



Proteger almacenes de datos y máquinas virtuales

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Tabla de contenidos

- Proteger almacenes de datos y máquinas virtuales 1
 - Proteger mediante la protección del clúster de host 1
 - Protéjase utilizando la protección SRA 2
 - Configurar SRA para proteger los almacenes de datos..... 2
 - Configurar SRA para entornos SAN y NAS 2
 - Configurar SRA para entornos de gran escalabilidad 4
 - Configurar SRA en el dispositivo VMware Live Site Recovery 5
 - Actualizar las credenciales de SRA..... 6
 - Configurar sitios protegidos y de recuperación 6
 - Configurar recursos de sitios protegidos y de recuperación 8
 - Verificar sistemas de almacenamiento replicados..... 12
 - Protección en abanico 12

Proteger almacenes de datos y máquinas virtuales

Proteger mediante la protección del clúster de host

Las ONTAP tools for VMware vSphere administran la protección de los clústeres de host. Todos los almacenes de datos que pertenecen a la SVM seleccionada y que están montados en uno o más hosts del clúster están protegidos bajo un clúster de hosts.

Antes de empezar

Asegúrese de que se cumplan los siguientes requisitos previos:

- El clúster de host tiene almacenes de datos solo de una SVM.
- El almacén de datos montado en el clúster de host no debe montarse en ningún host fuera del clúster.
- Todos los almacenes de datos montados en el clúster de host deben ser almacenes de datos VMFS con protocolo iSCSI/FC. No se admiten almacenes de datos vVols, NFS o VMFS con protocolos NVMe/FC y NVMe/TCP.
- Los almacenes de datos formadores de FlexVol/LUN montados en el clúster host no deben ser parte de ningún grupo de consistencia (CG) existente.
- Los almacenes de datos formadores de FlexVol/LUN montados en el clúster host no deben ser parte de ninguna relación SnapMirror existente.
- El clúster host debe tener al menos un almacén de datos.

Pasos

1. Inicie sesión en el cliente vSphere.
2. Haga clic con el botón derecho en un clúster de host y seleccione *** Herramientas de NetApp ONTAP * > * Proteger clúster ***.
3. En la ventana de protección del clúster, los detalles del tipo de almacén de datos y de la máquina virtual (VM) de almacenamiento de origen se completan automáticamente. Seleccione el enlace de almacenes de datos para ver los almacenes de datos protegidos.
4. Introduzca el **nombre del grupo de consistencia**.
5. Seleccione **Agregar relación**.
6. En la ventana **Agregar relación de SnapMirror ***, seleccione la ***VM de almacenamiento de destino** y el tipo de **Política**.

El tipo de política puede ser asíncrona o automatizada/conmutación por error dúplex.

Cuando agrega la relación SnapMirror como una política de tipo AutomatedFailOverDuplex, debe agregar la VM de almacenamiento de destino como back-end de almacenamiento al mismo vCenter donde se implementan las ONTAP tools for VMware vSphere .

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

7. Si elige tener una configuración de host no uniforme, seleccione el acceso al host (origen/destino) para cada host dentro de ese clúster.
8. Seleccione **Agregar**.
9. En la ventana **Proteger clúster**, no es posible editar el clúster protegido durante la operación de creación. Puedes eliminar y agregar protección nuevamente. Durante la operación de Modificar protección del clúster de host, la opción de edición está disponible. Puede editar o eliminar las relaciones utilizando las opciones del menú de puntos suspensivos.
10. Seleccione el botón **Proteger**.

Se crea una tarea de vCenter con detalles de ID de trabajo y su progreso se muestra en el panel de tareas recientes. Esta es una tarea asincrónica; la interfaz de usuario solo muestra el estado de envío de la solicitud y no espera a que se complete la tarea.
11. Para ver los clústeres de host protegidos, navegue a * Herramientas de NetApp ONTAP * > * Protección * > * Relaciones de clúster de host *.

Protéjase utilizando la protección SRA

Configurar SRA para proteger los almacenes de datos

Las ONTAP tools for VMware vSphere brindan la opción de habilitar la capacidad SRA para configurar la recuperación ante desastres.

Antes de empezar

- Debería haber configurado su instancia de vCenter Server y configurado el host ESXi.
- Debería haber implementado ONTAP tools for VMware vSphere.
- Deberías haber descargado el adaptador SRA .tar.gz archivo de la ["Sitio de soporte de NetApp"](#) .
- Los clústeres ONTAP de origen y destino deben tener las mismas programaciones SnapMirror personalizadas creadas antes de ejecutar los flujos de trabajo de SRA.
- ["Habilitar ONTAP tools for VMware vSphere"](#) para habilitar la capacidad SRA.

Pasos

1. Inicie sesión en la interfaz de administración del dispositivo VMware Live Site Recovery mediante la URL: `https://:<srm_ip>:5480` y luego vaya a Adaptadores de replicación de almacenamiento en la interfaz de administración del dispositivo VMware Live Site Recovery.
2. Seleccione **Nuevo adaptador**.
3. Cargue el instalador .tar.gz del complemento SRA en VMware Live Site Recovery.
4. Vuelva a escanear los adaptadores para verificar que los detalles estén actualizados en la página Adaptadores de replicación de almacenamiento de VMware Live Site Recovery.

Información relacionada

["Configurar la recuperación ante desastres para almacenes de datos NFS mediante VMware Site Recovery Manager"](#)

Configurar SRA para entornos SAN y NAS

Debe configurar los sistemas de almacenamiento antes de ejecutar el Adaptador de

replicación de almacenamiento (SRA) para VMware Live Site Recovery.

Configurar SRA para entornos SAN

Antes de empezar

Debe tener los siguientes programas instalados en el sitio protegido y en el sitio de recuperación:

- Recuperación de sitios en vivo de VMware

La documentación sobre la instalación de VMware Live Site Recovery está en el sitio de VMware.

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

- SRA

El adaptador está instalado en VMware Live Site Recovery.

Pasos

1. Verifique que los hosts ESXi principales estén conectados a los LUN en el sistema de almacenamiento primario en el sitio protegido.
2. Verifique que los LUN estén en igroups que tengan la `ostype` opción establecida en *VMware* en el sistema de almacenamiento principal.
3. Verifique que los hosts ESXi en el sitio de recuperación tengan conectividad iSCSI adecuada a 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 principal deben tener acceso al almacenamiento del sitio principal.

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

Configurar SRA para entornos NAS

Antes de empezar

Debe tener los siguientes programas instalados en el sitio protegido y en el sitio de recuperación:

- Recuperación de sitios en vivo de VMware

La documentación sobre la instalación de VMware Live Site Recovery se puede encontrar en el sitio de VMware.

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

- SRA

El adaptador está instalado en VMware Live Site Recovery y en el servidor SRA.

Pasos

1. Verifique que los almacenes de datos en el sitio protegido contengan máquinas virtuales que estén registradas en vCenter Server.
2. Verifique que los hosts ESXi en el sitio protegido hayan montado los volúmenes de exportaciones NFS

desde la máquina virtual de almacenamiento (SVM).

3. Verifique que se especifiquen direcciones válidas, como la dirección IP o el FQDN donde se encuentran las exportaciones NFS, en el campo **Direcciones NFS** al usar el asistente del Administrador de matrices para agregar matrices a VMware Live Site Recovery. No utilice el nombre de host NFS en el campo **Direcciones NFS**.
4. Utilice el `ping` comando en cada host ESXi en el sitio de recuperación para verificar que el host tenga un puerto VMkernel que pueda acceder a las direcciones IP que se utilizan para servir exportaciones NFS desde la SVM.

Configurar SRA para entornos de gran escalabilidad

Debe configurar los intervalos de tiempo de espera de almacenamiento según las configuraciones recomendadas para que el Adaptador de replicación de almacenamiento (SRA) funcione de manera óptima en entornos altamente escalables.

Configuración del proveedor de almacenamiento

Debe establecer los siguientes valores de tiempo de espera en VMware Live Site Recovery para el entorno escalado:

Configuración avanzada	Valores de tiempo de espera
<code>StorageProvider.resignatureTimeout</code>	Aumente el valor de la configuración de 900 segundos a 12000 segundos.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Establezca un valor alto (por ejemplo: 99999)

También deberías habilitar la `StorageProvider.autoResignatureMode` opción.

Referirse a "[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 superior.



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

Referirse a "[Cambiar la configuración de almacenamiento](#)" para modificar la configuración del proveedor SAN.

Configurar SRA en el dispositivo VMware Live Site Recovery

Después de implementar el dispositivo VMware Live Site Recovery, configure el Adaptador de replicación de almacenamiento (SRA) para habilitar la administración de recuperación ante desastres.

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

Antes de empezar

- Descargue el archivo `.tar.gz` desde ["Sitio de soporte de NetApp"](#).
- Habilitar servicios SRA en el Administrador de herramientas de ONTAP. Para obtener más información, consulte ["Habilitar servicios"](#) sección.
- Agregue servidores vCenter a las herramientas ONTAP para el dispositivo VMware vSphere. Para obtener más información, consulte ["Agregar servidores vCenter"](#) sección.
- Agregue backends de almacenamiento a las ONTAP tools for VMware vSphere. Para obtener más información, consulte ["Agregar backends de almacenamiento"](#) sección.

Pasos

1. En la pantalla del dispositivo VMware Live Site Recovery, seleccione **Adaptador de replicación de almacenamiento > Nuevo adaptador**.
2. Cargue el archivo `.tar.gz` en VMware Live Site Recovery.
3. Inicie sesión en el dispositivo VMware Live Site Recovery usando una cuenta de administrador a través de un cliente SSH como PuTTY.
4. Cambie al usuario root usando el comando: `su root`
5. Ejecutar el comando `cd /var/log/vmware/srm` para navegar al directorio de registro.
6. En la ubicación del registro, ingrese el comando para obtener el ID de Docker utilizado por SRA: `docker ps -l`
7. Para iniciar sesión en el ID del contenedor, ingrese el comando: `docker exec -it -u srm <container id> sh`
8. Configure VMware Live Site Recovery con ONTAP tools for VMware vSphere Dirección IP y contraseña mediante el comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Proporcione la contraseña entre comillas simples para que el script de Perl trate los caracteres especiales como parte de la contraseña, no como delimitadores.
 - Puede configurar el nombre de usuario y la contraseña de la aplicación (Proveedor VASA/SRA) en el Administrador de herramientas de ONTAP al habilitar estos servicios por primera vez. Utilice estas credenciales para registrar SRA con VMware Live Site Recovery.
 - Para ubicar el GUID de vCenter, vaya a la página de vCenter Server en el Administrador de herramientas de ONTAP después de agregar su instancia de vCenter. Referirse a ["Agregar servidores vCenter"](#) sección.
9. Vuelva a escanear los adaptadores para confirmar que los detalles actualizados aparezcan 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. SRA ahora puede comunicarse con el servidor SRA mediante la dirección IP, el puerto y las credenciales especificados.

Actualizar las credenciales de SRA

Para que VMware Live Site Recovery se comunice con SRA, debe actualizar las credenciales de SRA en el servidor de VMware Live Site Recovery si ha modificado las credenciales.

Antes de empezar

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

Pasos

1. Ejecute los siguientes comandos para eliminar el nombre de usuario y la contraseña de las herramientas ONTAP almacenadas en caché de la carpeta de la máquina 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. Ejecute el comando Perl para configurar SRA con las nuevas credenciales:

- a. `cd ..`
- b. ``perl command.pl -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`` Es necesario tener una comilla simple alrededor del valor de la contraseña.

Se muestra un mensaje de éxito que confirma que se guardaron las credenciales de almacenamiento. SRA puede comunicarse con el servidor SRA utilizando la dirección IP, el puerto y las credenciales proporcionados.

Configurar sitios protegidos y de recuperación

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

Al agregar un nuevo almacén de datos, puede incluirlo en el grupo de almacenes de datos existente o agregar uno nuevo y crear un nuevo volumen o grupo de consistencia para su protección. Después de agregar un nuevo almacén de datos a un grupo de consistencia o volumen protegido, actualice SnapMirror y realice la detección de almacenamiento tanto en el sitio protegido como en el de recuperación. Puede ejecutar la detección manualmente o de forma programada para garantizar que el nuevo almacén de datos se detecte y proteja.

Sitios de protección y recuperación de pares

Debe vincular los sitios protegidos y de recuperación creados con su cliente vSphere para permitir que el Adaptador de replicación de almacenamiento (SRA) descubra los sistemas de almacenamiento.



El adaptador de replicación de almacenamiento (SRA) admite la distribución en abanico con una relación de sincronización de tipo dúplex de conmutación por error automatizada y una relación asíncrona SnapMirror en un grupo de consistencia. Sin embargo, no se admite la distribución en abanico con dos SnapMirror asíncronos en un grupo de consistencia ni la distribución en abanico de SnapMirrors en un volumen.

Antes de empezar

- Debe tener VMware Live Site Recovery instalado en los sitios protegidos y de recuperación.
- Debe tener SRA instalado en los sitios protegidos y de recuperación.

Pasos

1. Haga doble clic en **Recuperación del sitio** en la página de inicio de vSphere Client y seleccione **Sitios**.
2. Seleccione **Objetos > Acciones > Emparejar sitios**.
3. En el cuadro de diálogo **Emparejar servidores de Site Recovery Manager**, ingrese la dirección del controlador de servicios de plataforma del sitio protegido y luego seleccione **Siguiente**.
4. En la sección Seleccionar vCenter Server, haga lo siguiente:
 - a. Verifique que el vCenter Server del sitio protegido aparezca como un candidato coincidente para el emparejamiento.
 - b. Ingrese las credenciales administrativas de SSO y luego seleccione **Finalizar**.
5. Si se le solicita, seleccione **Sí** para aceptar los certificados de seguridad.

Resultado

Tanto los sitios protegidos como los de recuperación aparecerán en el cuadro de diálogo Objetos.

Configurar grupos de protección

Antes de empezar

Debe asegurarse de que tanto el sitio de origen como el de destino estén configurados para lo siguiente:

- La misma versión de VMware Live Site Recovery instalada
- Máquinas virtuales
- Sitios protegidos y de recuperación emparejados
- Los almacenes de datos de origen y destino deben montarse en los sitios respectivos

Pasos

1. Inicie sesión en vCenter Server y seleccione **Site Recovery > Grupos de protección**.
2. En el panel **Grupos de protección**, seleccione **Nuevo**.
3. Especifique un nombre y una descripción para el grupo de protección, la dirección y seleccione **Siguiente**.
4. En el campo **Tipo**, seleccione la opción **Tipo...** como grupos de almacenes de datos (replicación basada en matrices) para almacenes de datos NFS y VMFS. El dominio de fallos no son más que máquinas virtuales de servicio (SVM) con replicación habilitada. Se muestran las SVM que solo tienen emparejamiento implementado y no presentan problemas.
5. En la pestaña Grupos de replicación, seleccione el par de matrices habilitado o los grupos de replicación que tienen la máquina virtual que configuró y luego seleccione **Siguiente**.

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

6. Puede seleccionar el plan de recuperación existente o crear uno nuevo seleccionando **Agregar al nuevo plan de recuperación**.
7. En la pestaña Listo para completar, revise los detalles del grupo de protección que creó y luego seleccione **Finalizar**.

Configurar recursos de sitios protegidos y de recuperación

Configurar asignaciones de red

Debe configurar las asignaciones de recursos, como redes de máquinas virtuales, hosts ESXi y carpetas en ambos sitios, para habilitar la asignación de cada recurso del sitio protegido al recurso apropiado en el sitio de recuperación.

Debes completar las siguientes configuraciones de recursos:

- Mapeos de red
- Asignaciones de carpetas
- Asignaciones de recursos
- Almacenes de datos de marcador de posición

Antes de empezar

Deberías haber conectado los sitios protegidos y de recuperación.

Pasos

1. Inicie sesión en vCenter Server y seleccione **Site Recovery > Sitios**.
2. Seleccione su sitio protegido y seleccione **Administrar**.
3. Seleccione **Asignaciones de red > Nuevo** en la pestaña de administración para crear una nueva asignación de red.
4. En el asistente Crear mapeo de red, haga lo siguiente:
 - a. Seleccione **Preparar asignaciones automáticamente para redes con nombres coincidentes** y seleccione **Siguiente**.
 - b. Seleccione los objetos del centro de datos necesarios para los sitios protegidos y de recuperación y seleccione **Agregar asignaciones**.
 - c. Seleccione **Siguiente** después de que las asignaciones se hayan creado correctamente.
 - d. Seleccione el objeto utilizado anteriormente para crear la asignación inversa y luego seleccione **Finalizar**.

Resultado

La página Asignaciones de red muestra los recursos del sitio protegido y los recursos del sitio de recuperación. Puede seguir los mismos pasos para otras redes de su entorno.

Configurar asignaciones de carpetas

Debe asignar sus carpetas en el sitio protegido y en el sitio de recuperación para habilitar la comunicación entre ellos.

Antes de empezar

Deberías haber conectado los sitios protegidos y de recuperación.

Pasos

1. Inicie sesión en vCenter Server y seleccione **Site Recovery > Sitios**.
2. Seleccione su sitio protegido y seleccione **Administrar**.
3. Seleccione **Asignaciones de carpetas** > ícono **Carpeta** en la pestaña Administrar para crear una nueva asignación de carpeta.
4. En el asistente para crear asignaciones de carpetas, realice lo siguiente:
 - a. Seleccione **Preparar automáticamente asignaciones para carpetas con nombres coincidentes** y seleccione **Siguiente**.
 - b. Seleccione los objetos del centro de datos necesarios para los sitios protegidos y de recuperación y seleccione **Agregar asignaciones**.
 - c. Seleccione **Siguiente** después de que las asignaciones se hayan creado correctamente.
 - d. Seleccione el objeto utilizado anteriormente para crear la asignación inversa y luego seleccione **Finalizar**.

Resultado

La página Asignaciones de carpetas muestra los recursos del sitio protegido y los recursos del sitio de recuperación. Puede seguir los mismos pasos para otras redes de su entorno.

Configurar asignaciones de recursos

Debe asignar sus recursos en el sitio protegido y en el sitio de recuperación para que las máquinas virtuales estén configuradas para conmutar por error en un grupo de hosts u otro.

Antes de empezar

Deberías haber conectado los sitios protegidos y de recuperación.



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

Pasos

1. Inicie sesión en vCenter Server y seleccione **Site Recovery > Sitios**.
2. Seleccione su sitio protegido y seleccione **Administrar**.
3. Seleccione **Asignaciones de recursos** > **Nuevo** en la pestaña de administración para crear una nueva asignación de recursos.
4. En el asistente Crear asignación de recursos, realice lo siguiente:
 - a. Seleccione **Preparar automáticamente asignaciones para recursos con nombres coincidentes** y seleccione **Siguiente**.
 - b. Seleccione los objetos del centro de datos necesarios para los sitios protegidos y de recuperación y seleccione **Agregar asignaciones**.
 - c. Seleccione **Siguiente** después de que las asignaciones se hayan creado correctamente.
 - d. Seleccione el objeto utilizado anteriormente para crear la asignación inversa y luego seleccione **Finalizar**.

Resultado

La página Asignaciones de recursos muestra los recursos del sitio protegido y los recursos del sitio de recuperación. Puede seguir los mismos pasos para otras redes de su entorno.

Configurar almacenes de datos de marcador de posición

Debe configurar un almacén de datos de marcador de posición para reservar un lugar en el inventario de vCenter, en el sitio de recuperación, para la máquina virtual (VM) protegida. No es necesario que el almacén de datos de marcador de posición sea grande, ya que las VM de marcador de posición son pequeñas y ocupan solo unos pocos cientos de kilobytes o menos.

Antes de empezar

- Deberías haber conectado los sitios protegidos y de recuperación.
- Deberías haber configurado tus asignaciones de recursos.

Pasos

1. Inicie sesión en vCenter Server y seleccione **Site Recovery > Sitios**.
2. Seleccione su sitio protegido y seleccione **Administrar**.
3. Seleccione **Almacenes de datos de marcador de posición > Nuevo** en la pestaña de administración para crear un nuevo almacén de datos de marcador de posición.
4. Seleccione el almacén de datos apropiado y seleccione **Aceptar**.



Los almacenes de datos de marcador de posición pueden ser locales o remotos y no deben replicarse.

5. Repita los pasos 3 a 5 para configurar un almacén de datos de marcador de posición para el sitio de recuperación.

Configurar SRA mediante el administrador de matrices

Puede configurar el Adaptador de replicación de almacenamiento (SRA) mediante el asistente del Administrador de matrices de VMware Live Site Recovery para habilitar interacciones entre VMware Live Site Recovery y las máquinas virtuales de almacenamiento (SVM).

Antes de empezar

- Debería haber emparejado los sitios protegidos y los sitios de recuperación en VMware Live Site Recovery.
- Debes haber configurado tu almacenamiento incorporado antes de configurar el administrador de matrices.
- Debería haber configurado y replicado las relaciones de SnapMirror entre los sitios protegidos y los sitios de recuperación.
- Debería haber habilitado los LIF de administración de SVM para habilitar la multitenencia.

SRA admite la gestión a nivel de clúster y la gestión a nivel de SVM. Si agrega almacenamiento a nivel de clúster, podrá descubrir y realizar operaciones en todas las SVM del clúster. Si agrega almacenamiento a un nivel de SVM, solo podrá administrar esa SVM específica.

Pasos

1. En VMware Live Site Recovery, seleccione **Administradores de matrices > Agregar administrador de matrices**.
2. Ingrese la siguiente información para describir la matriz en VMware Live Site Recovery:
 - a. Introduzca un nombre para identificar al administrador de la matriz en el campo **Nombre para mostrar**.
 - b. En el campo **Tipo de SRA**, seleccione * Adaptador de replicación de almacenamiento de NetApp para ONTAP*.
 - c. Ingrese la información para conectarse al clúster o al SVM:
 - Si se conecta a un clúster, debe ingresar al LIF de administración del clúster.
 - Si se conecta directamente a una SVM, debe ingresar la dirección IP del LIF de administración de SVM.



Al configurar el administrador de matrices, debe utilizar la misma conexión (dirección IP) para el sistema de almacenamiento que se utilizó para incorporar el sistema de almacenamiento en las ONTAP tools for VMware vSphere. Por ejemplo, si la configuración del administrador de matrices tiene alcance SVM, entonces el almacenamiento bajo las ONTAP tools for VMware vSphere se debe agregar en el nivel SVM.

- d. Si se conecta a un clúster, especifique el nombre de SVM en el campo **nombre de SVM** o déjelo en blanco para administrar todos los SVM en el clúster.
- e. Introduzca los volúmenes que se descubrirán en el campo **Lista de inclusión de volúmenes**.

Puede ingresar el volumen de origen en el sitio protegido y el volumen de destino replicado en el sitio de recuperación.

Por ejemplo, si desea descubrir el volumen *src_vol1* que está en una relación SnapMirror con el volumen *dst_vol1*, debe especificar *src_vol1* en el campo del sitio protegido y *dst_vol1* en el campo del sitio de recuperación.

- f. **(Opcional)** Ingrese los volúmenes que se excluirán del descubrimiento en el campo **Lista de exclusión de volúmenes**.

Puede ingresar el volumen de origen en el sitio protegido y el volumen de destino replicado en el sitio de recuperación.

Por ejemplo, si desea excluir el volumen *src_vol1* que está en una relación SnapMirror con el volumen *dst_vol1*, debe especificar *src_vol1* en el campo del sitio protegido y *dst_vol1* en el campo del sitio de recuperación.

3. Seleccione **Siguiente**.
4. Verifique que la matriz se descubra y se muestre en la parte inferior de la ventana Agregar administrador de matrices y seleccione **Finalizar**.

Puede seguir los mismos pasos para el sitio de recuperación utilizando las direcciones IP y credenciales de administración de SVM adecuadas. En la pantalla Habilitar pares de matrices del asistente Agregar administrador de matrices, debe verificar que esté seleccionado el par de matrices correcto y que se muestre como listo para ser habilitado.

Verificar sistemas de almacenamiento replicados

Debe verificar que el sitio protegido y el sitio de recuperación estén emparejados correctamente después de configurar el Adaptador de replicación de almacenamiento (SRA). El sistema de almacenamiento replicado debe ser detectable tanto por el sitio protegido como por el sitio de recuperación.

Antes de empezar

- Deberías haber configurado tu sistema de almacenamiento.
- Debería haber emparejado el sitio protegido y el sitio de recuperación mediante el administrador de matriz VMware Live Site Recovery.
- Debe haber habilitado 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.
- Debe tener las mismas políticas y programaciones de SnapMirror en los sitios de origen y destino.

Pasos

1. Inicie sesión en su vCenter Server.
2. Vaya a **Recuperación del sitio > Replicación basada en matriz**.
3. Seleccione el par de matrices requerido y verifique los detalles correspondientes.

Los sistemas de almacenamiento deben descubrirse en el sitio protegido y en el sitio de recuperación con el estado "Habilitado".

Protección en abanico

En una protección de abanico, el grupo de consistencia está doblemente protegido con una relación sincrónica en el primer clúster ONTAP de destino y con una relación asincrónica en el segundo clúster ONTAP de destino. Los flujos de trabajo de creación, edición y eliminación de protección de sincronización activa de SnapMirror mantienen la protección sincrónica. Los flujos de trabajo de conmutación por error y reprotcción de SRM mantienen la protección asincrónica.

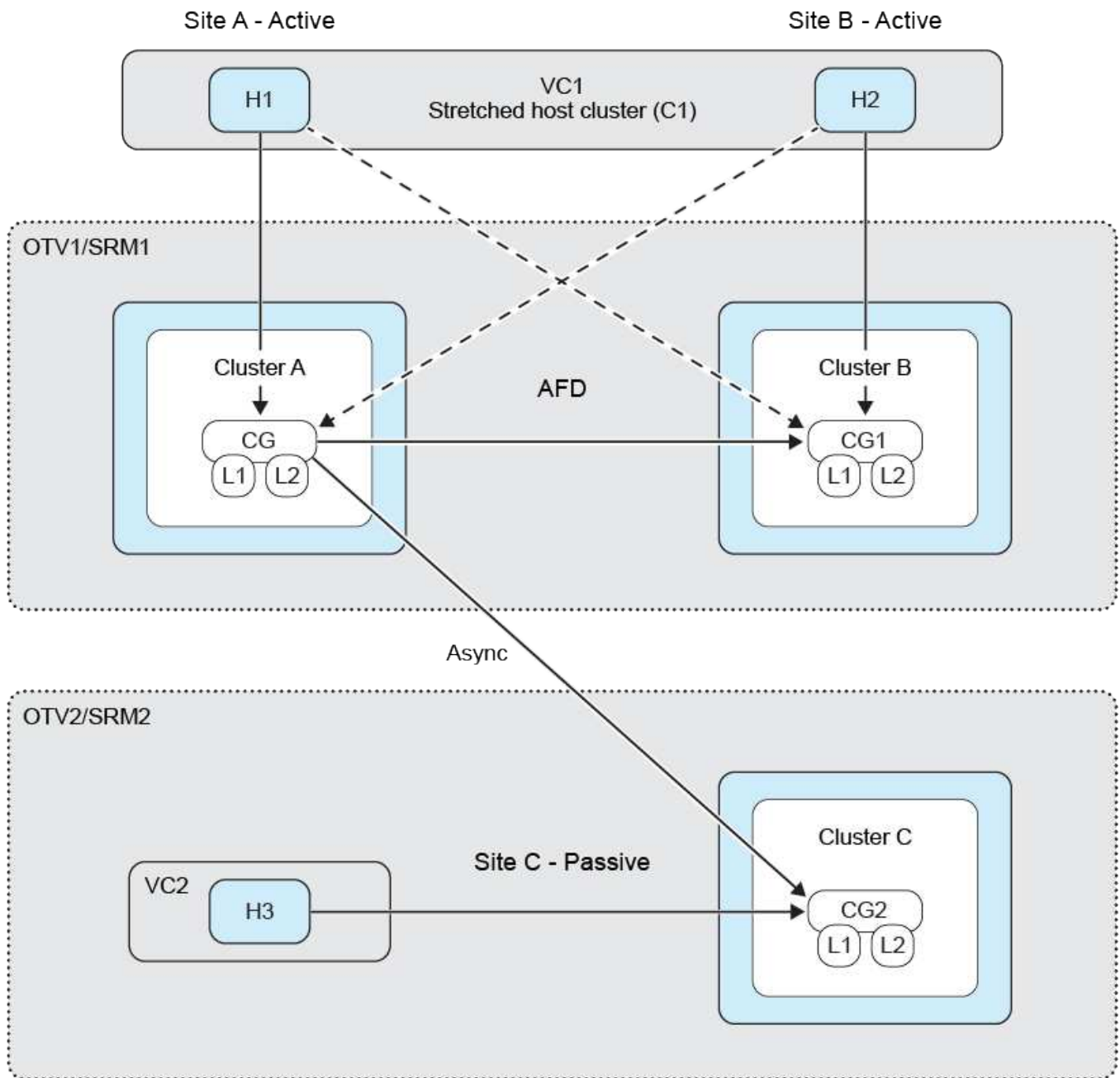
Para establecer la protección de distribución, es necesario conectar tres clústeres de sitios y SVM.

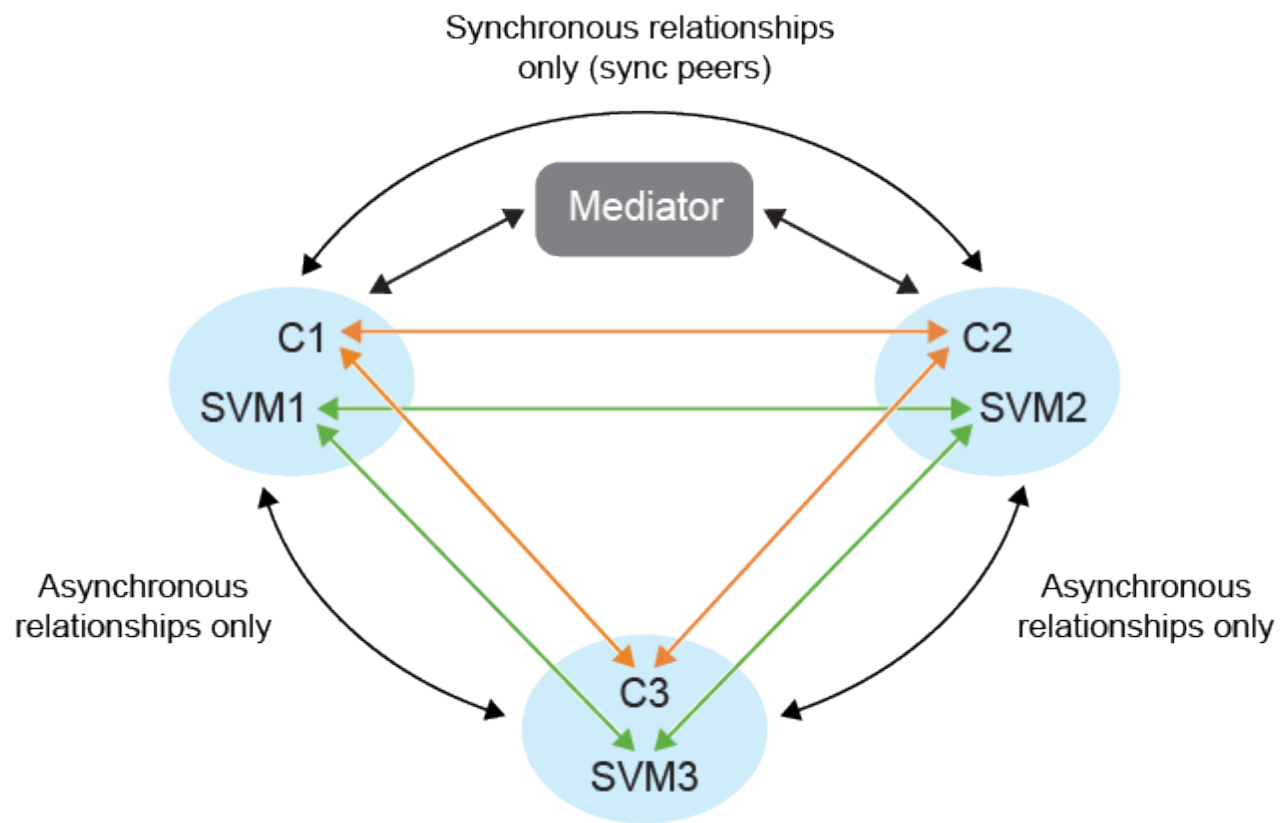
Ejemplo:

Si	entonces
----	----------

• El grupo de consistencia de origen está en el clúster c1 y SVM svm1 • El primer grupo de consistencia de destino está en el clúster c2 y SVM svm2 y • El segundo grupo de consistencia de destino está en el clúster c3 y SVM svm3	• El peering de clúster en el clúster ONTAP de origen será (C1, C2) y (C1, C3). • El peering de clúster en el primer clúster ONTAP de destino será (C2, C1) y (C2, C3) y • Los clústeres que se emparejan en el segundo clúster ONTAP de destino serán (C3, C1) y (C3, C2). • El peering SVM en el SVM de origen será (svm1, svm2) y (svm1, svm3). • El peering SVM en el primer SVM de destino será (svm2, svm1) y (svm2, svm3) y • El peering SVM en el segundo destino svm será (svm3, svm1) y (svm3, svm2).
--	--

El siguiente diagrama muestra la configuración de protección de abanico:





Pasos

1. Crear un nuevo almacén de datos de marcador de posición. Referirse "[Seleccionar un almacén de datos de marcador de posición](#)"
2. Agregar almacén de datos a la protección del clúster de host "[Modificar el clúster de host protegido](#)". Debe agregar tipos de políticas asincrónicas y sincrónicas.

Información de copyright

Copyright © 2025 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.