alto (por ejemplo: 99999)

También deberías activar la opción `StorageProvider.autoResignatureMode`.

Consulta ["Cambiar la configuración del proveedor de almacenamiento"](#) para obtener más información sobre cómo modificar la configuración del proveedor de almacenamiento.

Configuración de almacenamiento

Cuando llegues a un tiempo de espera, aumenta los valores de `storage.commandTimeout` y `storage.maxConcurrentCommandCnt` a un valor más alto.



El intervalo de tiempo de espera especificado es el valor máximo. No necesitas esperar a que se alcance el tiempo de espera máximo. La mayoría de los comandos terminan dentro del intervalo de tiempo de espera máximo establecido.

Consulta ["Cambiar la configuración de almacenamiento"](#) para modificar la configuración de SAN Provider.

Configura SRA en el dispositivo VMware Live Site Recovery usando ONTAP tools

Después de implementar el dispositivo VMware Live Site Recovery, configura el Storage Replication Adapter (SRA) para habilitar la gestión de recuperación ante desastres.

Configurar SRA en el dispositivo VMware Live Site Recovery guarda las credenciales de ONTAP tools for VMware vSphere dentro del dispositivo, lo que permite la comunicación entre VMware Live Site Recovery y SRA.

Antes de empezar

- Descarga el archivo `.tar.gz` de la ["Sitio de soporte de NetApp"](#).
- Habilita los servicios SRA en ONTAP tools Manager. Para más información, consulta la sección ["Activar servicios"](#).
- Agrega servidores vCenter a la aplicación ONTAP tools for VMware vSphere. Para más información, consulta la sección ["Agregar servidores vCenter"](#).
- Agrega backends de almacenamiento a ONTAP tools for VMware vSphere. Para más información, consulta la sección ["Agregar backends de almacenamiento"](#).



Si has aplicado el parche de certificado de vCenter desde ONTAP tools, actualiza la configuración de vCenter en el appliance de VMware Live Site Recovery usando el puerto (:5480). Para instrucciones, consulta ["Reconfigura el dispositivo Site Recovery Manager"](#).

Pasos

1. En la pantalla del dispositivo VMware Live Site Recovery, selecciona **Adaptador de replicación de almacenamiento > Nuevo adaptador**.
2. Sube el archivo `.tar.gz` a VMware Live Site Recovery.
3. Inicia sesión en el dispositivo VMware Live Site Recovery con una cuenta de administrador a través de un cliente SSH, como PuTTY.
4. Cambia al usuario raíz con el siguiente comando: `su root`
5. Ejecuta el comando `cd /var/log/vmware/srm` para acceder al directorio de registros.
6. En la ubicación del archivo de registro, introduce el comando para obtener el Docker ID utilizado por SRA:
`docker ps -l`
7. Para iniciar sesión en el ID del contenedor, introduce el comando: `docker exec -it -u srm <container id> sh`
8. Configura VMware Live Site Recovery con ONTAP tools for VMware vSphere dirección IP y contraseña usando el comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Introduce la contraseña entre comillas simples para que el script de Perl considere los caracteres especiales como parte de la contraseña, no como delimitadores.
 - Puedes configurar el nombre de usuario y la contraseña de la aplicación (VASA Provider/SRA) en ONTAP tools Manager al habilitar estos servicios por primera vez. Usa estas credenciales para registrar SRA con VMware Live Site Recovery.
 - Para localizar el GUID de vCenter, ve a la página vCenter Server en ONTAP tools Manager después de añadir tu instancia de vCenter. Consulta la sección ["Agregar servidores vCenter"](#).
9. Vuelve a escanear los adaptadores para comprobar que los datos actualizados aparecen en la página Adaptadores de replicación de almacenamiento de VMware Live Site Recovery.

Resultados Aparece un mensaje de confirmación indicando que se han guardado las credenciales de almacenamiento. Ahora ya puedes utilizar SRA para comunicarte con el servidor SRA usando la dirección IP, el puerto y las credenciales especificados.

Actualiza las credenciales de SRA en ONTAP tools

Para que VMware Live Site Recovery se comunique con SRA, debes actualizar las credenciales de SRA en el servidor de VMware Live Site Recovery si las has modificado.

Antes de empezar

Deberías haber ejecutado los pasos mencionados en el tema ["Configurar SRA en el appliance VMware Live Site Recovery"](#).

Pasos

1. Ejecuta los siguientes comandos para eliminar las credenciales de ONTAP tools almacenadas en caché del equipo VMware Live Site Recovery:
 - a. `sudo su <enter root password>`
 - b. `docker ps`
 - c. `docker exec -it <container_id> sh`
 - d. `cd conf/`

e. `rm -rf *`

2. Ejecuta el comando de Perl para configurar SRA con las nuevas credenciales:

a. `cd ..`

b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` Debes poner el valor de la contraseña entre comillas simples.

Aparece un mensaje de éxito que confirma que se han almacenado las credenciales de almacenamiento. SRA puede comunicarse con el servidor SRA utilizando la dirección IP, el puerto y las credenciales proporcionadas.

Reconfigura vCenter en el dispositivo VMware Live Site Recovery después de un cambio de certificado

Si el certificado de vCenter cambia, por ejemplo después de una actualización de vCenter, puedes encontrarte con un error de no coincidencia de huella digital en la extensión Site Recovery. Sigue estos pasos para resolverlo.

Pasos

1. Reconfigura vCenter en el dispositivo VMware Live Site Recovery

- Abre la interfaz de gestión del dispositivo VMware Live Site Recovery en un navegador:
`https://<SRM_IP>:5480`
- Selecciona la pestaña **Resumen**.
- Selecciona **Reconfigurar** para la conexión del servidor vCenter.

Esta opción obtiene y acepta la huella digital del certificado más reciente de vCenter.

2. Vuelve a conectar el emparejamiento del sitio (si persiste el error)

Si el error de no coincidencia de huella persiste tras la reconfiguración:

- Inicia sesión en la interfaz de usuario de vCenter.
- Navega hasta la extensión **Site Recovery**.
- Ubica la sección **Emparejamiento de sitios**.
- Selecciona **Reconectar** para restablecer el emparejamiento del sitio con el certificado actualizado.

Configura sitios protegidos y de recuperación en ONTAP tools

Debes crear grupos de protección para proteger un grupo de máquinas virtuales en el sitio protegido.

Cuando añades un nuevo almacén de datos, puedes incluirlo en el grupo de almacenes de datos existente o añadir un nuevo almacén de datos y crear un nuevo volumen o grupo de consistencia para protección. Después de añadir un nuevo almacén de datos a un grupo de consistencia o volumen protegido, actualiza SnapMirror y realiza el descubrimiento de almacenamiento tanto en el sitio protegido como en el de recuperación. Puedes ejecutar el descubrimiento manualmente o programarlo para asegurarte de que el nuevo almacén de datos se detecte y esté protegido.

Empareja los sitios protegidos y los de recuperación

Debes emparejar los sitios protegidos y de recuperación creados usando tu vSphere Client para que el Storage Replication Adapter (SRA) pueda detectar los sistemas de almacenamiento.



El adaptador de replicación de almacenamiento (SRA) admite fan-out con una relación de sincronización de tipo Automated Failover Duplex y una relación asíncrona SnapMirror en un grupo de consistencia. Sin embargo, no se admite fan-out con dos relaciones asíncronas SnapMirror en grupos de consistencia ni fan-out SnapMirror en volúmenes. Las relaciones de tipo Vault SnapMirror no se consideran dentro de estas restricciones de fan-out. La compatibilidad con grupos de consistencia en SRA se limita a protocolos SAN (iSCSI y canal de fibra) en sistemas de almacenamiento Unified y ASA r2. Los grupos de consistencia no son compatibles con NFS. Si los volúmenes de datastore NFS se incluyen en un grupo de consistencia, la operación de descubrimiento de dispositivos fallará.

Antes de empezar

- Debes tener instalado VMware Live Site Recovery tanto en el sitio protegido como en el de recuperación.
- Debes tener SRA instalado tanto en el sitio protegido como en el de recuperación.

Pasos

1. En la página de inicio del vSphere Client, haz doble clic en el icono **Site Recovery** y luego selecciona **Sites**.
2. Selecciona **Objetos > Acciones > Emparejar sitios**.
3. En el cuadro de diálogo **Emparejar servidores de Site Recovery Manager**, introduce la dirección del Platform Services Controller del sitio protegido y luego selecciona **Siguiente**.
4. En la sección Seleccionar servidor de vCenter, haz lo siguiente:
 - a. Verifica que el servidor vCenter del sitio protegido aparezca como candidato coincidente para emparejar.
 - b. Introduce las credenciales administrativas de SSO y, a continuación, selecciona **Finish**.
5. Si se te solicita, selecciona **Sí** para aceptar los certificados de seguridad.

Resultado

El cuadro de diálogo **Objetos** muestra tanto los sitios protegidos como los de recuperación.

Configura grupos de protección

Antes de empezar

Debes asegurarte de que tanto el sitio de origen como el de destino estén configurados de la siguiente manera:

- Misma versión de VMware Live Site Recovery instalada
- Máquinas virtuales
- Sitios de protección y recuperación emparejados
- Los almacenes de datos de origen y destino deben montarse en sus respectivos sitios

Pasos

1. Inicia sesión en vCenter Server y selecciona **Site Recovery > Protection Groups**.
2. En el panel **Grupos de protección**, selecciona **Nuevo**.

3. Indica un nombre y una descripción para el grupo de protección, la dirección y selecciona **Siguiente**.
4. En el campo **Type**, selecciona la opción **Type field option...** como grupos de almacenes de datos (replicación basada en arrays) para almacenes de datos NFS y VMFS. El dominio de fallos consiste en SVMs con replicación habilitada. Se muestran las SVMs que solo tienen implementado el peering y no tienen problemas.
5. En la pestaña «Grupos de replicación», selecciona el par de matrices habilitado o los grupos de replicación que tienen la máquina virtual que configuraste y luego selecciona **Siguiente**.

Todas las máquinas virtuales del grupo de replicación se añaden al grupo de protección.

6. Puedes seleccionar el plan de recuperación existente o crear uno nuevo seleccionando **Add to new recovery plan**.
7. En la pestaña «Listo para completar», revisa los detalles del grupo de protección que creaste y luego selecciona **Finalizar**.

Configura los recursos del sitio protegido y del sitio de recuperación

Configura las asignaciones de red en ONTAP tools

Debes configurar tus asignaciones de recursos, como las redes de VM, los hosts ESXi y las carpetas, en ambos sitios para permitir la asignación de cada recurso del sitio protegido al recurso correspondiente en el sitio de recuperación.

Debes realizar las siguientes configuraciones de recursos:

- Mapeos de red
- Asignaciones de carpetas
- Asignaciones de recursos
- Almacenes de datos placeholder

Antes de empezar

Ya deberías haber conectado los sitios protegidos y de recuperación.

Pasos

1. Inicia sesión en vCenter Server y selecciona **Site Recovery > Sitios**.
2. Selecciona tu sitio protegido y selecciona **Gestionar**.
3. Selecciona **Asignaciones de red > Nuevo** en la pestaña de gestionar para crear una nueva asignación de red.
4. En el asistente para crear una asignación de red, haz lo siguiente:
 - a. Selecciona **Preparar automáticamente las asignaciones para las redes con nombres coincidentes** y selecciona **Siguiente**.
 - b. Selecciona los objetos del centro de datos necesarios para los sitios protegidos y de recuperación y selecciona **Add Mappings**.
 - c. Selecciona **Siguiente** después de que las asignaciones se creen correctamente.
 - d. Selecciona el objeto utilizado anteriormente para crear la asignación inversa y luego selecciona **Finalizar**.

Resultado

La página «Asignaciones de red» muestra los recursos del sitio protegido y los del sitio de recuperación. Puedes seguir los mismos pasos para otras redes de tu entorno.

Configura las asignaciones de carpetas en ONTAP tools

Debes asignar tus carpetas en el sitio protegido y en el sitio de recuperación para permitir la comunicación entre ellos.

Antes de empezar

Ya deberías haber conectado los sitios protegidos y de recuperación.

Pasos

1. Inicia sesión en vCenter Server y selecciona **Site Recovery > Sitios**.
2. Selecciona tu sitio protegido y selecciona **Gestionar**.
3. Selecciona **Asignaciones de carpetas** > el icono **Carpeta** en la pestaña Manage para crear una nueva asignación de carpeta.
4. En el asistente para crear una asignación de carpetas, realiza lo siguiente:
 - a. Selecciona **Preparar automáticamente las asignaciones para las carpetas con nombres coincidentes** y selecciona **Siguiente**.
 - b. Selecciona los objetos del centro de datos necesarios para los sitios protegidos y de recuperación y selecciona **Add Mappings**.
 - c. Selecciona **Siguiente** después de que las asignaciones se creen correctamente.
 - d. Selecciona el objeto utilizado anteriormente para crear la asignación inversa y luego selecciona **Finalizar**.

Resultado

La página Folder Mappings muestra los recursos del sitio protegido y los recursos del sitio de recuperación. Puedes seguir los mismos pasos para otras carpetas de tu entorno.

Configura las asignaciones de recursos en ONTAP tools

Debes asignar tus recursos en el sitio protegido y en el sitio de recuperación, de modo que las máquinas virtuales estén configuradas para realizar la conmutación por error a uno u otro grupo de hosts.

Antes de empezar

Ya deberías haber conectado los sitios protegidos y de recuperación.



En VMware Live Site Recovery, los recursos pueden ser pools de recursos, hosts ESXi o clústeres de vSphere.

Pasos

1. Inicia sesión en vCenter Server y selecciona **Site Recovery > Sitios**.
2. Selecciona tu sitio protegido y selecciona **Gestionar**.
3. Selecciona **Asignaciones de recursos** > **Nuevo** en la pestaña de gestionar para crear una nueva asignación de recursos.

4. En el asistente para crear una asignación de recursos, realiza lo siguiente:
 - a. Selecciona **Automatically Prepare Mappings for Resources with Matching Names** y selecciona **Next**.
 - b. Selecciona los objetos del centro de datos necesarios para los sitios protegidos y de recuperación y selecciona **Add Mappings**.
 - c. Selecciona **Siguiente** después de que las asignaciones se creen correctamente.
 - d. Selecciona el objeto utilizado anteriormente para crear la asignación inversa y luego selecciona **Finalizar**.

Resultado

La página Resource Mappings muestra los recursos del sitio protegido y los recursos del sitio de recuperación. Puedes seguir los mismos pasos para otros recursos en tu entorno.

Configura los almacenes de datos de marcadores de posición en ONTAP tools

Configura un almacén de datos de marcador de posición para reservar espacio en el inventario de vCenter en el sitio de recuperación para las máquinas virtuales (VM) protegidas. Los almacenes de datos de marcador de posición requieren una capacidad mínima, porque las máquinas virtuales de marcador de posición son pequeñas y normalmente solo usan unos pocos cientos de kilobytes.

Antes de empezar

- Asegúrate de que los sitios de protección y recuperación estén conectados.
- Comprueba que se hayan configurado las asignaciones de recursos.

Pasos

1. Inicia sesión en vCenter Server y selecciona **Site Recovery > Sitios**.
2. Selecciona tu sitio protegido y selecciona **Gestionar**.
3. Selecciona **Placeholder Datastores > New** en la pestaña de gestión para crear un nuevo almacén de datos provisional.
4. Selecciona el almacén de datos adecuado y selecciona **OK**.



Los almacenes de datos provisionales pueden residir en un almacenamiento local o remoto, pero no requieren replicación.

5. Repite los pasos 3 a 5 para configurar un almacén de datos provisional para el sitio de recuperación.

Configura SRA usando el gestor de arrays en ONTAP tools

Puedes configurar el adaptador de replicación de almacenamiento (SRA) mediante el asistente Array Manager de VMware Live Site Recovery para habilitar la interacción entre VMware Live Site Recovery y las máquinas virtuales de almacenamiento (SVM).

Antes de empezar

- Deberías haber emparejado los sitios protegidos y los sitios de recuperación en VMware Live Site Recovery.
- Deberías haber configurado el almacenamiento integrado antes de configurar el array manager.

- Deberías haber configurado y replicado las relaciones de SnapMirror entre los sitios protegidos y los sitios de recuperación.
- Deberías haber habilitado los LIF de gestión de SVM para activar la multitenencia.

SRA admite la gestión a nivel de clúster y a nivel de SVM. Si añades almacenamiento a nivel de clúster, puedes descubrir y realizar operaciones en todas las SVM del clúster. Si añades almacenamiento a nivel de SVM, solo puedes gestionar esa SVM específica.

Pasos

1. En VMware Live Site Recovery, selecciona **Array Managers > Add Array Manager**.
2. Introduce la siguiente información para describir la matriz en VMware Live Site Recovery:
 - a. Introduce un nombre para identificar el gestor de matrices en el campo **Nombre para mostrar**.
 - b. En el campo **Tipo de SRA**, selecciona **NetApp Storage Replication Adapter for ONTAP**.
 - c. Introduce la información necesaria para conectarte al clúster o al SVM:
 - Si te estás conectando a un clúster, debes introducir el LIF de gestión del clúster.
 - Si te conectas directamente a un SVM, debes introducir la dirección IP del LIF de gestión del SVM.



Al configurar el gestor de matrices, debes utilizar la misma conexión (dirección IP) para el sistema de almacenamiento que se utilizó para integrarlo en ONTAP tools for VMware vSphere. Por ejemplo, si la configuración del gestor de matrices se limita al ámbito de un SVM, el almacenamiento que aparece en ONTAP tools for VMware vSphere debe añadirse a nivel de SVM.

- d. Si te conectas a un clúster, especifica el nombre del SVM en el campo **Nombre del SVM** o déjalo en blanco para gestionar todos los SVM del clúster.
- e. Introduce los volúmenes que deseas detectar en el campo **Lista de volúmenes incluidos**.

Puedes introducir el volumen de origen en el sitio protegido y el volumen de destino replicado en el sitio de recuperación.

Por ejemplo, si quieres descubrir el volumen `src_vol1` que está en una relación de SnapMirror con el volumen `dst_vol1`, debes especificar `src_vol1` en el campo de sitio protegido y `dst_vol1` en el campo de sitio de recuperación.

- f. **(Opcional)** Introduce los volúmenes que deseas excluir del proceso de detección en el campo **Volume exclude list**.

Puedes introducir el volumen de origen en el sitio protegido y el volumen de destino replicado en el sitio de recuperación.

Por ejemplo, si quieres excluir el volumen `src_vol1` que está en una relación de SnapMirror con el volumen `dst_vol1`, debes especificar `src_vol1` en el campo de sitio protegido y `dst_vol1` en el campo de sitio de recuperación.

3. Selecciona **Siguiente**.
4. Comprueba que la matriz se haya detectado y se muestre en la parte inferior de la ventana Add Array Manager y selecciona **Finalizar**.

Puedes seguir los mismos pasos para el sitio de recuperación utilizando las direcciones IP de gestión de SVM y las credenciales adecuadas. En la pantalla Enable Array Pairs del asistente Add Array Manager, debes

verificar que el par de matrices correcto esté seleccionado y que aparezca como listo para habilitarse.

Verifica los sistemas de almacenamiento replicados en ONTAP tools

Debes comprobar que el sitio protegido y el sitio de recuperación se hayan emparejado correctamente tras configurar Storage Replication Adapter (SRA). El sistema de almacenamiento replicado debe ser detectable tanto por el sitio protegido como por el sitio de recuperación.

Antes de empezar

- Ya deberías haber configurado tu sistema de almacenamiento.
- Deberías haber emparejado el sitio protegido y el sitio de recuperación mediante el array manager de VMware Live Site Recovery.
- Debes haber activado la licencia FlexClone y la licencia SnapMirror antes de realizar la operación de conmutación por error de prueba y la operación de conmutación por error para SRA.
- Debes tener las mismas políticas y programaciones de SnapMirror en los sitios de origen y de destino.
- Si utilizas políticas personalizadas de SnapMirror con un calendario personalizado, debes configurar el mismo calendario y la misma política tanto en el sitio protegido como en el de recuperación.
- Si utilizas políticas personalizadas de SnapMirror (con una programación predeterminada o personalizada), debes realizar la detección de almacenamiento desde ONTAP tools para que se reconozca la nueva política. Sin esto, los flujos de trabajo de SRA, incluyendo la conmutación por error de prueba y la conmutación por error, fallarán. Realiza la detección de almacenamiento en los siguientes puntos:
 - Después de crear la política personalizada en el sitio de recuperación.
 - Después de una operación de reprotcción, que recrea la política en el sitio protegido.

Pasos

1. Inicia sesión en tu servidor vCenter.
2. Ve a **Site Recovery > Array Based Replication**.
3. Selecciona el par de arrays que necesites y verifica los detalles correspondientes.

Los sistemas de almacenamiento deben descubrirse en el sitio protegido y en el sitio de recuperación con el estado **Enabled**.

Protección fan-out en las herramientas ONTAP

En un escenario de protección fan-out, el grupo de consistencia cuenta con doble protección: una relación síncrona con el primer clúster ONTAP de destino y una relación asíncrona con el segundo clúster ONTAP de destino. Los flujos de trabajo de crear, editar y eliminar SnapMirror active sync protection mantienen la protección síncrona. Los flujos de trabajo de conmutación por error y reprotcción del dispositivo VMware Live Site Recovery mantienen la protección asíncrona.



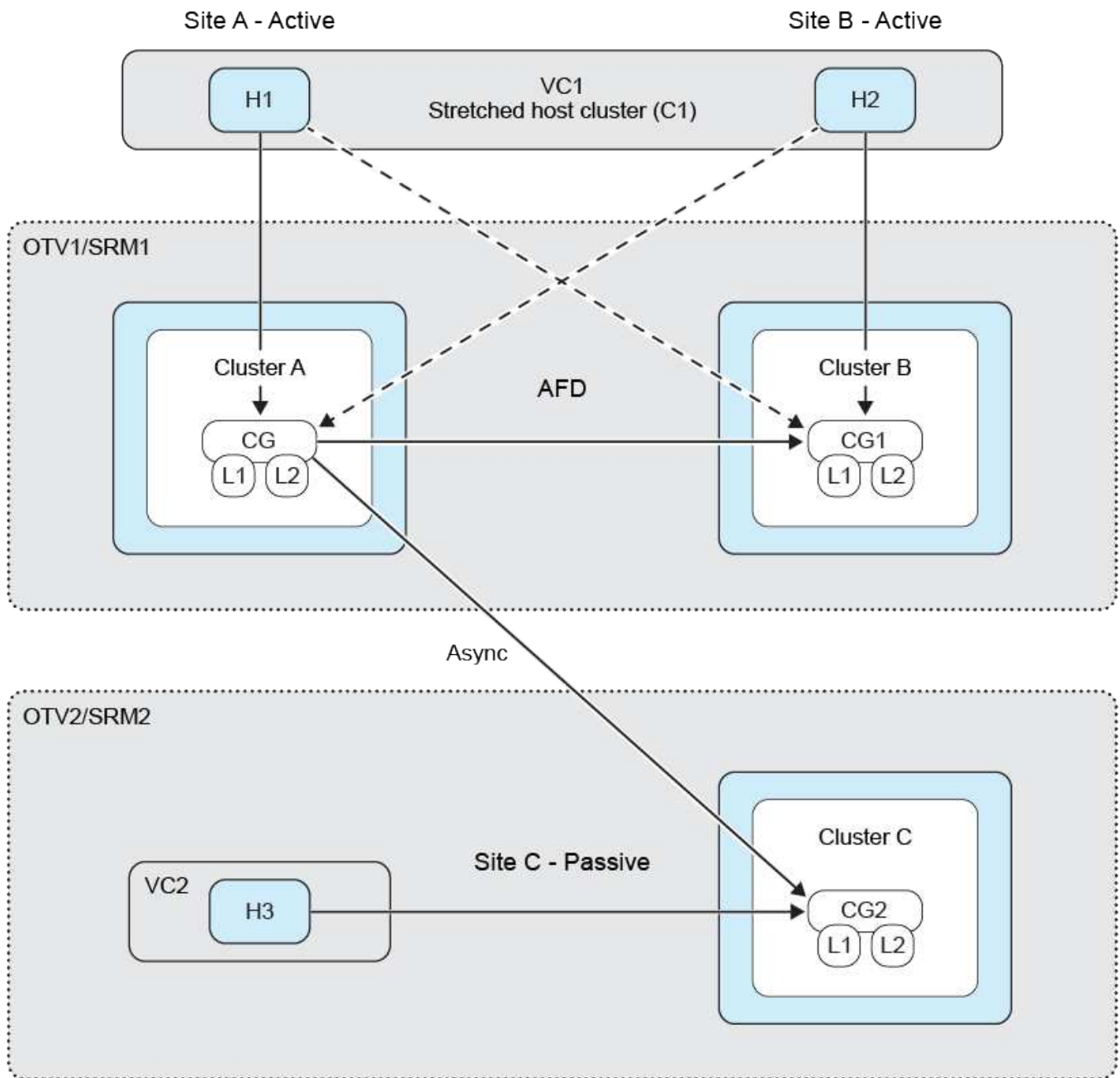
La salida en abanico no es compatible para los usuarios de SVM.

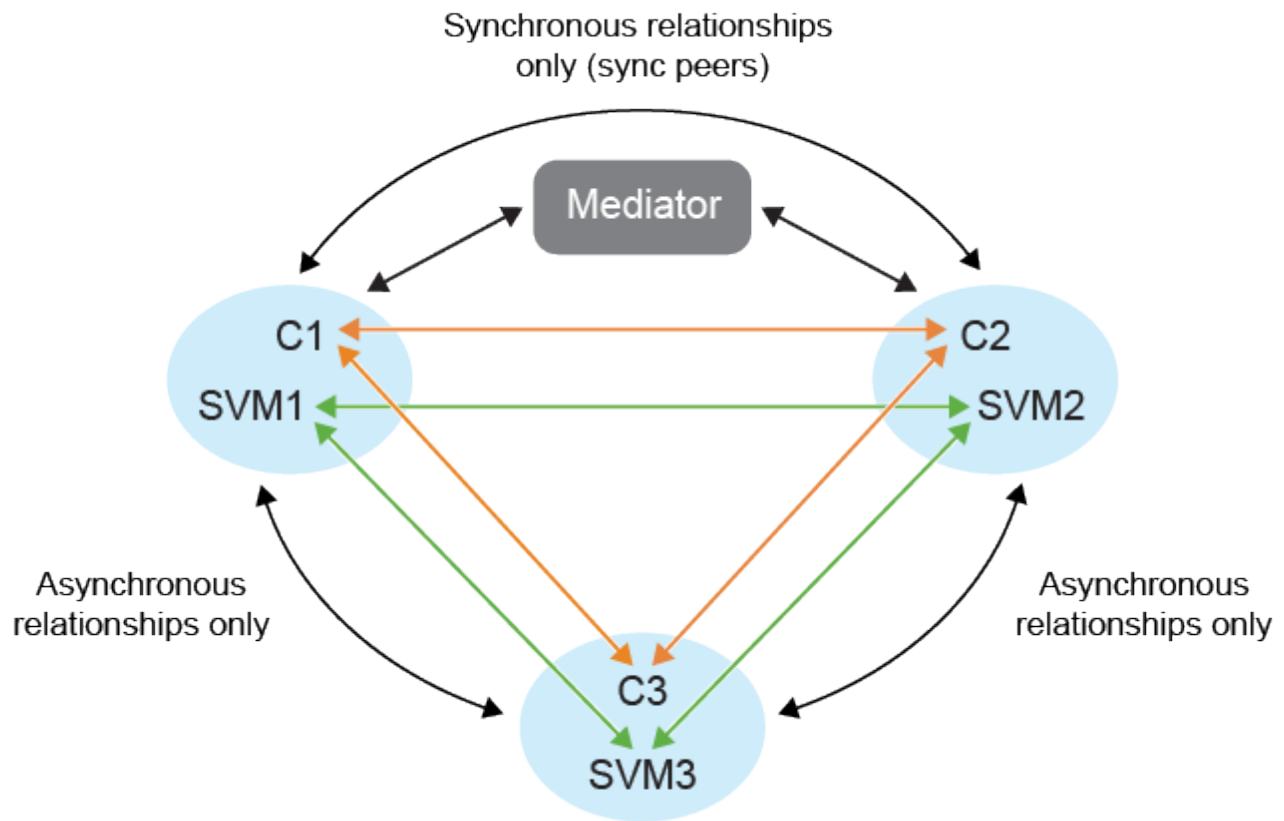
Para configurar la protección contra la dispersión, haz peer entre los tres clústeres de los sitios y las SVM.

Ejemplo:

Si	entonces
• El grupo de consistencia de origen está en el clúster c1 y la SVM svm1 • El primer grupo de consistencia de destino está en el clúster c2 y en la SVM svm2 y • El segundo grupo de consistencia de destino está en el clúster c3 y la SVM svm3	• La conexión entre clústeres en el clúster ONTAP de origen será (C1, C2) y (C1, C3). • La conexión entre clústeres en el primer clúster ONTAP de destino será (C2, C1) y (C2, C3) y • La conexión entre clústeres en el segundo clúster ONTAP de destino será (C3, C1) y (C3, C2). • El emparejamiento de SVM en el SVM de origen será (svm1, svm2) y (svm1, svm3). • Las relaciones de emparejamiento de SVM en el primer SVM de destino serán (svm2, svm1) y (svm2, svm3) y • El emparejamiento de SVM en el segundo SVM de destino será (svm3, svm1) y (svm3, svm2).

El siguiente diagrama muestra la configuración de protección fan-out:





Pasos

1. Selecciona un nuevo almacén de datos de marcador de posición. Los criterios de selección del almacén de datos de marcador de posición para la protección por fases son:
 - No coloques el almacén de datos de lugar reservado en el clúster de hosts que estás protegiendo.
 - Si necesitas incluir el almacén de datos de marcador de posición en el clúster de host, agrégalo al dispositivo VMware Live Site Recovery antes de configurar la protección de sincronización activa SnapMirror. Con esta configuración, puedes dejar el almacén de datos de marcador de posición fuera de la protección.

Para más información, consulta ["Selecciona un almacén de datos provisional"](#)

2. Agrega los datastores a la protección del clúster de hosts siguiendo ["Modificar el clúster de hosts protegidos"](#). Agrega ambos tipos de políticas: asíncronas y síncronas.

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.