



# **Configure las herramientas de ONTAP para VMware vSphere**

ONTAP tools for VMware vSphere 10

NetApp  
February 11, 2026

# Tabla de contenidos

- Configure las herramientas de ONTAP para VMware vSphere . . . . . 1
  - Agregar instancias de vCenter Server a las herramientas de ONTAP . . . . . 1
  - Registra el proveedor VASA con una instancia de vCenter Server en ONTAP tools . . . . . 2
  - Instalar el complemento NFS VAAI mediante las herramientas ONTAP . . . . . 3
  - Configura los ajustes del host ESXi en ONTAP tools . . . . . 4
    - Configure los ajustes de multivía y tiempo de espera del servidor ESXi . . . . . 4
    - Configure los valores de host ESXi . . . . . 5
  - Configura los roles y privilegios de usuario de ONTAP para ONTAP tools . . . . . 5
    - Requisitos de asignación de agregados de SVM . . . . . 6
    - Crear el usuario y el rol de ONTAP manualmente . . . . . 7
    - Actualice las herramientas de ONTAP para un usuario de VMware vSphere 10,1 a 10,3 usuario . . . . . 15
    - Actualice las herramientas de ONTAP para un usuario de VMware vSphere 10,3 a 10,4 usuario . . . . . 17
  - Agrega un backend de almacenamiento a ONTAP tools . . . . . 17
  - Asocia un backend de almacenamiento con una instancia de vCenter Server en ONTAP tools . . . . . 20
  - Configura el acceso a la red en ONTAP tools . . . . . 20
  - Crear un almacén de datos en ONTAP tools . . . . . 21

# Configure las herramientas de ONTAP para VMware vSphere

## Agregar instancias de vCenter Server a las herramientas de ONTAP

Añada instancias de vCenter Server a herramientas de ONTAP para VMware vSphere para configurar, gestionar y proteger sus almacenes de datos virtuales en el entorno de vCenter Server. Cuando agrega varias instancias de vCenter Server, se requieren certificados de CA personalizados para una comunicación segura entre las herramientas de ONTAP y cada vCenter Server.

### Acerca de esta tarea

Las herramientas de ONTAP se integran con vCenter Server para realizar tareas de almacenamiento como aprovisionamiento, instantáneas y protección de datos directamente desde el cliente vSphere.

### Antes de empezar

- Asegúrate de que el certificado del servidor vCenter incluya una extensión válida de nombre alternativo del sujeto (SAN) con entradas tanto de DNS como de dirección IP. Por ejemplo:

```
X509v3 extensions:  
    X509v3 Subject Alternative Name:  
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

Si el certificado no incluye una extensión SAN, o si la extensión SAN no contiene los valores DNS o de dirección IP correctos, las operaciones de ONTAP tools pueden fallar debido a errores de validación del certificado.

- El identificador de red primario (PNID) del vCenter Server debe incluirse en los detalles de la SAN. El PNID y el nombre DNS deben ser idénticos y resolubles en DNS.
- Se recomienda desplegar vCenter Server usando su nombre de dominio completo (FQDN) y asegurarte de que el SAN en el certificado incluya DNS Name=machine\_FQDN para una compatibilidad y soporte óptimos.
- Para más información, consulta la documentación de VMware:
  - ["vSphere requisitos de certificados para diferentes vías de solución"](#)
  - ["Sustituye el certificado SSL de máquina de vCenter por un certificado firmado por una autoridad de certificación personalizada"](#)
  - ["Error: el campo Subject Alternate Name \(SAN\) no contiene el PNID. Por favor, proporciona un certificado válido"](#)



Si el FQDN no está disponible, puedes establecer el PNID en la dirección IP e incluir la dirección IP en la SAN. Sin embargo, esto no es recomendable por VMware.

### Pasos

1. Abra un navegador web y vaya a la URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Inicie sesión con las herramientas de ONTAP para las credenciales de administrador de VMware vSphere que proporcionó durante la implementación.
3. Seleccione **vCenters > Add** para incorporar las instancias de vCenter Server. Proporcione la dirección IP o el nombre de host, el nombre de usuario, la contraseña y los detalles de puerto de vCenter.
4. En las opciones avanzadas, obtenga el certificado de vCenter Server automáticamente (autorícelo) o cárguelo manualmente.



No es necesario tener una cuenta de administrador para añadir instancias de vCenter a las herramientas de ONTAP. Se puede crear un rol personalizado sin la cuenta de administrador con permisos limitados. Consulte ["Utilice el control de acceso basado en roles de vCenter Server con herramientas de ONTAP para VMware vSphere 10"](#) para obtener más información.

Al agregar una instancia de vCenter Server a herramientas de ONTAP se activan automáticamente las siguientes acciones:

- Las herramientas ONTAP registran el complemento del cliente vCenter como un complemento remoto.
- Las Privileges personalizadas para los plugins y las API se aplican a la instancia de vCenter Server.
- Se crean roles personalizados para gestionar los usuarios.
- El plugin aparece como un acceso directo en la interfaz de usuario de vSphere.

## Registra el proveedor VASA con una instancia de vCenter Server en ONTAP tools

Utilice las ONTAP tools for VMware vSphere para registrar el proveedor VASA con una instancia de vCenter Server. Esto permite la gestión basada en políticas de almacenamiento, compatibilidad con vVols e integración con dispositivos VMware Live Site Recovery en sistemas ONTAP .

La configuración del proveedor VASA muestra el estado de registro del vCenter Server seleccionado.

### Pasos

1. Inicie sesión en el cliente de vSphere.
2. Seleccione **Atajos > Herramientas NetApp ONTAP** en la sección de plug-ins.
3. Seleccione **Configuración > Configuración del proveedor VASA**. Las herramientas ONTAP muestran el estado de registro del proveedor VASA como no registrado.
4. Seleccione el botón **Registrar** para registrar el proveedor VASA.
5. Ingrese un nombre y credenciales para el proveedor de VASA. El nombre de usuario solo puede contener letras, números y guiones bajos. Establezca la longitud de la contraseña entre 8 y 256 caracteres.
6. Seleccione **Registrar**.
7. Después de un registro exitoso y una actualización de página, las herramientas de ONTAP muestran el estado, el nombre y la versión del proveedor VASA registrado.

### El futuro

Compruebe que el proveedor de VASA incorporado aparezca en la lista en VASA Provider desde el cliente de vCenter:

## Pasos

1. Vaya a la instancia de vCenter Server.
2. Inicie sesión con las credenciales de administrador.
3. Seleccione **Proveedores de almacenamiento > Configurar**. Compruebe que el proveedor de VASA incorporado esté correctamente en la lista.

# Instalar el complemento NFS VAAI mediante las herramientas ONTAP

El complemento NFS vStorage API for Array Integration (NFS VAAI) conecta VMware vSphere con matrices de almacenamiento NFS. Utilice las ONTAP tools for VMware vSphere para instalar el complemento VAAI. Esto permite que la matriz de almacenamiento NFS gestione ciertas operaciones de almacenamiento en lugar de los hosts ESXi.

## Antes de empezar

- Descargue "[Plugin NFS de NetApp para VAAI de VMware](#)" el paquete de instalación.
- Asegúrese de que tiene el host ESXi y la revisión más reciente de vSphere 7.0U3 o versiones posteriores, y de ONTAP 9.14.1 o versiones posteriores.
- Montar un almacén de datos NFS.

## Pasos

1. Inicie sesión en el cliente de vSphere.
2. Seleccione **Atajos > Herramientas NetApp ONTAP** en la sección de plug-ins.
3. Seleccione **Configuración > Herramientas de VAAI NFS**.
4. Si ya ha cargado el complemento VAAI en vCenter Server, seleccione **Cambiar en Versión existente**. Si no lo has hecho, seleccione **Subir**.
5. Busque y seleccione el `.vib` archivo y seleccione **Cargar** para cargar el archivo en las herramientas de ONTAP.
6. Seleccione **Instalar en el HOST ESXi**, seleccione el host ESXi en el que desea instalar el plugin VAAI NFS y, a continuación, seleccione **Instalar**.

vSphere Web Client muestra solo los hosts ESXi que pueden instalar el complemento. Puede supervisar el progreso de la instalación en la sección de tareas recientes.

7. Reinicie el host ESXi manualmente después de la instalación.

Después de reiniciar el host ESXi, las ONTAP tools for VMware vSphere detectan y habilitan automáticamente el complemento NFS VAAI.

## El futuro

Después de instalar el complemento NFS VAAI y reiniciar su host ESXi, configure las políticas de exportación de NFS para la descarga de copias de VAAI. Asegúrese de que las normas de política de exportación cumplan estos requisitos:

- El volumen ONTAP relevante permite llamadas NFSv4.

- El usuario root permanece como root y se permite NFSv4 en todos los volúmenes principales de unión.
- La opción de compatibilidad con VAAI se configura en el servidor NFS correspondiente.

Para obtener más información, consulte ["Configure las políticas de exportación de NFS correctas para la copia de datos descargados de VAAI"](#) Artículo de KB.

#### Información relacionada

["Compatibilidad con VMware vStorage sobre NFS"](#)

["Habilitar o deshabilitar NFSv4.0"](#)

["Compatibilidad con ONTAP para NFSv4.2"](#)

## Configura los ajustes del host ESXi en ONTAP tools

La configuración de rutas múltiples y tiempos de espera del servidor ESXi ayuda a mantener la disponibilidad e integridad de los datos. Permite la conmutación por error automática a una ruta de almacenamiento de respaldo si la ruta principal deja de estar disponible.

### Configure los ajustes de multivía y tiempo de espera del servidor ESXi

Las herramientas de ONTAP para VMware vSphere comprueban y establecen la configuración de multivía del host ESXi y el tiempo de espera de HBA que funcionan mejor con los sistemas de almacenamiento de NetApp.

#### Acerca de esta tarea

Este proceso puede llevar tiempo, dependiendo de la configuración y la carga del sistema. Puede ver el progreso en el panel Tareas recientes.

#### Pasos

1. En la página de inicio de VMware vSphere Web Client, seleccione **Hosts and Clusters**.
2. En la página de accesos directos del cliente web de VMware vSphere, seleccione **NetApp ONTAP tools** en la sección de plugins.
3. Vaya a la tarjeta **Conformidad de host ESXi** en la descripción general (consola) de las herramientas de ONTAP para el complemento de VMware vSphere.
4. Seleccione **Aplicar ajustes recomendados** link.
5. En la ventana **Aplicar configuración de host recomendada**, seleccione los hosts que desea actualizar para usar la configuración recomendada de NetApp y seleccione **Siguiente**.



Puede expandir el host ESXi para ver los valores actuales.

6. En la página settings, seleccione los valores recomendados según sea necesario.
7. En el panel de resumen, compruebe los valores y seleccione **Finalizar**. Puede realizar un seguimiento del progreso en el panel de tareas recientes.

## Configure los valores de host ESXi

Utilice las ONTAP tools for VMware vSphere para establecer tiempos de espera y otros valores en los hosts ESXi para lograr un rendimiento y una conmutación por error óptimos. Establece estos valores en función de las pruebas de NetApp .

Puede configurar los siguientes valores en un host ESXi:

### Configuración del adaptador de HBA/CNA

Establece los siguientes parámetros en los valores predeterminados:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Tiempos de espera de FC HBA de Emulex
- Tiempos de espera de HBA FC de QLogic

### Configuración de MPIO

La configuración de MPIO elige las mejores rutas para los sistemas de almacenamiento de NetApp . La configuración de MPIO selecciona la mejor ruta y la utiliza.

Para entornos de alto rendimiento o al realizar pruebas con un único almacén de datos LUN, ajuste la configuración de equilibrio de carga de la política de selección de ruta (PSP) round-robin (VMW\_PSP\_RR) para mejorar el rendimiento. Establezca el valor de IOPS predeterminado de 1000 a 1.



La configuración de MPIO no se aplica a los protocolos NVMe, NVMe/FC y NVMe/TCP.

### Configuración de NFS

Parámetro	Definir este valor en...
NET.TcpipHeapSize	32
NET.TcpipHeapMax	1024MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 o superior
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

## Configura los roles y privilegios de usuario de ONTAP para ONTAP tools

Utilice esta sección para configurar los roles y privilegios de usuario de ONTAP para los backends de almacenamiento con ONTAP tools for VMware vSphere y ONTAP System Manager. Puede asignar roles utilizando los archivos JSON proporcionados, crear

usuarios y roles manualmente y aplicar los privilegios mínimos requeridos para cuentas que no sean de administrador.

### Antes de empezar

- Descargue el archivo de Privileges de ONTAP de las ONTAP tools for VMware vSphere usando [https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users\\_roles.zip](https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip). Después de descargar el archivo zip, encontrará dos archivos JSON. Utilice el archivo JSON específico de ASA r2 al configurar un sistema ASA r2.



Puede crear usuarios en el nivel de clúster o directamente en el nivel de máquinas virtuales de almacenamiento (SVM). Si no utiliza el archivo `user_roles.json`, asegúrese de que el usuario tenga los permisos SVM mínimos requeridos.

- Inicie sesión con privilegios de administrador para el backend de almacenamiento.

### Pasos

1. Extraiga el archivo [https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users\\_roles.zip](https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip) que descargó.
2. Acceda a ONTAP System Manager mediante la dirección IP de gestión del clúster.
3. Inicie sesión en el clúster con privilegios de administrador. Para configurar un usuario:
  - a. Para configurar un usuario de herramientas de clúster ONTAP, seleccione **Clúster > Configuración > Usuarios y roles**.
  - b. Para configurar un usuario de herramientas SVM ONTAP, seleccione **Almacenamiento SVM > Configuración > Usuarios y roles**.
  - c. Seleccione **Agregar** en Usuarios.
  - d. En el cuadro de diálogo **Agregar usuario**, seleccione **Productos de virtualización**.
  - e. **Explorar** para seleccionar y cargar el archivo JSON de Privileges de ONTAP. Para sistemas que no sean ASA r2, seleccione el archivo `users_roles.json` y, para sistemas ASA r2, seleccione el archivo `users_roles_ASAr2.json`.

Las herramientas ONTAP rellenan automáticamente el campo **Producto**.

- f. Seleccione la capacidad del producto como **VSC, Proveedor VASA y SRA** en el menú desplegable.

Las herramientas de ONTAP completan automáticamente el campo **Rol** según la capacidad del producto que seleccione.

- g. Introduzca el nombre de usuario y la contraseña necesarios.
- h. Seleccione los privilegios (Descubrimiento, Crear almacenamiento, Modificar almacenamiento, Destruir almacenamiento, Rol NAS/SAN) que necesita el usuario y luego seleccione **Agregar**.

Las herramientas ONTAP agregan el nuevo rol y usuario. Puede ver los privilegios bajo el rol que configuró.

### Requisitos de asignación de agregados de SVM

Al aprovisionar almacenes de datos mediante credenciales de usuario de SVM, las ONTAP tools for VMware vSphere crean volúmenes en el agregado especificado en la API POST de almacenes de datos. ONTAP evita que los usuarios de SVM creen volúmenes en agregados no asignados a SVM. Asigne la SVM a los agregados necesarios mediante la API REST de ONTAP o la CLI antes de crear volúmenes.



## API DE REST:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

## CLI de ONTAP:

```
still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State      Size Type      SnapLock
Type-----
-----svm_test      still15_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

## Crear el usuario y el rol de ONTAP manualmente

Cree usuarios y roles manualmente sin el archivo JSON.

1. Acceda a ONTAP System Manager mediante la dirección IP de gestión del clúster.
2. Inicie sesión en el clúster con la Privileges de administrador.
  - a. Para configurar los roles de las herramientas del clúster ONTAP , seleccione **Clúster > Configuración > Usuarios y roles**.
  - b. Para configurar los roles de las herramientas SVM ONTAP del clúster, seleccione **SVM de almacenamiento > Configuración > Usuarios y roles**.
3. Crear roles:
  - a. Seleccione **Agregar** en la tabla **Roles**.
  - b. Introduzca los detalles de **nombre de rol** y **atributos de rol**.

Agregue la **Ruta de API REST** y elija el acceso de la lista desplegable.
  - c. Agregue todas las API necesarias y guarde los cambios.
4. Crear usuarios:
  - a. Seleccione **Agregar** en la tabla **Usuarios**.
  - b. En el cuadro de diálogo **Agregar usuario**, seleccione **Administrador del sistema**.
  - c. Introduzca el **Nombre de usuario**.
  - d. Seleccione **Rol** de las opciones creadas en el paso **Crear Roles** anterior.
  - e. Introduzca las aplicaciones a las que desea acceder y el método de autenticación. ONTAPI y HTTP son las aplicaciones requeridas, y el tipo de autenticación es **Password**.
  - f. Establezca la **Contraseña para el usuario** y **Guardar** para el usuario.

### Lista de privilegios mínimos necesarios para el usuario de cluster de ámbito global no administrativo

Esta página enumera los privilegios mínimos requeridos para un usuario de clúster con ámbito global que no sea administrador y que no tenga un archivo JSON. Si un clúster está en el ámbito local, use el archivo JSON para crear usuarios porque las ONTAP tools for VMware vSphere necesitan más que solo privilegios de

lectura para el aprovisionamiento en ONTAP.

Puede acceder a la funcionalidad mediante API:

API	Nivel de acceso	Se utiliza para
/api/clúster	Solo lectura	Descubrimiento de la configuración del clúster
/api/cluster/licencias/licencias	Solo lectura	Comprobación de licencias para licencias específicas del protocolo
/api/cluster/nodos	Solo lectura	Detección de tipo de plataforma
/api/seguridad/cuentas	Solo lectura	Descubrimiento de privilegios
/api/seguridad/roles	Solo lectura	Descubrimiento de privilegios
/api/almacenamiento/agregados	Solo lectura	Comprobación del espacio agregado durante el aprovisionamiento de volúmenes o almacenes de datos
/api/almacenamiento/clúster	Solo lectura	Para obtener datos de espacio y eficiencia a nivel de clúster
/api/storage/disks	Solo lectura	Para obtener los discos asociados en un agregado
/api/almacenamiento/qos/políticas	Lectura/Crear/Modificar	Gestión de políticas de QoS y VM
/api/svm/svm	Solo lectura	Para obtener la configuración de SVM cuando el clúster se agrega localmente.
/api/network/ip/interfaces	Solo lectura	Agregar backend de almacenamiento: para identificar que el alcance de LIF de administración es clúster/SVM
/api/storage/availability-zones	Solo lectura	Descubrimiento de SAZ. Aplicable a versiones ONTAP 9.16.1 en adelante y sistemas ASA r2.
/api/clúster/metrocluster	Solo lectura	Obtiene el estado de MetroCluster y los detalles de configuración.

## Cree herramientas de ONTAP para usuario de ámbito de clúster basado en la API de VMware vSphere ONTAP



Se requieren privilegios de descubrimiento, creación, modificación y destrucción para las operaciones PATCH y la reversión automática en los almacenes de datos. La falta de permisos puede provocar problemas de flujo de trabajo y limpieza.

Un usuario basado en API de ONTAP con privilegios de descubrimiento, creación, modificación y destrucción puede administrar flujos de trabajo de herramientas de ONTAP .

Para crear un usuario de ámbito de cluster con todas las Privileges mencionadas anteriormente, ejecute los siguientes comandos:

```

security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api

```

```

/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logs -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

```

```

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly

```

Además, para las versiones 9.16.0 y posteriores de ONTAP, ejecute el siguiente comando:

```
security login rest-role create -role <role-name> -api  
/api/storage/storage-units -access all
```

Para los sistemas ASA R2 en ONTAP versiones 9.16.1 y posteriores, ejecute el siguiente comando:

```
security login rest-role create -role <role-name> -api  
/api/storage/availability-zones -access readonly
```

### Create ONTAP tools for VMware vSphere ONTAP API based SVM scoped user

Ejecute los siguientes comandos para crear un usuario con ámbito SVM con todos los privilegios:

```
security login rest-role create -role <role-name> -api  
/api/application/consistency-groups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/private/cli/snapmirror -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/igroups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/lun-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/snapmirror/relationships -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/volumes -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/storage/luns  
-access all -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/storage/namespaces -access all -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/cluster/schedules -access read_create -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/snapmirror/policies -access read_create -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/storage/file/clone -access read_create -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/storage/file/copy -access read_create -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/support/ems/application-logs -access read_create -vserver <vserver-  
name>
```

```
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster  
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster/jobs  
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster/peers  
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/name-  
services/name-mappings -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/network/ethernet/ports -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/network/fc/interfaces -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api  
/api/network/fc/logins -access readonly -vserver <vserver-name>
```

```

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>

```

Además, para las versiones 9.16.0 y posteriores de ONTAP, ejecute el siguiente comando:

```

security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>

```

Para crear un nuevo usuario basado en API utilizando los roles basados en API creados anteriormente, ejecute el siguiente comando:



```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Ejemplo:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

Ejecute el siguiente comando para desbloquear la cuenta y habilitar el acceso a la interfaz de administración:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Ejemplo:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

## Actualice las herramientas de ONTAP para un usuario de VMware vSphere 10,1 a 10,3 usuario

Para herramientas de ONTAP para usuarios de VMware vSphere 10,1 con un usuario en el ámbito del clúster creado con el archivo JSON, utilice los siguientes comandos de la CLI de ONTAP con la Privileges de administrador de usuario para actualizar a la versión 10,3.

Para las capacidades del producto:

- VSC
- VSC y proveedor VASA
- VSC y SRA
- VSC, proveedor VASA y SRA.

Privileges de clúster:

```
security login role create -role <existing-role-name> -cmddirname «vserver nvme namespace show» -access
all
```

```
security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem show» -access all
```

```
security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem host show»
-access all
```

```
security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem map show»
-access all
```

*security login role create -role <existing-role-name> -cmddirname «vserver nvme show-interface» -access read*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem host add»  
-access all*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem map add»  
-access all*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme namespace delete» -access  
all*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem delete» -access  
all*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem host remove»  
-access all*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem map remove»  
-access all*

Para herramientas de ONTAP para VMware vSphere 10,1 usuario con un usuario de ámbito de SVM creado con el archivo json, utilice los comandos de la CLI de ONTAP con Privileges del usuario administrador para actualizar a la versión 10,3.

Privileges de SVM:

*security login role create -role <existing-role-name> -cmddirname «vserver nvme namespace show» -access  
all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem show» -access all  
-vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem host show»  
-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem map show»  
-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme show-interface» -access read  
-vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem host add»  
-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem map add»  
-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme namespace delete» -access  
all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem delete» -access  
all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem host remove»  
-access all -vserver <vserver-name>*

```
security login role create -role <existing-role-name> -cmddirname «vserver nvme subsystem map remove»  
-access all -vserver <vserver-name>
```

Para habilitar los siguientes comandos, agregue los comandos *vserver nvme namespace show* y *vserver nvme subsystem show* a la función existente.

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

## Actualice las herramientas de ONTAP para un usuario de VMware vSphere 10,3 a 10,4 usuario

A partir de ONTAP 9.16.1, actualice las ONTAP tools for VMware vSphere 10.3 al usuario 10.4.

Para herramientas de ONTAP para VMware vSphere 10,3 usuario con un usuario de ámbito en el clúster creado con el archivo JSON y la versión 9.16.1 o posteriores de ONTAP, use el comando de la CLI de ONTAP con Privileges de usuario administrador para actualizar a la versión 10,4.

Para las capacidades del producto:

- VSC
- VSC y proveedor VASA
- VSC y SRA
- VSC, proveedor VASA y SRA.

Privileges de clúster:

```
security login role create -role <existing-role-name> -cmddirname "storage  
availability-zone show" -access all
```

## Agrega un backend de almacenamiento a ONTAP tools

Utilice las ONTAP tools for VMware vSphere para agregar y administrar backends de almacenamiento para sus hosts ESXi. Puede incorporar clústeres o SVM, habilitar la compatibilidad con MetroCluster y validar certificados para una conectividad segura. Puede configurar backends de almacenamiento mediante el Administrador de herramientas de ONTAP o el cliente vSphere, monitorear el estado del certificado y redescubrir recursos manualmente después de cambios en el clúster.

Para agregar un backend de almacenamiento localmente, use las credenciales del clúster o SVM en la interfaz de herramientas de ONTAP . Los backends de almacenamiento local solo están disponibles para el

vCenter Server seleccionado. Las herramientas de ONTAP asignan SVM al vCenter Server para la administración del almacén de datos vVols o VMFS. Para los almacenes de datos VMFS y los flujos de trabajo de SRA, puede usar credenciales de SVM sin asignar un clúster globalmente.

Para agregar un backend de almacenamiento global, use las credenciales del clúster ONTAP en el Administrador de herramientas ONTAP . Los backends de almacenamiento global permiten flujos de trabajo de descubrimiento para identificar los recursos del clúster necesarios para la administración de vVol. En entornos multiinquilino, puede agregar un usuario SVM localmente para administrar almacenes de datos vVols .

Si la compatibilidad con MetroCluster está habilitada en ONTAP, incorpore los clústeres de origen y destino como backends de almacenamiento locales o globales.

### **Antes de empezar**

Verifique que el certificado incluya un campo de Nombre alternativo del sujeto (SAN) válido. Los sistemas ONTAP utilizan el campo SAN para identificar LIF de administración de clústeres y SVM.

## Mediante el Administrador de herramientas de ONTAP



En una configuración multi-tenant, puede añadir un clúster back-end de almacenamiento de forma global y SVM de forma local para usar las credenciales de usuario de SVM.

### Pasos

1. Inicie ONTAP TOOLS Manager desde un explorador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las herramientas de ONTAP para las credenciales de administrador de VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Backends de almacenamiento** en la barra lateral.
4. Añada el back-end de almacenamiento y proporcione la dirección IP del servidor o el FQDN, el nombre de usuario y los detalles de la contraseña.



Se admiten los LIF de gestión de direcciones IPv4 y IPv6.

5. Obtenga los certificados del clúster ONTAP automáticamente y autorice el certificado, o cárguelo manualmente buscando su ubicación.



Si es necesario, puede deshabilitar la validación del nombre alternativo del sujeto (SAN) desde la consola de mantenimiento. Para obtener instrucciones, consulte ["Cambiar la bandera de validación del certificado"](#).

6. Si el backend de almacenamiento que agrega es parte de una configuración de MetroCluster, el Administrador de herramientas de ONTAP muestra un mensaje emergente para agregar el clúster emparejado. Seleccione **Agregar** y proporcione los detalles para el backend de almacenamiento de pares de MetroCluster.



Después de que el sistema ONTAP realice un cambio y un retorno, ejecute el descubrimiento de herramientas ONTAP manualmente.

## Mediante la interfaz de usuario del cliente de vSphere



Los almacenes de datos vVols no admiten la adición directa de un usuario SVM a través de la interfaz de usuario del cliente vSphere.

1. Inicie sesión en el cliente de vSphere.
2. En la página de accesos directos, seleccione **Herramientas de NetApp ONTAP** en la sección de plugins.
3. Seleccione **Backends de almacenamiento** en la barra lateral.
4. Añada el back-end de almacenamiento y proporcione la dirección IP del servidor, el nombre de usuario, la contraseña y los detalles del puerto.



Puede agregar un backend de almacenamiento utilizando credenciales basadas en clúster con LIF de administración IPv4 o IPv6. Para agregar un usuario SVM directamente, proporcione credenciales basadas en SVM junto con un LIF de administración de SVM. Si ya hay un clúster incorporado, no podrás incorporar nuevamente un usuario SVM desde ese clúster.

5. Obtenga los certificados del clúster ONTAP automáticamente y autorice el certificado, o cárguelo manualmente buscando su ubicación.
6. Si el backend de almacenamiento agregado es parte de la configuración de MetroCluster , las herramientas de ONTAP muestran la pantalla **Agregar par de MetroCluster \***. **Seleccione \*Agregar par** para agregar el backend de almacenamiento de pares.



Después de que el sistema ONTAP realice un cambio y un retorno, ejecute el descubrimiento de herramientas ONTAP manualmente.

#### ¿Cuál es el siguiente?

Las herramientas ONTAP actualizan la lista para mostrar el nuevo backend de almacenamiento.

Las herramientas de ONTAP enumeran el back-end de almacenamiento recientemente agregado en la página **Back-ends de almacenamiento**. Si un certificado vence en 30 días o menos, las herramientas de ONTAP muestran una advertencia en la columna de fecha de vencimiento del certificado. Después del vencimiento, las herramientas ONTAP marcan el backend de almacenamiento como desconocido porque no puede conectarse al sistema de almacenamiento.

#### Información relacionada

["Configuración de los clústeres en una configuración MetroCluster"](#)

## Asocia un backend de almacenamiento con una instancia de vCenter Server en ONTAP tools

Asocie un backend de almacenamiento con una instancia de vCenter Server para habilitar el acceso a todas las instancias de vCenter Server. Para la configuración de MetroCluster , cuando asocie un clúster de back-end de almacenamiento, asegúrese de asociar también su clúster par con vCenter Server.

#### Pasos

1. Inicie ONTAP TOOLS Manager desde un explorador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las herramientas de ONTAP para las credenciales de administrador de VMware vSphere que proporcionó durante la implementación.
3. Seleccione vCenter en la barra lateral.
4. Seleccione los puntos suspensivos verticales junto a la instancia de vCenter Server que desea conectar a los backends de almacenamiento.
5. En el menú desplegable, seleccione el backend de almacenamiento que desea asociar con la instancia de vCenter Server seleccionada.

## Configura el acceso a la red en ONTAP tools

De forma predeterminada, todas las direcciones IP detectadas desde el host ESXi se agregan automáticamente a la política de exportación, a menos que configure el acceso a la red. Puede modificar la política de exportación para permitir el acceso sólo desde direcciones IP específicas. Si un host ESXi excluido intenta una operación de montaje, la

operación falla.

#### Pasos

1. Inicie sesión en el cliente de vSphere.
2. Seleccione **Herramientas de NetApp ONTAP** en la página de accesos directos en la sección de plugins.
3. En el panel izquierdo de las herramientas de ONTAP , vaya a **Configuración > Administrar acceso a la red > Editar**.

Para agregar varias direcciones IP, separe la lista con comas, rango, enrutamiento entre dominios sin clases (CIDR) o una combinación de los tres.

4. Seleccione **Guardar**.

## Crear un almacén de datos en ONTAP tools

Cuando crea un almacén de datos en el nivel del clúster de host, las herramientas de ONTAP lo montan en todos los hosts de destino y habilitan la acción solo si tiene los privilegios necesarios.

### Interoperabilidad entre almacenes de datos nativos con vCenter Server y almacenes de datos administrados por herramientas ONTAP

A partir de las ONTAP tools for VMware vSphere 10.4, las herramientas ONTAP crean igroups anidados para almacenes de datos, con igroups principales específicos para los almacenes de datos y igroups secundarios asignados a los hosts. Puede crear igroups planos desde ONTAP System Manager y usarlos para crear almacenes de datos VMFS sin utilizar herramientas ONTAP . Referirse a "[Administrar iniciadores SAN y igroups](#)" Para más información.

Después de incorporar el almacenamiento y ejecutar el descubrimiento del almacén de datos, las herramientas de ONTAP cambian los igroups planos en los almacenes de datos VMFS a igroups anidados. No es posible utilizar igroups planos anteriores para crear nuevos almacenes de datos. Utilice la interfaz de herramientas ONTAP o la API REST para reutilizar igroups anidados.

## Cree un almacén de datos vVols

A partir de las ONTAP tools for VMware vSphere 10.3, puede crear un almacén de datos vVols en sistemas ASA r2 con eficiencia de espacio como thin.vVol. El proveedor VASA crea un contenedor y los puntos finales de protocolo deseados mientras crea el almacén de datos vVol. El proveedor VASA no asigna ningún volumen de respaldo a este contenedor.

### Antes de empezar

- Asegúrese de que los agregados raíz no estén asignados a SVM.
- Compruebe que el proveedor de VASA esté registrado en la instancia de vCenter seleccionada.
- En el sistema de almacenamiento ASA r2, la SVM debe asignarse al agregado para el usuario SVM.

### Pasos

1. Inicie sesión en el cliente de vSphere.
2. Haga clic con el botón derecho en un sistema host, un clúster de host o un centro de datos y seleccione **Herramientas de NetApp ONTAP \* > \*Crear almacén de datos**.
3. Seleccione vVols **Tipo de almacén de datos**.
4. Introduzca la información de **Nombre del almacén de datos** y **Protocolo**.



El sistema R2 de ASA es compatible con los protocolos iSCSI y FC para vVols.

5. Seleccione la máquina virtual de almacenamiento donde desea crear el almacén de datos.
6. En Opciones avanzadas:
  - Si selecciona la **Política de exportación personalizada**, asegúrese de ejecutar la detección en vCenter para todos los objetos. Se recomienda que no utilice esta opción.
  - Puede seleccionar el nombre de **Grupo de iniciadores personalizado** para los protocolos iSCSI y FC.



En el sistema de almacenamiento ASA r2 tipo SVM, no se crean unidades de almacenamiento (LUN/espacio de nombres) porque el almacén de datos es solo un contenedor lógico.

7. En el panel **Atributos de almacenamiento**, puede crear nuevos volúmenes o utilizar los volúmenes existentes. Sin embargo, no es posible combinar estos dos tipos de volúmenes para crear un almacén de datos vVols.

Al crear un nuevo volumen, puede habilitar QoS en el almacén de datos. De forma predeterminada, se crea un volumen por cada solicitud creada por LUN. Omita este paso para los almacenes de datos vVols en sistemas de almacenamiento ASA r2.

8. Revise su selección en el panel **Resumen** y seleccione **Finalizar**.

## Cree un almacén de datos NFS

Un almacén de datos NFS conecta hosts ESXi al almacenamiento compartido mediante el protocolo NFS. Son simples y flexibles y se utilizan en entornos VMware vSphere.

### Pasos

1. Inicie sesión en el cliente de vSphere.



2. Haga clic con el botón derecho en un sistema host, un clúster de host o un centro de datos y seleccione **Herramientas de NetApp ONTAP** \* > **\*Crear almacén de datos**.
3. Seleccione NFS en el campo **Datastore type**.
4. Introduzca el nombre del almacén de datos, el tamaño y la información del protocolo en el panel **Nombre y protocolo**. Seleccione **Datastore cluster** y **Kerberos authentication** en las opciones avanzadas.



La autenticación Kerberos solo está disponible cuando se selecciona el protocolo NFS 4,1.

5. Seleccione **Plataforma y Storage VM** en el panel **Almacenamiento**.
6. Si selecciona **Política de exportación personalizada** en las opciones avanzadas, ejecutará la detección en vCenter para todos los objetos. Se recomienda que no utilice esta opción.



No se puede crear un almacén de datos NFS utilizando la política de volumen raíz o predeterminada de SVM.

- En las opciones avanzadas, el botón de alternar **Asimétrico** solo es visible si se selecciona el rendimiento o la capacidad en el menú desplegable de la plataforma.
  - Cuando elige la opción **Cualquiera** en el menú desplegable de la plataforma, puede ver todas las SVM en vCenter. Plataforma y bandera asimétrica no afectan visibilidad.
7. Seleccione el agregado para la creación de volúmenes en el panel **Atributos de almacenamiento**. En las opciones avanzadas, elija **Space Reserve** y **Enable QoS** según sea necesario.
  8. Revise las selecciones en el panel **Resumen** y seleccione **Finalizar**.

Las herramientas ONTAP crean el almacén de datos NFS y lo montan en todos los hosts.

### Cree un almacén de datos de VMFS

VMFS es un sistema de archivos agrupado para almacenar archivos de máquinas virtuales. Varios hosts ESXi pueden acceder a los mismos archivos de VM simultáneamente para las funciones vMotion y alta disponibilidad.

En un clúster protegido:

- Solo puede crear almacenes de datos VMFS. Agregar un almacén de datos VMFS a un clúster protegido lo protege automáticamente.
- No es posible crear un almacén de datos en un centro de datos con uno o varios clústeres de hosts protegidos.
- No se puede crear un almacén de datos en un host ESXi si el clúster del host principal está protegido por una "Política de dúplex de conmutación por error automatizada" (configuración uniforme o no uniforme).
- Un almacén de datos VMFS solo se puede crear en un host ESXi protegido por una relación asíncrona. No se puede crear ni montar un almacén de datos en un host ESXi que forma parte de un clúster de hosts protegido por la política «Automatic Failover Duplex».

### Antes de empezar

- Habilite los servicios y las LIF para cada protocolo en el almacenamiento de ONTAP.
- Asigne SVM al agregado para el usuario de SVM en el sistema de almacenamiento ASA R2.

- Configure el host ESXi si utiliza el protocolo NVMe/TCP:

- a. Revise la ["Guía de compatibilidad de VMware"](#)



VMware vSphere 7,0 U3 y las versiones posteriores admiten el protocolo NVMe/TCP. Sin embargo, se recomienda VMware vSphere 8,0 y versiones posteriores.

- b. Compruebe si el proveedor de la tarjeta de interfaz de red (NIC) admite la NIC ESXi con el protocolo NVMe/TCP.
  - c. Configure la NIC ESXi para NVMe/TCP según las especificaciones del proveedor de NIC.
  - d. Cuando utilice la versión de VMware vSphere 7, siga las instrucciones del sitio de VMware ["Configure el enlace de VMkernel para el adaptador de NVMe over TCP"](#) para configurar el enlace de puerto NVMe/TCP. Al utilizar la versión VMware vSphere 8, siga ["Configurar NVMe over TCP en ESXi"](#) a , para configurar el enlace de puerto NVMe/TCP.
  - e. Para la versión de VMware vSphere 7, siga las instrucciones de la página ["Habilite los adaptadores de software de NVMe over RDMA o NVMe over TCP"](#) para configurar los adaptadores de software NVMe/TCP. Para la versión VMware vSphere 8, siga ["Añada adaptadores de software NVMe sobre RDMA o NVMe over TCP"](#) para configurar los adaptadores de software NVMe/TCP.
  - f. Ejecute ["Detectar sistemas de almacenamiento y hosts"](#) la acción en el host ESXi. Para obtener más información, consulte ["Cómo configurar NVMe/TCP con vSphere 8,0 Update 1 y ONTAP 9.13,1 para almacenes de datos VMFS"](#).
- Si utiliza el protocolo NVMe/FC, realice los siguientes pasos para configurar el host ESXi:
    - a. Si todavía no está habilitado, habilite NVMe over Fabrics(NVMe-oF) en los hosts ESXi.
    - b. Complete la división en zonas de SCSI.
    - c. Asegúrese de que los hosts ESXi y el sistema ONTAP estén conectados en una capa física y lógica.

Para configurar una SVM de ONTAP para el protocolo FC, consulte ["Configure una SVM para FC"](#) .

Para obtener más información sobre el uso del protocolo NVMe/FC con VMware vSphere 8,0, consulte ["Configuración de host de NVMe-oF para ESXi 8.x con ONTAP"](#) .

Para obtener más información sobre el uso de NVMe/FC con VMware vSphere 7,0, consulte ["Guía de configuración de hosts ONTAP NVMe/FC"](#) y ["TR-4684"](#).

## Pasos

1. Inicie sesión en el cliente de vSphere.
2. Haga clic con el botón derecho en un sistema host, un clúster de host o un centro de datos y seleccione **Herramientas de NetApp ONTAP \* > \*Crear almacén de datos**.
3. Seleccione el tipo de almacén de datos VMFS.
4. Ingrese el nombre del almacén de datos, el tamaño y la información del protocolo en el panel **Nombre y protocolo**. Para agregar el nuevo almacén de datos a un clúster VMFS existente, seleccione el clúster del almacén de datos en Opciones avanzadas.
5. Seleccione Storage VM en el panel **Storage**. Proporcione el **Nombre de grupo iniciador personalizado** en la sección **Opciones avanzadas** según sea necesario. Es posible seleccionar un igroup existente para el almacén de datos o crear un igroup nuevo con un nombre personalizado.

Cuando se selecciona el protocolo NVMe/FC o NVMe/TCP, se crea un nuevo subsistema de espacio de nombres y se utiliza para la asignación de espacios de nombres. Las herramientas ONTAP crean el subsistema de espacio de nombres utilizando el nombre generado automáticamente que incluye el nombre del almacén de datos. Puede cambiar el nombre del subsistema de espacio de nombres en el campo **nombre del subsistema de espacio de nombres personalizado** en las opciones avanzadas del panel **Almacenamiento**.

6. Desde el panel **storage attributes**:

- a. Seleccione **Aggregate** de las opciones desplegadas.



Para los sistemas de almacenamiento ASA r2, la opción **Agregar** no se muestra porque el almacenamiento está desagregado. Al elegir un sistema de almacenamiento ASA r2 de tipo SVM, la página de atributos de almacenamiento muestra las opciones para habilitar QoS.

- b. Las herramientas ONTAP crean una unidad de almacenamiento (LUN/espacio de nombres) con una reserva de espacio reducida según el protocolo seleccionado.



A partir de ONTAP 9.16.1, los sistemas de almacenamiento R2 de ASA admiten hasta 12 nodos por clúster.

- c. Seleccione el **Nivel de servicio de rendimiento** para los sistemas de almacenamiento ASA R2 con 12 nodos SVM que es un clúster heterogéneo. Esta opción no está disponible si la SVM seleccionada es un clúster homogéneo o utiliza un usuario de SVM.

'Any' es el valor de nivel de servicio de rendimiento (PSL) por defecto. Este ajuste crea la unidad de almacenamiento mediante el algoritmo de ubicación equilibrada de ONTAP. Sin embargo, puede seleccionar la opción Performance o Extreme según sea necesario.

- d. Seleccione **Usar volumen existente**, **Activar QoS** opciones según sea necesario, y proporcione los detalles.



En el tipo de almacenamiento ASA r2, la creación o selección de volumen no se aplica a la creación de unidades de almacenamiento (LUN/espacio de nombres). Por lo tanto, estas opciones no se muestran.



No puede utilizar el volumen existente para crear un almacén de datos VMFS con el protocolo NVMe/FC o NVMe/TCP. Cree un nuevo volumen para el almacén de datos VMFS.

7. Revise los detalles del almacén de datos en el panel **Summary** y seleccione **Finish**.



Si crea el almacén de datos en un clúster protegido, se muestra un mensaje de solo lectura que indica que el almacén de datos se está montando en un clúster protegido.

### Resultado

Las herramientas ONTAP crean el almacén de datos VMFS y lo montan en todos los hosts.

## 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.