



# Documentación de ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp  
September 29, 2025

# Tabla de contenidos

Documentación de ONTAP tools for VMware vSphere .....	1
Notas de la versión .....	2
Notas de la versión .....	2
Novedades en las ONTAP tools for VMware vSphere 10.4 .....	2
Comparación de características de las ONTAP tools for VMware vSphere 9 y ONTAP tools for VMware vSphere 10 .....	3
Conceptos .....	5
Descripción general de las ONTAP tools for VMware vSphere .....	5
Conceptos y términos clave .....	5
Control de acceso basado en roles .....	8
Obtenga más información sobre las ONTAP tools for VMware vSphere 10 RBAC .....	8
RBAC con VMware vSphere .....	9
RBAC con ONTAP .....	13
Alta disponibilidad de ONTAP tools for VMware vSphere .....	16
Interfaz de usuario del administrador de herramientas de ONTAP .....	16
Implementar ONTAP tools for VMware vSphere .....	19
Inicio rápido de las ONTAP tools for VMware vSphere .....	19
Flujo de trabajo de implementación de alta disponibilidad (HA) .....	21
Requisitos y límites de configuración de las ONTAP tools for VMware vSphere .....	21
Requisitos del sistema .....	21
Requisitos mínimos de almacenamiento y aplicación .....	22
Requisitos del puerto .....	22
Límites de configuración para implementar ONTAP tools for VMware vSphere .....	25
ONTAP tools for VMware vSphere : Adaptador de replicación de almacenamiento (SRA) .....	25
Antes de empezar... .....	26
Hoja de trabajo de implementación .....	26
Configuración del firewall de red .....	28
Configuración de almacenamiento de ONTAP .....	28
Implementar ONTAP tools for VMware vSphere .....	28
Códigos de error de implementación .....	33
Configurar ONTAP tools for VMware vSphere .....	36
Agregar instancias de vCenter Server .....	36
Registrar el proveedor VASA con una instancia de vCenter Server .....	36
Instalar el complemento NFS VAAI .....	37
Configurar los ajustes del host ESXi .....	38
Configurar las opciones de tiempo de espera y rutas múltiples del servidor ESXi .....	38
Establecer valores de host ESXi .....	39
Configurar roles y privilegios de usuario de ONTAP .....	40
Requisitos de mapeo agregado de SVM .....	41
Crear usuario y rol de ONTAP manualmente .....	41
Actualice las ONTAP tools for VMware vSphere de usuario 10.1 a usuario 10.3 .....	49
Actualice las ONTAP tools for VMware vSphere 10.3 a 10.4 .....	51
Agregar un backend de almacenamiento .....	52

Asociar un backend de almacenamiento con una instancia de vCenter Server . . . . .	53
Configurar el acceso a la red . . . . .	54
Crear un almacén de datos . . . . .	54
Proteger almacenes de datos y máquinas virtuales . . . . .	60
Proteger mediante la protección del clúster de host . . . . .	60
Protéjase utilizando la protección SRA . . . . .	61
Configurar SRA para proteger los almacenes de datos. . . . .	61
Configurar SRA para entornos SAN y NAS . . . . .	61
Configurar SRA para entornos de gran escalabilidad . . . . .	63
Configurar SRA en el dispositivo VMware Live Site Recovery . . . . .	63
Actualizar las credenciales de SRA . . . . .	65
Configurar sitios protegidos y de recuperación . . . . .	65
Configurar recursos de sitios protegidos y de recuperación . . . . .	67
Verificar sistemas de almacenamiento replicados . . . . .	71
Protección en abanico . . . . .	71
Administrar ONTAP tools for VMware vSphere . . . . .	75
Descripción general del panel de control de las ONTAP tools for VMware vSphere . . . . .	75
Interfaz de usuario del administrador de herramientas de ONTAP . . . . .	77
Comprenda los igroups y las políticas de exportación en las ONTAP tools for VMware vSphere . . . . .	78
Políticas de exportación . . . . .	82
Comprender los igroups administrados por las herramientas ONTAP . . . . .	83
Habilitar ONTAP tools for VMware vSphere . . . . .	86
Cambiar las ONTAP tools for VMware vSphere . . . . .	87
Administrar almacenes de datos . . . . .	88
Montar almacenes de datos NFS y VMFS . . . . .	88
Desmontar almacenes de datos NFS y VMFS . . . . .	89
Montar un almacén de datos vVols . . . . .	90
Cambiar el tamaño del almacén de datos NFS y VMFS . . . . .	90
Expandir almacenes de datos vVols . . . . .	90
Reducir el almacén de datos de vVols . . . . .	91
Eliminar almacenes de datos . . . . .	91
Vistas de almacenamiento de ONTAP para almacenes de datos . . . . .	92
Vista de almacenamiento de la máquina virtual . . . . .	93
Administrar los umbrales de almacenamiento . . . . .	93
Administrar backends de almacenamiento . . . . .	93
Descubra el almacenamiento . . . . .	94
Modificar los backends de almacenamiento . . . . .	94
Eliminar backends de almacenamiento . . . . .	94
Vista detallada del backend de almacenamiento . . . . .	95
Administrar instancias de vCenter Server . . . . .	96
Disociar los backends de almacenamiento con la instancia de vCenter Server . . . . .	96
Modificar una instancia de vCenter Server . . . . .	96
Eliminar una instancia de vCenter Server . . . . .	96
Administrar certificados . . . . .	97
Acceda a las ONTAP tools for VMware vSphere . . . . .	99

Descripción general de las ONTAP tools for VMware vSphere .....	99
Configurar el acceso de diagnóstico remoto .....	100
Iniciar SSH en otros nodos .....	101
Actualice las credenciales de vCenter Server y ONTAP .....	101
Informes de herramientas de ONTAP .....	101
Recopilar los archivos de registro .....	102
Administrar máquinas virtuales .....	103
Consideraciones para migrar o clonar máquinas virtuales .....	103
Migrar máquinas virtuales con almacenes de datos NFS y VMFS a almacenes de datos vVols .....	104
Limpieza de VASA .....	104
Conectar o desconectar un disco de datos de una máquina virtual .....	105
Descubra los sistemas de almacenamiento y hosts .....	105
Modificar la configuración del host ESXi mediante las herramientas ONTAP .....	106
Administrar contraseñas .....	107
Cambiar la contraseña del administrador de herramientas de ONTAP .....	107
Restablecer la contraseña del administrador de herramientas de ONTAP .....	107
Restablecer la contraseña del usuario de la aplicación .....	108
Restablecer la contraseña del usuario de la consola de mantenimiento .....	108
Administrar la protección del clúster de host .....	109
Modificar el clúster de host protegido .....	109
Eliminar la protección del clúster de host .....	112
Deshabilitar AutoSupport .....	112
Actualizar la URL del proxy de AutoSupport .....	113
Agregar servidores NTP .....	113
Crear copia de seguridad y recuperar la configuración de las herramientas ONTAP .....	113
Crear una copia de seguridad y descargar el archivo de copia de seguridad .....	114
Recuperar .....	114
Desinstalar las ONTAP tools for VMware vSphere .....	115
Eliminar volúmenes FlexVol .....	116
Actualice las ONTAP tools for VMware vSphere .....	117
Actualización de las ONTAP tools for VMware vSphere 10.x a 10.4 .....	117
Códigos de error de actualización .....	120
Migrar ONTAP tools for VMware vSphere 9.xx a 10.4 .....	125
Migrar de las ONTAP tools for VMware vSphere 9.xx a 10.4 .....	125
Migrar el proveedor VASA y actualizar el SRA .....	125
Pasos para migrar el proveedor VASA .....	125
Pasos para actualizar el adaptador de replicación de almacenamiento (SRA) .....	128
Automatizar utilizando la API REST .....	130
Obtenga más información sobre las ONTAP tools for VMware vSphere 10 REST API .....	130
Fundación de servicios web REST .....	130
Entorno del administrador de herramientas ONTAP .....	131
Detalles de implementación de las ONTAP tools for VMware vSphere 10 .....	131
Cómo acceder a la API REST .....	131
Detalles HTTP .....	132
Autenticación .....	133

Solicitudes sincrónicas y asincrónicas .....	133
Sus primeras ONTAP tools for VMware vSphere 10 .....	134
Antes de empezar .....	134
Paso 1: Adquirir un token de acceso .....	134
Paso 2: Emitir la llamada a la API REST .....	135
Referencia de API para las ONTAP tools for VMware vSphere 10 API REST .....	135
Avisos legales .....	136
Copyright .....	136
Marcas comerciales .....	136
Patentes .....	136
Política de privacidad .....	136
Código abierto .....	136

# Documentación de ONTAP tools for VMware vSphere

# Notas de la versión

## Notas de la versión

Obtenga información sobre las características nuevas y mejoradas disponibles en las ONTAP tools for VMware vSphere 10.4.

Para obtener una lista completa de nuevas funciones y mejoras, consulte [Novedades en las ONTAP tools for VMware vSphere 10.4](#) .

Para obtener más información sobre si la migración de las ONTAP tools for VMware vSphere 9 a las herramientas ONTAP 10.4 es adecuada para su implementación, consulte [Comparación de características de las ONTAP tools for VMware vSphere 9 y ONTAP tools for VMware vSphere 10](#) . Se admite la migración desde las ONTAP tools for VMware vSphere 9.12-D y 9.13-D a las ONTAP tools for VMware vSphere 10.4.

Para obtener más información, consulte la "[Notas de la versión de las ONTAP tools for VMware vSphere 10.4](#)" . Debe iniciar sesión con su cuenta de NetApp o crear una cuenta para acceder a las Notas de la versión.

## Novedades en las ONTAP tools for VMware vSphere 10.4

Conozca las nuevas capacidades disponibles en las ONTAP tools for VMware vSphere 10.4.

Actualizar	Descripción
<a href="#">"Compatibilidad con el sistema ASA r2 con 12 nodos por clúster"</a>	Las ONTAP tools for VMware vSphere 10.4 admiten flujos de trabajo para sistemas de almacenamiento ASA r2 con hasta 12 nodos por clúster, lo que mejora la eficiencia y la escalabilidad de la administración de datos. Admite almacenes de datos vVols con protocolos iSCSI y FC, y almacenes de datos VMFS con protocolos iSCSI, FC y NVMe, lo que proporciona opciones de almacenamiento flexibles y mejoradas.
<a href="#">"Mejoras en la interfaz de usuario del Administrador de herramientas de ONTAP"</a>	Ahora puede habilitar el servidor NTP para una sincronización horaria precisa en todo el entorno y configurar los ajustes de telemetría para monitorear y analizar el rendimiento del sistema desde la interfaz del Administrador de herramientas de ONTAP . Estas configuraciones ya no están disponibles en la consola de mantenimiento.
Capacidades de seguridad mejoradas	Las funciones de seguridad ahora ofrecen protección mejorada y cumplimiento con los estándares de la industria, brindando una experiencia sólida y fácil de usar para ayudar a los administradores a gestionar los entornos VMware de manera más efectiva.
<a href="#">"Capacidades mejoradas de recuperación ante desastres de SRA"</a>	Las ONTAP tools for VMware vSphere 10.4 ahora admiten operaciones de recuperación ante desastres mediante Site Recovery Appliance (SRA) con instantáneas con nombres personalizados, además de copias de instantáneas programadas de SnapMirror .

# Comparación de características de las ONTAP tools for VMware vSphere 9 y ONTAP tools for VMware vSphere 10

Descubra si migrar de las ONTAP tools for VMware vSphere 9 a las ONTAP tools for VMware vSphere 10.1 o versiones posteriores es adecuado para usted.



Para obtener la información de compatibilidad más actualizada, consulte "[Herramienta de matriz de interoperabilidad de NetApp](#)".

Característica	Herramientas ONTAP 9.13	Herramientas ONTAP 10.1	Herramientas ONTAP 10.2 en adelante
Propuesta de valor clave	Optimice y simplifique las operaciones del día 0 al día 2 con capacidades mejoradas de seguridad, cumplimiento y automatización.	Evolución de las herramientas ONTAP 10.x hacia la paridad 9.xx, ampliando al mismo tiempo los límites de alta disponibilidad, rendimiento y escala	Soporte ampliado para incluir FC para VMFS y vVols, y NVMe-oF/FC, NVMe-oF/TCP solo para VMFS. Facilidad de uso para NetApp SnapMirror, configuración sencilla para clústeres de almacenamiento metro vSphere y compatibilidad con VMware Live Site Recovery de tres sitios
Calificación de liberación de ONTAP	ONTAP 9.9.1 a ONTAP 9.16.1	ONTAP 9.12.1 a ONTAP 9.14.1	ONTAP 9.12.1 a ONTAP 9.15.1 para herramientas ONTAP 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 y 9.16.1 para herramientas ONTAP 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 y 9.16.1 para herramientas ONTAP 10.4. Se requiere ONTAP 9.16.1P3 y versiones posteriores para las herramientas ONTAP 10.4 cuando se utilizan sistemas ASA r2.
Compatibilidad con versiones de VMware	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 a VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 a VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 a VMware Live Site Recovery 9.0
Soporte de protocolo	Almacenes de datos NFS y VMFS: NFS (v3 y v4.1), VMFS (iSCSI y FCP) Almacenes de datos vVols : iSCSI, FCP, NVMe/FC, NFS v3	Almacenes de datos NFS y VMFS: NFS (v3 y v4.1), VMFS (iSCSI) Almacenes de datos vVols : iSCSI, NFS v3	Almacenes de datos NFS y VMFS: NFS (v3 y v4.1), VMFS (iSCSI/FCP/NVMe-oF) Almacenes de datos vVols : iSCSI, FCP, NFS v3

<b>Característica</b>	<b>Herramientas ONTAP 9.13</b>	<b>Herramientas ONTAP 10.1</b>	<b>Herramientas ONTAP 10.2 en adelante</b>
Escalabilidad	Hosts y máquinas virtuales: 300 hosts, hasta 10 000 máquinas virtuales Almacenes de datos: 600 NFS, hasta 50 VMFS, hasta 250 vVols vVols: hasta 14 000	Hosts y máquinas virtuales: 600 hosts vVols: hasta 140 000	Hosts y máquinas virtuales: 600 hosts vVols: hasta 140 000
Observabilidad	Paneles de rendimiento, capacidad y cumplimiento del host Informes dinámicos de máquinas virtuales y almacenes de datos	Paneles de control actualizados sobre rendimiento, capacidad y cumplimiento del host Informes dinámicos de máquinas virtuales y almacenes de datos	Paneles de control actualizados sobre rendimiento, capacidad y cumplimiento del host Informes dinámicos de máquinas virtuales y almacenes de datos
Protección de datos	Replicación SRA para VMFS y NFS Replicación basada en FlexVols para vVols Integración SCV e interoperable para respaldo	Replicación de SRA para almacenes de datos iSCSI VMFS y NFS v3	Replicación SRA para almacenes de datos iSCSI VMFS y NFS v3 con protección de tres sitios que combina SMAS y VMware Live Site Recovery.
Soporte del proveedor de VASA	VASA 4.0	VASA 3.0	VASA 3.0

# Conceptos

## Descripción general de las ONTAP tools for VMware vSphere

Las ONTAP tools for VMware vSphere son un conjunto de herramientas para la gestión del ciclo de vida de las máquinas virtuales. Se integra con el ecosistema VMware para ayudar con el aprovisionamiento del almacén de datos y brindar protección básica para las máquinas virtuales. Las ONTAP tools for VMware vSphere son una colección de microservicios escalables horizontalmente y basados en eventos, implementados como un dispositivo virtual abierto (OVA). Esta versión integra la API REST con ONTAP.

Las ONTAP tools for VMware vSphere constan de lo siguiente:

- Funcionalidad de máquina virtual como protección básica y recuperación ante desastres
- Proveedor VASA para la gestión granular de máquinas virtuales
- Gestión de almacenamiento basada en políticas
- Adaptador de replicación de almacenamiento (SRA)

## Conceptos y términos clave

La siguiente sección describe los conceptos y términos clave utilizados en el documento.

### Sistemas ASA r2

Los nuevos sistemas NetApp ASA r2 ofrecen una solución unificada de hardware y software que crea una experiencia simplificada específica para las necesidades de los clientes que solo utilizan SAN. ["Conozca los sistemas de almacenamiento ASA r2"](#) .

### Autoridad de certificación (CA)

CA es una entidad confiable que emite certificados Secure Sockets Layer (SSL).

### Grupo de consistencia (GC)

Un grupo de consistencia es una colección de volúmenes administrados como una sola unidad. Los CG están sincronizados para garantizar la coherencia de los datos en todas las unidades de almacenamiento y volúmenes. En ONTAP, proporcionan una gestión sencilla y una garantía de protección para una carga de trabajo de aplicaciones que abarca múltiples volúmenes. Obtenga más información sobre ["grupos de consistencia"](#) .

### Doble pila

Una red de doble pila es un entorno de red que admite el uso simultáneo de direcciones IPv4 e IPv6.

### Alta disponibilidad (HA)

Los nodos del clúster se configuran en pares de alta disponibilidad para operaciones sin interrupciones.

## Número de unidad lógica (LUN)

Un LUN es un número utilizado para identificar una unidad lógica dentro de una red de área de almacenamiento (SAN). Estos dispositivos direccionables suelen ser discos lógicos a los que se accede a través del protocolo de interfaz de sistema de computadora pequeña (SCSI) o uno de sus derivados encapsulados.

## Espacio de nombres y subsistema NVMe

Un espacio de nombres NVMe es una cantidad de memoria no volátil que se puede formatear en bloques lógicos. Los espacios de nombres son el equivalente a los LUN para los protocolos FC e iSCSI, y un subsistema NVMe es análogo a un igroup. Un subsistema NVMe se puede asociar con iniciadores para que los iniciadores asociados puedan acceder a espacios de nombres dentro del subsistema.

## Administrador de herramientas ONTAP

El Administrador de herramientas de ONTAP proporciona más control sobre las ONTAP tools for VMware vSphere sobre las instancias de vCenter Server administradas y los backends de almacenamiento integrados. Ayuda a administrar instancias de vCenter Server, backends de almacenamiento, certificados, contraseñas y descargas de paquetes de registros.

## Dispositivo virtual abierto (OVA)

OVA es un estándar abierto para empaquetar y distribuir dispositivos virtuales o software que deben ejecutarse en máquinas virtuales.

## Objetivo de punto de recuperación (RPO)

RPO mide la frecuencia con la que realiza copias de seguridad o replica datos. Especifica el punto exacto en el que debe restaurar los datos después de una interrupción para reanudar las operaciones comerciales. Por ejemplo, si una organización tiene un RPO de 4 horas, puede tolerar la pérdida de hasta 4 horas de datos en caso de desastre.

## Sincronización activa de SnapMirror

La sincronización activa de SnapMirror permite que los servicios empresariales sigan funcionando incluso ante una falla total del sitio, permitiendo que las aplicaciones conmuten por error de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos personalizadas para activar una conmutación por error con la sincronización activa de SnapMirror . Obtenga más información sobre ["Sincronización activa de SnapMirror"](#) .

## Backends de almacenamiento

Los backends de almacenamiento son la infraestructura de almacenamiento subyacente que el host ESXi utiliza para almacenar archivos, datos y otros recursos de la máquina virtual. Permiten que el host ESXi acceda y administre datos persistentes, proporcionando la capacidad de almacenamiento y el rendimiento necesarios para un entorno virtualizado.

## Clúster global (backend de almacenamiento)

Los backends de almacenamiento global, disponibles solo con credenciales de clúster ONTAP , se incorporan a través de la interfaz del Administrador de herramientas ONTAP . Se pueden agregar con privilegios mínimos para permitir el descubrimiento de recursos de clúster esenciales necesarios para la administración de vVols . Los clústeres globales son ideales para escenarios de múltiples inquilinos donde se agrega un usuario SVM localmente para la administración de vVols .

## Backend de almacenamiento local

Los backends de almacenamiento local con credenciales de clúster o SVM se agregan a través de la interfaz de usuario de las herramientas ONTAP y están limitados a un vCenter. Al utilizar credenciales de clúster localmente, las SVM asociadas se asignan automáticamente con vCenter para administrar vVols o VMFS. Para la administración de VMFS, incluido SRA, las herramientas ONTAP admiten credenciales SVM sin necesidad de un clúster global.

## Adaptador de replicación de almacenamiento (SRA)

SRA es el software específico del proveedor de almacenamiento instalado dentro del dispositivo VMware Live Site Recovery. El adaptador permite la comunicación entre Site Recovery Manager y un controlador de almacenamiento en el nivel de máquina virtual de almacenamiento (SVM) y la configuración de nivel de clúster.

## Máquina virtual de almacenamiento (SVM)

SVM es la unidad de multitenencia en ONTAP. Al igual que una máquina virtual que se ejecuta en un hipervisor, SVM es una entidad lógica que abstrae recursos físicos. SVM contiene volúmenes de datos y uno o más LIF a través de los cuales sirven datos a los clientes.

## Configuración uniforme y no uniforme

- **Acceso uniforme al host** significa que los hosts de dos sitios están conectados a todas las rutas a los clústeres de almacenamiento en ambos sitios. Los caminos que cruzan los sitios se extienden a lo largo de las distancias.
- **Acceso al host no uniforme** significa que los hosts en cada sitio están conectados solo al clúster en el mismo sitio. Las rutas entre sitios y las rutas estiradas no están conectadas.



El acceso uniforme al host es compatible con cualquier implementación de sincronización activa de SnapMirror ; el acceso no uniforme al host solo es compatible con implementaciones activas/activas simétricas. Obtenga más información sobre ["Descripción general de la sincronización activa de SnapMirror en ONTAP"](#) .

## Sistema de archivos de máquina virtual (VMFS)

VMFS es un sistema de archivos en clúster diseñado para almacenar archivos de máquinas virtuales en entornos VMware vSphere.

## Volúmenes virtuales (vVols)

vVols proporciona una abstracción a nivel de volumen para el almacenamiento utilizado por una máquina virtual. Incluye varios beneficios y proporciona una alternativa al uso de un LUN tradicional. Un almacén de datos vVol generalmente está asociado con un único LUN que actúa como contenedor para los vVols.

## Política de almacenamiento de máquinas virtuales

Las políticas de almacenamiento de VM se crean en vCenter Server en Políticas y perfiles. Para vVols , cree un conjunto de reglas utilizando reglas del proveedor de tipo de almacenamiento vVols de NetApp .

## Recuperación de sitios en vivo de VMware

VMware Live Site Recovery, anteriormente conocido como Site Recovery Manager (SRM), proporciona

continuidad comercial, recuperación ante desastres, migración de sitios y capacidades de prueba no disruptivas para entornos virtuales de VMware.

### **API de VMware vSphere para el reconocimiento de almacenamiento (VASA)**

VASA es un conjunto de API que integran matrices de almacenamiento con vCenter Server para su gestión y administración. La arquitectura se basa en varios componentes, incluido el proveedor VASA, que gestiona la comunicación entre VMware vSphere y los sistemas de almacenamiento.

### **API de almacenamiento de VMware vSphere: Integración de matrices (VAAI)**

VAAI es un conjunto de API que permite la comunicación entre los hosts VMware vSphere ESXi y los dispositivos de almacenamiento. Las API incluyen un conjunto de operaciones primitivas utilizadas por los hosts para descargar operaciones de almacenamiento a la matriz. VAAI puede proporcionar mejoras de rendimiento significativas para tareas que requieren un uso intensivo de almacenamiento.

### **Clúster de almacenamiento vSphere Metro**

vSphere Metro Storage Cluster (vMSC) es una arquitectura que habilita y admite vSphere en una implementación de clúster extendido. Las soluciones vMSC son compatibles con NetApp MetroCluster y SnapMirror Active Sync (anteriormente SMBC). Estas soluciones proporcionan una continuidad empresarial mejorada en caso de falla del dominio. El modelo de resiliencia se basa en sus opciones de configuración específicas. Obtenga más información sobre "[Clúster de almacenamiento VMware vSphere Metro](#)".

### **almacén de datos vVols**

El almacén de datos vVols es una representación lógica del almacén de datos de un contenedor vVols creado y mantenido por un proveedor VASA.

### **RPO cero**

RPO significa objetivo de punto de recuperación, la cantidad de pérdida de datos que se considera aceptable durante un tiempo determinado. RPO cero significa que no es aceptable ninguna pérdida de datos.

## **Control de acceso basado en roles**

### **Obtenga más información sobre las ONTAP tools for VMware vSphere 10 RBAC**

El control de acceso basado en roles (RBAC) es un marco de seguridad para controlar el acceso a los recursos dentro de una organización. RBAC simplifica la administración al definir roles con niveles específicos de autoridad para realizar acciones, en lugar de asignar autorización a usuarios individuales. Los roles definidos se asignan a los usuarios, lo que ayuda a reducir el riesgo de error y simplifica la gestión del control de acceso en toda la organización.

El modelo estándar RBAC consta de varias tecnologías o fases de implementación de complejidad creciente. El resultado es que las implementaciones reales de RBAC, basadas en las necesidades de los proveedores de software y sus clientes, pueden diferir y variar desde relativamente simples a muy complejas.

### **Componentes de RBAC**

En un nivel alto, hay varios componentes que generalmente se incluyen con cada implementación de RBAC.

Estos componentes están vinculados entre sí de diferentes maneras como parte de la definición de los procesos de autorización.

### **Privileges**

Un *privilegio* es una acción o capacidad que se puede permitir o denegar. Puede ser algo simple, como leer un archivo, o una operación más abstracta, específica de un sistema de software. También se pueden definir Privileges para restringir el acceso a los puntos finales de la API REST y a los comandos de la CLI. Toda implementación de RBAC incluye privilegios predefinidos y puede permitir a los administradores crear privilegios personalizados.

### **Roles**

Un *rol* es un contenedor que incluye uno o más privilegios. Los roles generalmente se definen en función de tareas o funciones laborales específicas. Cuando se asigna un rol a un usuario, a este se le otorgan todos los privilegios contenidos en el rol. Y al igual que con los privilegios, las implementaciones incluyen roles predefinidos y generalmente permiten la creación de roles personalizados.

### **Objetos**

Un *objeto* representa un recurso real o abstracto identificado dentro del entorno RBAC. Las acciones definidas a través de los privilegios se realizan en o con los objetos asociados. Dependiendo de la implementación, se pueden otorgar privilegios a un tipo de objeto o a una instancia de objeto específica.

### **Usuarios y grupos**

A los *usuarios* se les asigna o asocia un rol aplicado después de la autenticación. Algunas implementaciones de RBAC permiten que solo se asigne un rol a un usuario, mientras que otras permiten múltiples roles por usuario, quizás con solo un rol activo a la vez. Asignar roles a *grupos* puede simplificar aún más la administración de la seguridad.

### **Permisos**

Un *permiso* es una definición que vincula a un usuario o grupo junto con un rol a un objeto. Los permisos pueden ser útiles con un modelo de objetos jerárquico donde los hijos de la jerarquía pueden heredarlos opcionalmente.

## **Dos entornos RBAC**

Hay dos entornos RBAC distintos que debe tener en cuenta al trabajar con ONTAP tools for VMware vSphere 10.

### **Servidor VMware vCenter**

La implementación de RBAC en VMware vCenter Server se utiliza para restringir el acceso a los objetos expuestos a través de la interfaz de usuario de vSphere Client. Como parte de la instalación de las ONTAP tools for VMware vSphere 10, el entorno RBAC se amplía para incluir objetos adicionales que representan las capacidades de las herramientas ONTAP. El acceso a estos objetos se proporciona a través del complemento remoto. Ver "[Entorno RBAC de vCenter Server](#)" Para más información.

### **Clúster ONTAP**

Las ONTAP tools for VMware vSphere 10 se conectan a un clúster ONTAP a través de la API REST de ONTAP para realizar operaciones relacionadas con el almacenamiento. El acceso a los recursos de almacenamiento se controla a través de un rol de ONTAP asociado con el usuario de ONTAP proporcionado durante la autenticación. Ver "[Entorno RBAC de ONTAP](#)" Para más información.

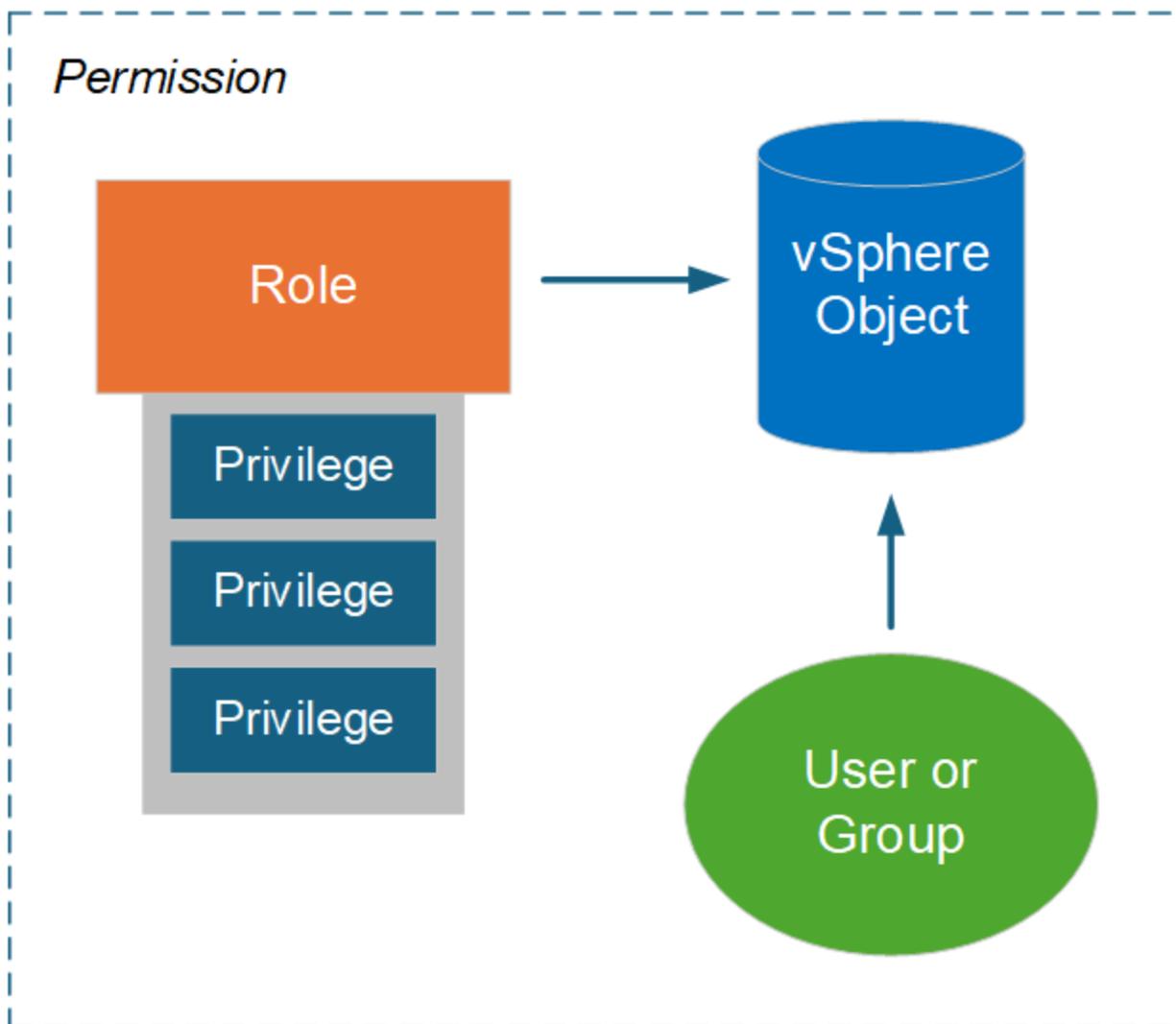
## **RBAC con VMware vSphere**

## Entorno RBAC de vCenter Server con ONTAP tools for VMware vSphere 10

VMware vCenter Server proporciona una capacidad RBAC que le permite controlar el acceso a los objetos de vSphere. Es una parte importante de los servicios de seguridad de autorización y autenticación centralizados de vCenter.

### Ilustración de un permiso de vCenter Server

Un permiso es la base para aplicar el control de acceso en el entorno de vCenter Server. Se aplica a un objeto vSphere con un usuario o grupo incluido en la definición de permiso. En la siguiente figura se proporciona una ilustración de alto nivel de un permiso de vCenter.



### Componentes de un permiso de vCenter Server

Un permiso de vCenter Server es un paquete de varios componentes que se vinculan entre sí cuando se crea el permiso.

## Objetos de vSphere

Los permisos están asociados con objetos de vSphere, como vCenter Server, hosts ESXi, máquinas virtuales, almacenes de datos, centros de datos y carpetas. Según los permisos asignados al objeto, vCenter Server determina qué acciones o tareas puede realizar cada usuario o grupo en el objeto. Para las tareas específicas de las ONTAP tools for VMware vSphere, todos los permisos se asignan y validan en el nivel raíz o de la carpeta raíz de vCenter Server. Ver "[Utilice RBAC con el servidor vCenter](#)" Para más información.

## Privilegios y roles

Hay dos tipos de privilegios de vSphere que se utilizan con las ONTAP tools for VMware vSphere 10. Para simplificar el trabajo con RBAC en este entorno, las herramientas ONTAP proporcionan roles que contienen los privilegios nativos y personalizados necesarios. Los privilegios incluyen:

- Privilegios nativos de vCenter Server

Estos son los privilegios que proporciona vCenter Server.

- Privilegios específicos de las herramientas ONTAP

Estos son privilegios personalizados exclusivos de las ONTAP tools for VMware vSphere.

## Usuarios y grupos

Puede definir usuarios y grupos mediante Active Directory o la instancia local de vCenter Server. En combinación con un rol, puede crear un permiso para un objeto en la jerarquía de objetos de vSphere. El permiso otorga acceso según los privilegios del rol asociado. cuenta que los roles no se asignan directamente a los usuarios de forma aislada. En su lugar, los usuarios y grupos obtienen acceso a un objeto mediante privilegios de rol como parte del permiso general de vCenter Server.

## Utilice vCenter Server RBAC con ONTAP tools for VMware vSphere 10

Hay varios aspectos de las ONTAP tools for VMware vSphere 10 RBAC con vCenter Server que debe considerar antes de usarlo en un entorno de producción.

### Roles de vCenter y la cuenta de administrador

Solo necesita definir y utilizar los roles personalizados de vCenter Server si desea limitar el acceso a los objetos de vSphere y las tareas administrativas asociadas. Si no es necesario limitar el acceso, puede utilizar una cuenta de administrador en su lugar. Cada cuenta de administrador se define con el rol de Administrador en el nivel superior de la jerarquía de objetos. Esto proporciona acceso completo a los objetos de vSphere, incluidos aquellos agregados por las ONTAP tools for VMware vSphere 10.

### Jerarquía de objetos de vSphere

El inventario de objetos de vSphere está organizado en una jerarquía. Por ejemplo, puede moverse hacia abajo en la jerarquía de la siguiente manera:

vCenter Server → Datacenter → Cluster → ESXi host → Virtual Machine

Todos los permisos se validan en la jerarquía de objetos de vSphere, excepto las operaciones del complemento VAAI, que se validan contra el host ESXi de destino.

## Roles incluidos con las ONTAP tools for VMware vSphere 10

Para simplificar el trabajo con vCenter Server RBAC, las ONTAP tools for VMware vSphere proporcionan roles predefinidos adaptados a diversas tareas de administración.



Puede crear nuevos roles personalizados si es necesario. En este caso, debe clonar uno de los roles de herramientas ONTAP existentes y editarlo según sea necesario. Después de realizar los cambios de configuración, los usuarios del cliente vSphere afectados deben cerrar sesión y volver a iniciarla para activar los cambios.

Para ver las ONTAP tools for VMware vSphere, seleccione **Menú** en la parte superior de vSphere Client y haga clic en **Administración** y luego en **Roles** a la izquierda. Hay tres roles predefinidos como se describe a continuación.

### Herramientas NetApp ONTAP tools for VMware vSphere Administrator

Proporciona todos los privilegios nativos de vCenter Server y los privilegios específicos de las herramientas ONTAP necesarios para realizar tareas de administrador de ONTAP tools for VMware vSphere.

### ONTAP tools for VMware vSphere NetApp ONTAP para VMware vSphere de solo lectura

Proporciona acceso de solo lectura a las herramientas ONTAP. Estos usuarios no pueden realizar ninguna acción de las ONTAP tools for VMware vSphere que tenga acceso controlado.

### Herramientas NetApp ONTAP tools for VMware vSphere Provision

Proporciona algunos de los privilegios nativos de vCenter Server y privilegios específicos de las herramientas ONTAP que se requieren para aprovisionar almacenamiento. Puede realizar las siguientes tareas:

- Crear nuevos almacenes de datos
- Administrar almacenes de datos

### Objetos de vSphere y backends de almacenamiento ONTAP

Los dos entornos RBAC trabajan juntos. Al realizar una tarea en la interfaz del cliente vSphere, primero se verifican los roles de las herramientas ONTAP definidos para vCenter Server. Si vSphere permite la operación, se examinan los privilegios del rol de ONTAP. Este segundo paso se realiza en función del rol de ONTAP asignado al usuario cuando se creó y configuró el backend de almacenamiento.

### Trabajar con vCenter Server RBAC

Hay algunas cosas a tener en cuenta al trabajar con los privilegios y permisos de vCenter Server.

### Privilegios requeridos

Para acceder a la interfaz de usuario de las ONTAP tools for VMware vSphere 10, debe tener el privilegio *View* específico de las herramientas ONTAP. Si inicia sesión en vSphere sin este privilegio y hace clic en el ícono de NetApp, las ONTAP tools for VMware vSphere muestran un mensaje de error y le impiden acceder a la interfaz de usuario.

El nivel de asignación en la jerarquía de objetos de vSphere determina a qué partes de la interfaz de usuario puede acceder. Al asignar el privilegio Ver al objeto raíz, podrá acceder a las ONTAP tools for VMware vSphere haciendo clic en el ícono de NetApp.

En lugar de ello, puede asignar el privilegio de visualización a otro nivel de objeto vSphere inferior. Sin embargo, esto limitará los menús de las ONTAP tools for VMware vSphere a los que puede acceder y utilizar.

## Asignación de permisos

Debe utilizar los permisos de vCenter Server si desea limitar el acceso a los objetos y tareas de vSphere. El lugar donde se asigna el permiso en la jerarquía de objetos de vSphere determina las tareas de las ONTAP tools for VMware vSphere 10 que los usuarios pueden realizar.



A menos que necesite definir un acceso más restrictivo, generalmente es una buena práctica asignar permisos en el nivel del objeto raíz o de la carpeta raíz.

Los permisos disponibles con las ONTAP tools for VMware vSphere 10 se aplican a objetos personalizados que no son vSphere, como los sistemas de almacenamiento. Si es posible, debe asignar estos permisos a las ONTAP tools for VMware vSphere porque no hay ningún objeto de vSphere al que pueda asignarlos. Por ejemplo, cualquier permiso que incluya un privilegio "Agregar/Modificar/Quitar sistemas de almacenamiento" de las ONTAP tools for VMware vSphere debe asignarse en el nivel del objeto raíz.

Al definir un permiso en un nivel superior en la jerarquía de objetos, puede configurar el permiso para que se transmita y sea heredado por los objetos secundarios. Si es necesario, puede asignar permisos adicionales a los objetos secundarios que anulen los permisos heredados del objeto principal.

Puede modificar un permiso en cualquier momento. Si cambia alguno de los privilegios dentro de un permiso, los usuarios asociados con el permiso deben cerrar sesión en vSphere y volver a iniciarla para habilitar el cambio.

## RBAC con ONTAP

### Entorno RBAC de ONTAP con ONTAP tools for VMware vSphere 10

ONTAP proporciona un entorno RBAC sólido y extensible. Puede utilizar la capacidad RBAC para controlar el acceso al almacenamiento y a las operaciones del sistema tal como se expone a través de la API REST y la CLI. Es útil estar familiarizado con el entorno antes de usarlo con una implementación de ONTAP tools for VMware vSphere 10.

#### Descripción general de las opciones administrativas

Hay varias opciones disponibles al usar ONTAP RBAC dependiendo de su entorno y sus objetivos. A continuación se presenta una visión general de las principales decisiones administrativas. Ver también ["Automatización de ONTAP : Descripción general de la seguridad de RBAC"](#) Para más información.



ONTAP RBAC está diseñado para un entorno de almacenamiento y es más simple que la implementación de RBAC proporcionada con vCenter Server. Con ONTAP, asignas un rol directamente al usuario. No es necesario configurar permisos explícitos, como los que se usan con vCenter Server, con ONTAP RBAC.

#### Tipos de roles y privilegios

Se requiere un rol ONTAP al definir un usuario ONTAP . Hay dos tipos de roles en ONTAP :

- DESCANSAR

Los roles REST se introdujeron con ONTAP 9.6 y generalmente se aplican a los usuarios que acceden a ONTAP a través de la API REST. Los privilegios incluidos en estos roles se definen en términos de acceso a los puntos finales de la API REST de ONTAP y las acciones asociadas.

- Tradicional

Estos son los roles heredados incluidos antes de ONTAP 9.6. Siguen siendo un aspecto fundamental del RBAC. Los privilegios se definen en términos de acceso a los comandos CLI de ONTAP .

Si bien los roles REST se introdujeron más recientemente, los roles tradicionales tienen algunas ventajas. Por ejemplo, se pueden incluir opcionalmente parámetros de consulta adicionales para que los privilegios definan con mayor precisión los objetos a los que se aplican.

### **Alcance**

Los roles de ONTAP se pueden definir con uno de dos alcances diferentes. Se pueden aplicar a un SVM de datos específico (nivel SVM) o a todo el clúster ONTAP (nivel de clúster).

### **Definiciones de roles**

ONTAP proporciona un conjunto de roles predefinidos tanto a nivel de clúster como de SVM. También puedes definir roles personalizados.

### **Trabajar con roles REST de ONTAP**

Hay varias consideraciones al utilizar los roles REST de ONTAP incluidos con las ONTAP tools for VMware vSphere 10.

### **Mapeo de roles**

Independientemente de si se utiliza un rol tradicional o REST, todas las decisiones de acceso a ONTAP se toman en función del comando CLI subyacente. Pero debido a que los privilegios en un rol REST se definen en términos de los puntos finales de la API REST, ONTAP necesita crear un rol tradicional *mapeado* para cada uno de los roles REST. Por lo tanto, cada rol REST se asigna a un rol tradicional subyacente. Esto permite que ONTAP tome decisiones de control de acceso de manera consistente independientemente del tipo de rol. No es posible modificar los roles mapeados en paralelo.

### **Definición de un rol REST mediante privilegios CLI**

Debido a que ONTAP siempre usa los comandos CLI para determinar el acceso en un nivel base, es posible expresar un rol REST usando privilegios de comandos CLI en lugar de puntos finales REST. Una ventaja de este enfoque es la granularidad adicional disponible con los roles tradicionales.

### **Interfaz administrativa al definir roles de ONTAP**

Puede crear usuarios y roles con la CLI de ONTAP y la API REST. Sin embargo, es más conveniente utilizar la interfaz del Administrador del sistema junto con el archivo JSON disponible a través del Administrador de herramientas de ONTAP . Ver "[Utilice ONTAP RBAC con ONTAP tools for VMware vSphere 10](#)" Para más información.

### **Utilice ONTAP RBAC con ONTAP tools for VMware vSphere 10**

Hay varios aspectos de las ONTAP tools for VMware vSphere 10 RBAC con ONTAP que debe considerar antes de usarlo en un entorno de producción.

### **Descripción general del proceso de configuración**

Las ONTAP tools for VMware vSphere 10 incluyen soporte para crear un usuario ONTAP con un rol personalizado. Las definiciones están empaquetadas en un archivo JSON que puedes cargar en el clúster ONTAP . Puede crear el usuario y adaptar el rol a su entorno y necesidades de seguridad.

A continuación se describen detalladamente los principales pasos de configuración. Referirse a "[Configurar](#)

[roles y privilegios de usuario de ONTAP](#)" Para más detalles.

### 1. Preparar

Debe tener credenciales administrativas tanto para el Administrador de herramientas de ONTAP como para el clúster de ONTAP .

### 2. Descargar el archivo de definición JSON

Después de iniciar sesión en la interfaz de usuario del Administrador de herramientas de ONTAP , puede descargar el archivo JSON que contiene las definiciones de RBAC.

### 3. Crear un usuario de ONTAP con un rol

Después de iniciar sesión en System Manager, puede crear el usuario y el rol:

1. Seleccione **Clúster** a la izquierda y luego **Configuración**.
2. Desplácese hacia abajo hasta **Usuarios y roles** y haga clic en **→** .
3. Seleccione **Agregar** en **Usuarios** y seleccione **Productos de virtualización**.
4. Seleccione el archivo JSON en su estación de trabajo local y cárguelo.

### 4. Configurar el rol

Como parte de la definición del rol, es necesario tomar varias decisiones administrativas. Ver [Configurar el rol mediante el Administrador del sistema](#) Para más detalles.

#### Configurar el rol mediante el Administrador del sistema

Después de comenzar a crear un nuevo usuario y rol con System Manager y haber cargado el archivo JSON, puede personalizar el rol según su entorno y sus necesidades.

#### Configuración de usuarios y roles principales

Las definiciones de RBAC están empaquetadas como varias capacidades de producto, incluidas combinaciones de VSC, VASA Provider y SRA. Debe seleccionar el entorno o los entornos donde necesita compatibilidad con RBAC. Por ejemplo, si desea que los roles admitan la capacidad de complemento remoto, seleccione VSC. También deberá elegir el nombre de usuario y la contraseña asociada.

#### Privilegios

Los privilegios de rol se organizan en cuatro conjuntos según el nivel de acceso necesario al almacenamiento de ONTAP . Los privilegios en los que se basan los roles incluyen:

- Descubrimiento

Esta función le permite agregar sistemas de almacenamiento.

- Crear almacenamiento

Esta función le permite crear almacenamiento. También incluye todos los privilegios asociados con el rol de descubrimiento.

- Modificar el almacenamiento

Esta función le permite modificar el almacenamiento. También incluye todos los privilegios asociados con el descubrimiento y la creación de roles de almacenamiento.

- Destruir almacenamiento

Esta función le permite destruir el almacenamiento. También incluye todos los privilegios asociados con el descubrimiento, la creación de almacenamiento y la modificación de roles de almacenamiento.

### Generar el usuario con un rol

Después de haber seleccionado las opciones de configuración para su entorno, haga clic en **Agregar** y ONTAP creará el usuario y el rol. El nombre del rol generado es una concatenación de los siguientes valores:

- Valor de prefijo constante definido en el archivo JSON (por ejemplo, "OTV\_10")
- Capacidad del producto que seleccionó
- Lista de los conjuntos de privilegios.

### Ejemplo

OTV\_10\_VSC\_Discovery\_Create

El nuevo usuario se agregará a la lista en la página "Usuarios y roles". Tenga en cuenta que se admiten los métodos de inicio de sesión de usuario HTTP y ONTAPI.

## Alta disponibilidad de ONTAP tools for VMware vSphere

Las ONTAP tools for VMware vSphere admiten una configuración de alta disponibilidad (HA) para ayudar a proporcionar una funcionalidad ininterrumpida de las ONTAP tools for VMware vSphere durante una falla.

La solución de alta disponibilidad (HA) permite una rápida recuperación ante interrupciones causadas por:

- Fallo del host



Solo se admite falla de un solo nodo.

- Fallo de red
- Fallo de la máquina virtual (fallo del sistema operativo invitado)
- Fallo de la aplicación (herramientas ONTAP )

No se requiere configuración adicional para que las ONTAP tools for VMware vSphere proporcionen alta disponibilidad (HA).



Las ONTAP tools for VMware vSphere no son compatibles con vCenter HA.

Para habilitar la función HA, la incorporación activa de CPU y la conexión activa de memoria deben habilitarse durante la implementación o más tarde en las ONTAP tools for VMware vSphere .

## Interfaz de usuario del administrador de herramientas de ONTAP

Las ONTAP tools for VMware vSphere son un sistema multiinquilino que puede

administrar múltiples instancias de vCenter Server. El administrador de herramientas de ONTAP proporciona más control al administrador de ONTAP tools for VMware vSphere sobre las instancias de vCenter Server administradas y los backends de almacenamiento incorporados.

El administrador de herramientas de ONTAP ayuda en:

- Administración de instancias de vCenter Server: agregue y administre instancias de vCenter Server a las herramientas de ONTAP .
- Administración del backend de almacenamiento: agregue y administre clústeres de almacenamiento de ONTAP a las ONTAP tools for VMware vSphere y asígneles a instancias de vCenter Server integradas a nivel mundial.
- Descargas de paquetes de registros: recopile archivos de registro para ONTAP tools for VMware vSphere.
- Gestión de certificados: cambie el certificado autofirmado a un certificado CA personalizado y renueve o actualice todos los certificados del proveedor VASA y las herramientas ONTAP .
- Gestión de contraseñas: restablece la contraseña de la aplicación OVA del usuario.

Para acceder al Administrador de herramientas de ONTAP , inicie

<https://<ONTAPtoolsIP>:8443/virtualization/ui/> desde el navegador e inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.

La sección de descripción general del Administrador de herramientas de ONTAP ayuda a administrar la configuración del dispositivo, como la administración de servicios, el aumento del tamaño de los nodos y la habilitación de alta disponibilidad (HA). También puede monitorear la información general de las herramientas ONTAP relacionadas con los nodos, como el estado, los detalles de la red y las alertas.

The screenshot displays the ONTAP tools Manager interface. The top navigation bar includes the ONTAP logo, the text 'ONTAP tools Manager', a refresh icon, and the user 'Administrator'. A left sidebar contains navigation links for Overview, Alerts, Jobs, Storage backends, vCenters, Log bundles, Certificates, and Settings. The main content area is titled 'Overview' and features an 'EDIT APPLIANCE SETTINGS' button. The 'Appliance' section shows a 'Healthy' status with a green checkmark and lists configuration details: Size: Small, HA: Enabled, VASA provider: Enabled, and SRA: Enabled. The 'Alerts' section, filtered for the 'Last 24 hours', shows 3 Error alerts (red exclamation mark), 2 Warning alerts (orange triangle), and 5 Info alerts (blue 'i'). Below this, the 'ONTAP tools nodes' section displays three nodes: nodename\_01, nodename\_02, and nodename\_03, each with a 'demo\_vm' instance and an 'Online' status. Each node card includes a 'VIEW DETAILS' link.

Tarjeta	Descripción
Tarjeta de electrodomésticos	La tarjeta del dispositivo proporciona el estado general del dispositivo de herramientas ONTAP . Muestra los detalles de configuración del dispositivo y el estado de los servicios habilitados. Para obtener información adicional sobre el dispositivo de herramientas ONTAP , seleccione el enlace <b>Ver detalles</b> . Cuando un trabajo de acción de edición de configuración del dispositivo está en progreso, el portlet del dispositivo muestra el estado y los detalles del trabajo.
Tarjeta de alertas	La tarjeta Alertas enumera las alertas de las herramientas ONTAP por tipo, incluidas las alertas a nivel de nodo de HA. Puede ver la lista de alertas seleccionando el texto de recuento (hipervínculo). El enlace lo dirige a la página de visualización de alertas filtradas por el tipo seleccionado.
vCenters	La tarjeta vCenter muestra el estado de salud de los vCenters en el sistema.
Backends de almacenamiento	La tarjeta de backends de almacenamiento muestra el estado de salud de los backends de almacenamiento en el sistema.
Tarjeta de nodos de herramientas ONTAP	La tarjeta de nodos de herramientas ONTAP muestra la lista de nodos con el nombre del nodo, el nombre de la máquina virtual del nodo, el estado y todos los datos relacionados con la red. Puede seleccionar <b>Ver detalles</b> para ver los detalles adicionales relacionados con el nodo seleccionado. [NOTA] En una configuración que no es HA, solo se muestra un nodo. En la configuración de HA, se muestran tres nodos.

# Implementar ONTAP tools for VMware vSphere

## Inicio rápido de las ONTAP tools for VMware vSphere

Configure las ONTAP tools for VMware vSphere con esta sección de inicio rápido.

Inicialmente, implementará ONTAP tools for VMware vSphere como una configuración de nodo único de tamaño pequeño que proporciona servicios básicos para soportar almacenes de datos NFS y VMFS. Si necesita ampliar su configuración para usar almacenes de datos vVols y alta disponibilidad (HA), lo hará después de finalizar este flujo de trabajo. Para obtener más información, consulte la ["Flujo de trabajo de implementación de HA"](#).

1

### Planifique su implementación

Verifique que las versiones de sus hosts vSphere, ONTAP y ESXi sean compatibles con la versión de las herramientas de ONTAP. Asigne suficiente CPU, memoria y espacio en disco. Según sus reglas de seguridad, podría necesitar configurar firewalls u otras herramientas de seguridad para permitir el tráfico de red.

Asegúrese de que vCenter Server esté instalado y sea accesible.

- ["Herramienta de matriz de interoperabilidad"](#)
- ["Requisitos y límites de configuración de las ONTAP tools for VMware vSphere"](#)
- ["Antes de empezar"](#)

2

### Implementar ONTAP tools for VMware vSphere

Inicialmente, implementará las ONTAP tools for VMware vSphere como una configuración pequeña de un solo nodo que proporciona servicios básicos para almacenes de datos NFS y VMFS. Si planea ampliar su configuración para usar almacenes de datos vVols y alta disponibilidad (HA), lo hará después de finalizar este flujo de trabajo. Para ampliar a una configuración de alta disponibilidad, asegúrese de que la adición de CPU y la conexión de memoria en caliente estén habilitadas.

- ["Implementar ONTAP tools for VMware vSphere"](#)

3

### Agregar instancias de vCenter Server

Agregue instancias de vCenter Server a las ONTAP tools for VMware vSphere para configurar, administrar y proteger almacenes de datos virtuales en el entorno de vCenter Server.

- ["Agregar instancias de vCenter Server"](#)

4

### Configurar roles y privilegios de usuario de ONTAP

Configure nuevos roles y privilegios de usuario para administrar backends de almacenamiento utilizando el archivo JSON proporcionado con las ONTAP tools for VMware vSphere.

- ["Configurar roles y privilegios de usuario de ONTAP"](#)

**5**

### **Configurar los backends de almacenamiento**

Agregue un backend de almacenamiento a un clúster ONTAP . Para configuraciones de múltiples inquilinos donde vCenter actúa como inquilino con un SVM asociado, utilice el Administrador de herramientas de ONTAP para agregar el clúster. Asocie el backend de almacenamiento con vCenter Server para asignarlo globalmente a la instancia de vCenter Server incorporada.

Agregue los backends de almacenamiento local con credenciales de clúster o SVM mediante la interfaz de usuario de las herramientas ONTAP . Estos backends de almacenamiento están limitados a un único vCenter. Al utilizar credenciales de clúster localmente, las SVM asociadas se asignan automáticamente al vCenter para administrar vVols o VMFS. Para la administración de VMFS, incluido SRA, las herramientas ONTAP admiten credenciales SVM sin necesidad de un clúster global.

- ["Agregar un backend de almacenamiento"](#)
- ["Asociar el backend de almacenamiento con una instancia de vCenter Server"](#)

**6**

### **Actualice los certificados si está trabajando con varias instancias de vCenter Server**

Al trabajar con varias instancias de vCenter Server, actualice el certificado autofirmado a un certificado firmado por una autoridad de certificación (CA).

- ["Administrar certificados"](#)

**7**

### **(Opcional) Configurar la protección SRA**

Habilite la capacidad de SRA para configurar la recuperación ante desastres y proteger almacenes de datos NFS o VMFS.

- ["Habilitar ONTAP tools for VMware vSphere"](#)
- ["Configurar SRA en el dispositivo VMware Live Site Recovery"](#)

**8**

### **(Opcional) Habilitar la protección de sincronización activa de SnapMirror**

Configure las ONTAP tools for VMware vSphere para administrar la protección del clúster de host para la sincronización activa de SnapMirror . Realice el peering de clúster ONTAP y SVM en sistemas ONTAP para usar la sincronización activa de SnapMirror . Esto se aplica únicamente a almacenes de datos VMFS.

- ["Proteger mediante la protección del clúster de host"](#)

**9**

### **Configure la copia de seguridad y la recuperación para sus ONTAP tools for VMware vSphere**

Programar copias de seguridad de sus ONTAP tools for VMware vSphere que pueda usar para recuperar la configuración en caso de una falla.

- ["Crear copia de seguridad y recuperar la configuración de las herramientas ONTAP"](#)

# Flujo de trabajo de implementación de alta disponibilidad (HA)

Si utiliza almacenes de datos vVols , debe ampliar la implementación inicial de las herramientas ONTAP a una configuración de alta disponibilidad (HA) y habilitar los servicios del proveedor VASA.

1

## Ampliar la implementación

Puede ampliar las ONTAP tools for VMware vSphere para aumentar la cantidad de nodos en la implementación y cambiar la configuración a una configuración de alta disponibilidad.

- ["Cambiar las ONTAP tools for VMware vSphere"](#)

2

## Habilitar servicios

Para configurar los almacenes de datos vVols , debe habilitar el servicio del proveedor VASA. Registre el proveedor VASA con vCenter y asegúrese de que sus políticas de almacenamiento cumplan con los requisitos de alta disponibilidad, incluidas las configuraciones de red y almacenamiento adecuadas.

Habilite los servicios SRA para utilizar las herramientas ONTAP Adaptador de replicación de almacenamiento (SRA) para VMware Site Recovery Manager (SRM) o VMware Live Site Recovery (VLSR).

- ["Habilitar los servicios de proveedor VASA y SRA"](#)

3

## Actualizar los certificados

Si utiliza almacenes de datos vVol con varias instancias de vCenter Server, actualice el certificado autofirmado a un certificado firmado por una autoridad de certificación (CA).

- ["Administrar certificados"](#)

## Requisitos y límites de configuración de las ONTAP tools for VMware vSphere

Antes de implementar las ONTAP tools for VMware vSphere, debe familiarizarse con los requisitos de espacio para el paquete de implementación y algunos requisitos básicos del sistema host.

Puede utilizar ONTAP tools for VMware vSphere con VMware vCenter Server Virtual Appliance (vCSA). Debe implementar ONTAP tools for VMware vSphere en un cliente vSphere compatible que incluya el sistema ESXi.

### Requisitos del sistema

- **Requisitos de espacio del paquete de instalación por nodo**
  - 15 GB para instalaciones con aprovisionamiento ligero
  - 348 GB para instalaciones con aprovisionamiento grueso

- **Requisitos de tamaño del sistema host** La memoria recomendada según el tamaño de la implementación se muestra en la siguiente tabla. Para implementar alta disponibilidad (HA), necesitará tres veces el tamaño del dispositivo especificado en la tabla.

Tipo de despliegue	CPU por nodo	Memoria (GB) por nodo	Espacio en disco (GB) provisionado en grueso por nodo
Pequeño	9	18	350
Medio	13	26	350
NOTA grande: La implementación grande es solo para configuración de alta disponibilidad.	17	34	350



Cuando la copia de seguridad está habilitada, cada clúster de herramientas ONTAP necesita otros 50 GB de espacio en el almacén de datos donde se implementan las máquinas virtuales. Por lo tanto, la modalidad sin alta disponibilidad requiere 400 GB, y la modalidad con alta disponibilidad requiere 1100 GB de espacio en total.

## Requisitos mínimos de almacenamiento y aplicación

Almacenamiento, host y aplicaciones	Requisitos de versión
ONTAP	9.14.1, 9.15.1, 9.16.0, 9.16.1 y 9.16.1P3 FAS, ASA Serie A, ASA Serie C, AFF Serie A, AFF Serie C y ASA r2.
Hosts ESXi compatibles con herramientas ONTAP	7.0.3 en adelante
Herramientas ONTAP compatibles con vCenter Server	7.0U3 en adelante
Proveedor de VASA	3,0
Solicitud OVA	10,4
Host ESXi para implementar la máquina virtual de herramientas ONTAP	7.0U3 y 8.0U3
vCenter Server para implementar la máquina virtual de herramientas ONTAP	7.0 y 8.0



A partir de las ONTAP tools for VMware vSphere 10.4, el hardware de la máquina virtual cambia de la versión 10 a la 17.

La herramienta Matriz de interoperabilidad (IMT) contiene la información más reciente sobre las versiones compatibles de ONTAP, vCenter Server, hosts ESXi y aplicaciones complementarias.

["Herramienta de matriz de interoperabilidad"](#)

## Requisitos del puerto

La siguiente tabla describe los puertos de red que utiliza NetApp y sus funciones. Asegúrese de que estos

puertos estén abiertos y accesibles para facilitar el correcto funcionamiento y la comunicación dentro del sistema. Asegúrese de que las configuraciones de red necesarias permitan el tráfico en estos puertos para que los servicios asociados funcionen correctamente. Según sus políticas de seguridad, podría necesitar configurar firewalls u otros dispositivos de seguridad para permitir este tráfico dentro de su red.

Puerto	Protocolo	Descripción
8143	TCP	Conexiones HTTP/HTTPS para herramientas ONTAP .
8043	TCP	Conexiones HTTP/HTTPS para herramientas ONTAP .
9060	TCP	Conexiones HTTP/HTTPS para herramientas ONTAP .
22	TCP	Ansible utiliza este puerto SSH para la comunicación durante el aprovisionamiento del clúster. Este puerto es necesario para funcionalidades como cambiar la contraseña del usuario de mantenimiento, los mensajes de estado y para actualizar valores en los tres nodos en caso de configuración de HA.
443	TCP	Este es el puerto de paso para la comunicación entrante para el servicio del proveedor VASA. El certificado autofirmado del proveedor VASA y el certificado CA personalizado están alojados en este puerto.
8443	TCP	Este puerto aloja la documentación de la API a través de Swagger y la aplicación de interfaz de usuario Manager.
2379	TCP	Este es el puerto predeterminado para solicitudes de clientes como obtener, colocar, eliminar o buscar claves en el almacén de valores de clave etcd.
2380	TCP	Este es el puerto predeterminado para la comunicación de servidor a servidor para el clúster etcd utilizado para el algoritmo de consenso raft del que se basa etcd para la replicación y la consistencia de los datos.
7472	TCP/UDP	Este es el puerto del servicio de métricas de Prometheus.

7946	TCP/UDP	Este puerto se utiliza para el descubrimiento de la red de contenedores de Docker.
9083	TCP	Este puerto es un puerto de servicio utilizado internamente para el servicio del proveedor VASA.
1162	UDP	Este es el puerto de paquetes de trampa SNMP.
6443	TCP	Fuente: Nodos de agentes RKE2. Destino: nodos del servidor REK2. Descripción: API de Kubernetes
9345	TCP	Fuente: Nodos de agentes RKE2. Destino: nodos del servidor REK2. Descripción: API de supervisor REK2
8472	TCP+UDP	Todos los nodos deben poder comunicarse con otros nodos a través del puerto UDP 8472 cuando se utiliza VXLAN de franela. Fuente: todos los nodos RKE2. Destino: todos los nodos REK2. Descripción: Canal CNI con VXLAN
10250	TCP	Fuente: todos los nodos RKE2. Destino: todos los nodos REK2. Descripción: Métricas de Kubelet
30000-32767	TCP	Fuente: todos los nodos RKE2. Destino: todos los nodos REK2. Descripción: Rango de puertos NodePort
123	TCP	Ntpd utiliza este puerto para realizar la validación del servidor NTP.
137-139	TCP/UDP	Paquetes compartidos SMB/Windows.
6789	TCP	Monitor cefalométrico (MON)
3300	TCP	Monitor cefalométrico (MON)
6800-7300	TCP	Administradores Ceph, OSD y sistemas de archivos (MDS).
80	TCP	Puerta de enlace Ceph RADOS (RGW)
9080	TCP	Conexiones VP HTTP/HTTPS (solo desde 127.0.0.0/8 para IPv4 o ::1/128 para IPv6).

## Límites de configuración para implementar ONTAP tools for VMware vSphere

Puede utilizar la siguiente tabla como guía para configurar las ONTAP tools for VMware vSphere.

Despliegue	Tipo	Número de vVols	Número de hosts
No HA	Pequeño (S)	~12 mil	32
No HA	Mediano (M)	~24K	64
Alta disponibilidad	Pequeño (S)	~24K	64
Alta disponibilidad	Mediano (M)	~50k	128
Alta disponibilidad	Grande (L)	~100k	256 [NOTA] La cantidad de hosts en la tabla muestra la cantidad total de hosts de varios vCenters.

## ONTAP tools for VMware vSphere : Adaptador de replicación de almacenamiento (SRA)

La siguiente tabla muestra los números admitidos por instancia de VMware Live Site Recovery mediante ONTAP tools for VMware vSphere.

Tamaño de implementación de vCenter	Pequeño	Medio
Número total de máquinas virtuales configuradas para protección mediante replicación basada en matrices	2000	5000
Número total de grupos de protección de replicación basados en matrices	250	250
Número total de grupos de protección por plan de recuperación	50	50
Número de almacenes de datos replicados	255	255
Número de máquinas virtuales	4000	7000

La siguiente tabla muestra la cantidad de VMware Live Site Recovery y las ONTAP tools for VMware vSphere .

Número de instancias de VMware Live Site Recovery	* Tamaño de implementación de las herramientas ONTAP *
Hasta 4	Pequeño
4 a 8	Medio
Más de 8	Grande

Para más información, consulte "[Límites operativos de VMware Live Site Recovery](#)".

## Antes de empezar...

Asegúrese de que se cumplan los siguientes requisitos antes de continuar con la implementación:

Requisitos	Tu estado
La versión de vSphere, la versión de ONTAP y la versión del host ESXi son compatibles con la versión de las herramientas ONTP.	<input type="checkbox"/> Sí <input type="checkbox"/> No
El entorno de vCenter Server está instalado y configurado	<input type="checkbox"/> Sí <input type="checkbox"/> No
Se elimina la caché del navegador	<input type="checkbox"/> Sí <input type="checkbox"/> No
Tienes las credenciales del servidor vCenter principal	<input type="checkbox"/> Sí <input type="checkbox"/> No
Tiene las credenciales de inicio de sesión para la instancia de vCenter Server, a la que se conectarán las ONTAP tools for VMware vSphere después de la implementación para el registro.	<input type="checkbox"/> Sí <input type="checkbox"/> No
El nombre de dominio en el que se emite el certificado se asigna a la dirección IP virtual en una implementación de varios vCenter donde los certificados CA personalizados son obligatorios.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Ha ejecutado la comprobación nslookup en el nombre de dominio para verificar si el dominio se está resolviendo en la dirección IP deseada.	<input type="checkbox"/> Sí <input type="checkbox"/> No
El certificado se crea con el nombre de dominio y la dirección IP de las herramientas ONTAP .	<input type="checkbox"/> Sí <input type="checkbox"/> No
Se puede acceder a la aplicación de herramientas ONTAP y a los servicios internos desde vCenter Server.	<input type="checkbox"/> Sí <input type="checkbox"/> No
Al utilizar SVM multiinquilino, tiene un LIF de administración de SVM en cada SVM.	<input type="checkbox"/> Sí <input type="checkbox"/> No

## Hoja de trabajo de implementación

### Para implementación de un solo nodo

Utilice la siguiente hoja de trabajo para recopilar la información necesaria para las ONTAP tools for VMware vSphere :

Requisito	Tu valor
Dirección IP para la aplicación de herramientas ONTAP . Esta es la dirección IP para acceder a la interfaz web de las herramientas ONTAP	

Requisito	Tu valor
Dirección IP virtual de herramientas ONTAP para comunicación interna. Esta dirección IP se utiliza para la comunicación interna en una configuración con múltiples instancias de herramientas ONTAP . Esta dirección IP no debe ser la misma que la dirección IP de la aplicación de herramientas ONTAP .	
Nombre de host DNS para el primer nodo	
Servidor DNS primario	
Servidor DNS secundario	
Dominio de búsqueda DNS	
Dirección IPv4 para el primer nodo. Es una dirección IPv4 única para la interfaz de administración de nodos en la red de administración.	
Máscara de subred para la dirección IPv4	
Puerta de enlace predeterminada para la dirección IPv4	
Dirección IPv6 (opcional)	
Longitud del prefijo IPv6 (opcional)	
Puerta de enlace para la dirección IPv6 (opcional)	



Cree registros DNS para todas las direcciones IP mencionadas anteriormente. Antes de asignar nombres de host, asíguelos a las direcciones IP libres en el DNS. Todas las direcciones IP deben estar en la misma VLAN seleccionada para la implementación.

### Para implementación de alta disponibilidad (HA)

Además de los requisitos de implementación de un solo nodo, necesitará la siguiente información para la implementación de HA:

Requisito	Tu valor
Servidor DNS primario	
Servidor DNS secundario	
Dominio de búsqueda DNS	
Nombre de host DNS para el segundo nodo	
Dirección IP del segundo nodo	
Nombre de host DNS para el tercer nodo	
Dirección IP del tercer nodo	

## Configuración del firewall de red

Abra los puertos necesarios para las direcciones IP en el firewall de su red. Las herramientas ONTAP deben poder llegar a este LIF a través del puerto 443. Referirse a "[Requisitos del puerto](#)" Para obtener las últimas actualizaciones.

## Configuración de almacenamiento de ONTAP

Para garantizar una integración perfecta del almacenamiento de ONTAP con las ONTAP tools for VMware vSphere, tenga en cuenta las siguientes configuraciones:

- Si está utilizando Fibre Channel (FC) para la conectividad de almacenamiento, configure la zonificación en sus conmutadores FC para conectar los hosts ESXi con los LIF FC de la SVM. "[Obtenga más información sobre la zonificación FC y FCoE con los sistemas ONTAP](#)"
- Para utilizar la replicación de SnapMirror administrada por herramientas de ONTAP, el administrador de almacenamiento de ONTAP debe crear "[Relaciones entre pares del clúster ONTAP](#)" y "[Relaciones entre pares de SVM entre clústeres de ONTAP](#)" en ONTAP antes de usar SnapMirror.

## Implementar ONTAP tools for VMware vSphere

Las ONTAP tools for VMware vSphere se implementan como un único nodo pequeño con servicios básicos para soportar almacenes de datos NFS y VMFS. El proceso de implementación de las herramientas ONTAP puede tardar hasta 45 minutos.

### Antes de empezar

Una biblioteca de contenido en VMware es un contenedor que almacena plantillas de máquinas virtuales, plantillas de vApp y otros tipos de archivos. La implementación con biblioteca de contenido proporciona una experiencia fluida, ya que no depende de la conectividad de red.



Debe almacenar la biblioteca de contenido en un almacén de datos compartido para que todos los hosts dentro de un clúster puedan acceder a ella. Cree una biblioteca de contenido para almacenar el OVA antes de configurar el dispositivo con la configuración HA. No elimine la plantilla de la biblioteca de contenido después de la implementación.



Para habilitar la implementación de HA más adelante, no implemente la máquina virtual que aloja las herramientas ONTAP directamente en un host ESXi. En su lugar, impleméntelo en un clúster o grupo de recursos.

Si no tienes una biblioteca de contenido, sigue estos pasos para crear una:

**Crear una biblioteca de contenido** Si planea utilizar solo una implementación pequeña de un solo nodo, no es necesario crear una biblioteca de contenido.

1. Descargue el archivo que contiene los binarios (.ova) y los certificados firmados para las ONTAP tools for VMware vSphere desde "[Sitio de soporte de NetApp](#)".
2. Inicie sesión en el cliente vSphere
3. Seleccione el menú del cliente vSphere y seleccione **Bibliotecas de contenido**.
4. Seleccione **Crear** a la derecha de la página.
5. Proporcione un nombre para la biblioteca y cree la biblioteca de contenido.

- Navegue hasta la biblioteca de contenido que ha creado.
- Seleccione **Acciones** a la derecha de la página y seleccione **Importar elemento** e importe el archivo OVA.



Para obtener más información, consulte "[Creación y uso de la biblioteca de contenido](#)" blog.



Antes de continuar con la implementación, configure el Programador de recursos distribuidos (DRS) del clúster en el inventario en "Conservador". Esto garantiza que las máquinas virtuales no se migren durante la instalación.

Las ONTAP tools for VMware vSphere se implementan inicialmente como una configuración sin alta disponibilidad. Para escalar a la implementación de HA, necesitará habilitar la conexión en caliente de la CPU y la conexión en caliente de la memoria. Puede realizar este paso como parte del proceso de implementación o editar la configuración de la máquina virtual después de la implementación.

### Pasos

- Descargue el archivo que contiene los binarios (.ova) y los certificados firmados para las ONTAP tools for VMware vSphere desde "[Sitio de soporte de NetApp](#)" Si ha importado el OVA a la biblioteca de contenido, puede omitir este paso y continuar con el siguiente.
- Inicie sesión en el servidor vSphere.
- Navegue hasta el grupo de recursos, el clúster o el host donde desea implementar el OVA.



Nunca almacene ONTAP tools for VMware vSphere en almacenes de datos vVols que administra.

- Puede implementar el OVA desde la biblioteca de contenido o desde el sistema local.

Desde el sistema local	De la biblioteca de contenidos
a. Haga clic derecho y seleccione <b>Implementar plantilla OVF....</b> b. Seleccione el archivo OVA desde la URL o busque su ubicación y seleccione <b>Siguiente</b> .	a. Vaya a su biblioteca de contenido y seleccione el elemento que desea implementar. b. Seleccione <b>Acciones &gt; Nueva máquina virtual de esta plantilla</b> .

- En el campo **Seleccionar un nombre y carpeta**, ingrese el nombre de la máquina virtual y elija su ubicación.
  - Si está utilizando la versión vCenter Server 8.0.3, seleccione la opción **Personalizar el hardware de esta máquina virtual**, que activará un paso adicional llamado **Personalizar hardware** antes de pasar a la ventana **Listo para completar**.
  - Si está utilizando la versión vCenter Server 7.0.3, siga los pasos de la sección **¿Qué sigue?** al final de la implementación.

## netapp-ontap-tools-for-vmware-vmware-10.4-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder**
- 4 Select a compute resource
- 5 Review details
- 6 Select storage
- 7 Ready to complete

### Select a name and folder

Specify a unique name and target location

Virtual machine name: demooty

Select a location for the virtual machine.

vcf-vc01.ontappmtme.openenglab.netapp.com

> Raleigh

- Customize the operating system
- Customize this virtual machine's hardware

CANCEL

BACK

NEXT

6. Seleccione un recurso informático y seleccione **Siguiente**. Opcionalmente, marque la casilla para **Encender automáticamente la máquina virtual implementada**.
7. Revise los detalles de la plantilla y seleccione **Siguiente**.
8. Lea y acepte el acuerdo de licencia y seleccione **Siguiente**.
9. Seleccione el almacenamiento para la configuración y el formato del disco y seleccione **Siguiente**.
10. Seleccione la red de destino para cada red de origen y seleccione **Siguiente**.
11. En la ventana **Personalizar plantilla**, complete los campos obligatorios y seleccione **Siguiente**

netapp-ontap-tools-for-vmware-vmphere-10.4-1743069300 - New Virtual Machine from Content Library

- 1 Select a name and folder
- 2 Select a compute resource
- 3 Review details
- 4 License agreements
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

### Customize template X

NTP Servers	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware tools based time synchronization will be used
▼ Deployment Configuration	2 settings
ONTAP tools IP address*	This will be the primary interface for communication with ONTAP tools
ONTAP tools virtual IP address*	ONTAP tools uses this IP address for internal communication
▼ Node Configuration	10 settings
HostName*	<input type="text"/>
Primary DNS*	<input type="text"/>
Secondary DNS*	<input type="text"/>
Search domains*	Specify the search domain name to use when resolving the hostname
IPv4 address*	<input type="text"/>
IPv4 subnet mask*	<input type="text"/>

CANCEL
BACK
NEXT

- La información se valida durante la instalación. Si hay una discrepancia, aparece un mensaje de error en la consola web y se le solicita que lo corrija.
- Los nombres de host deben incluir letras (AZ, az), dígitos (0-9) y guiones (-). Para configurar la pila dual, especifique el nombre de host asignado a la dirección IPv6.



No se admite IPv6 puro. El modo mixto es compatible con VLAN que contienen direcciones IPv6 e IPv4.

- La dirección IP de las herramientas ONTAP es la interfaz principal para comunicarse con las herramientas ONTAP .
  - IPv4 es el componente de dirección IP de la configuración del nodo, que se puede utilizar para habilitar el shell de diagnóstico y el acceso SSH en el nodo con fines de depuración y mantenimiento.
12. Al utilizar la versión vCenter Server 8.0.3, en la ventana **Personalizar hardware**, habilite las opciones **Adición activa de CPU** y **Conexión activa de memoria** para permitir la funcionalidad de alta disponibilidad.

## netapp-ontap-tools-for-vmware-vsphere-10.4-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder
- 4 Select a compute resource
- 5 Review details
- 6 License agreements
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Customize hardware**
- 11 Ready to complete

Customize hardware

Virtual Hardware VM Options Advanced Parameters

ADD NEW DEVICE

**CPU \*** 9 Sockets: 9

Cores per Socket 1 Sockets: 9

CPU Hot Plug  Enable CPU Hot Add

Reservation 0 MHz

Limit Unlimited MHz

Shares Normal 1000

Hardware virtualization  Expose hardware assisted virtualization to the guest OS

Performance Counters  Enable virtualized CPU performance counters

Scheduling Affinity

**Memory \*** 18 GB

Reservation 0 MB  Reserve all guest memory (All locked)

Limit Unlimited MB

Shares Normal 368640

Memory Hot Plug  Enable

CANCEL BACK NEXT

13. Revise los detalles en la ventana **Listo para completar**, seleccione **Finalizar**.

A medida que se crea la tarea de implementación, el progreso se muestra en la barra de tareas de vSphere.

14. Encienda la VM después de completar la tarea si no se seleccionó la opción para encender automáticamente la VM.

Puede seguir el progreso de la instalación dentro de la consola web de la máquina virtual.

Si hay discrepancias en el formulario OVF, un cuadro de diálogo solicitará una acción correctiva. Utilice el botón de tabulación para navegar, realizar los cambios necesarios y seleccionar **Aceptar**. Tiene tres intentos para resolver cualquier problema. Si los problemas continúan después de tres intentos, el proceso de instalación se detendrá y se recomienda volver a intentar la instalación en una nueva máquina virtual.

### ¿Que sigue?

Si tiene ONTAP tools for VMware vSphere con vCenter Server 7.0.3, siga estos pasos después de la implementación.

1. Inicie sesión en el cliente vCenter
2. Apague el nodo de herramientas ONTAP .

3. Vaya a las ONTAP tools for VMware vSphere en **Inventarios** y seleccione la opción **Editar configuración**.
4. En las opciones de **CPU**, marque la casilla de verificación **Habilitar adición activa de CPU**
5. En las opciones de **Memoria**, marque la casilla de verificación **Habilitar** junto a **Conexión en caliente de memoria**.

## Códigos de error de implementación

Es posible que encuentre códigos de error durante las operaciones de implementación, reinicio y recuperación de las ONTAP tools for VMware vSphere . Los códigos de error tienen cinco dígitos, donde los dos primeros dígitos representan el script que encontró el problema y los tres últimos dígitos representan el flujo de trabajo específico dentro de ese script.

Todos los registros de errores se graban en el archivo `ansible-perl-errors.log` para facilitar el seguimiento y la resolución de problemas. Este archivo de registro contiene el código de error y la tarea de Ansible fallida.



Los códigos de error proporcionados en esta página son sólo para referencia. Comuníquese con el equipo de soporte si el error persiste o si no se menciona ninguna solución.

La siguiente tabla enumera los códigos de error y los nombres de archivos correspondientes.

Código de error	Nombre del guión
00	firstboot-network-config.pl, modo de implementación
01	firstboot-network-config.pl, actualización de modo
02	validación de entradas de firstboot.pl
03	firstboot-deploy-otv-ng.pl, implementar, HA
04	firstboot-deploy-otv-ng.pl, implementación, sin HA
05	firstboot-deploy-otv-ng.pl, reiniciar
06	firstboot-deploy-otv-ng.pl, actualización, alta disponibilidad
07	firstboot-deploy-otv-ng.pl, actualización, sin alta disponibilidad
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Los últimos tres dígitos del código de error indican el error de flujo de trabajo específico dentro del script:

Código de error de implementación	Flujo de trabajo	Resolución
049	Para la red y la validación, el script de Perl también los asignará en breve.	-

050	Error en la generación de clave SSH	Reinicie la máquina virtual (VM) principal.
053	Error al instalar RKE2	Ejecute lo siguiente y reinicie la máquina virtual principal o vuelva a implementarla: <code>sudo rke2-killall.sh</code> (todas las máquinas virtuales) <code>sudo rke2-uninstall.sh</code> (todas las máquinas virtuales).
054	Error al configurar kubeconfig	Redistribuir
055	Error al implementar el registro	Si el pod de registro está presente, espere hasta que esté listo y luego reinicie la máquina virtual principal o vuelva a implementarla.
059	La implementación de KubeVip ha fallado	Asegúrese de que la dirección IP virtual para el plano de control de Kubernetes y la dirección IP de las herramientas ONTAP proporcionadas durante la implementación pertenezcan a la misma VLAN y sean direcciones IP libres. Reiniciar si todos los puntos anteriores son correctos. De lo contrario, vuelva a implementarlo.
060	La implementación del operador ha fallado	Reanudar
061	La implementación de los servicios ha fallado	Realice la depuración básica de Kubernetes, como obtener pods, obtener rs, obtener svc, etc., en el espacio de nombres ntv-system para obtener más detalles y registros de errores en <code>/var/log/ansible-perl-errors.log</code> y <code>/var/log/ansible-run.log</code> y vuelva a implementar.
062	La implementación de los servicios de herramientas ONTAP ha fallado	Consulte los registros de errores en <code>/var/log/ansible-perl-errors.log</code> para obtener más detalles y volver a implementar.
065	La URL de la página Swagger no es accesible	Redistribuir
066	Los pasos posteriores a la implementación del certificado de puerta de enlace han fallado	Haga lo siguiente para recuperar/completar la actualización: * Habilite el shell de diagnóstico. * Ejecute el comando <code>'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'</code> . * Consulte los registros en <code>/var/log/post-deploy-upgrade.log</code> .

088	La configuración de rotación de registros para journald ha fallado	Verifique la configuración de red de la máquina virtual que sea compatible con el host en el que está alojada la máquina virtual. Puede intentar migrar a otro host y reiniciar la máquina virtual.
089	El cambio de propiedad del archivo de configuración de rotación del registro de resumen ha fallado	Reinicie la máquina virtual principal.
096	Instalar el proveedor de almacenamiento dinámico	-
108	Falló el script de siembra	-

<b>Código de error de reinicio</b>	<b>Flujo de trabajo</b>	<b>Resolución</b>
067	Se agotó el tiempo de espera del servidor rke2.	-
101	No se pudo restablecer la contraseña del usuario de mantenimiento/consola.	-
102	No se pudo eliminar el archivo de contraseña durante el restablecimiento de la contraseña del usuario de mantenimiento/consola.	-
103	No se pudo actualizar la nueva contraseña de usuario de mantenimiento/consola en la bóveda.	-
088	La configuración de rotación de registro para journald ha fallado.	Verifique la configuración de red de la máquina virtual que sea compatible con el host en el que está alojada la máquina virtual. Puede intentar migrar a otro host y reiniciar la máquina virtual.
089	Se ha producido un error al cambiar la propiedad del archivo de configuración de rotación del registro de resumen.	Reinicie la máquina virtual.

# Configurar ONTAP tools for VMware vSphere

## Agregar instancias de vCenter Server

Agregue instancias de vCenter Server a las ONTAP tools for VMware vSphere para configurar, administrar y proteger sus almacenes de datos virtuales en su 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

Al integrarse con vCenter, las herramientas de ONTAP le permiten realizar tareas de almacenamiento como aprovisionamiento, instantáneas y protección de datos directamente desde el cliente vSphere, eliminando la necesidad de cambiar a consolas de administración de almacenamiento independientes.

### Pasos

1. Abra un navegador web y navegue hasta la URL:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **vCenters** > **Agregar** para incorporar las instancias de vCenter Server. Proporcione su dirección IP o nombre de host de vCenter, nombre de usuario, contraseña y detalles del puerto.



No necesita una cuenta de administrador para agregar instancias de vCenter a las herramientas de ONTAP. Puede crear un rol personalizado sin la cuenta de administrador con permisos limitados. Referirse a "[Utilice vCenter Server RBAC con ONTAP tools for VMware vSphere 10](#)" Para más detalles.

Agregar una instancia de vCenter Server a las herramientas de ONTAP activa automáticamente las siguientes acciones:

- El complemento del cliente vCenter está registrado como un complemento remoto.
- Los privilegios personalizados para los complementos y las API se aplican a la instancia de vCenter Server.
- Se crean roles personalizados para administrar a los usuarios.
- El complemento aparece como un acceso directo en la interfaz de usuario de vSphere.

## Registrar el proveedor VASA con una instancia de vCenter Server

Puede registrar el proveedor VASA con una instancia de vCenter Server utilizando ONTAP tools for VMware vSphere. La sección de configuración del proveedor VASA muestra el estado de registro del proveedor VASA para el vCenter Server seleccionado. En una implementación de varios vCenter, asegúrese de tener certificados CA personalizados para cada instancia de vCenter Server.

## Pasos

1. Inicie sesión en el cliente vSphere.
2. Seleccione **Accesos directos** > \*Herramientas de NetApp ONTAP \* en la sección de complementos.
3. Seleccione **Configuración** > **Configuración del proveedor VASA**. El estado de registro del proveedor VASA se mostrará como no registrado.
4. Seleccione el botón **Registrarse** 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. La longitud de la contraseña debe estar entre 8 y 256 caracteres.
6. Seleccione **Registrarse**.
7. Después de un registro exitoso y una actualización de página, se muestran el estado, el nombre y la versión del proveedor VASA registrado. Después del registro, se activa la acción de cancelar el registro.

## ¿Qué sigue?

Verifique que el proveedor VASA incorporado aparezca en la lista de proveedores VASA del cliente vCenter:

## Pasos

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

# Instalar el complemento NFS VAAI

El complemento NFS vStorage API for Array Integration (NFS VAAI) es un componente de software que integra VMware vSphere y matrices de almacenamiento NFS. Instale el complemento NFS VAAI usando las ONTAP tools for VMware vSphere para aprovechar las capacidades avanzadas de su matriz de almacenamiento NFS para descargar ciertas operaciones relacionadas con el almacenamiento desde los hosts ESXi a la matriz de almacenamiento en sí.

## Antes de empezar

- Descargar el "[Complemento NFS de NetApp para VMware VAAI](#)" paquete de instalación.
- Asegúrese de tener el host ESXi y el último parche de vSphere 7.0U3 o versiones posteriores y ONTAP 9.14.1 o versiones posteriores.
- Montar un almacén de datos NFS.

## Pasos

1. Inicie sesión en el cliente vSphere.
2. Seleccione **Accesos directos** > \*Herramientas de NetApp ONTAP \* en la sección de complementos.
3. Seleccione **Configuración** > **Herramientas NFS VAAI**.
4. Cuando el complemento VAAI se cargue en vCenter Server, seleccione **Cambiar** en la sección **Versión existente**. Si no se carga un complemento VAAI en vCenter Server, seleccione el botón **Cargar**.
5. Busque y seleccione el `.vib` archivo y seleccione **Cargar** para cargar el archivo a las herramientas ONTAP .

6. Seleccione **Instalar en host ESXi**, seleccione el host ESXi en el que desea instalar el complemento NFS VAAI y luego seleccione **Instalar**.

Solo se muestran los hosts ESXi elegibles para la instalación del complemento. Puede supervisar el progreso de la instalación en la sección de tareas recientes de vSphere Web Client.

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

Cuando el administrador de VMware reinicia el host ESXi, las ONTAP tools for VMware vSphere detectan y habilitan automáticamente el complemento NFS VAAI.

### ¿Que sigue?

Después de instalar el complemento NFS VAAI y reiniciar su host ESXi, debe configurar las políticas de exportación NFS correctas para la descarga de copias VAAI. Al configurar VAAI en un entorno NFS, configure las reglas de la política de exportación teniendo en cuenta los siguientes requisitos:

- El volumen ONTAP relevante debe permitir llamadas NFSv4.
- El usuario root debe permanecer como root y se debe permitir NFSv4 en todos los volúmenes principales de unión.
- La opción de compatibilidad con VAAI debe configurarse en el servidor NFS correspondiente.

Para obtener más información sobre el procedimiento, consulte ["Configurar las políticas de exportación NFS correctas para la descarga de copias VAAI"](#) Artículo de KB.

### Información relacionada

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

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

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

## Configurar los ajustes del host ESXi

La configuración de rutas múltiples y tiempos de espera del servidor ESXi garantiza una alta disponibilidad e integridad de los datos al permitir cambiar sin problemas a una ruta de almacenamiento de respaldo si falla una ruta principal.

### Configurar las opciones de tiempo de espera y rutas múltiples del servidor ESXi

Las ONTAP tools for VMware vSphere verifican y establecen las configuraciones de múltiples rutas del host ESXi y las configuraciones de tiempo de espera de HBA que funcionan mejor con los sistemas de almacenamiento NetApp .

### Acerca de esta tarea

Dependiendo de su configuración y la carga del sistema, este proceso puede tardar mucho tiempo. El progreso de la tarea se muestra en el panel Tareas recientes.

### Pasos

1. Desde la página de inicio del cliente web VMware vSphere, seleccione **Hosts y clústeres**.
2. Haga clic con el botón derecho en un host y seleccione **Herramientas de NetApp ONTAP \* > \*Actualizar**

### datos del host.

3. En la página de accesos directos del cliente web VMware vSphere, seleccione \*Herramientas de NetApp ONTAP\* en la sección de complementos.
4. Vaya a la tarjeta **Cumplimiento de host ESXi** en la descripción general (panel de control) del complemento de ONTAP tools for VMware vSphere .
5. Seleccione el enlace **Aplicar configuración recomendada**.
6. En la ventana **Aplicar configuración de host recomendada**, seleccione los hosts que desea actualizar para cumplir con la configuración recomendada de NetApp y seleccione **Siguiente**.



Puede expandir el host ESXi para ver los valores actuales.

7. En la página de configuración, seleccione los valores recomendados según sea necesario.
8. En el panel de resumen, verifique los valores y seleccione **Finalizar**. Puede seguir el progreso en el panel de tareas recientes.

## Establecer valores de host ESXi

Al utilizar las ONTAP tools for VMware vSphere, puede establecer tiempos de espera y otros valores en los hosts ESXi para garantizar el mejor rendimiento y una conmutación por error exitosa. Los valores que establecen las ONTAP tools for VMware vSphere se basan en pruebas internas de NetApp .

Puede establecer los siguientes valores en un host ESXi:

### Configuración del adaptador HBA/CNA

Establece los siguientes parámetros a valores predeterminados:

- Disco.QFullSampleSize
- Disco.QFullThreshold
- Tiempos de espera del HBA del Emulex FC
- Tiempos de espera de HBA FC de QLogic

### Configuración de MPIO

La configuración de MPIO define las rutas preferidas para los sistemas de almacenamiento de NetApp . Determinan cuáles de las rutas disponibles están optimizadas (a diferencia de las rutas no optimizadas que atraviesan el cable de interconexión) y establecen la ruta preferida para una de esas rutas.

En entornos de alto rendimiento, o cuando esté probando el rendimiento con un único almacén de datos LUN, considere cambiar la configuración de equilibrio de carga de la política de selección de ruta (PSP) round-robin (VMW\_PSP\_RR) de la configuración de IOPS predeterminada de 1000 a un valor de 1.



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

### Configuración de NFS

Parámetro	Establezca este valor en...
Tamaño del montón de Net.Tcpip	32

Net.TcpipHeapMax	1024 MB
NFS.Volúmenes máximos	256
NFS41.MaxVolumes	256
NFS.Profundidad máxima de cola	128 o superior
Fallas máximas de latidos del corazón de NFS	10
NFS.Frecuencia de latidos del corazón	12
Tiempo de espera del latido del corazón de NFS	5

## Configurar roles y privilegios de usuario de ONTAP

Puede configurar nuevos roles y privilegios de usuario para administrar backends de almacenamiento utilizando el archivo JSON proporcionado con las ONTAP tools for VMware vSphere y ONTAP System Manager.

### Antes de empezar

- Debería haber descargado el archivo de privilegios 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).
- Deberías haber descargado el archivo de Privilegios de ONTAP desde las herramientas de ONTAP usando [https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users\\_roles.zip](https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip).



Puede crear usuarios a nivel de clúster o directamente a nivel de máquinas virtuales de almacenamiento (SVM). También puede crear usuarios sin utilizar el archivo user\_roles.json y, si lo hace, deberá tener un conjunto mínimo de privilegios en el nivel SVM.

- Debería haber iniciado 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) descargado.
2. Acceda a ONTAP System Manager utilizando la dirección IP de administración del clúster.
3. Inicie sesión en el clúster con privilegios de administrador. Para configurar un usuario, realice los siguientes pasos:
  - a. Para configurar el usuario de las herramientas de Cluster ONTAP , seleccione el panel **Cluster > Configuración > Usuarios y roles**.
  - b. Para configurar el usuario de las 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 Privilegios de ONTAP .

El campo Producto se completa automáticamente.

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

El campo **Rol** se completa automáticamente según la capacidad del producto seleccionada.

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

Se agregan el nuevo rol y usuario, y puedes ver los privilegios detallados bajo el rol que has configurado.

## Requisitos de mapeo agregado de SVM

Para utilizar las credenciales de usuario de SVM para aprovisionar almacenes de datos, internamente las ONTAP tools for VMware vSphere crean volúmenes en el agregado especificado en la API POST de los almacenes de datos. ONTAP no permite la creación de volúmenes en agregados no mapeados en una SVM usando credenciales de usuario de SVM. Para resolver esto, debe asignar las SVM con los agregados utilizando la API REST de ONTAP o la CLI como se describe aquí.

API 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 usuario y rol de ONTAP manualmente

Siga las instrucciones de esta sección para crear el usuario y los roles manualmente sin utilizar el archivo JSON.

1. Acceda a ONTAP System Manager utilizando la dirección IP de administración del clúster.
2. Inicie sesión en el clúster con privilegios de administrador.
  - a. Para configurar los roles de las herramientas del clúster ONTAP , seleccione el panel **Clúster > Configuración > Usuarios y roles**.
  - b. Para configurar los roles de las herramientas SVM ONTAP del clúster, seleccione **SVM de almacenamiento > Configuración > panel Usuarios y roles**
3. Crear roles:
  - a. Seleccione **Agregar** en la tabla **Roles**.
  - b. Ingrese los detalles de **Nombre del rol** y **Atributos del rol**.

Agregue la **Ruta de API REST** y el acceso respectivo desde el menú 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. Ingrese las aplicaciones a las que dará acceso y el método de autenticación. ONTAPI y HTTP son las aplicaciones requeridas, y el tipo de autenticación es **Contraseña**.
- f. Establezca la **Contraseña para el usuario** y **Guarde** el usuario.

### Lista de privilegios mínimos necesarios para usuarios de clúster de ámbito global que no sean administradores

En esta sección se detallan los privilegios mínimos necesarios para usuarios no administradores de clústeres de ámbito global creados sin usar el archivo JSON de usuarios. Si se agrega un clúster de ámbito local, se recomienda usar el archivo JSON para crear los usuarios, ya que las ONTAP tools for VMware vSphere requieren más que solo privilegios de lectura para el aprovisionamiento en ONTAP.

Usando APIs:

API	Nivel de acceso	Utilizado para
/api/clúster	Sólo lectura	Descubrimiento de configuración de clúster
/api/cluster/licencias/licencias	Sólo lectura	Comprobación de licencias para licencias específicas del protocolo
/api/cluster/nodos	Sólo lectura	Descubrimiento del tipo de plataforma
/api/seguridad/cuentas	Sólo lectura	Descubrimiento de privilegios
/api/seguridad/roles	Sólo lectura	Descubrimiento de privilegios
/api/almacenamiento/agregados	Sólo lectura	Comprobación del espacio agregado durante el aprovisionamiento de almacén de datos/volumen
/api/almacenamiento/clúster	Sólo lectura	Para obtener los datos de espacio y eficiencia a nivel de clúster
/api/almacenamiento/discos	Sólo lectura	Para obtener los discos asociados en un agregado
/api/almacenamiento/qos/políticas	Leer/Crear/Modificar	Gestión de políticas de QoS y VM
/api/svm/svms	Sólo lectura	Para obtener la configuración de SVM en el caso de que el clúster se agregue localmente.
/api/red/ip/interfaces	Sólo lectura	Agregar backend de almacenamiento: para identificar que el alcance de LIF de administración es Clúster/SVM

/api/almacenamiento/zonas-de-disponibilidad	Sólo lectura	Descubrimiento SAZ. Aplicable a versiones ONTAP 9.16.1 en adelante y sistemas ASA r2.
---	--------------	---

## Cree ONTAP tools for VMware vSphere ONTAP



Necesita descubrir, crear, modificar y destruir Privileges para realizar operaciones de PATCH y reversión automática en caso de falla en los almacenes de datos. La falta de todos estos privilegios en conjunto conduce a interrupciones del flujo de trabajo y problemas de limpieza.

Creación de ONTAP tools for VMware vSphere La API de ONTAP basada en usuarios con privilegios de descubrimiento, creación de almacenamiento, modificación de almacenamiento y destrucción de almacenamiento permite iniciar descubrimientos y administrar flujos de trabajo de herramientas ONTAP .

Para crear un usuario con ámbito de clúster con todos los privilegios mencionados 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/logins -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

```

Además, para las versiones 9.16.0 y superiores 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 superiores, ejecute el siguiente comando:

```

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

```

### **Cree ONTAP tools for VMware vSphere ONTAP**

Para crear un usuario con ámbito SVM con todos los privilegios, ejecute los siguientes comandos:

```

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 superiores 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_
```

Para desbloquear la cuenta y habilitar el acceso a la interfaz de administración, ejecute el siguiente comando:

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

Ejemplo:

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

## Actualice las ONTAP tools for VMware vSphere de usuario 10.1 a usuario 10.3

Para las ONTAP tools for VMware vSphere 10.1 con un usuario con ámbito de clúster creado mediante el archivo JSON, utilice los siguientes comandos CLI de ONTAP con privilegios de administrador de usuario para actualizar a la versión 10.3.

Para las capacidades del producto:

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

Privilegios del clúster:

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme namespace show"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem show"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem host show"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem map show"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme show-interface" -access  
read
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem host add"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem map add"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme namespace delete"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem delete"  
-access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem host  
remove" -access all
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem map  
remove" -access all
```

Para las ONTAP tools for VMware vSphere 10.1 con un usuario con ámbito SVM creado mediante el archivo json, use los comandos CLI de ONTAP con privilegios de usuario administrador para actualizar a la versión 10.3.

Privilegios de SVM:

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme namespace show"  
-access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem show"  
-access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem host show"  
-access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem map show"  
-access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme show-interface" -access  
read -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem host add"
-access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem map add"
-access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme namespace delete"
-access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem delete"
-access all -vserver <nombre-del-servidor>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem host
remove" -access all -vserver <nombre-del-vserver>
```

```
security login role create -role <nombre-del-rol-existente> -cmddirname "vserver nvme subsystem map
remove" -access all -vserver <nombre-del-servidor>
```

Al agregar el comando `vserver nvme namespace show` y `vserver nvme subsystem show` al rol existente, se agregan los siguientes comandos.

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

## Actualice las ONTAP tools for VMware vSphere 10.3 a 10.4

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

Para las ONTAP tools for VMware vSphere 10.3 con un usuario con ámbito de clúster creado mediante el archivo JSON y la versión 9.16.1 o superior de ONTAP, utilice el comando CLI de ONTAP con privilegios de usuario administrador para actualizar a la versión 10.4.

Para las capacidades del producto:

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

Privilegios del clúster:

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

# Agregar un backend de almacenamiento

Agregar un backend de almacenamiento le permite incorporar un clúster ONTAP .

## Acerca de esta tarea

En el caso de configuraciones de múltiples inquilinos donde vCenter actúa como inquilino con un SVM asociado, utilice el Administrador de herramientas de ONTAP para agregar el clúster. Asocie el backend de almacenamiento con vCenter Server para asignarlo globalmente a la instancia de vCenter Server incorporada. El inquilino de vCenter debe incorporar las máquinas virtuales de almacenamiento (SVM) deseadas. Esto permite que un usuario de SVM aprovisiona almacenes de datos vVols . Puede agregar almacenamiento en vCenter usando SVM.

Agregue los backends de almacenamiento local con credenciales de clúster o SVM mediante la interfaz de usuario de las herramientas ONTAP . Estos backends de almacenamiento están limitados a un único vCenter. Al utilizar credenciales de clúster localmente, las SVM asociadas se asignan automáticamente al vCenter para administrar vVols o VMFS. Para la administración de VMFS, incluido SRA, las herramientas ONTAP admiten credenciales SVM sin necesidad de un clúster global.

## Uso del Administrador de herramientas de ONTAP



En una configuración de múltiples inquilinos, puede agregar un clúster de backend de almacenamiento a nivel global y SVM a nivel local para usar las credenciales de usuario de SVM.

### Pasos

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



Se admiten LIF de gestión de direcciones IPv4 e IPv6.

### Uso de la interfaz de usuario del cliente vSphere



Al configurar un backend de almacenamiento a través de la interfaz de usuario del cliente vSphere, es importante tener en cuenta que los almacenes de datos vVols no admiten la adición directa de un usuario SVM.

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



Para agregar un usuario SVM directamente, puede agregar credenciales basadas en clúster y LIF de administración de direcciones IPv4 e IPv6 o proporcionar credenciales basadas en SVM con un LIF de administración de SVM.

### ¿Que sigue?

La lista se actualiza y puedes ver el backend de almacenamiento recientemente agregado en la lista.

## Asociar un backend de almacenamiento con una instancia de vCenter Server

Asocie un back-end de almacenamiento con vCenter Server para crear una asignación entre el back-end de almacenamiento y la instancia de vCenter Server incorporada a nivel global.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione vCenter en la barra lateral.
4. Seleccione los puntos suspensivos verticales contra la instancia de vCenter Server que desea asociar con los backends de almacenamiento.
5. Seleccione el back-end de almacenamiento del menú desplegable para asociar la instancia de vCenter Server con el back-end de almacenamiento requerido.

## Configurar el acceso a la red

Si no ha configurado el acceso a la red, todas las direcciones IP descubiertas del host ESXi se agregan a la política de exportación de forma predeterminada. Puede configurarlo para agregar algunas direcciones IP específicas a la política de exportación y excluir el resto. Sin embargo, cuando se realiza una operación de montaje en los hosts ESXi excluidos, la operación falla.

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Seleccione \*Herramientas NetApp ONTAP\* en la página de accesos directos en la sección de complementos.
3. En el panel izquierdo de las herramientas de ONTAP, navegue 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

Cuando se crea un almacén de datos en el nivel del clúster de host, el almacén de datos se crea y se monta en todos los hosts del destino, y la acción se habilita solo si el usuario actual tiene el privilegio para ejecutarla.

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

Las ONTAP tools for VMware vSphere 10 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 el administrador del sistema ONTAP y usarlos para crear almacenes de datos VMFS sin utilizar herramientas ONTAP. Referirse a "[Administrar iniciadores SAN y igroups](#)" Para más información.

Cuando el almacenamiento se incorpora a las herramientas de ONTAP y se ejecuta el descubrimiento del almacén de datos, los igroups planos y los almacenes de datos VMFS pasan a ser administrados por las herramientas de ONTAP y se convierten en igroups anidados. No puede utilizar los igroups planos anteriores para crear nuevos almacenes de datos; debe utilizar la interfaz de usuario de las herramientas ONTAP o la

API REST para reutilizar los igroups anidados.

## Crear 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. Este contenedor no tendrá ningún volumen de respaldo.

### Antes de empezar

- Asegúrese de que los agregados raíz no estén asignados a SVM.
- Asegúrese de que el proveedor VASA esté registrado en el vCenter seleccionado.
- En el sistema de almacenamiento ASA r2, SVM se debe asignar al agregado para el usuario SVM.

### Pasos

1. Inicie sesión en el cliente 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. Ingrese el **Nombre del almacén de datos** y la información del **Protocolo**.



El sistema ASA r2 admite 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 un nombre de **Grupo de iniciador 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. Este paso no es aplicable a almacenes de datos vVols que utilizan los sistemas de almacenamiento ASA r2.

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

## Crear un almacén de datos NFS

Un almacén de datos de VMware Network File System (NFS) utiliza el protocolo NFS para conectar hosts ESXi a un dispositivo de almacenamiento compartido a través de una red. Los almacenes de datos NFS se utilizan comúnmente en entornos VMware vSphere y ofrecen varias ventajas, como simplicidad y flexibilidad.

### Pasos

1. Inicie sesión en el cliente 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 **Tipo de almacén de datos**.
4. Ingrese el nombre del almacén de datos, el tamaño y la información del protocolo en el panel **Nombre y protocolo**. Seleccione **Clúster de almacén de datos** y **Autenticación Kerberos** en las opciones avanzadas.



La autenticación Kerberos solo está disponible cuando se selecciona el protocolo NFS 4.1.

5. Seleccione **Plataforma y VM de almacenamiento** 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/predeterminada de SVM.

- En las opciones avanzadas, el botón de alternancia **Asimétrico** solo está visible si se selecciona rendimiento o capacidad en el menú desplegable de la plataforma.
  - Cuando elige la opción **Cualquiera** en el menú desplegable de la plataforma, puede ver las SVM que forman parte del vCenter independientemente de la plataforma o el indicador asimétrico.
7. Seleccione el agregado para la creación de volumen en el panel **Atributos de almacenamiento**. En las opciones avanzadas, elija **Reserva de espacio** y **Habilitar QoS** según sea necesario.
  8. Revise las selecciones en el panel **Resumen** y seleccione **Finalizar**.

El almacén de datos NFS se crea y se monta en todos los hosts.

### Crear un almacén de datos VMFS

El sistema de archivos de máquina virtual (VMFS) es un sistema de archivos agrupado que almacena archivos de máquinas virtuales en entornos VMware vSphere. VMFS permite que varios hosts ESXi accedan a los mismos archivos de máquina virtual simultáneamente, lo que habilita funciones como vMotion y alta disponibilidad.

En un clúster protegido:

- Solo puedes crear almacenes de datos VMFS. Cuando agrega un almacén de datos VMFS a un clúster protegido, el almacén de datos pasa a estar protegido automáticamente.
- No se puede crear un almacén de datos en un centro de datos con uno o más clústeres de host protegidos.
- No se puede crear un almacén de datos en el host ESXi si el clúster del host principal está protegido con una relación de tipo "Política de dúplex de conmutación por error automatizada" (configuración uniforme/no uniforme).
- Puede crear un almacén de datos VMFS solo en un host ESXi protegido por una relación asincrónica. No se puede crear ni montar un almacén de datos en un host ESXi que sea parte de un clúster de host protegido por la política "Dúplex de conmutación por error automatizada".

### Antes de empezar

- Habilite servicios y LIF para cada protocolo en el lado de almacenamiento de ONTAP .
- Asigne SVM para agregarlo al usuario SVM en el sistema de almacenamiento ASA r2.
- Configure el host ESXi si está utilizando el protocolo NVMe/TCP:
  - a. Revisar el ["Guía de compatibilidad de VMware"](#)



VMware vSphere 7.0 U3 y versiones posteriores admiten el protocolo NVMe/TCP. Sin embargo, se recomiendan VMware vSphere 8.0 y versiones posteriores.

- b. Valide 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. Al utilizar la versión VMware vSphere 7, siga las instrucciones del sitio de VMware ["Configurar el enlace de VMkernel para el adaptador NVMe sobre TCP"](#) para configurar la vinculación del puerto NVMe/TCP. Al utilizar la versión VMware vSphere 8, siga ["Configuración de NVMe sobre TCP en ESXi"](#) , para configurar el enlace del puerto NVMe/TCP.
  - e. Para la versión VMware vSphere 7, siga las instrucciones de la página ["Habilitar adaptadores de software NVMe sobre RDMA o NVMe sobre TCP"](#) para configurar adaptadores de software NVMe/TCP. Para la versión VMware vSphere 8, siga ["Agregue adaptadores de software NVMe sobre RDMA o NVMe sobre TCP"](#) para configurar los adaptadores de software NVMe/TCP.
  - f. Correr ["Descubra los sistemas de almacenamiento y hosts"](#) acción en el host ESXi. Para más información, consulte ["Cómo configurar NVMe/TCP con vSphere 8.0 Update 1 y ONTAP 9.13.1 para almacenes de datos VMFS"](#) .
- Si está utilizando el protocolo NVMe/FC, realice los siguientes pasos para configurar el host ESXi:
    - a. Si aún no está habilitado, habilite NVMe over Fabrics (NVMe-oF) en sus hosts ESXi.
    - b. Zonificación SCSI completa.
    - c. Asegúrese de que los hosts ESXi y el sistema ONTAP estén conectados en una capa física y lógica.

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

Para obtener más información sobre el uso del protocolo NVMe/FC con VMware vSphere 8.0, consulte ["Configuración de host 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 host NVMe/FC de ONTAP"](#) y ["TR-4684"](#) .

## Pasos

1. Inicie sesión en el cliente 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**. Si elige agregar el nuevo almacén de datos a un clúster de almacén de datos VMFS existente, seleccione el selector de clúster de almacén de datos en Opciones avanzadas.
5. Seleccione la máquina virtual de almacenamiento en el panel **Almacenamiento**. Proporcione el **Nombre del grupo de iniciadores personalizados** en la sección **Opciones avanzadas** según sea necesario. Puede elegir un igroup existente para el almacén de datos o crear un nuevo igroup 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. El subsistema de espacio de nombres se crea 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 **atributos de almacenamiento**:

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



En los sistemas de almacenamiento ASA r2, la opción **Agregar** no se muestra porque el almacenamiento ASA r2 es 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. Según el protocolo seleccionado, se crea una unidad de almacenamiento (LUN/Espacio de nombres) con una reserva de espacio de tipo delgado.



A partir de ONTAP 9.16.1, los sistemas de almacenamiento ASA r2 admiten hasta 12 nodos por clúster.

- c. Seleccione el **Nivel de servicio de rendimiento** para los sistemas de almacenamiento ASA r2 con SVM de 12 nodos que es un clúster heterogéneo. Esta opción no está disponible si el SVM seleccionado es un clúster homogéneo o utiliza un usuario SVM.

"Cualquiera" es el valor de nivel de servicio de rendimiento (PSL) predeterminado. Esta configuración crea la unidad de almacenamiento utilizando el algoritmo de ubicación equilibrada ONTAP . Sin embargo, puede seleccionar la opción de rendimiento o extrema según sea necesario.

- d. Seleccione las opciones **Usar volumen existente**, **Habilitar QoS** 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; debe crear un nuevo volumen.

7. Revise los detalles del almacén de datos en el panel **Resumen** y seleccione **Finalizar**.



Si crea el almacén de datos en un clúster protegido, podrá ver un mensaje de solo lectura: "El almacén de datos se está montando en un clúster protegido".

**Resultado**

El almacén de datos VMFS se crea y se monta en todos los hosts.

# 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.

### 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 asincrónica 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.

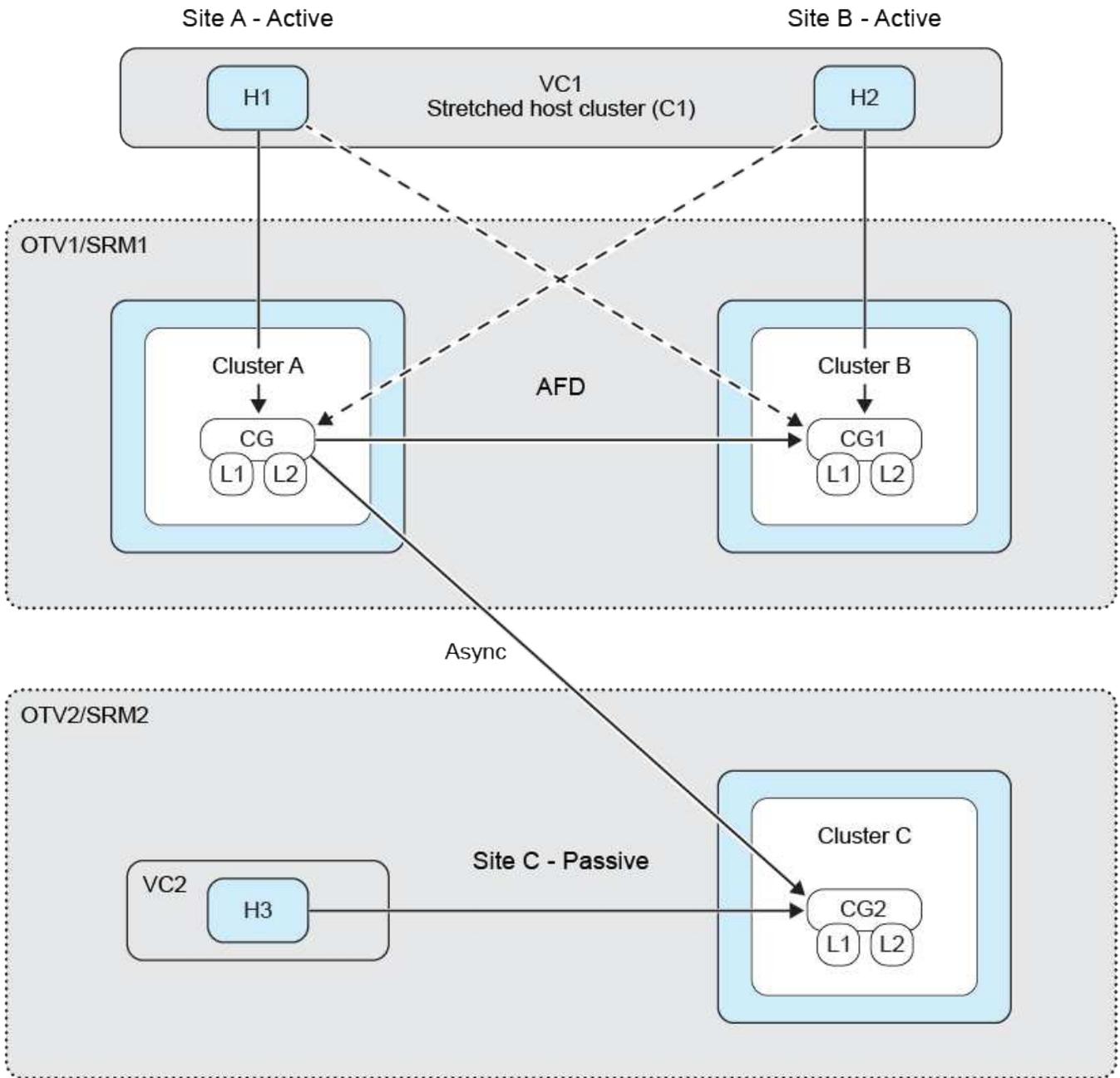
Para establecer la protección de distribución, es necesario conectar tres clústeres de sitios y SVM.

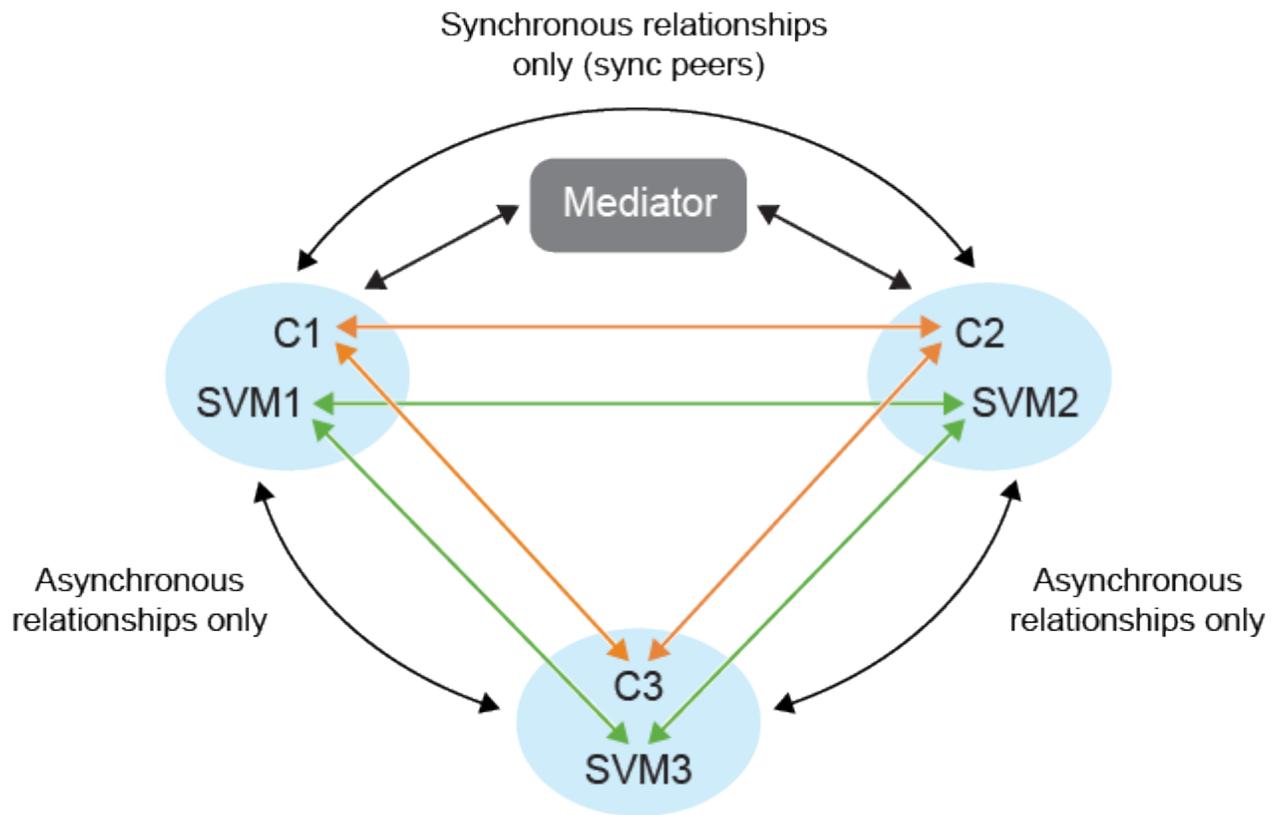
Ejemplo:

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

<ul style="list-style-type: none"> <li>• El grupo de consistencia de origen está en el clúster c1 y SVM svm1</li> <li>• El primer grupo de consistencia de destino está en el clúster c2 y SVM svm2 y</li> <li>• El segundo grupo de consistencia de destino está en el clúster c3 y SVM svm3</li> </ul>	<ul style="list-style-type: none"> <li>• El peering de clúster en el clúster ONTAP de origen será (C1, C2) y (C1, C3).</li> <li>• El peering de clúster en el primer clúster ONTAP de destino será (C2, C1) y (C2, C3) y</li> <li>• Los clústeres que se emparejan en el segundo clúster ONTAP de destino serán (C3, C1) y (C3, C2).</li> <li>• El peering SVM en el SVM de origen será (svm1, svm2) y (svm1, svm3).</li> <li>• El peering SVM en el primer SVM de destino será (svm2, svm1) y (svm2, svm3) y</li> <li>• El peering SVM en el segundo destino svm será (svm3, svm1) y (svm3, svm2).</li> </ul>
--	--

El siguiente diagrama muestra la configuración de protección de abanico:





### Pasos

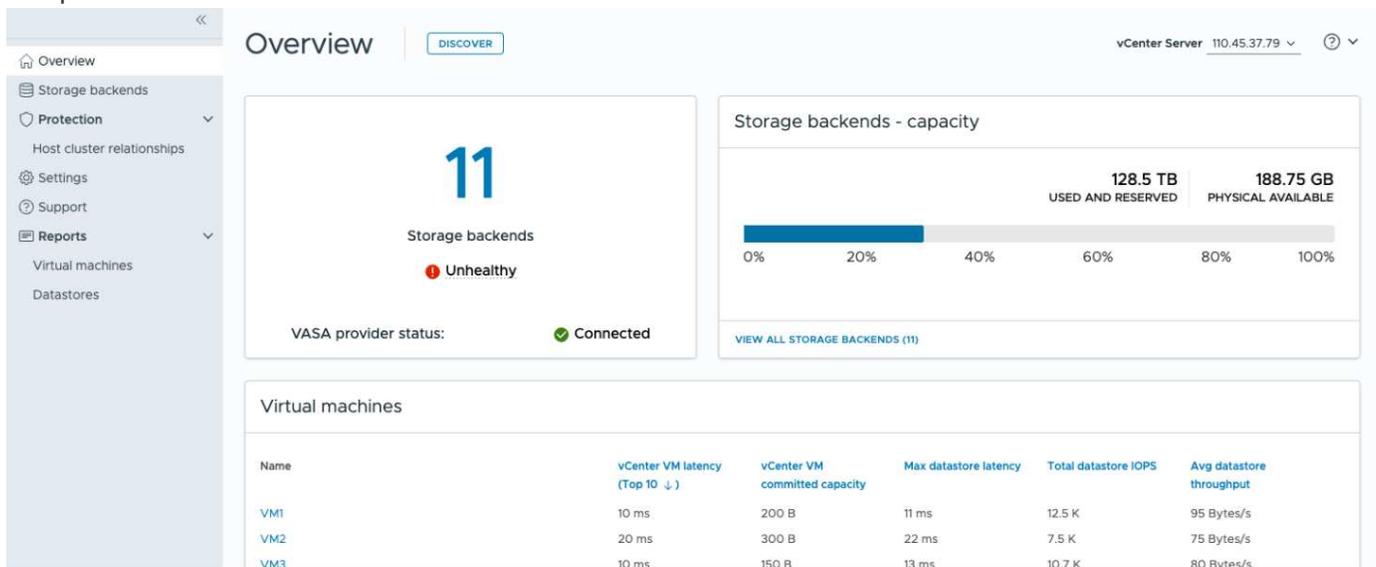
1. Crear un nuevo almacén de datos de marcador de posición. Referirse "[Seleccionar un almacén de datos de marcador de posición](#)"
2. Agregar almacén de datos a la protección del clúster de host "[Modificar el clúster de host protegido](#)". Debe agregar tipos de políticas asincrónicas y sincrónicas.

# Administrar ONTAP tools for VMware vSphere

## Descripción general del panel de control de las ONTAP tools for VMware vSphere

Cuando selecciona el ícono del complemento de ONTAP tools for VMware vSphere en la sección de accesos directos del cliente vCenter, la interfaz de usuario navega a la página de descripción general. Esta página actúa como un panel que le proporciona el resumen de las ONTAP tools for VMware vSphere .

En el caso de la configuración del modo vinculado mejorado (ELM), aparece el menú desplegable de selección de vCenter Server y puede seleccionar el vCenter Server que desee para ver los datos relevantes para él. Este menú desplegable está disponible para todas las demás vistas de listado del complemento. La selección de vCenter Server realizada en una página persiste en las pestañas del complemento.



Desde la página de descripción general, puede ejecutar la acción **Descubrimiento**. La acción de descubrimiento ejecuta el descubrimiento a nivel de vCenter para detectar cualquier backend de almacenamiento, host, almacén de datos y estado/relaciones de protección recientemente agregados o actualizados. Puede ejecutar un descubrimiento de entidades a pedido sin tener que esperar el descubrimiento programado.



El botón de acción se habilitará solo si tiene el privilegio de realizar la acción de descubrimiento.

Una vez enviada la solicitud de descubrimiento, puede seguir el progreso de la acción en el panel de tareas recientes.

El tablero tiene varias tarjetas que muestran diferentes elementos del sistema. La siguiente tabla muestra las diferentes cartas y lo que representan.

Tarjeta	Descripción
---------	-------------

Estado	<p>La tarjeta de estado muestra la cantidad de backends de almacenamiento y el estado general de salud de los backends de almacenamiento y del proveedor VASA. El estado de los backends de almacenamiento se muestra como <b>Saludable</b> cuando el estado de todos los backends de almacenamiento es normal y se muestra como <b>No saludable</b> si alguno de los backends de almacenamiento tiene un problema (estado Desconocido/Inalcanzable/Degradado). Seleccione la información sobre herramientas para abrir los detalles de estado de los backends de almacenamiento. Puede seleccionar cualquier backend de almacenamiento para obtener más detalles. El enlace <b>Otros estados del proveedor VASA</b> muestra el estado actual del proveedor VASA que está registrado en vCenter Server.</p>
Backends de almacenamiento - Capacidad	<p>Esta tarjeta muestra la capacidad agregada, utilizada y disponible, de todos los backends de almacenamiento para la instancia de vCenter Server seleccionada. En el caso de los sistemas de almacenamiento ASA r2, los datos de capacidad no se muestran porque se trata de un sistema desagregado.</p>
Máquinas virtuales	<p>Esta tarjeta muestra las 10 principales máquinas virtuales ordenadas por métrica de rendimiento. Puede seleccionar el encabezado para obtener las 10 máquinas virtuales principales para la métrica seleccionada ordenadas en orden ascendente o descendente. Los cambios de clasificación y filtrado realizados en la tarjeta persisten hasta que usted cambie o borre la memoria caché del navegador.</p>
Almacenes de datos	<p>Esta tarjeta muestra los 10 principales almacenes de datos ordenados según una métrica de rendimiento. Puede seleccionar el encabezado para obtener los 10 principales almacenes de datos para la métrica seleccionada ordenados en orden ascendente o descendente. Los cambios de clasificación y filtrado realizados en la tarjeta persisten hasta que usted cambie o borre la memoria caché del navegador. Hay un menú desplegable Tipo de almacén de datos para seleccionar el tipo de almacén de datos: NFS, VMFS o vVols.</p>
Tarjeta de conformidad del host ESXi	<p>Esta tarjeta muestra el estado de cumplimiento general de todas las configuraciones de hosts ESXi (para el vCenter seleccionado) con respecto a las configuraciones de host NetApp recomendadas por grupo/categoría de configuración. Puede seleccionar el enlace <b>Aplicar configuración recomendada</b> para aplicar la configuración recomendada. Puede seleccionar el estado compatible de los hosts para ver la lista de hosts.</p>

# Interfaz de usuario del administrador de herramientas de ONTAP

Las ONTAP tools for VMware vSphere son un sistema multiinquilino que puede administrar múltiples instancias de vCenter Server. El administrador de herramientas de ONTAP proporciona más control al administrador de ONTAP tools for VMware vSphere sobre las instancias de vCenter Server administradas y los backends de almacenamiento incorporados.

El administrador de herramientas de ONTAP ayuda en:

- Administración de instancias de vCenter Server: agregue y administre instancias de vCenter Server a las herramientas de ONTAP .
- Administración del backend de almacenamiento: agregue y administre clústeres de almacenamiento de ONTAP a las ONTAP tools for VMware vSphere y asígneles a instancias de vCenter Server integradas a nivel mundial.
- Descargas de paquetes de registros: recopile archivos de registro para ONTAP tools for VMware vSphere.
- Gestión de certificados: cambie el certificado autofirmado a un certificado CA personalizado y renueve o actualice todos los certificados del proveedor VASA y las herramientas ONTAP .
- Gestión de contraseñas: restablece la contraseña de la aplicación OVA del usuario.

Para acceder al Administrador de herramientas de ONTAP , inicie

<https://<ONTAPtoolsIP>:8443/virtualization/ui/> desde el navegador e inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.

La sección de descripción general del Administrador de herramientas de ONTAP ayuda a administrar la configuración del dispositivo, como la administración de servicios, el aumento del tamaño de los nodos y la habilitación de alta disponibilidad (HA). También puede monitorear la información general de las herramientas ONTAP relacionadas con los nodos, como el estado, los detalles de la red y las alertas.

The screenshot displays the ONTAP tools Manager interface. At the top, the header shows 'ONTAP tools Manager' on the left and a user profile 'Administrator' on the right. A navigation sidebar on the left includes links for Overview, Alerts, Jobs, Storage backends, vCenters, Log bundles, Certificates, and Settings. The main content area is titled 'Overview' and features an 'EDIT APPLIANCE SETTINGS' button. The 'Appliance' section shows a 'Healthy' status with a green checkmark and lists configuration details: Size: Small, HA: Enabled, VASA provider: Enabled, and SRA: Enabled. The 'Alerts' section, filtered for the 'Last 24 hours', shows 3 Error alerts, 2 Warning alerts, and 5 Info alerts. Below these are three 'ONTAP tools nodes' cards, each representing a node (nodename\_01, nodename\_02, nodename\_03) with an 'Online' status and a 'demo\_vm' instance. Each node card includes a 'VIEW DETAILS' link.

Tarjeta	Descripción
Tarjeta de electrodomésticos	La tarjeta del dispositivo proporciona el estado general del dispositivo de herramientas ONTAP . Muestra los detalles de configuración del dispositivo y el estado de los servicios habilitados. Para obtener información adicional sobre el dispositivo de herramientas ONTAP , seleccione el enlace <b>Ver detalles</b> . Cuando un trabajo de acción de edición de configuración del dispositivo está en progreso, el portlet del dispositivo muestra el estado y los detalles del trabajo.
Tarjeta de alertas	La tarjeta Alertas enumera las alertas de las herramientas ONTAP por tipo, incluidas las alertas a nivel de nodo de HA. Puede ver la lista de alertas seleccionando el texto de recuento (hipervínculo). El enlace lo dirige a la página de visualización de alertas filtradas por el tipo seleccionado.
vCenters	La tarjeta vCenter muestra el estado de salud de los vCenters en el sistema.
Backends de almacenamiento	La tarjeta de backends de almacenamiento muestra el estado de salud de los backends de almacenamiento en el sistema.
Tarjeta de nodos de herramientas ONTAP	La tarjeta de nodos de herramientas ONTAP muestra la lista de nodos con el nombre del nodo, el nombre de la máquina virtual del nodo, el estado y todos los datos relacionados con la red. Puede seleccionar <b>Ver detalles</b> para ver los detalles adicionales relacionados con el nodo seleccionado. [NOTA] En una configuración que no es HA, solo se muestra un nodo. En la configuración de HA, se muestran tres nodos.

## Comprenda los igroups y las políticas de exportación en las ONTAP tools for VMware vSphere

Los grupos de iniciadores (igroups) son tablas de nombres de puertos mundiales (WWPN) de host de protocolo FC o nombres de nodos calificados de host iSCSI. Puede definir igroups y asignarlos a LUN para controlar qué iniciadores tienen acceso a los LUN.

En las ONTAP tools for VMware vSphere 9.x, los igroups se creaban y administraban en una estructura plana, donde cada almacén de datos en vCenter estaba asociado con un solo igroup. Este modelo limitó la flexibilidad y la reutilización de igroups en múltiples almacenes de datos. Las ONTAP tools for VMware vSphere 10.x introducen igroups anidados, donde cada almacén de datos en vCenter está asociado con un igroup principal, mientras que cada host está vinculado a un igroup secundario bajo ese principal. Puede definir igroups principales personalizados con nombres definidos por el usuario para reutilizarlos en múltiples almacenes de datos, lo que permite una administración más flexible e interconectada de los igroups. Comprender el flujo de trabajo de igroup es esencial para administrar LUN y almacenes de datos de manera eficaz en las ONTAP tools for VMware vSphere. Los diferentes flujos de trabajo generan distintas

configuraciones de igroup, como se muestra en los siguientes ejemplos:



Los nombres mencionados son sólo para fines ilustrativos y no se refieren a nombres de igroups reales. Los igroups administrados por herramientas ONTAP usan el prefijo “otv\_”. A los igroups personalizados se les puede dar cualquier nombre.

Término	Descripción
DS<número>	Almacén de datos
iqn<número>	Iniciador IQN
host<número>	Anfitrión MoRef
lun<número>	Identificación de LUN
<DSName>igroup<número>	igroup padre predeterminado (administrado por herramientas ONTAP )
<Host-Moref>igroup<número>	igroup infantil
Customlgroup<número>	igroup padre personalizado definido por el usuario
Classiclgroup<número>	Igroup utilizado en las versiones 9.x de las herramientas ONTAP .

### Ejemplo 1:

Crear un almacén de datos en un único host con un iniciador

**Flujo de trabajo:** [Crear] DS1 (lun1): host1 (iqn1)

### Resultado:

- Grupo DS1l:
  - host1lgroup → (iqn1: lun1)

Se crea un igroup padre DS1lgroup en los sistemas ONTAP para DS1, con un igroup hijo host1lgroup asignado a lun1. Los LUN siempre se asignan a igroups secundarios.

### Ejemplo 2:

Montar el almacén de datos existente en un host adicional

**Flujo de trabajo:** [Montaje] DS1 (lun1): host2 (iqn2)

### Resultado:

- Grupo DS1l:
  - host1lgroup → (iqn1: lun1)
  - host2lgroup → (iqn2: lun1)

Se crea un igroup secundario host2lgroup y se agrega al igroup principal existente DS1lgroup.

### Ejemplo 3:

Desmontar un almacén de datos de un host

**Flujo de trabajo:** [Desmontar] DS1 (lun1): host1 (iqn1)

**Resultado:**

- Grupo DS11:
  - host2lgroup → (iqn2: lun1)

El host1lgroup se elimina de la jerarquía. Los igroups infantiles no se eliminan explícitamente. La eliminación se produce en estas dos condiciones:

- Si no se asigna ningún LUN, el sistema ONTAP elimina el igroup secundario.
- Un trabajo de limpieza programado elimina los igroups secundarios colgantes sin asignaciones de LUN. Estos escenarios solo se aplican a los igroups administrados por herramientas ONTAP , no a los creados de forma personalizada.

**Ejemplo 4:**

Eliminar almacén de datos

**Flujo de trabajo:** [Eliminar] DS1 (lun1): host2 (iqn2)

**Resultado:**

- Grupo DS11:
  - host2lgroup → (iqn2: lun1)

Los igroups padre e hijo se eliminan si otro almacén de datos no reutiliza el igroup padre. Los igroups infantiles nunca se eliminan explícitamente

**Ejemplo 5:**

Crear múltiples almacenes de datos bajo un igroup principal personalizado

**Flujo de trabajo:**

- [Crear] DS2 (lun2): host1 (iqn1), host2 (iqn2)
- [Crear] DS3 (lun3): host1 (iqn1), host3 (iqn3)

**Resultado:**

- Grupo personalizado1:
  - host1lgrupo → (iqn1: lun2, lun3)
  - host2lgroup → (iqn2: lun2)
  - host3lgroup → (iqn3: lun3)

Customlgroup1 se crea para DS2 y se reutiliza para DS3. Los igroups secundarios se crean o actualizan bajo el padre compartido, y cada igroup secundario se asigna a sus LUN relevantes.

**Ejemplo 6:**

Eliminar un almacén de datos bajo un igroup principal personalizado.

**Flujo de trabajo:** [Eliminar] DS2 (lun2): host1 (iqn1), host2 (iqn2)

**Resultado:**

- Grupo personalizado1:
  - host1lgroup → (iqn1: lun3)
  - host3lgroup → (iqn3: lun3)
- Aunque Customlgroup1 no se reutiliza, no se elimina.
- Si no se asignan LUN, el sistema ONTAP elimina host2lgroup.
- El igroup de host1 no se elimina porque está asignado a lun3 de DS3. Los igroups personalizados nunca se eliminan, independientemente del estado de reutilización.

### **Ejemplo 7:**

Expandir el almacén de datos vVols (Agregar volumen)

#### **Flujo de trabajo:**

Antes de la expansión:

[Expandir] DS4 (lun4): host4 (iqn4)

- Grupo DS4l: grupo host4l → (iqn4: lun4)

Después de la expansión:

[Expandir] DS4 (lun4, lun5): host4 (iqn4)

- DS4lgroup: host4lgroup → (iqn4: lun4, lun5)

Se crea un nuevo LUN y se asigna al igroup secundario existente host4lgroup.

### **Ejemplo 8:**

Reducir el almacén de datos de vVols (eliminar volumen)

#### **Flujo de trabajo:**

Antes de encogerse:

[Reducir] DS4 (lun4, lun5): host4 (iqn4)

- DS4lgroup: host4lgroup → (iqn4: lun4, lun5)

Después de encoger:

[Reducir] DS4 (lun4): host4 (iqn4)

- Grupo DS4l: grupo host4l → (iqn4: lun4)

El LUN especificado (lun5) no está asignado al igroup secundario. El igroup permanece activo mientras tenga al menos un LUN asignado.

### **Ejemplo 9:**

Migración de las herramientas ONTAP 9 a 10 (normalización de igroups)

#### **Flujo de trabajo**

Las herramientas ONTAP para las versiones VMware vSphere 9.x no admiten igroups jerárquicos. Durante la

migración a versiones 10.3 o superiores, los igroups deben normalizarse en la estructura jerárquica.

Antes de la migración:

[Migración] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classiclgroup1 (iqn6 e iqn7: lun6, lun7)

La lógica de las herramientas ONTAP 9.x permite múltiples iniciadores por igroup sin imponer una asignación de host uno a uno.

Después de la migración:

[Migración] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classiclgroup1: otv\_Classiclgroup1 (iqn6 e iqn7: lun6, lun7)

Durante la migración:

- Se crea un nuevo igroup padre (Classiclgroup1).
- El igroup original cambia de nombre con el prefijo otv\_ y se convierte en un igroup secundario.

Esto garantiza el cumplimiento del modelo jerárquico.

### Temas relacionados

["Acerca de igroups"](#)

## Políticas de exportación

Las políticas de exportación controlan el acceso a los almacenes de datos NFS en las ONTAP tools for VMware vSphere. Definen qué clientes pueden acceder a los almacenes de datos y qué permisos tienen. Las políticas de exportación se crean y administran en sistemas ONTAP y pueden asociarse con almacenes de datos NFS para aplicar el control de acceso. Cada política de exportación consta de reglas que especifican los clientes (direcciones IP o subredes) a los que se les permite el acceso y los permisos otorgados (solo lectura o lectura y escritura).

Cuando crea un almacén de datos NFS en las ONTAP tools for VMware vSphere, puede seleccionar una política de exportación existente o crear una nueva. Luego, la política de exportación se aplica al almacén de datos, garantizando que solo los clientes autorizados puedan acceder a él.

Cuando se monta un almacén de datos NFS en un nuevo host ESXi, las ONTAP tools for VMware vSphere agregan la dirección IP del host a la política de exportación existente asociada con el almacén de datos. Esto permite que el nuevo host acceda al almacén de datos sin crear una nueva política de exportación.

Cuando elimina o desmonta un almacén de datos NFS de un host ESXi, las ONTAP tools for VMware vSphere eliminan la dirección IP del host de la política de exportación. Si ningún otro host utiliza esa política de exportación, se eliminará. Cuando elimina un almacén de datos NFS, las ONTAP tools for VMware vSphere eliminan la política de exportación asociada con ese almacén de datos si no la reutilizan otros almacenes de datos. Si se reutiliza la política de exportación, conserva la dirección IP del host y permanece sin cambios. Cuando se eliminan los almacenes de datos, la política de exportación anula la asignación de la dirección IP del host y asigna una política de exportación predeterminada, de modo que los sistemas ONTAP puedan acceder a ellos si es necesario.

La asignación de la política de exportación varía según se reutilice en diferentes almacenes de datos. Al reutilizar la política de exportación, se puede añadir la nueva dirección IP del host. Al eliminar o desmontar un almacén de datos que utiliza una política de exportación compartida, esta no se eliminará. Permanecerá sin cambios y la dirección IP del host no se eliminará, ya que se comparte con los demás almacenes de datos. No se recomienda reutilizar las políticas de exportación, ya que puede causar problemas de acceso y latencia.

## Temas relacionados

["Crear una política de exportación"](#)

# Comprender los igroups administrados por las herramientas ONTAP

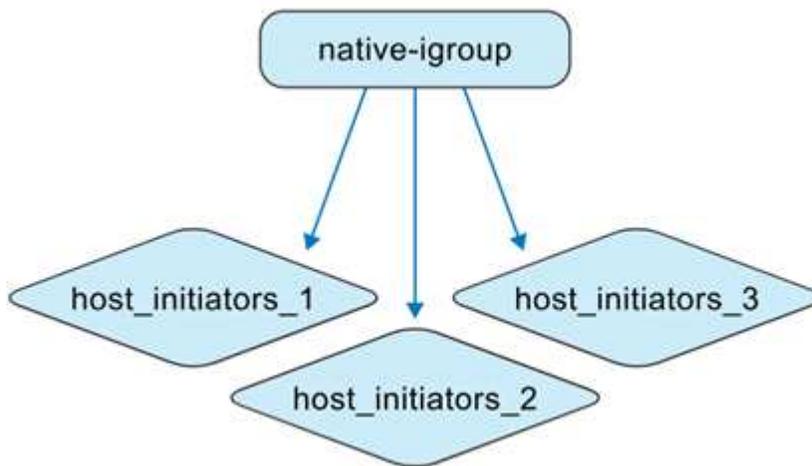
Al administrar máquinas virtuales de herramientas ONTAP y sistemas de almacenamiento ONTAP, es fundamental comprender el comportamiento de igroup, especialmente cuando se migran almacenes de datos desde entornos que no son de herramientas ONTAP a la administración de herramientas ONTAP. Esta sección describe cómo se actualizan los igroups durante esta transición.

Las ONTAP tools for VMware vSphere 10.4 simplifican la administración de almacenes de datos al automatizar la creación y el mantenimiento de objetos ONTAP y vCenter dentro de entornos de centros de datos de VMware.

Las ONTAP tools for VMware vSphere 10.4 interpretan los igroups en dos contextos diferentes:

### igroups administrados por herramientas que no son de ONTAP

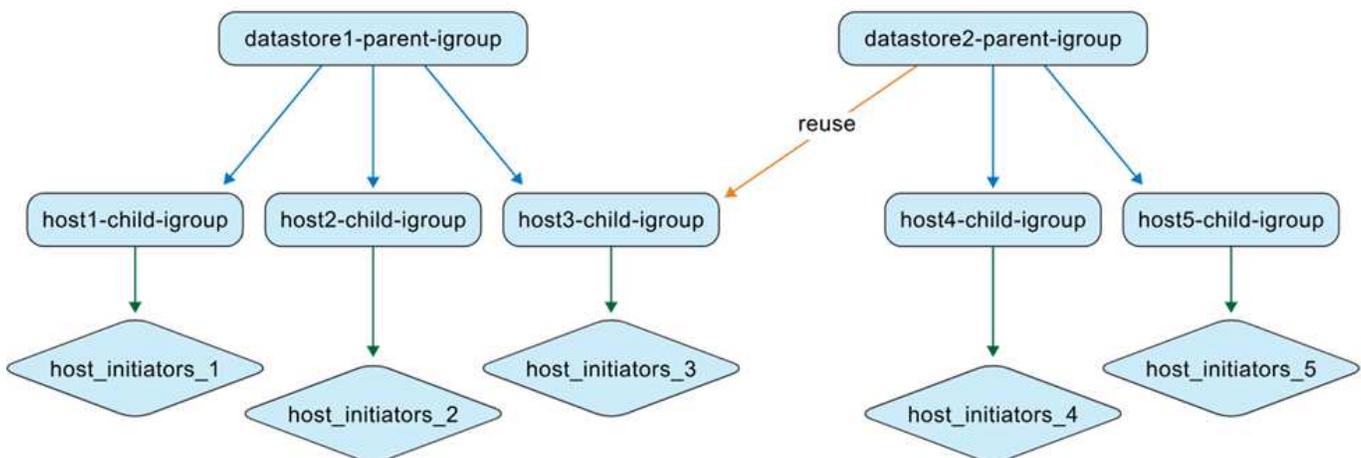
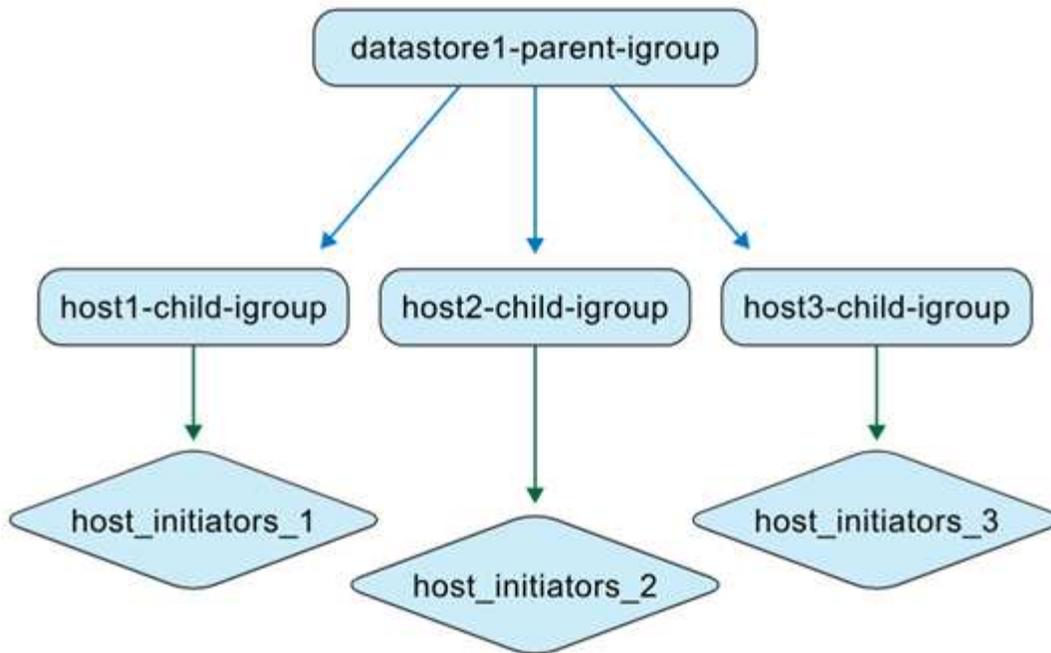
Como administrador de almacenamiento, puede crear igroups en el sistema ONTAP como estructuras planas o anidadas. La ilustración muestra un igroup plano creado en el sistema ONTAP.



### igroups administrados por herramientas ONTAP

Cuando crea almacenes de datos, las ONTAP tools for VMware vSphere 10.4 crean automáticamente igroups utilizando una estructura anidada para facilitar la asignación de LUN.

Por ejemplo, cuando se crea y monta el almacén de datos1 en los hosts 1, 2 y 3, y se crea y monta un nuevo almacén de datos (almacén de datos2) en los hosts 3, 4 y 5, las herramientas de ONTAP reutilizan el igroup a nivel de host para una gestión eficiente.



A continuación se muestran algunos casos de ONTAP tools for VMware vSphere .

### Cuando creas un almacén de datos con la configuración de igroup predeterminada

Cuando crea un almacén de datos y deja el campo igroup en blanco (configuración predeterminada), las herramientas de ONTAP generan automáticamente una estructura igroup anidada para ese almacén de datos. El igroup padre en el nivel del almacén de datos se nombra utilizando el patrón: `otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>`. Cada igroup secundario a nivel de host sigue el patrón: `otv_<hostMoref>_<vcguid>`. Puede ver la asociación entre los igroups padre (nivel de almacén de datos) y los igroups hijo (nivel de host) en la sección **Grupo iniciador padre** de la interfaz de almacenamiento de ONTAP .

Con el enfoque de igroup anidado, los LUN se asignan solo a los igroups secundarios. Luego, el inventario de vCenter Server muestra el nuevo almacén de datos.

### Cuando creas un almacén de datos con un nombre de igroup personalizado

Durante la creación del almacén de datos en las herramientas de ONTAP , puede ingresar un nombre de

igroup personalizado en lugar de seleccionarlo en el menú desplegable. Luego, las herramientas de ONTAP crean un igroup principal en el nivel del almacén de datos usando el nombre especificado. Si se utiliza el mismo host para varios almacenes de datos, se reutiliza el igroup de nivel de host (secundario) existente. Como resultado, el LUN del nuevo almacén de datos se asigna a este igroup secundario existente, que ahora puede estar asociado con múltiples igroups principales (uno para cada almacén de datos). La lista de almacenes de datos de la interfaz de usuario de vCenter Server confirma la creación exitosa del nuevo almacén de datos con el nombre de igroup personalizado.

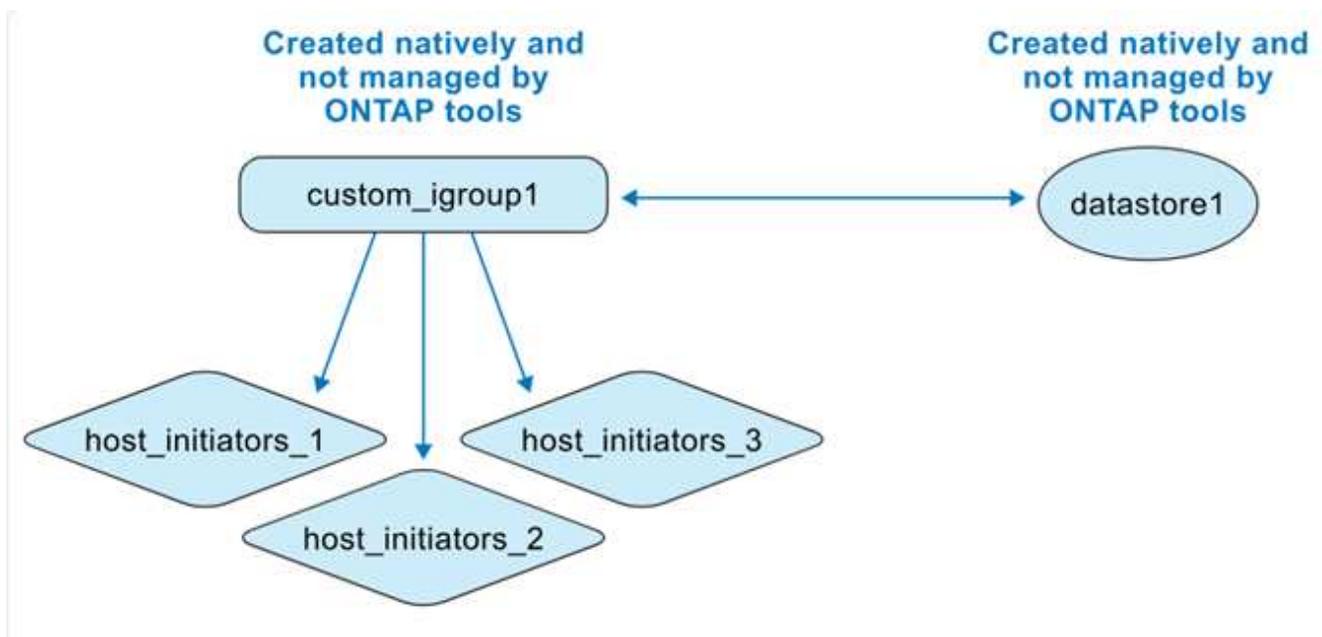
### Cuando reutiliza el nombre del igroup durante la creación del almacén de datos

Al crear un almacén de datos mediante la interfaz de usuario de las herramientas ONTAP, puede elegir un igroup padre personalizado existente de la lista desplegable. Después de reutilizar el igroup principal para crear otro almacén de datos, la interfaz de usuario de los sistemas ONTAP muestra esta asociación. El nuevo almacén de datos también aparece en la interfaz de usuario de vCenter Server.

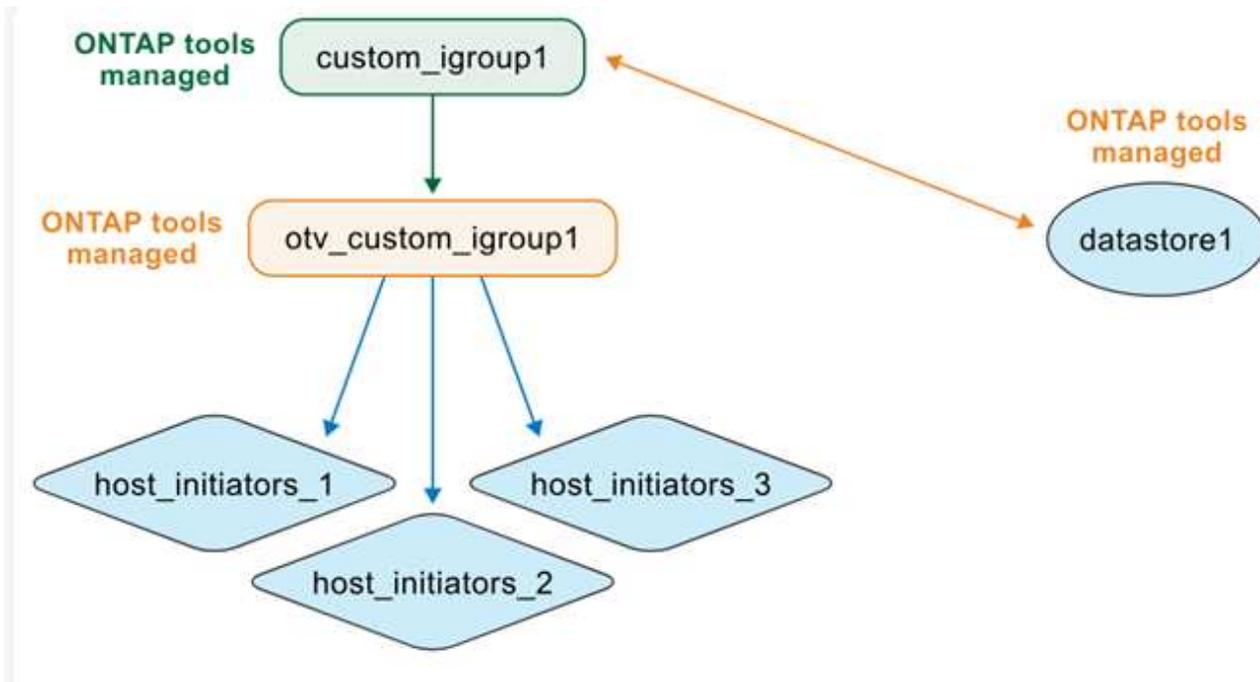
Esta operación también se puede realizar mediante la API. Para reutilizar un igroup existente durante la creación del almacén de datos, especifique el UUID del igroup en la carga útil de la solicitud de API.

### Cuando crea un almacén de datos y un igroup de forma nativa desde ONTAP y vCenter

Si crea el igroup y el almacén de datos directamente en sistemas ONTAP y entornos VMware, las herramientas de ONTAP no administran estos objetos al principio. Esto crea una estructura de igroup plana.



Para administrar un almacén de datos y un igroup existente con herramientas ONTAP, debe realizar un descubrimiento del almacén de datos. Las herramientas ONTAP identifican y registran el almacén de datos y el igroup, y los convierten en una estructura anidada en su base de datos. Se crea un nuevo igroup padre usando el nombre personalizado, mientras que el igroup existente se renombra con el prefijo "otv\_" y se convierte en el igroup hijo. Las asignaciones del iniciador permanecen sin cambios. Sólo los igroups asignados a almacenes de datos se convierten durante el descubrimiento. Después de esto, la estructura del igroup se parece a la ilustración siguiente.



Puede crear un almacén de datos directamente en vCenter Server y luego ponerlo bajo la administración de herramientas ONTAP . Primero, cree un igroup plano en sistemas ONTAP y asígnele un LUN. Después de ejecutar el descubrimiento del almacén de datos en las herramientas ONTAP , el igroup plano se convierte en una estructura anidada. Luego, las herramientas de ONTAP administran el igroup y lo renombran con el prefijo 'otv\_'. El LUN permanece asignado al mismo igroup durante todo este proceso.

### Cómo las herramientas de ONTAP reutilizan igroups creados de forma nativa

Puede aprovisionar un almacén de datos en las herramientas de ONTAP utilizando un igroup creado originalmente en los sistemas de ONTAP , después de que las herramientas de ONTAP lo administren. Estos igroups aparecen en la lista desplegable del nombre del grupo iniciador personalizado. Luego, el nuevo LUN del almacén de datos se asigna al igroup secundario normalizado correspondiente, como "otv\_Nativegroup1".

Las ONTAP tools for VMware vSphere no detectan ni utilizan igroups creados en el sistema ONTAP que no estén administrados por herramientas ONTAP o vinculados a un almacén de datos.

## Habilitar ONTAP tools for VMware vSphere

Puede cambiar la contraseña de administrador mediante el Administrador de herramientas de ONTAP para habilitar servicios como VASA Provider, importación de configuración de vVols y recuperación ante desastres (SRA) mediante el Administrador de herramientas de ONTAP .

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Editar configuración del dispositivo** en la sección de descripción general.
4. En la sección **Servicios**, puede habilitar servicios opcionales como VASA Provider, importación de

configuración de vVols y recuperación ante desastres (SRA) según sus necesidades.

Al habilitar los servicios por primera vez, debe crear las credenciales de proveedor VASA y SRA. Se utilizan para registrar o habilitar los servicios SRA y del proveedor VASA en vCenter Server. El nombre de usuario solo puede contener letras, números y guiones bajos. La longitud de la contraseña debe estar entre 8 y 256 caracteres.



Antes de deshabilitar cualquier servicio opcional, asegúrese de que los servidores vCenter administrados por las herramientas de ONTAP no los utilicen.

La opción \*Permitir importación de configuración de vVols\* se muestra solo cuando el servicio del proveedor VASA está habilitado. Esta opción habilita la migración de datos vVols de las herramientas ONTAP 9.xx a las herramientas ONTAP 10.4.

## Cambiar las ONTAP tools for VMware vSphere

Al utilizar el Administrador de herramientas de ONTAP, escale la configuración de las ONTAP tools for VMware vSphere para aumentar la cantidad de nodos en la implementación o cambiar la configuración a una configuración de alta disponibilidad (HA). Las ONTAP tools for VMware vSphere se implementan inicialmente en una configuración de nodo único que no es de alta disponibilidad.



Para migrar a HA cuando la copia de seguridad que no es de HA está habilitada, primero deshabilite la copia de seguridad y vuelva a habilitarla después de la migración.

### Antes de empezar

- Asegúrese de que su plantilla OVA tenga la misma versión OVA que el Nodo 1. El nodo 1 es el nodo predeterminado donde se implementan inicialmente las ONTAP tools for VMware vSphere OVA.
- Asegúrese de que la adición activa de CPU y la conexión activa de memoria estén habilitadas.
- En vCenter Server, configure el nivel de automatización del Servicio de recuperación ante desastres (DRS) en parcialmente automatizado. Después de implementar HA, vuelva a automatizarlo por completo.
- Los nombres de host de los nodos en la configuración de HA deben estar en minúsculas.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Editar configuración del dispositivo** en la sección de descripción general.
4. En la sección **Configuración**, puede escalar para aumentar el tamaño del nodo y habilitar la configuración de HA según sus necesidades. Necesita las credenciales de vCenter Server para realizar cualquier cambio.

Cuando las herramientas ONTAP están en configuración HA, puede cambiar los detalles de la biblioteca de contenido. Debes proporcionar la contraseña nuevamente para enviar la nueva edición.



En las ONTAP tools for VMware vSphere, solo se permite aumentar el tamaño del nodo; no se puede reducir el tamaño del nodo. En una configuración que no es HA, solo se admite una configuración de tamaño mediano. En una configuración de alta disponibilidad, se admiten configuraciones medianas y grandes.

5. Utilice el botón de alternancia HA para habilitar la configuración de HA. En la página **Configuración de HA**, asegúrese de que:

- La biblioteca de contenido pertenece al mismo vCenter Server donde se ejecutan las máquinas virtuales del nodo de herramientas de ONTAP. Las credenciales de vCenter Server se utilizan para validar y descargar la plantilla OVA para los cambios del dispositivo.
- La máquina virtual que aloja las herramientas ONTAP no está implementada directamente en un host ESXi. La máquina virtual debe implementarse en un clúster o en un grupo de recursos.



Una vez habilitada la configuración de HA, no es posible volver a una configuración de nodo único que no sea de HA.

6. En la sección **Configuración de HA** de la ventana **Editar configuración del dispositivo**, puede ingresar los detalles de los nodos 2 y 3. Las ONTAP tools for VMware vSphere admiten tres nodos en la configuración de alta disponibilidad.



La mayoría de las opciones de entrada están rellenas previamente con detalles de la red del Nodo 1 para facilitar el flujo de trabajo. Sin embargo, puede editar los datos de entrada antes de navegar a la página final del asistente. Puede ingresar detalles de la dirección IPv6 para los otros dos nodos solo cuando la dirección IPv6 esté habilitada en el primer nodo.

Asegúrese de que un host ESXi contenga solo una máquina virtual de herramientas ONTAP. Las entradas se validan cada vez que se pasa a la siguiente ventana.

7. Revise los detalles en la sección **Resumen** y **Guarde** los cambios.

### ¿Que sigue?

La página **Descripción general** muestra el estado de la implementación. Al utilizar el ID del trabajo, también puede rastrear el estado del trabajo de edición de configuración del dispositivo desde la vista de trabajos.

Si la implementación de HA falla y el estado del nuevo nodo se muestra como "Nuevo", elimine la nueva VM en vCenter antes de volver a intentar la operación de habilitación de HA.

La pestaña **Alertas** en el panel izquierdo enumera las alertas de las ONTAP tools for VMware vSphere.

## Administrar almacenes de datos

### Montar almacenes de datos NFS y VMFS

Al montar un almacén de datos se proporciona acceso de almacenamiento a hosts adicionales. Puede montar el almacén de datos en los hosts adicionales después de agregar los hosts a su entorno VMware.

#### Acerca de esta tarea

- Algunas acciones de clic derecho están deshabilitadas o no están disponibles según la versión del cliente

vSphere y el tipo de almacén de datos seleccionado.

- Si está utilizando el cliente vSphere 8.0 o versiones posteriores, algunas de las opciones de clic derecho están ocultas.
- Desde las versiones vSphere 7.0U3 a vSphere 8.0, aunque aparezcan las opciones, la acción estará deshabilitada.
- La opción de montaje del almacén de datos está deshabilitada cuando el clúster de host está protegido con configuraciones uniformes.

## Pasos

1. Desde la página de inicio de vSphere Client, seleccione **Hosts y clústeres**.
2. En el panel de navegación izquierdo, seleccione los centros de datos que contienen los hosts.
3. Para montar almacenes de datos NFS/VMFS en un host o un clúster de hosts, haga clic con el botón derecho y seleccione \* Herramientas de NetApp ONTAP \* > \* Montar almacenes de datos \*.
4. Seleccione los almacenes de datos que desea montar y seleccione **Montar**.

## ¿Que sigue?

Puede seguir el progreso en el panel de tareas recientes.

## Desmontar almacenes de datos NFS y VMFS

La acción Desmontar almacén de datos desmonta un almacén de datos NFS o VMFS de los hosts ESXi. La acción Desmontar almacén de datos está habilitada para almacenes de datos NFS y VMFS descubiertos o administrados por las ONTAP tools for VMware vSphere.

## Pasos

1. Inicie sesión en el cliente vSphere.
2. Haga clic con el botón derecho en un objeto de almacén de datos NFS o VMFS y seleccione **Desmontar almacén de datos**.

Se abre un cuadro de diálogo que enumera los hosts ESXi en los que está montado el almacén de datos. Cuando la operación se realiza en un almacén de datos protegido, se muestra un mensaje de advertencia en la pantalla.

3. Seleccione uno o más hosts ESXi para desmontar el almacén de datos.

No es posible desmontar el almacén de datos de todos los hosts. La interfaz de usuario sugiere que utilice la operación de eliminación del almacén de datos en su lugar.

4. Seleccione el botón **Desmontar**.

Si el almacén de datos es parte de un clúster de host protegido, se muestra un mensaje de advertencia.



Si se desmonta el almacén de datos protegido, la configuración de protección existente podría resultar en una protección parcial. Consulte "[Modificar el clúster de host protegido](#)" para permitir una protección completa.

## ¿Que sigue?

Puede seguir el progreso en el panel de tareas recientes.

## Montar un almacén de datos vVols

Puede montar un almacén de datos de VMware Virtual Volumes (vVols) en uno o más hosts adicionales para proporcionar acceso de almacenamiento a hosts adicionales. Puede desmontar el almacén de datos vVols solo a través de las API.

### Pasos

1. Desde la página de inicio de vSphere Client, seleccione **Hosts y clústeres**.
2. En el panel de navegación, seleccione el centro de datos que contiene el almacén de datos.
3. Haga clic con el botón derecho en el almacén de datos y seleccione \* Herramientas de NetApp ONTAP \* > \* Montar almacén de datos \*.
4. En el cuadro de diálogo **Montar almacenes de datos en hosts**, seleccione los hosts en los que desea montar el almacén de datos y luego seleccione **Montar**.

Puede seguir el progreso en el panel de tareas recientes.

## Cambiar el tamaño del almacén de datos NFS y VMFS

Cambiar el tamaño de un almacén de datos le permite aumentar el almacenamiento para los archivos de su máquina virtual. Puede cambiar el tamaño de un almacén de datos a medida que cambian sus requisitos de infraestructura.

### Acerca de esta tarea

Solo puede aumentar el tamaño de los almacenes de datos NFS y VMFS. Un FlexVol volume que forma parte de un almacén de datos NFS y VMFS no puede reducirse por debajo del tamaño existente, pero puede crecer hasta un 120 % como máximo.

### Pasos

1. Desde la página de inicio de vSphere Client, seleccione **Hosts y clústeres**.
2. En el panel de navegación, seleccione el centro de datos que contiene el almacén de datos.
3. Haga clic con el botón derecho en el almacén de datos NFS o VMFS y seleccione \* Herramientas de NetApp ONTAP \* > \* Cambiar tamaño del almacén de datos \*.
4. En el cuadro de diálogo Cambiar tamaño, especifique un nuevo tamaño para el almacén de datos y seleccione **Aceptar**.

## Expandir almacenes de datos vVols

Al hacer clic con el botón derecho en el objeto de almacén de datos en la vista de objetos de vCenter, las acciones compatibles con las ONTAP tools for VMware vSphere se muestran en la sección de complementos. Se habilitan acciones específicas según el tipo de almacén de datos y los privilegios del usuario actual.



La operación de expansión del almacén de datos vVols no se aplica a los almacenes de datos vVols basados en el sistema ASA r2.

### Pasos

1. Desde la página de inicio de vSphere Client, seleccione **Hosts y clústeres**.

2. En el panel de navegación, seleccione el centro de datos que contiene el almacén de datos.
3. Haga clic con el botón derecho en el almacén de datos y seleccione \* Herramientas de NetApp ONTAP \* > \* Agregar almacenamiento al almacén de datos \*.
4. En la ventana **Crear o Seleccionar volúmenes**, puede crear nuevos volúmenes o elegir entre los volúmenes existentes. La interfaz de usuario se explica por sí sola. Siga las instrucciones según su elección.
5. En la ventana **Resumen**, revise las selecciones y seleccione **Expandir**. Puede seguir el progreso en el panel de tareas recientes.

## Reducir el almacén de datos de vVols

La acción Eliminar almacén de datos elimina el almacén de datos cuando no hay vVols en el almacén de datos seleccionado.



La operación de reducción del almacén de datos vVols no es compatible con el almacén de datos vVols basado en el sistema ASA r2.

### Pasos

1. Desde la página de inicio de vSphere Client, seleccione **Hosts y clústeres**.
2. En el panel de navegación, seleccione el centro de datos que contiene el almacén de datos.
3. Haga clic con el botón derecho en el almacén de datos vVol y seleccione \* Herramientas de NetApp ONTAP \* > \* Quitar almacenamiento del almacén de datos \*.
4. Seleccione los volúmenes que no tengan vVols y seleccione **Eliminar**.



La opción para seleccionar el volumen en el que reside vVols está deshabilitada.

5. En la ventana emergente **Quitar almacenamiento**, seleccione la casilla de verificación **Eliminar volúmenes del clúster ONTAP \* para eliminar los volúmenes del almacén de datos y del almacenamiento ONTAP y seleccione \*Eliminar**.

## Eliminar almacenes de datos

La acción Eliminar almacenamiento del almacén de datos es compatible con todas las ONTAP tools for VMware vSphere almacenes de datos vVols detectados o administrados por VMware vSphere en vCenter Server. Esta acción permite la eliminación de volúmenes de los almacenes de datos vVols .

La opción de eliminar está deshabilitada cuando hay vVols que residen en un volumen particular. Además de eliminar volúmenes del almacén de datos, puede eliminar el volumen seleccionado en el almacenamiento ONTAP .

La tarea Eliminar almacén de datos de las ONTAP tools for VMware vSphere en vCenter Server hace lo siguiente:

- Desmonta el contenedor vVol.
- Limpia el igroup. Si igroup no está en uso, elimina iqn de igroup.
- Elimina el contenedor Vvol.

- Deje los volúmenes Flex en la matriz de almacenamiento.

Siga los pasos a continuación para eliminar el almacén de datos NFS, VMFS o vVOL de las herramientas de ONTAP desde vCenter Server:

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Haga clic con el botón derecho en un sistema host, en un clúster de host o en un centro de datos y seleccione **Herramientas de NetApp ONTAP \* > \*Eliminar almacén de datos.**



No puedes eliminar los almacenes de datos si hay máquinas virtuales que utilizan ese almacén de datos. Debe mover las máquinas virtuales a un almacén de datos diferente antes de eliminar el almacén de datos. No puede seleccionar la casilla de verificación Eliminar volumen si el almacén de datos pertenece a un clúster de host protegido.

- a. En el caso de un almacén de datos NFS o VMFS, aparece un cuadro de diálogo con la lista de máquinas virtuales que utilizan el almacén de datos.
  - b. Si el almacén de datos VMFS se crea en sistemas ASA r2 y es parte de la protección, debe desproteger el almacén de datos antes de eliminarlo.
  - c. En el caso de almacenes de datos vVols , la acción de eliminar almacén de datos elimina el almacén de datos solo cuando no hay vVols asociados a él. El cuadro de diálogo Eliminar almacén de datos proporciona una opción para eliminar volúmenes del clúster ONTAP .
  - d. En el caso de almacenes de datos vVols basados en sistemas ASA r2, la casilla de verificación para eliminar los volúmenes de respaldo no es aplicable.
3. Para eliminar los volúmenes de respaldo en el almacenamiento de ONTAP , seleccione \*Eliminar volúmenes en el clúster de ONTAP \*.



No se puede eliminar el volumen del clúster ONTAP de un almacén de datos VMFS que forma parte del clúster de host protegido.

## Vistas de almacenamiento de ONTAP para almacenes de datos

Las ONTAP tools for VMware vSphere muestran la vista lateral del almacenamiento ONTAP de los almacenes de datos y sus volúmenes en la pestaña de configuración.

### Pasos

1. Desde el cliente vSphere, navegue hasta el almacén de datos.
2. Seleccione la pestaña **Configurar** en el panel derecho.
3. Seleccione \* Herramientas NetApp ONTAP \* > \* Almacenamiento ONTAP \*. Dependiendo del tipo de almacén de datos, la vista cambia. Consulte la siguiente tabla para obtener información:

Tipo de almacén de datos	Información disponible
almacén de datos NFS	La página <b>Detalles de almacenamiento</b> contiene información de backends de almacenamiento, agregados y volumen. La página <b>Detalles de NFS</b> contiene datos relacionados con el almacén de datos NFS.

Almacenes de datos VMFS	La página <b>Detalles de almacenamiento</b> contiene detalles de backend de almacenamiento, agregado, volumen y zona de disponibilidad de almacenamiento (SAZ). La página <b>Detalles de la unidad de almacenamiento</b> contiene detalles de la unidad de almacenamiento.
almacenes de datos vVols	Enumera todos los volúmenes. Puede expandir o eliminar almacenamiento desde el panel de almacenamiento de ONTAP . Esta vista no es compatible con el almacén de datos vVols basado en el sistema ASA r2.

## Vista de almacenamiento de la máquina virtual

La vista de almacenamiento muestra la lista de vVols creados por la máquina virtual.



Esta vista es aplicable a la máquina virtual que tiene al menos un disco relacionado con el almacén de datos vVols administrado ONTAP tools for VMware vSphere montado en ella.

### Pasos

1. Desde vSphere Client, navegue hasta la máquina virtual.
2. Seleccione la pestaña **Monitor** en el panel derecho.
3. Seleccione **Herramientas NetApp ONTAP \* > \*Almacenamiento**. Los detalles de **Almacenamiento** aparecen en el panel derecho. Puede ver la lista de vVols que están presentes en la VM.

Puede utilizar la opción 'Administrar columnas' para ocultar o mostrar diferentes columnas.

## Administrar los umbrales de almacenamiento

Puede establecer el umbral para recibir notificaciones en vCenter Server cuando el volumen y la capacidad agregada alcanzan determinados niveles.

### Pasos:

1. Inicie sesión en el cliente vSphere.
2. En la página de accesos directos, seleccione **\*Herramientas de NetApp ONTAP \*** en la sección de complementos.
3. En el panel izquierdo de las herramientas de ONTAP , navegue a **Configuración > Configuración de umbral > Editar**.
4. En la ventana **Editar umbral**, proporcione los valores deseados en los campos **Casi lleno** y **Completo** y seleccione **Guardar**. Puede restablecer los números a los valores recomendados, que son 80 para casi lleno y 90 para lleno.

## Administrar backends de almacenamiento

Los backends de almacenamiento son sistemas que los hosts ESXi utilizan para el almacenamiento de datos.

## Descubra el almacenamiento

Puede ejecutar el descubrimiento de un backend de almacenamiento a pedido sin esperar a que un descubrimiento programado actualice los detalles del almacenamiento.

Siga los pasos a continuación para descubrir los backends de almacenamiento.

### Pasos

1. Inicie sesión en el cliente vSphere.
2. En la página de accesos directos, seleccione \*Herramientas de NetApp ONTAP\* en la sección de complementos.
3. En el panel izquierdo de las herramientas de ONTAP, navegue hasta **Backends de almacenamiento** y seleccione un backend de almacenamiento.
4. Seleccione el menú de puntos suspensivos verticales y seleccione **Descubrir almacenamiento**

Puede seguir el progreso en el panel de tareas recientes.

## Modificar los backends de almacenamiento

Siga los pasos de esta sección para modificar un backend de almacenamiento.

1. Inicie sesión en el cliente vSphere.
2. En la página de accesos directos, seleccione \*Herramientas de NetApp ONTAP\* en la sección de complementos.
3. En el panel izquierdo de las herramientas de ONTAP, navegue hasta **Backends de almacenamiento** y seleccione un backend de almacenamiento.
4. Seleccione el menú de puntos suspensivos verticales y seleccione **Modificar** para modificar las credenciales o el nombre del puerto. Puede seguir el progreso en el panel de tareas recientes.

Puede realizar la operación Modificar para clústeres ONTAP globales mediante el Administrador de herramientas ONTAP siguiendo estos pasos.

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione los backends de almacenamiento en la barra lateral.
4. Seleccione el backend de almacenamiento que desea modificar.
5. Seleccione el menú de puntos suspensivos verticales y seleccione **Modificar**.
6. Puede modificar las credenciales o el puerto. Introduzca el **Nombre de usuario** y la **Contraseña** para modificar el backend de almacenamiento.

## Eliminar backends de almacenamiento

Debe eliminar todos los almacenes de datos adjuntos al back-end de almacenamiento antes de eliminar el back-end de almacenamiento. Siga los pasos a continuación para eliminar un backend de almacenamiento.

1. Inicie sesión en el cliente vSphere.

2. En la página de accesos directos, seleccione \*Herramientas de NetApp ONTAP\* en la sección de complementos.
3. En el panel izquierdo de las herramientas de ONTAP, navegue hasta **Backends de almacenamiento** y seleccione un backend de almacenamiento.
4. Seleccione el menú de puntos suspensivos verticales y seleccione **Eliminar**. Asegúrese de que el backend de almacenamiento no contenga ningún almacén de datos. Puede seguir el progreso en el panel de tareas recientes.

Puede realizar la operación de eliminación de clústeres ONTAP globales mediante el Administrador de herramientas de ONTAP.

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Backends de almacenamiento** en la barra lateral.
4. Seleccione el backend de almacenamiento que desea eliminar.
5. Seleccione el menú de puntos suspensivos verticales y seleccione **Eliminar**.

## Vista detallada del backend de almacenamiento

La página del backend de almacenamiento enumera todos los backends de almacenamiento. Puede realizar operaciones de descubrimiento, modificación y eliminación de almacenamiento en los backends de almacenamiento que agregó y no en la SVM secundaria individual del clúster.

Cuando selecciona el clúster principal o el secundario en el backend de almacenamiento, puede ver el resumen general del componente. Cuando selecciona el clúster principal, tiene el menú desplegable de acciones desde el cual puede realizar operaciones de descubrimiento de almacenamiento, modificación y eliminación.

La página de resumen proporciona los siguientes detalles:

- Estado del backend de almacenamiento
- Información de capacidad
- Información básica sobre la máquina virtual
- Información de red como la dirección IP y el puerto de la red. Para el SVM secundario, la información será la misma que la del backend de almacenamiento principal.
- Privilegios permitidos y restringidos para el backend de almacenamiento. Para el SVM secundario, la información será la misma que la del backend de almacenamiento principal. Los Privilegios solo se muestran en los backends de almacenamiento basados en clúster. Si agrega SVM como back-end de almacenamiento, no se mostrará la información de privilegios.
- La vista detallada del clúster del sistema ASA r2 no incluye la pestaña de niveles locales cuando la propiedad desagregada está configurada como "verdadera" para la SVM o el clúster.
- Para los sistemas SVM ASA r2, no se muestra el portlet de capacidad. El portal de capacidad solo es necesario cuando la propiedad desagregada está configurada como "verdadera" para la SVM o el clúster.
- Para los sistemas SVM ASA r2, la sección de información básica muestra el tipo de plataforma.

La pestaña de interfaz proporciona información detallada sobre la interfaz.

La pestaña de niveles locales proporciona información detallada sobre la lista agregada.

## Administrar instancias de vCenter Server

Las instancias de vCenter Server son plataformas de administración central que le permiten controlar hosts, máquinas virtuales y backends de almacenamiento.

### Disociar los backends de almacenamiento con la instancia de vCenter Server

La página de listado de vCenter Server muestra la cantidad de backends de almacenamiento asociados. Cada instancia de vCenter Server tiene la opción de asociarse o desasociarse con un backend de almacenamiento.

#### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione la instancia de vCenter Server requerida en la barra lateral.
4. Seleccione los puntos suspensivos verticales contra el vCenter Server que desea asociar o disociar con los backends de almacenamiento.
5. Seleccione **Disociar backend de almacenamiento**.

### Modificar una instancia de vCenter Server

Siga los pasos a continuación para modificar una instancia de vCenter Server.

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione la instancia de vCenter Server correspondiente en la barra lateral
4. Seleccione los puntos suspensivos verticales contra el vCenter Server que desea modificar y seleccione **Modificar**.
5. Modifique los detalles de la instancia de vCenter Server y seleccione **Modificar**.

### Eliminar una instancia de vCenter Server

Debes eliminar todos los backends de almacenamiento conectados al vCenter Server antes de eliminarlo.

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione las instancias de vCenter Server aplicables desde la barra lateral
4. Seleccione los puntos suspensivos verticales contra el vCenter Server que desea eliminar y seleccione **Eliminar**.



Después de eliminar instancias de vCenter Server, la aplicación ya no las mantendrá.

Al eliminar instancias de vCenter Server en las herramientas de ONTAP , se realizan automáticamente las siguientes acciones:

- El complemento no está registrado.
- Se eliminan los privilegios y roles del complemento.

## Administrar certificados

Se genera un certificado autofirmado para las herramientas ONTAP y el proveedor VASA de forma predeterminada durante la implementación. Utilizando la interfaz del Administrador de herramientas de ONTAP , puede renovar el certificado o actualizarlo a una CA personalizada. Los certificados CA personalizados son obligatorios en una implementación de varios vCenter.

### Antes de empezar

- El nombre de dominio en el que se emite el certificado debe asignarse a la dirección IP virtual.
- Ejecute la comprobación nslookup en el nombre de dominio para verificar si el dominio se está resolviendo en la dirección IP deseada.
- Los certificados deben crearse con el nombre de dominio y la dirección IP de las herramientas ONTAP .



Una dirección IP de herramientas ONTAP debe corresponder a un nombre de dominio completo (FQDN). Los certificados deben contener el mismo FQDN asignado a la dirección IP de las herramientas ONTAP en los nombres de sujeto o alternativos de sujeto.



No es posible cambiar de un certificado firmado por una CA a un certificado autofirmado.

## Actualizar el certificado de herramientas ONTAP

La pestaña de herramientas de ONTAP muestra detalles como el tipo de certificado (autofirmado/firmado por CA) y el nombre de dominio. Durante la implementación, se genera un certificado autofirmado de forma predeterminada. Puede renovar el certificado o actualizar el certificado a CA.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Certificados > Herramientas ONTAP \*** > **\*Renovar** para renovar los certificados.

Puede renovar el certificado si ha expirado o está próximo a expirar. La opción de renovación está disponible cuando el tipo de certificado está firmado por CA. En la ventana emergente, proporcione el certificado del servidor, la clave privada, la CA raíz y los detalles del certificado intermedio.



El sistema estará fuera de línea hasta que se renueve el certificado y se cerrará la sesión de la interfaz del Administrador de herramientas de ONTAP .

4. Para actualizar el certificado autofirmado a un certificado CA personalizado, seleccione la opción **Certificados > Herramientas ONTAP \*** > **\*Actualizar a CA**.
  - a. En la ventana emergente, cargue el certificado del servidor, la clave privada del certificado del servidor, el certificado de CA raíz y los archivos del certificado intermedio.
  - b. Ingrese el nombre de dominio para el cual generó este certificado y actualice el certificado.



El sistema estará fuera de línea hasta que se complete la actualización y se cerrará su sesión de la interfaz del Administrador de herramientas de ONTAP .

## Actualizar el certificado de proveedor de VASA

Las ONTAP tools for VMware vSphere se implementan con un certificado autofirmado para el proveedor VASA. Con esto, solo se puede administrar una instancia de vCenter Server para los almacenes de datos de vVols . Cuando administra varias instancias de vCenter Server y desea habilitar la capacidad vVols en ellas, debe cambiar el certificado autofirmado a un certificado CA personalizado.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Certificados > Proveedor VASA o Herramientas ONTAP \*** > **\*Renovar** para renovar los certificados.
4. Seleccione **Certificados > Proveedor VASA o Herramientas ONTAP \*** > **\*Actualizar a CA** para actualizar el certificado autofirmado a un certificado CA personalizado.
  - a. En la ventana emergente, cargue el certificado del servidor, la clave privada del certificado del servidor, el certificado de CA raíz y los archivos del certificado intermedio.
  - b. Ingrese el nombre de dominio para el cual generó este certificado y actualice el certificado.



El sistema estará fuera de línea hasta que se complete la actualización y se cerrará su sesión de la interfaz del Administrador de herramientas de ONTAP .

## Acceda a las ONTAP tools for VMware vSphere

### Descripción general de las ONTAP tools for VMware vSphere

Puede administrar sus configuraciones de aplicaciones, sistemas y redes mediante la consola de mantenimiento de las herramientas ONTAP . Puede cambiar su contraseña de administrador y su contraseña de mantenimiento. También puede generar paquetes de soporte, establecer diferentes niveles de registro, ver y administrar configuraciones de TLS e iniciar diagnósticos remotos.

Debe tener las herramientas de VMware instaladas después de implementar las ONTAP tools for VMware vSphere para acceder a la consola de mantenimiento. Deberías usar `maint` como el nombre de usuario y la contraseña que configuró durante la implementación para iniciar sesión en la consola de mantenimiento de las herramientas ONTAP . Debes usar `nano` para editar los archivos en la consola de inicio de sesión de mantenimiento o root.



Debes establecer una contraseña para el `diag` usuario mientras habilita el diagnóstico remoto.

Debe utilizar la pestaña **Resumen** de las ONTAP tools for VMware vSphere para acceder a la consola de mantenimiento. Cuando seleccionas  , se inicia la consola de mantenimiento.

Menú de la consola	Opciones
Configuración de la aplicación	<ol style="list-style-type: none"> <li>1. Mostrar resumen del estado del servidor</li> <li>2. Cambiar el nivel de LOG para los servicios de proveedor de VASA y los servicios de SRA</li> </ol>
Configuración del sistema	<ol style="list-style-type: none"> <li>1. Reiniciar la máquina virtual</li> <li>2. Apagar la máquina virtual</li> <li>3. Cambiar la contraseña del usuario 'maint'</li> <li>4. Cambiar zona horaria</li> <li>5. Aumentar el tamaño del disco de la cárcel (/jail)</li> <li>6. Mejora</li> <li>7. Instalar VMware Tools</li> </ol>

Configuración de red	<ol style="list-style-type: none"> <li>1. Mostrar la configuración de la dirección IP</li> <li>2. Mostrar la configuración de búsqueda de nombres de dominio</li> <li>3. Cambiar la configuración de búsqueda del nombre de dominio</li> <li>4. Mostrar rutas estáticas</li> <li>5. Cambiar rutas estáticas</li> <li>6. Confirmar cambios</li> <li>7. Hacer ping a un host</li> <li>8. Restaurar la configuración predeterminada</li> </ol>
Soporte y diagnóstico	<ol style="list-style-type: none"> <li>1. Acceso al shell de diagnóstico</li> <li>2. Habilitar el acceso de diagnóstico remoto</li> <li>3. Proporcionar credenciales de vCenter para la copia de seguridad</li> <li>4. Tomar copia de seguridad</li> </ol>

## Configurar el acceso de diagnóstico remoto

Puede configurar las ONTAP tools for VMware vSphere para habilitar el acceso SSH para el usuario diag.

### Antes de empezar

La extensión del proveedor VASA debe estar habilitada para su instancia de vCenter Server.

### Acerca de esta tarea

El uso de SSH para acceder a la cuenta de usuario diag tiene las siguientes limitaciones:

- Solo se permite una cuenta de inicio de sesión por activación de SSH.
- El acceso SSH a la cuenta de usuario diag se deshabilita cuando ocurre una de las siguientes situaciones:
  - El tiempo expira.

La sesión de inicio de sesión seguirá siendo válida solo hasta la medianoche del día siguiente.

- Vuelve a iniciar sesión como usuario diag usando SSH.

### Pasos

1. Desde vCenter Server, abra una consola en VASA Provider.
2. Inicie sesión como usuario de mantenimiento.
3. Ingresar 4 para seleccionar Soporte y Diagnóstico.
4. Ingresar 2 para seleccionar Habilitar acceso a diagnóstico remoto.
5. Ingresar **y** en el cuadro de diálogo Confirmación para habilitar el acceso de diagnóstico remoto.

6. Introduzca una contraseña para el acceso de diagnóstico remoto.

## Iniciar SSH en otros nodos

Debe iniciar SSH en otros nodos antes de actualizar.

### Antes de empezar

La extensión del proveedor VASA debe estar habilitada para su instancia de vCenter Server.

### Acerca de esta tarea

Realice este procedimiento en cada uno de los nodos antes de actualizar.

### Pasos

1. Desde vCenter Server, abra una consola en VASA Provider.
2. Inicie sesión como usuario de mantenimiento.
3. Ingresar 4 para seleccionar Soporte y Diagnóstico.
4. Ingresar 1 para seleccionar Acceder al shell de diagnóstico.
5. Ingresar y Para proceder.
6. Ejecute el comando *sudo systemctl restart ssh*.

## Actualice las credenciales de vCenter Server y ONTAP

Puede actualizar la instancia de vCenter Server y las credenciales de ONTAP mediante la consola de mantenimiento.

### Antes de empezar

Necesita tener credenciales de inicio de sesión de usuario de mantenimiento.

### Acerca de esta tarea

Si ha cambiado las credenciales de vCenter Server, ONTAP o Data LIF después de la implementación, deberá actualizarlas mediante este procedimiento.

### Pasos

1. Desde vCenter Server, abra una consola en VASA Provider.
2. Inicie sesión como usuario de mantenimiento.
3. Ingresar 2 para seleccionar el Menú de Configuración del Sistema.
4. Ingresar 9 para cambiar las credenciales de ONTAP .
5. Ingresar 10 para cambiar las credenciales de vCenter.

## Informes de herramientas de ONTAP

El complemento de ONTAP tools for VMware vSphere proporciona informes para máquinas virtuales y almacenes de datos. Cuando selecciona el ícono del complemento de herramientas NetApp ONTAP tools for VMware vSphere en la sección de accesos

directos del cliente vCenter, la interfaz de usuario navega a la página Descripción general. Seleccione la pestaña Informes para ver el informe de la máquina virtual y del almacén de datos.

El informe de máquinas virtuales muestra la lista de máquinas virtuales descubiertas (deben tener al menos un disco de los almacenes de datos basados en almacenamiento ONTAP ) con métricas de rendimiento. Al expandir el registro de VM, se muestra toda la información del almacén de datos relacionada con el disco.

El informe de almacenes de datos muestra la lista de ONTAP tools for VMware vSphere que se aprovisionan desde el backend de almacenamiento ONTAP de todo tipo con métricas de rendimiento.

Puede utilizar la opción Administrar columnas para ocultar o mostrar diferentes columnas.

## Recopilar los archivos de registro

Puede recopilar archivos de registro de las ONTAP tools for VMware vSphere desde las opciones disponibles en la interfaz de usuario del Administrador de herramientas ONTAP . Es posible que el soporte técnico le solicite que recopile los archivos de registro para ayudar a solucionar un problema.



La generación de registros desde el Administrador de herramientas de ONTAP incluye todos los registros de todas las instancias de vCenter Server. La generación de registros desde la interfaz de usuario del cliente vCenter está limitada al servidor vCenter seleccionado.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Paquetes de registro** en la barra lateral.

Esta operación puede tardar varios minutos.

4. Seleccione **Generar** para generar los archivos de registro.
5. Ingrese la etiqueta para el paquete de registro y seleccione **Generar**.

Descargue el archivo tar.gz y envíelo al soporte técnico.

Siga los pasos a continuación para generar un paquete de registros mediante la interfaz de usuario del cliente vCenter:

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Desde la página de inicio de vSphere Client, vaya a **Soporte > Paquete de registros > Generar**.
3. Proporcione la etiqueta del paquete de registro y genere el paquete. Podrá ver la opción de descarga cuando se generen los archivos. La descarga puede tardar un poco.



El paquete de registros generado reemplaza el paquete de registros que se generó en los últimos 3 días o 72 horas.

## Administrar máquinas virtuales

### Consideraciones para migrar o clonar máquinas virtuales

Debe tener en cuenta algunas consideraciones al migrar máquinas virtuales existentes en su centro de datos.

#### Migrar máquinas virtuales protegidas

Puede migrar las máquinas virtuales protegidas a:

- El mismo almacén de datos vVols en un host ESXi diferente
- Diferentes almacenes de datos vVols compatibles en el mismo host ESXi
- Diferentes almacenes de datos vVols compatibles en un host ESXi diferente

Si la máquina virtual se migra a un FlexVol volume diferente, el archivo de metadatos correspondiente también se actualiza con la información de la máquina virtual. Si se migra una máquina virtual a un host ESXi diferente pero al mismo almacenamiento, el archivo de metadatos del FlexVol volume subyacente no se modificará.

#### Clonar máquinas virtuales protegidas

Puede clonar máquinas virtuales protegidas de la siguiente manera:

- El mismo contenedor del mismo FlexVol volume usando el grupo de replicación

El mismo archivo de metadatos del volumen FlexVol se actualiza con los detalles de la máquina virtual clonada.

- El mismo contenedor de un FlexVol volume diferente que utiliza un grupo de replicación

El FlexVol volume donde se coloca la máquina virtual clonada, el archivo de metadatos se actualiza con los detalles de la máquina virtual clonada.

- Diferentes almacenes de datos de contenedores o vVols

El FlexVol volume donde se coloca la máquina virtual clonada, el archivo de metadatos obtiene detalles actualizados de la máquina virtual.

Actualmente, VMware no admite máquinas virtuales clonadas en una plantilla de VM.

Se admite la clonación de clones de una máquina virtual protegida.

Referirse a "[Creación de una máquina virtual para clonar](#)" Para más detalles.

#### Instantáneas de máquinas virtuales

Actualmente solo se admiten instantáneas de máquinas virtuales sin memoria. Si la máquina virtual tiene una instantánea con memoria, entonces la máquina virtual no se considera para protección.

Tampoco puedes proteger máquinas virtuales desprotegidas que tengan instantáneas de memoria. Para esta versión, se espera que elimine la instantánea de memoria antes de habilitar la protección para la máquina virtual.

Para las máquinas virtuales de Windows con tipo de almacenamiento ASA r2, cuando toma una instantánea de la máquina virtual, será una instantánea de solo lectura. Cuando hay energía disponible para la VM, el proveedor VASA crea un LUN usando la instantánea de solo lectura y luego lo habilita para IOPS. Durante la solicitud de apagado, VASA Provider elimina el LUN que se creó y luego deshabilita las IOPS.

## Migrar máquinas virtuales con almacenes de datos NFS y VMFS a almacenes de datos vVols

Puede migrar máquinas virtuales desde almacenes de datos NFS y VMFS a almacenes de datos de Virtual Volumes (vVols) para aprovechar la administración de máquinas virtuales basada en políticas y otras capacidades de vVols . Los almacenes de datos de vVols le permiten cumplir con los requisitos de mayor carga de trabajo.

### Antes de empezar

Asegúrese de que VASA Provider no se esté ejecutando en ninguna de las máquinas virtuales que planea migrar. Si migra una máquina virtual que ejecuta VASA Provider a un almacén de datos vVols , no podrá realizar ninguna operación de administración, incluido el encendido de las máquinas virtuales que están en almacenes de datos vVols .

### Acerca de esta tarea

Cuando migra desde un almacén de datos NFS y VMFS a un almacén de datos vVols , vCenter Server utiliza las API de vStorage para la descarga de integración de matrices (VAAI) al mover datos desde almacenes de datos VMFS, pero no desde un archivo VMDK de NFS. Las descargas de VAAI normalmente reducen la carga en el host.

### Pasos

1. Haga clic derecho en la máquina virtual que desea migrar y seleccione **Migrar**.
2. Seleccione **Cambiar solo almacenamiento** y luego seleccione **Siguiente**.
3. Seleccione un formato de disco virtual, una política de almacenamiento de VM y un almacén de datos vVol que coincida con las características del almacén de datos que está migrando.
4. Revise la configuración y seleccione **Finalizar**.

## Limpieza de VASA

Utilice los pasos de esta sección para realizar la limpieza de VASA.



Se recomienda que elimine todos los almacenes de datos vVols antes de realizar la limpieza de VASA.

### Pasos

1. Anule el registro del complemento yendo a [https://OTV\\_IP:8143/Register.html](https://OTV_IP:8143/Register.html)
2. Verifique que el complemento ya no esté disponible en vCenter Server.
3. Apague las ONTAP tools for VMware vSphere VM.
4. Eliminar ONTAP tools for VMware vSphere VM.

## Conectar o desconectar un disco de datos de una máquina virtual

### Adjuntar un disco de datos a una máquina virtual

Conecte un disco de datos a una máquina virtual para ampliar la capacidad de almacenamiento.

#### Pasos

1. Inicie sesión en el cliente vSphere.
2. Haga clic derecho en una máquina virtual en el inventario y seleccione **Editar configuración**.
3. En la pestaña **Hardware virtual**, seleccione **Disco duro existente**.
4. Seleccione la máquina virtual donde existe el disco.
5. Seleccione el disco que desea conectar y seleccione **Aceptar**

#### Resultado

El disco duro aparece en la lista de dispositivos de hardware virtual.

### Desconectar un disco de datos de la máquina virtual

Puede desconectar un disco de datos conectado a una máquina virtual cuando ya no sea necesario. Cuando se separa el disco de la máquina virtual, no se elimina automáticamente; permanece en el sistema de almacenamiento ONTAP .

#### Pasos

1. Inicie sesión en el cliente vSphere.
2. Haga clic derecho en una máquina virtual en el inventario y seleccione **Editar configuración**.
3. Mueva el puntero sobre el disco y seleccione **Quitar**.



El disco se elimina de la máquina virtual. Si otras máquinas virtuales comparten el disco, los archivos del disco no se eliminan.

#### Información relacionada

["Agregar un nuevo disco duro a una máquina virtual"](#)

["Agregar un disco duro existente a una máquina virtual"](#)

## Descubra los sistemas de almacenamiento y hosts

Cuando ejecuta por primera vez las ONTAP tools for VMware vSphere en un cliente vSphere, las herramientas ONTAP detectan los hosts ESXi, sus LUN y exportaciones NFS, y los sistemas de almacenamiento NetApp que poseen esos LUN y exportaciones.

#### Antes de empezar

- Todos los hosts ESXi deben estar encendidos y conectados.
- Todas las máquinas virtuales de almacenamiento (SVM) que se van a descubrir deben estar en ejecución, y cada nodo del clúster debe tener al menos un LIF de datos configurado para el protocolo de almacenamiento en uso (NFS o iSCSI).

#### Acerca de esta tarea

Puede descubrir nuevos sistemas de almacenamiento o actualizar información sobre sistemas de almacenamiento existentes para obtener la información más reciente sobre capacidad y configuración en cualquier momento. También puede modificar las credenciales que las ONTAP tools for VMware vSphere utilizan para iniciar sesión en los sistemas de almacenamiento.

Al descubrir los sistemas de almacenamiento, las ONTAP tools for VMware vSphere recopilan información de los hosts ESXi administrados por la instancia de vCenter Server.

### Pasos

1. Desde la página de inicio de vSphere Client, seleccione **Hosts y clústeres**.
2. Haga clic con el botón derecho en el centro de datos requerido y seleccione \* Herramientas de NetApp ONTAP \* > \* Actualizar datos del host \*.

En el cuadro de diálogo **Confirmar**, confirme su elección.

3. Seleccione los controladores de almacenamiento detectados que tengan el estado `Authentication Failure` y seleccione **Acciones > Modificar**.
4. Complete la información requerida en el cuadro de diálogo **Modificar sistema de almacenamiento**.
5. Repita los pasos 4 y 5 para todos los controladores de almacenamiento con `Authentication Failure` estado.

Una vez completado el proceso de descubrimiento, realice las siguientes acciones:

- Utilice las ONTAP tools for VMware vSphere para configurar los ajustes del host ESXi para los hosts que muestran el ícono de alerta en la columna de configuración del adaptador, la columna de configuración de MPIO o la columna de configuración de NFS.
- Proporcione las credenciales del sistema de almacenamiento.

## Modificar la configuración del host ESXi mediante las herramientas ONTAP

Puede utilizar el panel de ONTAP tools for VMware vSphere para editar la configuración de su host ESXi.

### Antes de empezar

Si hay un problema con la configuración de su host ESXi, el problema se muestra en el portlet de sistemas de host ESXi del panel. Puede seleccionar el problema para ver el nombre del host o la dirección IP del host ESXi que tiene el problema.

### Pasos

1. Inicie sesión en el cliente vSphere.
2. En la página de accesos directos, seleccione \*Herramientas de NetApp ONTAP\* en la sección de complementos.
3. Vaya al portlet **Cumplimiento de host ESXi** en la Descripción general (panel de control) del complemento de ONTAP tools for VMware vSphere .
4. Seleccione el enlace **Aplicar configuración recomendada**.
5. En la ventana **Aplicar configuración de host recomendada**, seleccione los hosts que desea que cumplan con la configuración de host recomendada de NetApp y seleccione **Siguiente**.



Puede expandir el host ESXi para ver los valores actuales.

6. En la página de configuración, seleccione los valores recomendados según sea necesario.
7. En el panel de resumen, verifique los valores y seleccione **Finalizar**. Puede seguir el progreso en el panel de tareas recientes.

#### Información relacionada

["Configurar los ajustes del host ESXi"](#)

## Administrar contraseñas

### Cambiar la contraseña del administrador de herramientas de ONTAP

Puede cambiar la contraseña de administrador utilizando el Administrador de herramientas de ONTAP .

#### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione el ícono de **administrador** en la esquina superior derecha de la pantalla y seleccione **Cambiar contraseña**.
4. En la ventana emergente de cambio de contraseña, ingrese la contraseña anterior y los detalles de la nueva contraseña. La restricción para cambiar la contraseña se muestra en la pantalla de la interfaz de usuario.
5. Seleccione **Cambiar** para implementar los cambios.

### Restablecer la contraseña del administrador de herramientas de ONTAP

Si olvidó la contraseña del administrador de herramientas de ONTAP , puede restablecer las credenciales de administrador usando el token generado por la consola de mantenimiento de ONTAP tools for VMware vSphere .

#### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. En la pantalla de inicio de sesión, seleccione la opción **Restablecer contraseña**.

Para restablecer la contraseña del administrador, debe generar el token de restablecimiento utilizando las ONTAP tools for VMware vSphere .

- a. Desde vCenter Server, abra la consola de mantenimiento
  - b. Ingrese '2' para seleccionar la opción Configuración del sistema
  - c. Introduzca '3' para cambiar la contraseña del usuario 'maint'.
3. En la ventana emergente de cambio de contraseña, ingrese el token de restablecimiento de contraseña, el nombre de usuario y los detalles de la nueva contraseña.

4. Seleccione **Restablecer** para implementar los cambios. Después de restablecer exitosamente la contraseña, podrá usar la nueva contraseña para iniciar sesión.

## Restablecer la contraseña del usuario de la aplicación

La contraseña del usuario de la aplicación se utiliza para el registro del proveedor SRA y VASA con vCenter Server.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Configuración** en la barra lateral.
4. En la pantalla **Credenciales VASA/SRA**, seleccione **Restablecer contraseña**.
5. Proporcione una nueva contraseña y confirme la entrada de la nueva contraseña.
6. Seleccione **Restablecer** para implementar los cambios.

## Restablecer la contraseña del usuario de la consola de mantenimiento

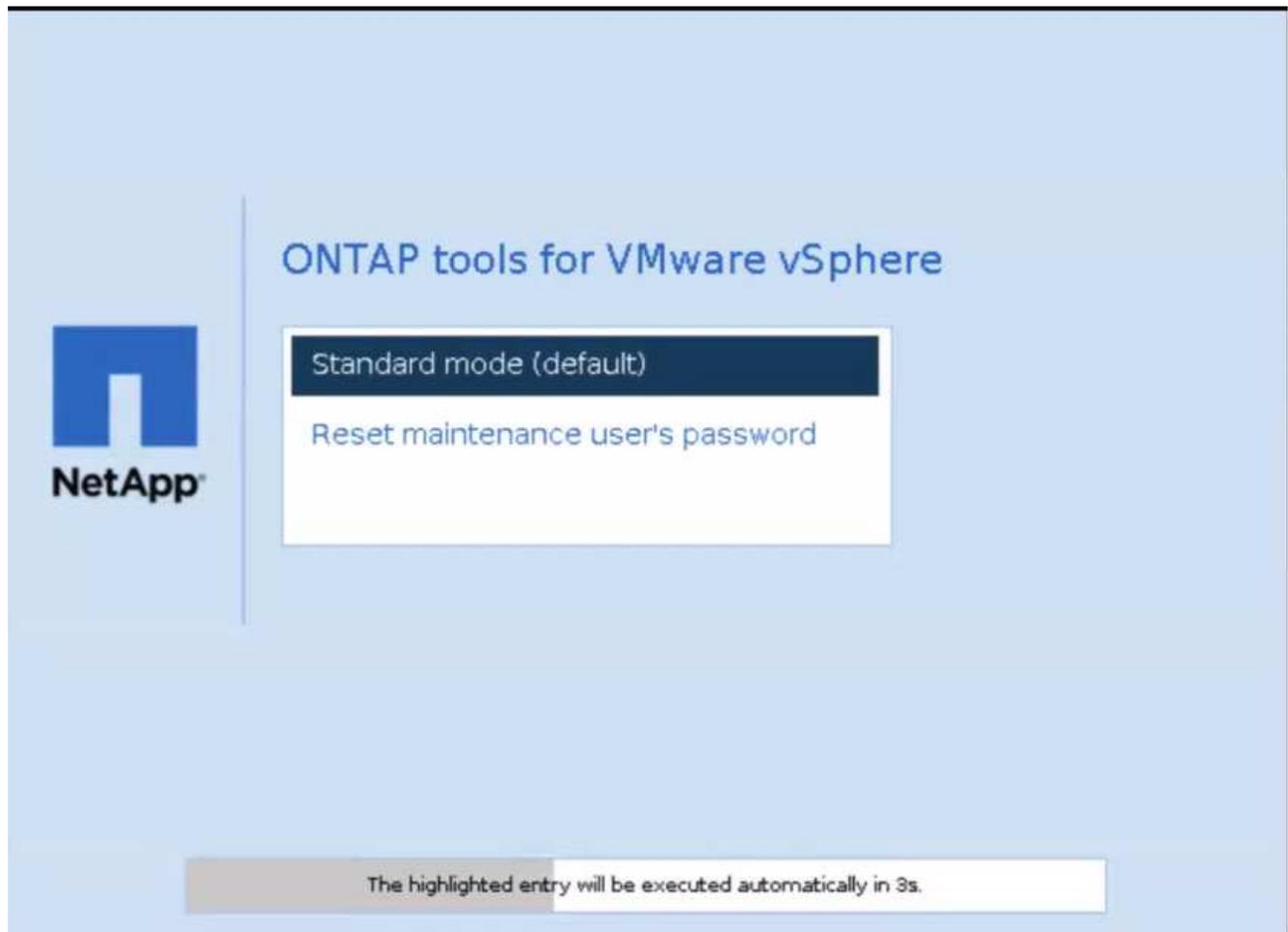
Durante el reinicio del sistema operativo invitado, el menú de grub muestra una opción para restablecer la contraseña del usuario de la consola de mantenimiento. Esta opción se utiliza para actualizar la contraseña del usuario de la consola de mantenimiento presente en la máquina virtual correspondiente. Una vez restablecida la contraseña, la máquina virtual se reinicia para establecer la nueva. En una implementación de alta disponibilidad (HA), tras reiniciar la máquina virtual, la contraseña se actualiza automáticamente en las otras dos máquinas virtuales.



Para las ONTAP tools for VMware vSphere HA, debe cambiar la contraseña del usuario de la consola de mantenimiento en el primer nodo, que es el nodo1.

### Pasos

1. Inicie sesión en su vCenter Server
2. Haga clic derecho en la máquina virtual y seleccione **Encendido > Reiniciar sistema operativo invitado**. Durante el reinicio del sistema, aparecerá la siguiente pantalla:



Tienes 5 segundos para elegir tu opción. Presione cualquier tecla para detener el progreso y congelar el menú de GRUB.

3. Seleccione la opción **Restablecer contraseña de usuario de mantenimiento**. Se abre la consola de mantenimiento.
4. En la consola, ingrese los detalles de la nueva contraseña. La nueva contraseña y los detalles de la nueva contraseña reingresada deben coincidir para restablecer la contraseña exitosamente. Tienes tres oportunidades para ingresar la contraseña correcta. El sistema se reinicia después de ingresar exitosamente la nueva contraseña.
5. Presione Enter para continuar. La contraseña se actualiza en la VM.



El mismo menú de GRUB también aparece durante el encendido de la VM. Sin embargo, debe utilizar la opción de restablecer contraseña solo con la opción **Reiniciar sistema operativo invitado**.

## Administrar la protección del clúster de host

### Modificar el clúster de host protegido

Puede realizar las siguientes tareas como parte de la protección contra modificaciones. Puede realizar todos los cambios en el mismo flujo de trabajo.

- Agregue nuevos almacenes de datos o hosts al clúster protegido.
- Agregue nuevas relaciones SnapMirror a la configuración de protección.
- Eliminar las relaciones SnapMirror existentes de la configuración de protección.
- Modificar una relación SnapMirror existente.

## Supervisar la protección del clúster de host

Utilice este procedimiento para supervisar el estado de la protección del clúster del host. Puede supervisar cada clúster de host protegido junto con su estado de protección, relaciones de SnapMirror, almacenes de datos y el estado de SnapMirror correspondiente.

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Vaya a **Herramientas de NetApp ONTAP** > **Protección** > **Relaciones de clúster de host**.

El icono debajo de la columna de protección muestra el estado de la protección.

3. Pase el cursor sobre el ícono para ver más detalles.

## Agregar nuevos almacenes de datos o hosts

Utilice este procedimiento para proteger los almacenes de datos o hosts recién agregados. Puede agregar nuevos hosts al clúster protegido o crear nuevos almacenes de datos en el clúster de hosts mediante la interfaz de usuario nativa de vCenter.

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Para editar las propiedades de un clúster protegido, puede:
  - a. Vaya a **Herramientas de NetApp ONTAP** > **Protección** > **Relaciones de clúster de host**, seleccione el menú de puntos suspensivos frente al clúster y seleccione **Editar** o
  - b. Haga clic con el botón derecho en un clúster de host y seleccione **Herramientas de NetApp ONTAP** > **Proteger clúster**.
3. Si ha creado un almacén de datos en la interfaz de usuario nativa de vCenter, ese almacén de datos se muestra como desprotegido. La interfaz de usuario muestra todos los almacenes de datos del clúster y su estado de protección en un cuadro de diálogo. Seleccione el botón **Proteger** para habilitar la protección completa.
4. Si ha agregado un nuevo host ESXi, el estado de protección se muestra como parcialmente protegido. Seleccione el menú de puntos suspensivos en la configuración de SnapMirror y seleccione **Editar** para establecer la proximidad del host ESXi recién agregado.



En el caso de una relación asíncrona, no se admite la acción de edición porque no se puede agregar el SVM de destino del sitio terciario a la misma instancia de herramientas de ONTAP. Sin embargo, se puede usar el administrador del sistema o la CLI del SVM de destino para cambiar la configuración de la relación.

5. Seleccione **Guardar** después de realizar los cambios necesarios.
6. Puede ver los cambios en la ventana **Proteger clúster**.

Se crea una tarea de vCenter y puedes seguir el progreso en el panel **Tarea reciente**.

## Agregar una nueva relación SnapMirror

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Para editar las propiedades de un clúster protegido, puede:
  - a. Vaya a \* Herramientas de NetApp ONTAP \* > \* Protección \* > \* Relaciones de clúster de host \* , seleccione el menú de puntos suspensivos frente al clúster y seleccione \* Editar \* o
  - b. Haga clic con el botón derecho en un clúster de host y seleccione \* Herramientas de NetApp ONTAP \* > \* Proteger clúster \* .
3. Seleccione **Agregar relación**.
4. Agregue una nueva relación como tipo de política **Asincrónica** o **AutomatedFailOverDuplex**.
5. Seleccione **Proteger**.

Puede ver los cambios en la ventana **Proteger clúster**.

Se crea una tarea de vCenter y puedes seguir el progreso en el panel **Tarea reciente**.

### Eliminar una relación SnapMirror existente

Para eliminar una relación SnapMirror asincrónica, se debe agregar un SVM o clúster del sitio secundario como back-end de almacenamiento en las ONTAP tools for VMware vSphere. No puedes eliminar todas las relaciones de SnapMirror . Cuando se elimina una relación, también se elimina la relación correspondiente en el clúster ONTAP . Cuando se elimina una relación AutomatedFailOverDuplex SnapMirror , los almacenes de datos en el destino se desasignan y el grupo de consistencia, los LUN, los volúmenes y los igroups se eliminan del clúster ONTAP de destino.

Al eliminar la relación, se activa un nuevo escaneo en el sitio secundario para eliminar el LUN no asignado como ruta activa de los hosts.

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Para editar las propiedades de un clúster protegido, puede:
  - a. Vaya a \* Herramientas de NetApp ONTAP \* > \* Protección \* > \* Relaciones de clúster de host \* , seleccione el menú de puntos suspensivos frente al clúster y seleccione \* Editar \* o
  - b. Haga clic con el botón derecho en un clúster de host y seleccione \* Herramientas de NetApp ONTAP \* > \* Proteger clúster \* .
3. Seleccione el menú de puntos suspensivos en la configuración de SnapMirror y seleccione **Eliminar**.

Se crea una tarea de vCenter y puedes seguir el progreso en el panel **Tarea reciente**.

### Modificar una relación SnapMirror existente

Para modificar una relación SnapMirror asincrónica, se debe agregar un SVM o clúster de sitio secundario como back-end de almacenamiento en las ONTAP tools for VMware vSphere. Si se trata de una relación AutomatedFailOverDuplex SnapMirror , puede modificar la proximidad del host en caso de configuración uniforme y el acceso al host en caso de configuración no uniforme. No se pueden intercambiar los tipos de políticas Asynchronous y AutomatedFailOverDuplex. Puede configurar la proximidad o el acceso para los hosts recién descubiertos en el clúster.



No se puede editar una relación SnapMirror asincrónica existente.

### Pasos

1. Inicie sesión en el cliente vSphere.
2. Para editar las propiedades de un clúster protegido, puede:
  - a. Vaya a \* Herramientas de NetApp ONTAP \* > \* Protección \* > \* Relaciones de clúster de host \* , seleccione el menú de puntos suspensivos frente al clúster y seleccione \* Editar \* o
  - b. Haga clic con el botón derecho en un clúster de host y seleccione \* Herramientas de NetApp ONTAP \* > \* Proteger clúster \* .
3. Si se selecciona el tipo de política AutomatedFailOverDuplex, agregue detalles de proximidad del host o acceso del host.
4. Seleccione el botón **Proteger**.

Se crea una tarea de vCenter y puedes seguir el progreso en el panel **Tarea reciente**.

## Eliminar la protección del clúster de host

Cuando se elimina la protección del clúster del host, los almacenes de datos quedan desprotegidos.

### Pasos

1. Para ver los clústeres de host protegidos, navegue a \* Herramientas de NetApp ONTAP \* > \* Protección \* > \* Relaciones de clúster de host \* .

En esta página, puede supervisar los clústeres de host protegidos junto con su estado de protección, la relación de SnapMirror y su estado de SnapMirror correspondiente.

2. En la ventana **Protección del clúster de host**, seleccione el menú de puntos suspensivos frente al clúster y, a continuación, seleccione **Eliminar protección**.

## Deshabilitar AutoSupport

Al configurar su sistema de almacenamiento por primera vez, AutoSupport está habilitado de forma predeterminada. Envía mensajes al soporte técnico 24 horas después de su habilitación. Al desactivar AutoSupport, ya no recibirá soporte ni supervisión proactiva.



Se recomienda que mantenga habilitado el AutoSupport . Ayuda a acelerar la detección y resolución de problemas. El sistema recopila información de AutoSupport y la almacena localmente, incluso cuando está deshabilitado. Sin embargo, no envía el informe a ninguna red.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione la opción **Configuración > Telemetría > Editar**.

4. Deseleccione la opción \* AutoSupport\* y guarde los cambios.

## Actualizar la URL del proxy de AutoSupport

Actualice la URL del proxy de AutoSupport para garantizar el correcto funcionamiento de la función AutoSupport en escenarios donde se utiliza un servidor proxy para el control de acceso a la red o medidas de seguridad. Permite que los datos de AutoSupport se enruten a través del proxy apropiado, lo que posibilita la transmisión segura y el cumplimiento.

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione **Configuración** en la barra lateral.
4. Seleccione la opción **Configuración > Telemetría > Editar**.
5. Ingrese una **URL de proxy** válida y guarde los cambios.

Si deshabilita AutoSupport, la URL del proxy también se deshabilitará.

## Agregar servidores NTP

Ingrese los detalles del servidor NTP para sincronizar los relojes de tiempo del dispositivo de herramientas ONTAP .

### Pasos

1. Inicie el Administrador de herramientas de ONTAP desde un navegador web:  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicie sesión con las credenciales de administrador de las ONTAP tools for VMware vSphere que proporcionó durante la implementación.
3. Seleccione la opción **Configuración > Servidor NTP > Editar**.
4. Ingrese el nombre de dominio completo (FQDN) separado por comas, direcciones IPv4 o IPv6.

Actualice la pantalla para ver los valores actualizados.

## Crear copia de seguridad y recuperar la configuración de las herramientas ONTAP

A partir de las ONTAP tools for VMware vSphere 10.3, el dispositivo utiliza un proveedor de almacenamiento dinámico, por lo que no es posible alcanzar un RPO cero. Sin embargo, es posible alcanzar un RPO cercano a cero. Para lograr un RPO cercano a cero, debe crear una copia de seguridad de la configuración y restaurarla en una nueva máquina virtual.



Para migrar a HA cuando la copia de seguridad que no es de HA está habilitada, primero deshabilite la copia de seguridad y vuelva a habilitarla después de la migración.

## Crear una copia de seguridad y descargar el archivo de copia de seguridad

### Pasos

1. Desde vCenter Server, abra la consola de mantenimiento.
2. Inicie sesión como usuario de mantenimiento.
3. Ingresar 4 para seleccionar **Soporte y Diagnóstico**.
4. Ingresar 3 para seleccionar la opción **Habilitar copia de seguridad del sistema**.
5. En caso de no ser HA, ingrese las credenciales de vCenter donde está implementada la máquina virtual de herramientas ONTAP .
6. Introduzca el valor de frecuencia de copia de seguridad entre 5 y 60 minutos.
7. Presione **Enter**

Esto crea la copia de seguridad y la envía al almacén de datos de la máquina virtual a intervalos regulares.

8. Para acceder a la copia de seguridad, navegue a la sección de almacenamiento y seleccione el almacén de datos de la máquina virtual
9. Seleccione la sección **Archivos**.

En la sección de archivos, puedes ver el directorio. El nombre del directorio será la dirección IP de las herramientas ONTAP , donde los puntos (.) se reemplazan por guiones bajos, con el sufijo *backup*.

10. Para obtener más información sobre la copia de seguridad, descargue el archivo backup\_info.txt desde **Archivos > Descargar**.

## Recuperar

Para recuperar la configuración, apague la máquina virtual existente e implemente una nueva máquina virtual utilizando el OVA que se utilizó en la implementación inicial.

Debe utilizar la misma dirección IP de las herramientas ONTAP para la nueva máquina virtual y la configuración del sistema, como los servicios habilitados, el tamaño del nodo y el modo HA, deben ser los mismos que en la implementación inicial.

Realice los siguientes pasos para recuperar la configuración desde el archivo de respaldo.

1. Desde vCenter Server, abra la consola de mantenimiento.
2. Inicie sesión como usuario de mantenimiento.
3. Ingresar 4 para seleccionar **Soporte y Diagnóstico**.
4. Ingresar 2 para seleccionar la opción **Habilitar acceso de diagnóstico remoto** y crear una nueva contraseña para el acceso de diagnóstico.
5. Seleccione cualquier copia de seguridad del directorio descargado. El nombre del último archivo de respaldo se registra en el archivo *backup\_info.txt*.
6. Ejecute el siguiente comando para copiar la copia de seguridad a la nueva máquina virtual e ingrese la

contraseña de diagnóstico cuando se le solicite.

```
scp <Backup_X.tar.enc> diag@<node_ip>:/home/diag/system_recovery.tar.enc
```



No altere la ruta de destino ni el nombre del archivo (/home/diag/system\_recovery.tar.enc) mencionados en el comando.

7. Después de copiar el archivo de respaldo, inicie sesión en el shell de diagnóstico y ejecute el siguiente comando:

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

Los registros se graban en el archivo */var/log/post-deploy-upgrade.log*.

8. Después de una recuperación exitosa, se restauran los servicios y los objetos de vCenter.

## Desinstalar las ONTAP tools for VMware vSphere

Al desinstalar las ONTAP tools for VMware vSphere se eliminan todos los datos de las herramientas.

### Pasos

1. Elimine o mueva todas las máquinas virtuales de las ONTAP tools for VMware vSphere .
  - Para eliminar las máquinas virtuales, consulte ["Eliminar y volver a registrar máquinas virtuales y plantillas de máquinas virtuales"](#)
  - Para moverlos a un almacén de datos no administrado, consulte ["Cómo migrar su máquina virtual con Storage vMotion"](#)
2. ["Eliminar almacenes de datos"](#) Creado en ONTAP tools for VMware vSphere.
3. Si ha habilitado el proveedor VASA, seleccione **Configuración > Configuración del proveedor VASA > Cancelar registro** en las herramientas de ONTAP para cancelar el registro de los proveedores VASA de todos los servidores vCenter.
4. Desasociar todos los backends de almacenamiento de la instancia de vCenter Server. Consulte ["Disociar los backends de almacenamiento con la instancia de vCenter Server"](#) .
5. Eliminar todos los backends de almacenamiento. Consulte ["Administrar backends de almacenamiento"](#) .
6. Eliminar el adaptador SRA de VMware Live Site Recovery:
  - a. Inicie sesión como administrador en la interfaz de administración del dispositivo VMware Live Site Recovery mediante el puerto 5480.
  - b. Seleccione **Adaptadores de replicación de almacenamiento**.
  - c. Seleccione la tarjeta SRA adecuada y, en el menú desplegable, seleccione **Eliminar**.
  - d. Confirme que conoce los resultados de eliminar el adaptador y seleccione **Eliminar**.
7. Eliminar las instancias del servidor vCenter incorporadas a las ONTAP tools for VMware vSphere. Consulte ["Administrar instancias de vCenter Server"](#) .
8. Apague las ONTAP tools for VMware vSphere desde vCenter Server y elimine las máquinas virtuales.

## ¿Que sigue?

["Eliminar volúmenes FlexVol"](#)

# Eliminar volúmenes FlexVol

Cuando se utiliza un clúster ONTAP dedicado para herramientas ONTAP para la implementación de VMware, se crean muchos volúmenes FlexVol sin usar. Después de eliminar las ONTAP tools for VMware vSphere, debe eliminar los volúmenes FlexVol para evitar posibles impactos en el rendimiento.

## Pasos

1. Determine las ONTAP tools for VMware vSphere desde la primera máquina virtual del nodo.

```
cat /opt/netapp/meta/ansible_vars.yml | grep -i protocolo
```

Si se trata de una implementación iSCSI, también deberá eliminar los igroups.

2. Obtenga la lista de volúmenes FlexVol .

```
kubectl describe volúmenes persistentes | grep nombreInterno | awk -F=' ' '{print $2}'
```

3. Eliminar las máquinas virtuales del vCenter Server. Referirse a ["Eliminar y volver a registrar máquinas virtuales y plantillas de máquinas virtuales"](#) .
4. Eliminar volúmenes FlexVol . Referirse a ["Eliminar un FlexVol volume"](#) . En el comando CLI para eliminar un volumen, proporcione el nombre exacto de los volúmenes FlexVol .
5. Eliminar igroups SAN del sistema de almacenamiento ONTAP en caso de implementación de iSCSI. Referirse a ["Ver y administrar iniciadores SAN y igroups"](#) .

# Actualice las ONTAP tools for VMware vSphere

## Actualización de las ONTAP tools for VMware vSphere 10.x a 10.4

Puede actualizar las ONTAP tools for VMware vSphere 10.2 o 10.3 a 10.4. Sin embargo, no se admite la actualización directa de las herramientas ONTAP 10.0 o 10.1 a 10.4.

NOTA:

- En los sistemas ASA r2, debe actualizar a las ONTAP tools for VMware vSphere 10.4 con ONTAP 9.16.1 antes de agregar más zonas de disponibilidad de almacenamiento (SAZ).
- Si falla la actualización de las ONTAP tools for VMware vSphere 10.2 o 10.3 a la versión 10.4, no se admite la reversión. Para recuperar la configuración, utilice RPO para ONTAP tools for VMware vSphere 10.2 y RPO cercano a cero o recuperación de instantáneas para ONTAP tools for VMware vSphere 10.3.

### Antes de empezar

Para una actualización que no sea de alta disponibilidad, apague la máquina virtual (VM) de herramientas ONTAP y, para una actualización de alta disponibilidad, apague el primer nodo antes de realizar los siguientes cambios en la configuración de la máquina virtual (VM).

Si actualiza desde las ONTAP tools for VMware vSphere 10.2 o 10.3, debe completar los siguientes pasos antes de continuar con la actualización: \* Agregue 100 GB de disco duro adicionales a cada nodo, ya que los datos de servicio se almacenan localmente en la máquina virtual. \* Cambie la CPU y la memoria de la máquina virtual apagada según la versión de su implementación. Habilite el complemento activo para CPU y RAM.

+

Tipo de implementación	CPU (núcleo) por nodo	Memoria (GB) por nodo	Espacio en disco (GB) por nodo	CPU total (núcleo)	Memoria (GB)	Espacio total en disco (GB)
Pequeño sin HA	9	18	350	9	18	350
Medio sin HA	13	26	350	13	26	350
HA Pequeño	9	18	350	27	54	1050
HA Medio	13	26	350	39	78	1050
HA grande	17	34	350	51	102	1050

- Encienda la máquina virtual después de realizar los cambios y espere a que los servicios pasen a un estado de ejecución.
- En caso de implementación de HA, realice los cambios de recursos, habilite el complemento activo para CPU y RAM, y agregue discos duros de 100 GB para el segundo y el tercer nodo también. No es necesario reiniciar estos nodos.
- Si el dispositivo se implementó como una ruta local (implementación fácil) con las herramientas ONTAP 10.2, debe tomar una instantánea de inactividad antes de actualizar.

Si está actualizando las ONTAP tools for VMware vSphere 10.0 a 10.1, debe completar los siguientes pasos antes de continuar con la tarea de actualización: **Habilitar diagnósticos**

1. Desde vCenter Server, abra una consola en las herramientas de ONTAP .
2. Inicie sesión como usuario de mantenimiento.
3. Ingrese **4** para seleccionar **Soporte y diagnóstico**.
4. Ingrese **2** para seleccionar **Habilitar acceso de diagnóstico remoto**.
5. Ingrese **y** para establecer la contraseña de su elección.
6. Inicie sesión en la dirección IP de la VM desde la terminal/putty con el usuario 'diag' y la contraseña que se configuró en el paso anterior.

### Realice una copia de seguridad de MongoDB

Ejecute los siguientes comandos para realizar una copia de seguridad de MongoDB:

- `kn exec -it ntv-mongodb-0 sh - kn` es un alias de `kubectl -n ntv-system`.
- Ejecute el comando `env | grep MONGODB_ROOT_PASSWORD` dentro del pod.
- Ejecute el comando `exit` para salir del pod.
- Ejecute el comando `kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip` para reemplazar el conjunto `MONGO_ROOT_PASSWORD` del comando anterior.
- Ejecute el comando `kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz` para copiar la copia de seguridad de mongodb creada con el comando anterior desde el pod al host.

### Toma la instantánea de todos los volúmenes

- Ejecute el comando 'kn get pvc' y guarde el resultado del comando.
- Tome instantáneas de todos los volúmenes uno por uno utilizando uno de los siguientes métodos:
  - Desde la CLI, ejecute el comando `volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>`
  - Desde la interfaz de usuario de ONTAP System Manager, busque el volumen por su nombre en la barra de búsqueda, luego abra ese volumen seleccionando el nombre. Vaya a la instantánea y agregue la instantánea de ese volumen.

### Tome la instantánea de las ONTAP tools for VMware vSphere en vCenter (3 máquinas virtuales en caso de implementación de alta disponibilidad, 1 máquina virtual en caso de implementación que no sea de alta disponibilidad)

- En la interfaz de usuario del cliente vSphere, seleccione la VM.
- Vaya a la pestaña de instantáneas y seleccione el botón **Tomar instantánea**. Tome una instantánea inactiva de la máquina virtual. Referirse a "[Tomar una instantánea de una máquina virtual](#)" Para más detalles.

Antes de realizar la actualización, elimine los pods completados del paquete de registro con el prefijo "generate-support-bundle-job". Si la generación del paquete de soporte está en progreso, espere a que se complete y luego elimine el pod.

Para cualquier tipo de actualización, es necesario agregar un disco duro (HDD) adicional de 100 GB. Para agregar un disco duro, realice la siguiente tarea.

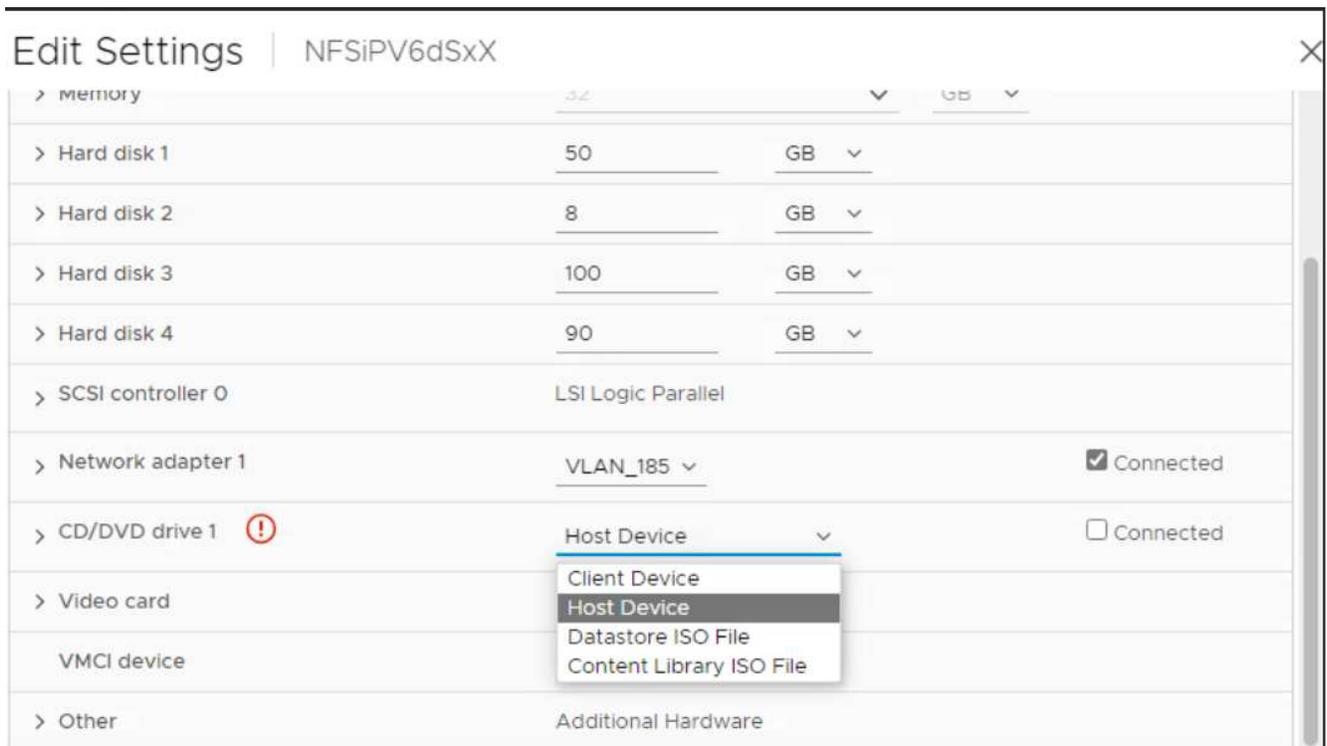
1. Seleccione la VM en la configuración de nodo único o las tres VM en la configuración de HA.
2. Haga clic derecho en la(s) máquina(s) virtual(es) y seleccione **Agregar nuevo dispositivo > Disco duro**
3. Agregue un disco duro de 100 GB en el campo **Nuevo disco duro**.
4. Seleccione **Aplicar**

Después de agregar el disco duro, actualice los recursos de la VM para las configuraciones respectivas y reinicie la VM principal.

Se creará un nuevo disco duro. El proveedor de almacenamiento dinámico utiliza este disco duro para generar o replicar los volúmenes.

#### Pasos

1. Cargue las ONTAP tools for VMware vSphere a la biblioteca de contenido.
2. En la página principal de la máquina virtual, seleccione **Acciones > Editar configuración**
3. Seleccione el archivo ISO de la biblioteca de contenido en la ventana de edición de configuración, debajo del campo **Unidad de CD/DVD**.
4. Seleccione el archivo ISO y seleccione **Aceptar**. Seleccione la casilla de verificación conectada en el campo **Unidad de CD/DVD**



5. Desde vCenter Server, abra una consola en las herramientas de ONTAP .
6. Inicie sesión como usuario de mantenimiento.
7. Introduzca **3** para seleccionar el menú de Configuración del Sistema.
8. Introduzca **7** para seleccionar la opción de actualización.
9. Al actualizar, se realizan automáticamente las siguientes acciones:
  - a. Actualización del certificado
  - b. Actualización remota del complemento

Después de actualizar a las ONTAP tools for VMware vSphere 10.4, puede:

- Deshabilitar los servicios desde la interfaz de usuario del administrador
- Pasar de una configuración sin alta disponibilidad a una configuración con alta disponibilidad
- Amplíe una configuración pequeña sin alta disponibilidad a una configuración mediana sin alta disponibilidad o a una configuración mediana o grande con alta disponibilidad.
- En caso de una actualización que no sea de alta disponibilidad, reinicie la máquina virtual de herramientas ONTAP para reflejar los cambios. En caso de una actualización de HA, reinicie el primer nodo para reflejar los cambios en el nodo.

### ¿Qué sigue?

Después de actualizar desde versiones anteriores de las ONTAP tools for VMware vSphere a 10.4, vuelva a escanear los adaptadores SRA para verificar que los detalles estén actualizados en la página Adaptadores de replicación de almacenamiento de VMware Live Site Recovery.

Después de actualizar exitosamente, elimine los volúmenes Trident de ONTAP manualmente mediante el siguiente procedimiento:



Estos pasos no son necesarios si las ONTAP tools for VMware vSphere 10.1 o 10.2 estaban en configuraciones pequeñas o medianas (ruta local) que no eran de alta disponibilidad.

1. Desde vCenter Server, abra una consola en las herramientas de ONTAP .
2. Inicie sesión como usuario de mantenimiento.
3. Introduzca **4** para seleccionar el menú **Soporte y diagnóstico**.
4. Introduzca **1** para seleccionar la opción **Acceder al shell de diagnóstico**.
5. Ejecute el siguiente comando

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. Ingrese el nombre de usuario y contraseña de ONTAP

Esto elimina todos los volúmenes Trident en ONTAP utilizados en las ONTAP tools for VMware vSphere 10.1/10.2.

### Información relacionada

["Migrar de las ONTAP tools for VMware vSphere 9.xx a 10.4"](#)

## Códigos de error de actualización

Es posible que encuentre códigos de error durante la operación de actualización de las ONTAP tools for VMware vSphere . Los códigos de error tienen cinco dígitos, donde los dos primeros dígitos representan el script que encontró el problema y los tres últimos dígitos representan el flujo de trabajo específico dentro de ese script.

Todos los registros de errores se graban en el archivo ansible-perl-errors.log para facilitar el seguimiento y la resolución de problemas. Este archivo de registro contiene el código de error y la tarea de Ansible fallida.



Los códigos de error proporcionados en esta página son sólo para referencia. Comuníquese con el equipo de soporte si el error persiste o si no se menciona ninguna solución.

La siguiente tabla enumera los códigos de error y los nombres de archivos correspondientes.

Código de error	Nombre del guión
00	firstboot-network-config.pl, modo de implementación
01	firstboot-network-config.pl, actualización de modo
02	validación de entradas de firstboot.pl
03	firstboot-deploy-otv-ng.pl, implementar, HA
04	firstboot-deploy-otv-ng.pl, implementación, sin HA
05	firstboot-deploy-otv-ng.pl, reiniciar
06	firstboot-deploy-otv-ng.pl, actualización, alta disponibilidad
07	firstboot-deploy-otv-ng.pl, actualización, sin alta disponibilidad
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Los últimos tres dígitos del código de error indican el error de flujo de trabajo específico dentro del script:

Código de error de actualización	Flujo de trabajo	Resolución
052	La ISO podría ser la misma que la versión actual o dos versiones superiores a la versión actual.	Utilice una versión ISO compatible para actualizar desde su versión actual.
068	La reversión de los paquetes Debian ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
069	Error al restaurar archivos	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
070	Error al eliminar la copia de seguridad	-
071	El clúster de Kubernetes no estaba en buen estado	-
074	El montaje ISO ha fallado	Verifique /var/log/upgrade-run.log y vuelva a intentar la actualización.
075	Las comprobaciones previas a la actualización han fallado	Vuelva a intentar la actualización.
076	La actualización del registro ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.

<b>Código de error de actualización</b>	<b>Flujo de trabajo</b>	<b>Resolución</b>
077	La reversión del registro ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
078	La actualización del operador ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
079	La reversión del operador ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
080	La actualización de servicios ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
081	La reversión de los servicios ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
082	Error al eliminar imágenes antiguas del contenedor	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
083	La eliminación de la copia de seguridad ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
084	Error al cambiar JobManager a Producción	Siga los pasos a continuación para recuperar/completar la actualización. 1. Habilitar el Shell de diagnóstico 2. Ejecute el comando: <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Consulte los registros en <i>/var/log/post-deploy-upgrade.log</i>
087	Los pasos posteriores a la actualización fallaron.	Realice los siguientes pasos para recuperar/completar la actualización. 1. Habilitar el Shell de diagnóstico 2. Ejecute el comando <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Consulte los registros en <i>/var/log/post-deploy-upgrade.log</i>
088	La configuración de rotación de registros para journald ha fallado	Verifique la configuración de red de la VM compatible con el host en el que está alojada la VM. Puede intentar migrar la máquina virtual a otro host y reiniciar.

<b>Código de error de actualización</b>	<b>Flujo de trabajo</b>	<b>Resolución</b>
089	El cambio de propiedad del archivo de configuración de rotación del registro de resumen ha fallado	Vuelva a intentar la actualización.
095	La actualización del sistema operativo falló	No hay recuperación para la actualización del sistema operativo. Los servicios de herramientas ONTAP se actualizan y se ejecutarán nuevos pods.
096	Instalar el proveedor de almacenamiento dinámico	Verifique los registros de actualización y vuelva a intentar la actualización.
097	La desinstalación de servicios para la actualización ha fallado	Utilice RPO cero o recuperación basada en instantáneas y vuelva a intentar la actualización.
098	La copia del secreto de DockerCred desde el sistema NTV al espacio de nombres del proveedor de almacenamiento dinámico ha fallado.	Verifique los registros de actualización y vuelva a intentar la actualización.
099	No se pudo validar la adición del nuevo HDD	Agregue el nuevo HDD a todos los nodos en caso de alta disponibilidad y a un nodo en caso de una implementación que no sea alta disponibilidad.
108	Falló el script de siembra	-
109	La copia de seguridad de los datos del volumen persistente ha fallado	Verifique los registros de actualización y vuelva a intentar la actualización.
110	La restauración de los datos del volumen persistente ha fallado	Utilice la recuperación basada en instantáneas o RPO cero y vuelva a intentar la actualización.
111	La actualización de los parámetros de tiempo de espera de etcd para RKE2 ha fallado	Verifique los registros de actualización y vuelva a intentar la actualización.
112	La desinstalación del proveedor de almacenamiento dinámico ha fallado	-
113	La actualización de recursos en los nodos secundarios ha fallado	Verifique los registros de actualización y vuelva a intentar la actualización.
104	El reinicio del nodo secundario ha fallado	Reinicie los nodos manualmente uno por uno
100	La reversión del kernel ha fallado	-

<b>Código de error de actualización</b>	<b>Flujo de trabajo</b>	<b>Resolución</b>
051	La actualización del proveedor de almacenamiento dinámico ha fallado	Verifique los registros de actualización y vuelva a intentar la actualización.
056	La eliminación de la copia de seguridad de la migración ha fallado	N / A



A partir de las ONTAP tools for VMware vSphere 10.3, no se admite RPO cero.

Obtenga más información sobre ["Cómo restaurar las ONTAP tools for VMware vSphere si falla la actualización de la versión 10.0 a la 10.1"](#)

# Migrar ONTAP tools for VMware vSphere 9.xx a 10.4

## Migrar de las ONTAP tools for VMware vSphere 9.xx a 10.4

Mover las herramientas NetApp ONTAP tools for VMware vSphere de la versión 9.xx a la 10.x requiere un proceso de migración debido a las importantes actualizaciones y mejoras del producto en las versiones.

Puede migrar desde las ONTAP tools for VMware vSphere 9.12D1, 9.13D2 y 9.13P2 a las ONTAP tools for VMware vSphere 10.4.

Si tiene almacenes de datos NFS y VMFS y ningún almacén de datos vVols en su configuración, simplemente desinstale las herramientas ONTAP 9.xx e implemente las herramientas ONTAP 10.x. Sin embargo, si su configuración contiene almacenes de datos vVols, tendrá que pasar por un proceso de migración del proveedor VASA y el SRA.

La siguiente tabla describe el proceso de migración en estos dos escenarios diferentes.

*Si la configuración tiene almacenes de datos vVols *	Si la configuración solo contiene almacenes de datos NFS y VMFS
Pasos: 1. <a href="#">"Migrar el proveedor VASA"</a> 2. <a href="#">"Crear políticas de almacenamiento de máquinas virtuales"</a>	Pasos: 1. Elimine las herramientas ONTAP 9.xx de su entorno. Referirse a <a href="#">"Cómo eliminar OTV 9.xx de tu entorno"</a> Artículo de la base de conocimientos de NetApp . 2. <a href="#">"Implementar y configurar ONTAP tools for VMware vSphere 10.4"</a> 3. <a href="#">"Actualizar la SRA"</a> 4. <a href="#">"Crear políticas de almacenamiento de máquinas virtuales"</a>



Después de migrar de las ONTAP tools for VMware vSphere 9.xx a 10.4, los almacenes de datos vVols que usan el protocolo NVMe/FC dejan de estar operativos porque las herramientas ONTAP 10.4 admiten el protocolo NVMe-oF solo con almacenes de datos VMFS.

## Migrar el proveedor VASA y actualizar el SRA

### Pasos para migrar el proveedor VASA

1. Para habilitar Derby PORT 1527 en las ONTAP tools for VMware vSphere, habilite el usuario root e inicie sesión en la CLI a través de SSH. Luego, ejecute el siguiente comando:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Implementar OVA para ONTAP tools for VMware vSphere 10.4.
3. Agregue la instancia de vCenter Server que desea migrar a las ONTAP tools for VMware vSphere 10.4. Consulte ["Agregar una instancia de vCenter Server"](#) Para más información.
4. Integre el backend de almacenamiento localmente desde las API del servidor vCenter para el

complemento de herramientas ONTAP .

5. Emita la siguiente API desde Swagger o en Postman para migrar.

```
curl -X POST
https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-
jobs`
```

Puedes acceder a Swagger a través de esta URL: `https://$FQDN_IP_PORT/`, for example: `\https://10.67.25.33:8443` .

### Método y punto final HTTP

Esta llamada a la API REST utiliza el siguiente método y punto de conexión.

Método HTTP	Camino
CORREO	/api/v1

### Tipo de procesamiento

Asincrónico

### Ejemplo de rizo

```
curl -X PUBLICACIÓN'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-
jobs' \ --header 'x-auth: <token_de_autenticación>' \ --header 'Tipo-de-contenido: aplicación/json' \
--data '{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "nombre_de_usuario": "xxxxx",
"contraseña": "" }, "contraseña_de_base_de_datos": "" }'
```

Cuerpo de la solicitud para otra migración de versión:

```
{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "nombre de usuario": "xxxxx", "contraseña": ""
} }
```

### Ejemplo de salida JSON

Se devuelve un objeto de trabajo. Debes guardar el identificador del trabajo para usarlo en el siguiente paso.

```
{ "id": 123, "id_migración": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "estado": "en ejecución" }
```

6. Utilice la siguiente URI en Swagger para comprobar el estado:

```
curl
\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID
>?includeSubJobsAndTasks=true`
```

Después de completar el trabajo, revise el informe de migración. Este informe está incluido en los datos del trabajo y se puede acceder a él desde la respuesta del trabajo.

7. Agregue las ONTAP tools for VMware vSphere al vCenter Server y "[Registrar al proveedor de VASA](#)" con ONTAP tools for VMware vSphere.
8. "[Habilitar proveedor VASA](#)" Servicio en ONTAP tools for VMware vSphere 10.4.
9. Detenga el servicio del proveedor VASA de las ONTAP tools for VMware vSphere 9.10/9.11/9.12/9.13 desde la consola de mantenimiento.

No elimine el proveedor VASA.

Tras detener el antiguo proveedor VASA, vCenter Server conmuta por error a las ONTAP tools for VMware vSphere. Todos los almacenes de datos y máquinas virtuales se vuelven accesibles y se sirven desde las ONTAP tools for VMware vSphere.

10. Los almacenes de datos NFS y VMFS migrados desde las ONTAP tools for VMware vSphere 9.xxx son visibles en las ONTAP tools for VMware vSphere 10.4 solo después de que se activa el trabajo de descubrimiento del almacén de datos, que puede tardar hasta 30 minutos en completarse. Verifique que los almacenes de datos estén visibles en la página de descripción general de la página de interfaz de usuario de las herramientas de ONTAP para el complemento VMware vSphere.
11. Realice la migración del parche utilizando la siguiente API en Swagger o en Postman:

### Método y punto final HTTP

Esta llamada a la API REST utiliza el siguiente método y punto de conexión.

Método HTTP	Camino
PARCHE	/api/v1

### Tipo de procesamiento

Asincrónico

### Ejemplo de rizo

```
curl -X PATCH
```

```
https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43
```

### Ejemplo de salida JSON

Se devuelve un objeto de trabajo. Debes guardar el identificador del trabajo para usarlo en el siguiente paso.

```
{ "id": 123, "id_migración": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "estado": "en ejecución" }
```

El cuerpo de la solicitud está vacío para la operación de parche.



UUID es el UUID de migración devuelto en respuesta a la API posterior a la migración.

Después de ejecutar la API de migración de parches, todas las máquinas virtuales cumplen con la política de almacenamiento.

## ¿Qué sigue?

Después de completar la migración y registrar las herramientas ONTAP 10.4 en vCenter Server, siga estos pasos:

- Espere a que se complete el **Descubrimiento**, los certificados se actualizarán automáticamente en todos los hosts.
- Espere suficiente tiempo antes de iniciar las operaciones del almacén de datos y la máquina virtual. El tiempo de espera requerido varía según la cantidad de hosts, almacenes de datos y máquinas virtuales en la configuración. Si no se espera, podrían producirse fallos operativos intermitentes.

Después de la actualización, si el estado de cumplimiento de la máquina virtual está desactualizado, vuelva a aplicar la política de almacenamiento siguiendo estos pasos:

1. Navegue hasta el almacén de datos y seleccione **Resumen > Políticas de almacenamiento de VM**.

El estado de cumplimiento bajo **Cumplimiento de la política de almacenamiento de VM** se muestra como **Desactualizado**.

2. Seleccione la política de VM de almacenamiento y la VM correspondiente
3. Seleccione **Aplicar**

El estado de cumplimiento bajo **Cumplimiento de la política de almacenamiento de VM** ahora se muestra como compatible.

## Información relacionada

- ["Obtenga más información sobre las ONTAP tools for VMware vSphere 10 RBAC"](#)
- ["Actualización de las ONTAP tools for VMware vSphere 10.x a 10.4"](#)

## Pasos para actualizar el adaptador de replicación de almacenamiento (SRA)

### Antes de empezar

En el plan de recuperación, el sitio protegido se refiere a la ubicación donde se ejecutan las máquinas virtuales, mientras que el sitio de recuperación es donde se recuperarán. La interfaz de SRM muestra el estado del plan de recuperación con detalles sobre los sitios protegidos y de recuperación. En el plan de recuperación, los botones **CleanupP** y **Reprotect** están deshabilitados, mientras que los botones TEST y RUN permanecen habilitados. Esto indica que el sitio está preparado para la recuperación de datos. Antes de migrar el SRA, verifique que un sitio esté en estado protegido y el otro en estado de recuperación.



No comience la migración si se ha completado la conmutación por error pero la nueva protección está pendiente. Asegúrese de que el proceso de re-protección se haya completado antes de continuar con la migración. Si hay una conmutación por error de prueba en curso, limpie la conmutación por error de prueba e inicie la migración.

1. Siga estos pasos para eliminar el adaptador SRA de herramientas ONTAP para VMware vSphere 9.xx en VMware Site Recovery:
  - a. Vaya a la página de administración de configuración de VMware Live Site Recovery
  - b. Vaya a la sección **Adaptador de replicación de almacenamiento**.
  - c. Desde el menú de puntos suspensivos seleccione **Restablecer configuración**.
  - d. Desde el menú de puntos suspensivos seleccione **Eliminar**.

2. Realice estos pasos en los sitios de protección y recuperación.
  - a. ["Habilitar ONTAP tools for VMware vSphere"](#)
  - b. Instale las ONTAP tools for VMware vSphere 10.4 SRA siguiendo los pasos que se indican en ["Configurar SRA en el dispositivo VMware Live Site Recovery"](#) .
  - c. En la página de la interfaz de usuario de VMware Live Site Recovery, realice las operaciones **Descubrir matrices** y **Descubrir dispositivos** y confirme que los dispositivos se muestran como antes de la migración.

# Automatizar utilizando la API REST

## Obtenga más información sobre las ONTAP tools for VMware vSphere 10 REST API

Las ONTAP tools for VMware vSphere 10 son un conjunto de herramientas para la gestión del ciclo de vida de las máquinas virtuales. Incluye una API REST robusta que puedes utilizar como parte de tus procesos de automatización.

### Fundación de servicios web REST

Transferencia de estado representacional (REST) es un estilo para crear aplicaciones web distribuidas que incluye el diseño de API de servicios web. Establece un conjunto de tecnologías para exponer recursos basados en servidores y gestionar sus estados.

#### Recursos y representación estatal

Los recursos son los componentes fundamentales de una aplicación de servicios web REST. Hay dos tareas iniciales importantes al diseñar una API REST:

- Identificar los recursos del sistema o del servidor
- Definir los estados de los recursos y las operaciones de transición de estados asociadas

Las aplicaciones cliente pueden mostrar y cambiar los estados de los recursos a través de flujos de mensajes bien definidos.

#### Mensajes HTTP

El Protocolo de Transferencia de Hipertexto (HTTP) es el protocolo utilizado por el cliente y el servidor de servicios web para intercambiar mensajes sobre los recursos. Sigue el modelo CRUD basado en las operaciones genéricas crear, leer, actualizar y eliminar. El protocolo HTTP incluye encabezados de solicitud y respuesta, así como códigos de estado de respuesta.

#### Formato de datos JSON

Si bien hay varios formatos de mensajes disponibles, la opción más popular es la Notación de objetos JavaScript (JSON). JSON es un estándar de la industria para representar estructuras de datos simples en texto simple y se utiliza para transferir información de estado que describe los recursos y las acciones deseadas.

#### Seguridad

La seguridad es un aspecto importante de una API REST. Además del protocolo de seguridad de la capa de transporte (TLS) utilizado para proteger el tráfico HTTP a través de la red, las ONTAP tools for VMware vSphere 10 también utilizan tokens de acceso para la autenticación. Debe adquirir un token de acceso y usarlo en llamadas API posteriores.

#### Soporte para solicitudes asincrónicas

Las ONTAP tools for VMware vSphere 10 ejecutan la mayoría de las solicitudes de forma sincrónica y devuelven un código de estado cuando se completa la operación. También admite el procesamiento asincrónico para tareas que requieren más tiempo para completarse.

## Entorno del administrador de herramientas ONTAP

Hay varios aspectos del entorno del Administrador de herramientas de ONTAP que debe tener en cuenta.

### Máquina virtual

Las ONTAP tools for VMware vSphere 10 se implementan mediante la arquitectura del complemento remoto de vSphere. El software, incluido el soporte para la API REST, se ejecuta en una máquina virtual separada.

### Dirección IP de las herramientas ONTAP

Las ONTAP tools for VMware vSphere 10 exponen una única dirección IP que proporciona una puerta de enlace a las capacidades de la máquina virtual. Debe proporcionar la dirección durante la configuración inicial y se asigna a un componente de balanceador de carga interno. La dirección es utilizada por la interfaz de usuario del Administrador de herramientas de ONTAP, así como para acceder directamente a la página de documentación de Swagger y a la API REST.

### Dos API REST

Además de las ONTAP tools for VMware vSphere 10, el clúster ONTAP tiene su propia API REST. El administrador de herramientas de ONTAP utiliza la API REST de ONTAP como cliente para realizar tareas relacionadas con el almacenamiento. Es importante tener en cuenta que estas dos API son independientes y distintas. Para más información, consulte ["Automatización de ONTAP"](#).

## Detalles de implementación de las ONTAP tools for VMware vSphere 10

Si bien REST establece un conjunto común de tecnologías y mejores prácticas, la implementación exacta de cada API puede variar según las opciones de diseño. Debe familiarizarse con el diseño de las ONTAP tools for VMware vSphere 10 REST API antes de usarlas.

La API REST incluye varias categorías de recursos, como vCenters y agregados. Revisar el ["Referencia de API"](#) Para más información.

### Cómo acceder a la API REST

Puede acceder a las ONTAP tools for VMware vSphere 10 a través de la dirección IP de las herramientas ONTAP junto con el puerto. La URL completa consta de varias partes, entre ellas:

- Dirección IP y puerto de las herramientas ONTAP
- Versión API
- Categoría de recurso
- Recurso específico

Debe configurar la dirección IP durante la configuración inicial, mientras el puerto permanece fijo en 8443. La primera parte de la URL es consistente para cada instancia de las ONTAP tools for VMware vSphere 10; solo la categoría del recurso y el recurso específico cambian entre los puntos finales.



Los valores de dirección IP y puerto en los ejemplos siguientes son sólo para fines ilustrativos. Debe cambiar estos valores para su entorno.

### Ejemplo para acceder a servicios de autenticación

`https://10.61.25.34:8443/virtualization/api/v1/auth/login`

Esta URL se puede utilizar para solicitar un token de acceso mediante el método POST.

### Ejemplo para listar los servidores vCenter

`https://10.61.25.34:8443/virtualization/api/v1/vcenters`

Esta URL se puede utilizar para solicitar una lista de las instancias del servidor vCenter definidas mediante el método GET.

## Detalles HTTP

Las ONTAP tools for VMware vSphere 10 utilizan HTTP y parámetros relacionados para actuar en las instancias y colecciones de recursos. A continuación se presentan detalles de la implementación HTTP.

### Métodos HTTP

Los métodos o verbos HTTP admitidos por la API REST se presentan en la siguiente tabla.

Método	CRUD	Descripción
CONSEGUIR	Leer	Recupera propiedades de objeto para una instancia o colección de recursos. Esto se considera una operación de lista cuando se utiliza con una colección.
CORREO	Crear	Crea una nueva instancia de recurso basada en los parámetros de entrada.
PONER	Actualizar	Actualiza una instancia de recurso completa con el cuerpo de la solicitud JSON proporcionado. Se conservan los valores clave que no son modificables por el usuario.
PARCHE	Actualizar	Solicita que se aplique un conjunto de cambios seleccionados en la solicitud a la instancia del recurso.
BORRAR	Borrar	Elimina una instancia de recurso existente.

### Encabezados de solicitud y respuesta

La siguiente tabla resume los encabezados HTTP más importantes utilizados con la API REST.

Encabezado	Tipo	Notas de uso
Acceptar	Pedido	Este es el tipo de contenido que la aplicación cliente puede aceptar. Los valores válidos incluyen <code>*/*</code> o <code>application/json</code> .
x-auth	Pedido	Contiene un token de acceso que identifica al usuario que emite la solicitud a través de la aplicación cliente.
Tipo de contenido	Respuesta	Devuelto por el servidor en función de la <code>Accept</code> encabezado de solicitud.

### Códigos de estado HTTP

A continuación se describen los códigos de estado HTTP utilizados por la API REST.

Código	Significado	Descripción
200	DE ACUERDO	Indica el éxito de las llamadas que no crean una nueva instancia de recurso.
201	Creado	Se ha creado exitosamente un objeto con un identificador único para la instancia del recurso.
202	Aceptado	Se ha aceptado la solicitud y se ha creado un trabajo en segundo plano para ejecutarla.
204	Sin contenido	La solicitud fue exitosa aunque no se devolvió ningún contenido.
400	Solicitud incorrecta	La entrada solicitada no se reconoce o es inadecuada.
401	No autorizado	El usuario no está autorizado y debe autenticarse.
403	Prohibido	Se deniega el acceso debido a un error de autorización.
404	Extraviado	El recurso al que se refiere la solicitud no existe.
409	Conflicto	Se produjo un error al intentar crear un objeto porque el objeto ya existe.
500	Error interno	Se produjo un error interno general en el servidor.

## Autenticación

La autenticación de un cliente a la API REST se realiza mediante un token de acceso. Las características relevantes del token y del proceso de autenticación incluyen:

- El cliente debe solicitar un token utilizando las credenciales de administrador del administrador de herramientas de ONTAP (nombre de usuario y contraseña).
- Los tokens tienen el formato JSON Web Token (JWT).
- Cada token caduca después de 60 minutos.
- Las solicitudes de API de un cliente deben incluir el token en el `x-auth` encabezado de solicitud.

Referirse a "[Su primera llamada a la API REST](#)" para ver un ejemplo de cómo solicitar y utilizar un token de acceso.

## Solicitudes sincrónicas y asincrónicas

La mayoría de las llamadas a la API REST se completan rápidamente y, por lo tanto, se ejecutan de forma sincrónica. Es decir, devuelven un código de estado (como 200) después de que se ha completado una solicitud. Las solicitudes que tardan más en completarse se ejecutan de forma asincrónica mediante un trabajo en segundo plano.

Después de emitir una llamada API que se ejecuta de forma asincrónica, el servidor devuelve un código de estado HTTP 202. Esto indica que la solicitud ha sido aceptada pero aún no se ha completado. Puede consultar el trabajo en segundo plano para determinar su estado, incluido si fue exitoso o fallido.

El procesamiento asincrónico se utiliza para varios tipos de operaciones de ejecución prolongada, incluidas las operaciones de almacén de datos y vVol. Consulte la categoría del administrador de trabajos de la API REST en la página de Swagger para obtener más información.

# Sus primeras ONTAP tools for VMware vSphere 10

Puede emitir una llamada API usando curl para comenzar a utilizar las ONTAP tools for VMware vSphere 10.

## Antes de empezar

Debes revisar la información requerida y los parámetros necesarios en los ejemplos de curl.

### Información requerida

Necesitarás lo siguiente:

- ONTAP tools for VMware vSphere 10 Dirección IP o FQDN, así como el puerto
- Credenciales para el administrador de herramientas de ONTAP (nombre de usuario y contraseña)

### Parámetros y variables

Los ejemplos de curl que se presentan a continuación incluyen variables de estilo Bash. Puede configurar estas variables en el entorno Bash o actualizarlas manualmente antes de emitir los comandos. Si configura las variables, el shell sustituirá los valores en cada comando antes de ejecutarlo. Las variables se describen en la siguiente tabla.

Variable	Descripción
\$FQDN_IP_PORT	El nombre de dominio completo o la dirección IP del Administrador de herramientas de ONTAP junto con el número de puerto.
\$MIUSUARIO	Nombre de usuario para la cuenta de administrador de herramientas de ONTAP .
\$MICONTRASEÑA	Contraseña asociada al nombre de usuario del administrador de herramientas de ONTAP .
\$TOKEN DE ACCESO	El token de acceso emitido por el administrador de herramientas de ONTAP .

Los siguientes comandos y resultados en la CLI de Linux ilustran cómo se puede configurar y mostrar una variable:

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

## Paso 1: Adquirir un token de acceso

Necesita adquirir un token de acceso para utilizar la API REST. A continuación se presenta un ejemplo de cómo solicitar un token de acceso. Debes sustituir los valores apropiados para tu entorno.

```
curl --request POST \  
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login" \  
--header "Content-Type: application/json" \  
--header "Accept: */*" \  
-d '{"username": "$MYUSER", "password": "$MYPASSWORD}"
```

Copie y guarde el token de acceso proporcionado en la respuesta.

## Paso 2: Emitir la llamada a la API REST

Una vez que tenga un token de acceso, puede usar curl para emitir una llamada a la API REST. Incluya el token de acceso adquirido en el primer paso.

### Ejemplo de rizo

```
curl --request GET \  
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \  
--header "Accept: */*" \  
--header "x-auth: $ACCESS_TOKEN"
```

La respuesta JSON incluye una lista de las instancias de VMware vCenter configuradas en el Administrador de herramientas de ONTAP .

## Referencia de API para las ONTAP tools for VMware vSphere 10 API REST

La referencia de la API REST de las ONTAP tools for VMware vSphere 10 contiene detalles sobre todas las llamadas API. Esta referencia es útil al desarrollar aplicaciones de automatización.

Puede acceder a la documentación de la API REST de las ONTAP tools for VMware vSphere 10 en línea a través de la interfaz de usuario Swagger. Necesita la dirección IP o el FQDN de las ONTAP tools for VMware vSphere 10, así como el puerto.

### Pasos

1. Escriba la siguiente URL en su navegador sustituyendo la dirección IP y la combinación de puerto adecuadas para la variable y presione **Enter**.

```
https://$FQDN_IP_PORT/
```

### Ejemplo

```
https://10.61.25.33:8443/
```

2. Como ejemplo de una llamada API individual, desplácese hacia abajo hasta la categoría **vCenters** y seleccione **GET** junto al punto final `/virtualization/api/v1/vcenters`

# Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

## Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de Marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Patentes

Puede encontrar una lista actualizada de las patentes propiedad de NetApp en:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Política de privacidad

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

["Aviso para las ONTAP tools for VMware vSphere 10.4"](#)

## 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 INTERRUPTIÓN 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.