



Documentación de ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Tabla de contenidos

Documentación de ONTAP tools for VMware vSphere	1
Notas de publicación	2
Notas de la versión de ONTAP tools	2
Novedades de las herramientas de ONTAP para VMware vSphere 10.5	2
Plataformas ONTAP compatibles y versiones de vCenter Server	3
Comparativa de características de ONTAP tools for VMware vSphere 9 y 10	3
Conceptos	5
Conoce las herramientas de ONTAP	5
Conceptos y términos clave en ONTAP tools	5
Control de acceso basado en roles (RBAC)	8
Conoce las herramientas RBAC de ONTAP	9
RBAC con VMware vSphere	10
RBAC con ONTAP	17
Implementa ONTAP tools para VMware vSphere	21
Guía de inicio rápido para ONTAP tools for VMware vSphere	21
Flujo de trabajo de despliegue de alta disponibilidad para ONTAP tools	23
Requisitos y límites de configuración de ONTAP tools for VMware vSphere	24
Requisitos del sistema	24
Requisitos mínimos de almacenamiento y aplicaciones	24
Requisitos de puertos	25
Límites de configuración para desplegar ONTAP tools for VMware vSphere para almacenes de datos vVols	27
Límites de configuración para desplegar ONTAP tools for VMware vSphere para almacenes de datos VMFS y NFS	28
ONTAP tools for VMware vSphere - Adaptador de replicación de almacenamiento (SRA)	28
Requisitos previos a la implementación de las ONTAP tools	29
Hoja de trabajo de implementación	30
Configuración del cortafuegos de red	31
Configuración del almacenamiento ONTAP	31
Implementa las herramientas ONTAP	31
Soluciona errores de despliegue de ONTAP tools	37
Recopila los archivos de registro	37
Códigos de error de implementación	37
Configura ONTAP tools para VMware vSphere	42
Agrega instancias de vCenter Server a ONTAP tools	42
Registra el proveedor VASA con una instancia de vCenter Server en ONTAP tools	43
Instala el complemento NFS VAAI usando ONTAP tools	44
Configura los ajustes del host ESXi en ONTAP tools	45
Configura los parámetros de multivía y tiempo de espera del servidor ESXi	45
Configura los valores del host ESXi	45
Configura los roles y privilegios de usuario de ONTAP para ONTAP tools	46
Requisitos de mapeo de agregados de SVM	47
Crear usuario y rol de ONTAP manualmente	48

Actualiza ONTAP tools for VMware vSphere usuario 10.1 a usuario 10.3	56
Actualiza ONTAP tools for VMware vSphere 10.3 user a 10.4 user	58
Agrega un backend de almacenamiento a ONTAP tools	58
Asocia un backend de almacenamiento con una instancia de vCenter Server en ONTAP tools	61
Configura el acceso a la red en ONTAP tools	61
Crear un almacén de datos en ONTAP tools	62
Protege los almacenes de datos y las máquinas virtuales	67
Protege un clúster de hosts en ONTAP tools	67
Proteger usando la protección SRA	68
Configura SRA en ONTAP tools para proteger los datastores	68
Configura SRA en ONTAP tools para entornos SAN y NAS	69
Configura SRA en ONTAP tools para entornos altamente escalados	70
Configura SRA en el dispositivo VMware Live Site Recovery usando ONTAP tools	71
Actualiza las credenciales de SRA en ONTAP tools	72
Configura sitios protegidos y de recuperación en ONTAP tools	73
Configura los recursos del sitio protegido y del sitio de recuperación	75
Verifica los sistemas de almacenamiento replicados en ONTAP tools	79
Protección fan-out en las herramientas ONTAP	79
Administra ONTAP tools for VMware vSphere	83
Conoce el panel de ONTAP tools	83
Cómo las herramientas de ONTAP gestionan los igroups y las políticas de exportación	85
Políticas de exportación	88
Cómo las herramientas de ONTAP gestionan los igroups	89
Resumen rápido del comportamiento	89
Contextos de igroup	90
Comportamiento de la nomenclatura	91
Comportamiento por escenario	91
Reutilización personalizada de igroups y comportamiento de la API	92
Vista de conversión de nativo a gestionado	92
Reutilización de los igroups nativos descubiertos	93
Conoce la interfaz de usuario de ONTAP tools Manager	93
Gestiona la configuración de ONTAP tools Manager	95
Editar la configuración de AutoSupport de ONTAP tools	95
Agrega servidores NTP a las herramientas ONTAP	96
Restablece las credenciales de VASA Provider y SRA en ONTAP tools	96
Editar la configuración de copia de seguridad de ONTAP tools	97
Habilitar los servicios de ONTAP tools	97
Cambiar la configuración del dispositivo ONTAP tools	98
Agrega hosts de VMware vSphere a las ONTAP tools	99
Gestiona almacenes de datos	100
Monta almacenes de datos NFS y VMFS en ONTAP tools	100
Desmonta los almacenes de datos NFS y VMFS en ONTAP tools	100
Monta un almacén de datos vVols en ONTAP tools	101
Redimensiona los almacenes de datos NFS y VMFS en ONTAP tools	101
Amplía los datastores vVols en ONTAP tools	102

Reduce un almacén de datos vVols en ONTAP tools	102
Eliminar almacenes de datos en ONTAP tools	103
Vistas de almacenamiento ONTAP para datastores en ONTAP tools	104
Vista de almacenamiento de máquinas virtuales en ONTAP tools	104
Administra los umbrales de almacenamiento en ONTAP tools	105
Administra los backends de almacenamiento en ONTAP tools	105
Descubre almacenamiento	105
Modificar los backends de almacenamiento	106
Eliminar backends de almacenamiento	106
Vista detallada del backend de almacenamiento	107
Administra instancias de vCenter Server en ONTAP tools	107
Desvincula los backends de almacenamiento de la instancia de vCenter Server	107
Modifica una instancia de vCenter Server	108
Eliminar una instancia de vCenter Server	108
Renueva el certificado del servidor vCenter	108
Administra los certificados de ONTAP tools	110
Accede a las herramientas de ONTAP para VMware vSphere consola de mantenimiento	112
Conoce la consola de mantenimiento de las herramientas ONTAP	112
Configura el acceso remoto de diagnóstico para las herramientas ONTAP	113
Inicia SSH en otros nodos de ONTAP tools	114
Actualiza las credenciales de vCenter Server en ONTAP tools	114
Cambia el indicador de validación de certificados en ONTAP tools	114
Informes de ONTAP tools	116
Gestiona máquinas virtuales	117
Consideraciones sobre la migración y clonación de máquinas virtuales para ONTAP tools	117
Migra máquinas virtuales a almacenes de datos vVols en ONTAP tools	118
Limpia las configuraciones VASA en ONTAP tools	119
Conectar o desconectar un disco de datos de una máquina virtual en ONTAP tools	119
Descubre sistemas de almacenamiento y hosts en las herramientas ONTAP	120
Modificar la configuración del host ESXi usando ONTAP tools	121
Gestionar contraseñas	121
Cambiar la contraseña de ONTAP tools Manager	121
Restablecer la contraseña de ONTAP tools Manager	122
Restablecer la contraseña de usuario de la aplicación en ONTAP tools	122
Restablece la contraseña de la consola de mantenimiento de las ONTAP tools	122
Gestiona la protección del clúster de hosts	124
Modifica un clúster de hosts protegidos en ONTAP tools	124
Eliminar la protección de clúster de host en ONTAP tools	127
Recupera la configuración de las herramientas de ONTAP	127
Desinstala ONTAP tools	128
Elimina los volúmenes FlexVol después de desinstalar ONTAP tools	129
Actualiza ONTAP tools para VMware vSphere	130
Actualiza desde ONTAP tools for VMware vSphere 10.x a 10.5	130
Códigos de error de actualización de ONTAP tools	132
Migra ONTAP tools for VMware vSphere 9.xx a 10.5	138

Migra desde ONTAP tools for VMware vSphere 9.xx a 10.5	138
Migra el proveedor VASA y actualiza el SRA en ONTAP tools	138
Pasos para migrar el proveedor VASA	138
Pasos para actualizar el adaptador de replicación de almacenamiento (SRA)	143
Automatiza usando la API de REST	145
Conoce la API de REST de las herramientas ONTAP	145
Fundamentos de los servicios web REST	145
Entorno de ONTAP tools Manager	145
Detalles de implementación de la API de REST de ONTAP tools	146
Cómo acceder a la API de REST	146
Detalles de HTTP	147
Autenticación	148
Solicitudes síncronas y asíncronas	148
Haz tu primera llamada a la API de REST de ONTAP tools	149
Antes de empezar	149
Paso 1: adquirir un token de acceso	149
Paso 2: Realizar la llamada a la API de REST	150
Referencia de la API de REST de ONTAP tools	150
Avisos legales	151
Copyright	151
Marcas registradas	151
Patentes	151
Política de privacidad	151
Código abierto	151

Documentación de ONTAP tools for VMware vSphere

Notas de publicación

Notas de la versión de ONTAP tools

Descubre las funciones nuevas y mejoradas disponibles en ONTAP tools for VMware vSphere 10.5.

Para ver la lista completa de nuevas funciones y mejoras, consulta [Novedades en ONTAP tools for VMware vSphere 10.5](#).

Para obtener la información más actualizada sobre compatibilidad, consulta "[Herramienta NetApp Interoperability Matrix Tool](#)".

Se admite la migración desde ONTAP tools for VMware vSphere 9.12D1, 9.13D2 y 9.13P2 a ONTAP tools for VMware vSphere 10.5.

Para obtener más información, consulta la "[ONTAP tools for VMware vSphere 10.5 Notas de la versión](#)". Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las Release Notes.

Novedades de las herramientas de ONTAP para VMware vSphere 10.5

Descubre las nuevas funciones disponibles en ONTAP tools for VMware vSphere 10.5.

- **Calificación de la plataforma**

ONTAP tools for VMware vSphere 10.5 incorpora compatibilidad con los sistemas ASA r2, proporcionando compatibilidad con las últimas configuraciones de hardware y software. Esta versión también incluye integración con ONTAP 9.16.1 y 9.17.1, ampliando los entornos compatibles.

- **Cualificaciones y certificaciones de VMware**

Las herramientas ONTAP para VMware vSphere 10.5 cumplen con los estándares actuales de certificación de interoperabilidad de VMware y son compatibles tanto con los hosts ESXi como con el servidor vCenter.

- **Compatibilidad con MetroCluster**

Esta versión incorpora compatibilidad con configuraciones de MetroCluster, mejorando las capacidades de alta disponibilidad y recuperación ante desastres.

- **Seguridad y gestión de certificados**

Esta versión introduce una gestión optimizada de los certificados autofirmados, lo que mejora tanto la experiencia del usuario como el cumplimiento de las normas de seguridad. Ofrece flujos de trabajo mejorados para la validación de certificados para proteger las comunicaciones de ONTAP y ONTAP tools for VMware vSphere.

- **Mejoras en la replicación**

Esta versión es compatible con la replicación VMFS con grupos jerárquicos de consistencia, incluyendo SRA y la sincronización activa de SnapMirror en sistemas ASA r2. Admite copias de seguridad con RPO cero para mejorar la protección y recuperación de datos.

- **Actualización y migración**

El proceso de actualización y migración desde versiones anteriores de ONTAP tools for VMware vSphere a ONTAP tools for VMware vSphere 10.5 está diseñado para ser fluido y eficiente, minimizando el tiempo de inactividad y asegurando una transición sin problemas.

Plataformas ONTAP compatibles y versiones de vCenter Server

ONTAP tools for VMware vSphere 10.5 P1 admite configuraciones de alta disponibilidad (HA) de vCenter para los componentes SRA y SnapMirror active sync. vVols no es compatible en esta configuración. Durante una conmutación por error de HA, vCenter podría no estar disponible durante varios minutos. En entornos grandes o si ocurre un error, los tiempos de conmutación por error pueden superar los 15 minutos.

Para más información, consulta el ["vCenter documentación sobre alta disponibilidad"](#). Para preguntas sobre vCenter HA, contacta con ["Soporte de Broadcom"](#).

Para obtener la información más reciente sobre la compatibilidad entre versiones, consulta ["Herramienta NetApp Interoperability Matrix Tool"](#).

Comparativa de características de ONTAP tools for VMware vSphere 9 y 10

Descubre si te conviene migrar de ONTAP tools for VMware vSphere 9 a ONTAP tools for VMware vSphere 10.2 o versiones posteriores.



Para obtener la información más actualizada sobre compatibilidad, consulta ["Herramienta NetApp Interoperability Matrix Tool"](#).

Característica	ONTAP tools 9.13	ONTAP tools a partir de la versión 10.2
Propuesta de valor clave	Optimiza y simplifica las operaciones desde el día 0 hasta el día 2 con funcionalidades mejoradas de seguridad, cumplimiento y automatización	Ampliación de la compatibilidad para incluir FC para VMFS y NVMe-oF solo para VMFS. Facilidad de uso para NetApp SnapMirror, configuración sencilla para clústeres de almacenamiento metro de vSphere y compatibilidad con VMware Live Site Recovery en tres sitios.
Calificación de la versión de ONTAP	ONTAP 9.9.1 a ONTAP 9.16.1	ONTAP 9.12.1 a 9.15.1 para ONTAP tools 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 y 9.16.1 para ONTAP tools 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 y 9.16.1 para ONTAP tools 10.4. ONTAP 9.16.1P3 y versiones posteriores es obligatorio para ONTAP tools 10.4 cuando usas sistemas ASA r2. ONTAP 9.15.1, 9.16.1 y 9.17.0 para ONTAP tools 10.5

Característica	ONTAP tools 9.13	ONTAP tools a partir de la versión 10.2
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 vSphere 9.0 a partir de ONTAP tools 10.5 en adelante VMware Site Recovery Manager (SRM) 8.7 a VMware Live Site Recovery 9.0 NOTA: En ONTAP tools 10.x, SRM admite sitios compartidos, lo que permite una mayor escalabilidad y un mejor rendimiento.
Compatibilidad con protocolos	Almacenes de datos NFS y VMFS: NFS (v3 y v4.1), VMFS (iSCSI y FCP)	Almacenes de datos NFS y VMFS: NFS (v3 y v4.1), VMFS (iSCSI/FCP/NVMe-oF)
Escalabilidad	Hosts y máquinas virtuales: 300 hosts, hasta 10 000 máquinas virtuales Almacenes de datos: 600 NFS, hasta 50 VMFS	Servidores y máquinas virtuales: 600 hosts
Observabilidad	Cuadros de mando de rendimiento, capacidad y cumplimiento de hosts. Informes dinámicos de máquinas virtuales y almacenes de datos	Cuadros de mando actualizados de rendimiento, capacidad y cumplimiento de hosts. Informes dinámicos de máquinas virtuales y almacenes de datos
Protección de datos	Replicación SRA para VMFS y NFS. Integración con SCV e interoperabilidad para copias de seguridad.	Replicación SRA para almacenes de datos iSCSI VMFS y NFS v3, protección en tres sitios que combina SMAS y VMware Live Site Recovery. Compatibilidad de SRA con FCP y VMFS.
Compatibilidad con VASA Provider	VASA 4.0	VASA 3.0

Conceptos

Conoce las herramientas de ONTAP

ONTAP tools for VMware vSphere es un conjunto de herramientas para la gestión del ciclo de vida de las máquinas virtuales. Se integra con el ecosistema de VMware para simplificar el aprovisionamiento de datastores y proporcionar protección básica para las máquinas virtuales. Es una colección de microservicios escalables horizontalmente y basados en eventos, implementados como un Open Virtual Appliance (OVA).

ONTAP tools for VMware vSphere es compatible con:

- Funciones básicas de las máquinas virtuales (VM), como la protección y la recuperación ante desastres
- VASA Provider para la gestión basada en políticas de almacenamiento
- Gestión basada en políticas de almacenamiento
- Adaptador de replicación de almacenamiento (SRA)

Alta disponibilidad para ONTAP tools for VMware

ONTAP tools for VMware vSphere ofrece compatibilidad con alta disponibilidad (HA) para ayudar a mantener un funcionamiento ininterrumpido durante fallos.

La solución HA te ayuda a recuperarte rápidamente de los siguientes tipos de interrupciones:

- Fallo del servidor: solo se admite el fallo de un único nodo.
- Fallo de red
- Fallo de la máquina virtual (sistema operativo invitado)
- Fallo de la aplicación (ONTAP tools)

No necesitas realizar ninguna configuración adicional para habilitar la alta disponibilidad (HA) de ONTAP tools for VMware vSphere.



ONTAP tools for VMware vSphere no es compatible con vCenter HA.

Para utilizar la función HA, asegúrate de que la incorporación en caliente de CPU y la memoria conectable en caliente están activadas durante la implementación o en la configuración de la máquina virtual.

Conceptos y términos clave en ONTAP tools

La siguiente sección describe los conceptos y términos clave que se usan en el documento.

Autoridad de certificación (CA)

Una CA es una entidad de confianza que emite certificados Secure Sockets Layer (SSL).

Grupo de coherencia

Un grupo de coherencia es una colección de volúmenes gestionados como una única unidad. Los grupos de coherencia se sincronizan para garantizar la coherencia de los datos entre las unidades de almacenamiento y los volúmenes. En ONTAP, proporcionan una gestión sencilla y garantías de protección para una carga de trabajo de aplicaciones que abarca varios volúmenes. Más información sobre ["grupos de coherencia"](#).

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 que se utiliza 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 Small Computer System Interface (SCSI) o de uno de sus derivados encapsulados.

Espacio de nombres y subsistema NVMe

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

Administrador de ONTAP tools

ONTAP tools Manager proporciona ONTAP tools para administradores de VMware vSphere con un mayor control sobre las instancias de vCenter Server gestionadas y los backends de almacenamiento incorporados. Ayuda a gestionar las instancias de vCenter Server, los backends de almacenamiento, los certificados, las contraseñas y los paquetes de registro.

Open Virtual Appliance (OVA)

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

Objetivo de punto de recuperación (RPO)

El RPO mide la frecuencia con la que haces copias de seguridad o replicas datos. Especifica el punto exacto en el tiempo al que necesitas restaurar los datos después de una interrupción para reanudar las operaciones del negocio. 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.

SnapMirror active sync

SnapMirror active sync permite que los servicios empresariales sigan operando incluso ante un fallo total del sitio, permitiendo que las aplicaciones hagan la conmutación por error de forma transparente usando una copia secundaria. No necesitas intervención manual ni scripts personalizados para activar una conmutación por error con SnapMirror active sync. Más información sobre ["SnapMirror active sync"](#).

Backends de almacenamiento

Los backends de almacenamiento son la infraestructura de almacenamiento subyacente que utiliza el host ESXi para almacenar archivos, datos y otros recursos de las máquinas virtuales. Permiten al host ESXi acceder y gestionar datos persistentes, proporcionando la capacidad de almacenamiento y el rendimiento necesarios para un entorno virtualizado.

Clúster global (backend de almacenamiento)

Los backends de almacenamiento globales, disponibles únicamente con credenciales del clúster ONTAP, se integran a través de la interfaz de ONTAP tools Manager. Se pueden añadir con privilegios mínimos para permitir la detección de los recursos esenciales del clúster necesarios para la gestión de vVols. Los clústeres globales son ideales para escenarios de multitenancy en los que se añade un usuario SVM localmente para la gestión de vVols.

Backend de almacenamiento local

Los backends de almacenamiento local con credenciales de clúster o SVM se añaden a través de la interfaz de usuario de ONTAP tools y están limitados a un vCenter. Cuando se utilizan credenciales de clúster a nivel local, las SVM asociadas se asignan automáticamente con el vCenter para gestionar vVols o VMFS. Para la gestión de VMFS, incluido SRA, ONTAP tools admite credenciales de SVM sin necesidad de un clúster global.

Adaptador de replicación de almacenamiento (SRA)

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

Máquina virtual de almacenamiento (SVM)

SVM es la unidad de multitenancy 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 sirve datos a los clientes.

Configuración uniforme y no uniforme

- **Acceso uniforme a los hosts** significa que los hosts de dos sitios están conectados a todas las rutas hacia los clústeres de almacenamiento en ambos sitios. Las rutas entre sitios se extienden a lo largo de las distancias.
- **«Acceso no uniforme a los hosts»** significa que los hosts de cada sitio están conectados únicamente al clúster del mismo sitio. Las rutas entre sitios y las rutas extendidas no están conectadas.



Se admite el acceso uniforme al host para cualquier implementación de sincronización activa de SnapMirror; el acceso no uniforme al host solo se admite para implementaciones simétricas activo/activo. Más información sobre "[SnapMirror descripción general de active sync en ONTAP](#)".

Sistema de archivos de máquinas virtuales (VMFS)

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

Volúmenes virtuales (vVols)

vVols proporcionan 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 datastore vVol se asocia típicamente con un único LUN que actúa como contenedor para vVols.

Política de almacenamiento de máquinas virtuales

Las políticas de almacenamiento de máquinas virtuales se crean en el servidor vCenter en Políticas y perfiles. Para vVols, crea un conjunto de reglas usando reglas del proveedor de tipo de almacenamiento NetApp vVols.

VMware Live Site Recovery

VMware Live Site Recovery, anteriormente conocido como Site Recovery Manager (SRM), ofrece funciones de continuidad del negocio, recuperación ante desastres, migración de sitios y pruebas sin interrupciones para entornos virtuales de VMware.

APIs de VMware vSphere para Storage Awareness (VASA)

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

APIs de almacenamiento de VMware vSphere - Integración de cabinas (VAAI)

VAAI es un conjunto de API que permite la comunicación entre los hosts ESXi de VMware vSphere y los dispositivos de almacenamiento. Las API incluyen un conjunto de operaciones primitivas que utilizan los hosts para delegar las operaciones de almacenamiento a la matriz. VAAI puede aportar mejoras significativas en el rendimiento para tareas que requieren un uso intensivo del almacenamiento.

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) es una arquitectura que permite y admite vSphere en un despliegue de clúster ampliado. Las soluciones vMSC son compatibles con NetApp MetroCluster y SnapMirror active sync (anteriormente SMBC). Estas soluciones proporcionan una continuidad de negocio mejorada en caso de fallo del dominio. El modelo de resistencia se basa en tus opciones de configuración específicas. Más información sobre ["VMware vSphere Metro Storage Cluster"](#).

vVols almacén de datos

El datastore vVols es una representación lógica de un contenedor vVols creado y mantenido por un VASA Provider.

RPO cero

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

Control de acceso basado en roles (RBAC)

Conoce las herramientas RBAC de ONTAP

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 tu organización.

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

Componentes de RBAC

A grandes rasgos, hay varios componentes que generalmente se incluyen en toda implementación de RBAC. Estos componentes se unen 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 la capacidad de leer un archivo, o una operación más abstracta específica de un sistema de software determinado. Los privilegios también se pueden definir para restringir el acceso a los endpoints de la API de REST y a los comandos CLI. Cada implementación RBAC incluye privilegios predefinidos y también puede permitir a los administradores crear privilegios personalizados.

Roles

Un *rol* es un contenedor que incluye uno o más privilegios. Los roles se definen generalmente en función de tareas concretas o funciones laborales. Cuando se asigna un rol a un usuario, el usuario recibe todos los privilegios que contiene el rol. Y al igual que con los privilegios, las implementaciones incluyen roles predefinidos y generalmente permiten crear roles personalizados.

Objetos

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

Usuarios y grupos

A los *usuarios* se les asigna o se les asocia un rol tras la autenticación. Algunas implementaciones de RBAC solo permiten asignar un rol a un usuario, mientras que otras permiten varios roles por usuario, quizá 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 jerárquico de objetos donde pueden, opcionalmente, ser heredados por los hijos en la jerarquía.

Dos entornos RBAC

Hay dos entornos RBAC distintos que debes tener en cuenta al trabajar con ONTAP tools for VMware vSphere 10. ONTAP tools for VMware vSphere 10 requiere privilegios específicos tanto en vCenter como en ONTAP para realizar sus operaciones. Aunque ONTAP tools automatiza las tareas de gestión del almacenamiento, no

crea cuentas de usuario ni en vCenter ni en ONTAP. Las cuentas de servicio deben ser creadas por un administrador de vSphere según sea necesario. Esta documentación ofrece orientación a los administradores para asignar los roles y permisos necesarios para una gestión eficaz de ONTAP tools.

VMware vCenter Server

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 ONTAP tools for VMware vSphere 10, el entorno RBAC se amplía para incluir objetos adicionales que representan las capacidades de ONTAP tools. El acceso a estos objetos se proporciona a través del complemento remoto. Consulta ["vCenter servidor entorno RBAC"](#) para más información.

Clúster ONTAP

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

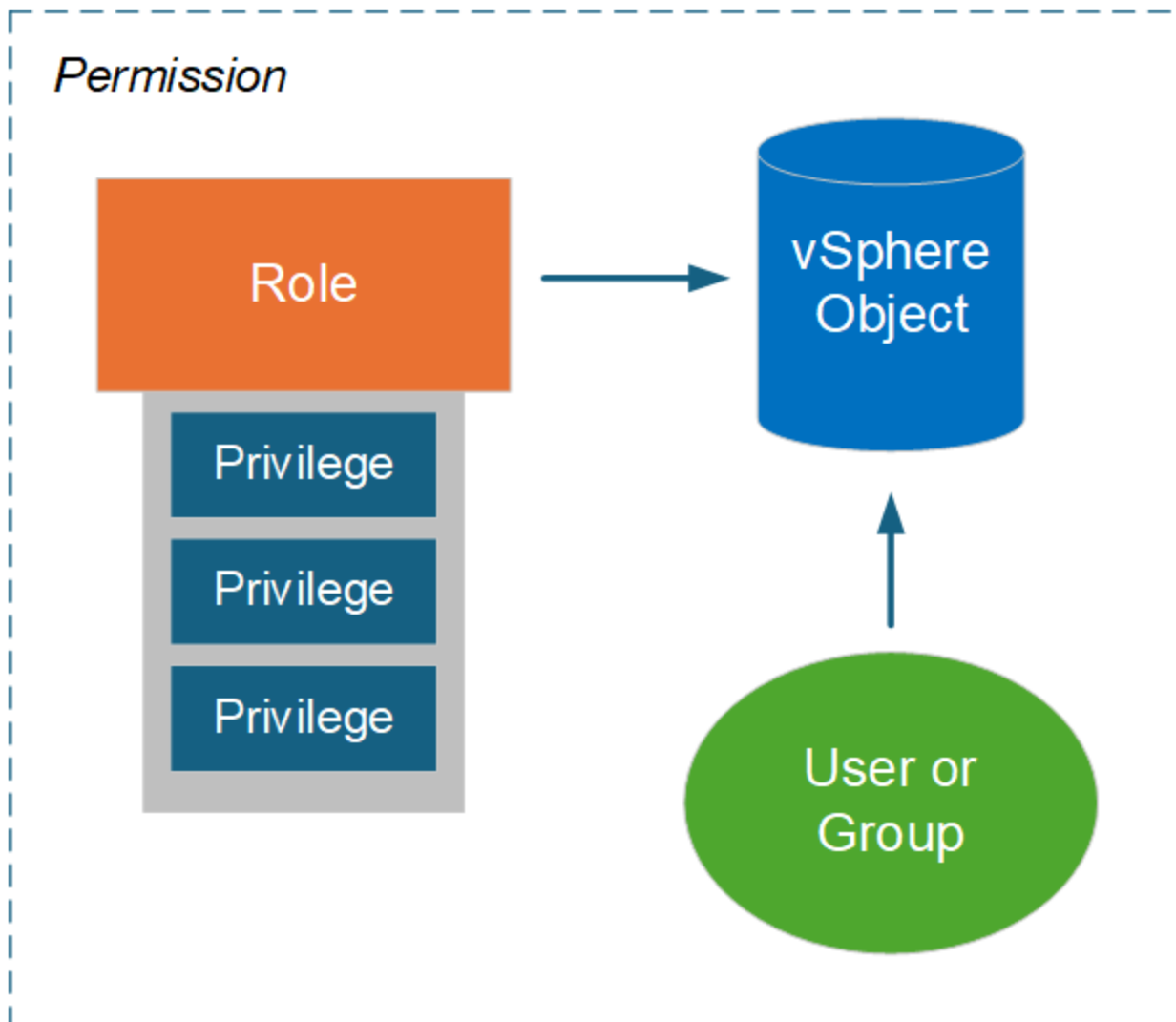
RBAC con VMware vSphere

Cómo funciona vCenter Server RBAC con ONTAP tools

VMware vCenter Server ofrece una función de RBAC que te permite controlar el acceso a los objetos de vSphere. Es una parte importante de los servicios de seguridad de autenticación y autorización 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 de vSphere con un usuario o grupo incluido en la definición del permiso. A grandes rasgos, se muestra una ilustración de un permiso de vCenter en la figura de abajo.



Componentes de un permiso de vCenter Server

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

vSphere objetos

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

Privilegios y roles

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

- Privilegios nativos del servidor vCenter

Estos son los privilegios que ofrece vCenter Server.

- Privilegios específicos de las herramientas de ONTAP

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

Usuarios y grupos

Puedes definir usuarios y grupos usando Active Directory o la instancia local de vCenter Server. Combinado con un rol, puedes crear un permiso sobre un objeto en la jerarquía de objetos de vSphere. El permiso otorga acceso según los privilegios del rol asociado. Ten en cuenta que los roles no se asignan directamente a los usuarios de forma aislada. En cambio, los usuarios y grupos obtienen acceso a un objeto a través de los privilegios del rol como parte del permiso más amplio de vCenter Server.

vCenter consideraciones sobre RBAC de Server para ONTAP tools

Hay varios aspectos de las ONTAP tools for VMware vSphere 10 en la implementación de RBAC con vCenter Server que debes considerar antes de usarlas en un entorno de producción.

vCenter roles y la cuenta de administrador

Solo necesitas definir y usar los roles personalizados de vCenter Server si quieres limitar el acceso a los objetos de vSphere y a las tareas administrativas asociadas. Si no es necesario limitar el acceso, puedes usar 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 los añadidos por ONTAP tools for VMware vSphere 10.

vSphere jerarquía de objetos

El inventario de objetos de vSphere está organizado en una jerarquía. Por ejemplo, puedes desplazarte 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 en el host ESXi de destino.

Roles incluidos con ONTAP tools for VMware vSphere 10

Para simplificar el trabajo con vCenter Server RBAC, ONTAP tools for VMware vSphere proporciona roles predefinidos adaptados a diversas tareas administrativas.



Puedes crear nuevos roles personalizados si lo necesitas. Para hacerlo, clona uno de los roles existentes de ONTAP tools y editálo según lo necesites. Después de hacer los cambios de configuración, los usuarios afectados del cliente vSphere deben cerrar sesión y volver a iniciarla para activar los cambios.

Para ver las herramientas de ONTAP para los roles de VMware vSphere, selecciona **Menú** en la parte superior del vSphere Client y haz clic en **Administración** y luego en **Roles** a la izquierda. Los siguientes privilegios deben estar incluidos en el rol asignado al usuario vCenter responsable de desplegar o incorporar

vCenter Server. Asegúrate de que estos privilegios estén configurados como requisito previo para el proceso de despliegue o incorporación.

- Alarmas
 - Confirmar alarma
- Biblioteca de contenidos
 - Agregar elemento a la biblioteca
 - Registrar en una plantilla
 - Echa un vistazo a una plantilla
 - Descargar archivos
 - Importar almacenamiento
 - Almacenamiento de lectura
 - Sincronizar elemento de la biblioteca
 - Sincroniza la biblioteca a la que estás suscrito
 - Ver configuración
- Almacén de datos
 - Asignar espacio
 - Examinar almacén de datos
 - Operaciones de archivo de bajo nivel
 - Eliminar archivo
 - Actualizar los archivos de la máquina virtual
 - Actualizar metadatos de máquina virtual
- ESX Agent Manager
 - Ver
- Carpeta
 - Crear carpeta
- Host
 - Configuración
 - Ajustes avanzados
 - Cambiar configuración
 - Configuración de red
 - Recursos del sistema
 - Configuración del inicio automático de la máquina virtual
 - Operaciones locales
 - Crear máquina virtual
 - Eliminar máquina virtual
 - Reconfigurar la máquina virtual
- Red

- Asignar red
- Configura
- OvfManager
 - OvfConsumer Acceso
- Perfil del host
 - Ver
- Recurso
 - Asignar máquina virtual a un pool de recursos
- Tarea programada
 - Crear tareas
 - Modificar tarea
 - Ejecutar tarea
- Tareas
 - Crear tarea
 - Actualizar tarea
- vApp
 - Agregar máquina virtual
 - Asignar pool de recursos
 - Asignar vApp
 - Crear
 - Importar
 - Mover
 - Apagar
 - Encender
 - Obtener de una URL
 - Ver el entorno OVF
- Máquina virtual
 - Modificar la configuración
 - Agregar disco existente
 - Agregar nuevo disco
 - Agregar o eliminar dispositivo
 - Configuración avanzada
 - Cambiar el recuento de CPU
 - Cambiar memoria
 - Cambiar la configuración
 - Cambiar recurso
 - Ampliar el disco virtual

- Modificar la configuración del dispositivo
- Quitar disco
- Restablecer la información del huésped
- Actualizar la compatibilidad de la máquina virtual
- Editar inventario
 - Crear desde existente
 - Crear nuevo
 - Mover
 - Regístrate
 - Quitar
 - Cancelar registro
- Interacción
 - Operación de copia de seguridad en una máquina virtual
 - Configura el medio CD
 - Configura los disquetes
 - Conectar dispositivos
 - Interacción con la consola
 - Administración del sistema operativo invitado mediante la API de VIX
 - Apagar
 - Encender
 - Restablecer
 - Suspende
- Aprovisionamiento
 - Permitir el acceso al disco
 - Clonar plantilla
 - Personaliza invitado
 - Implementar plantilla
 - Modificar especificación de personalización
 - Leer especificaciones de personalización
- Gestión de instantáneas
 - Crear instantánea
 - Eliminar instantánea
 - Renombrar snapshot
 - Revertir a la instantánea

Hay tres roles predefinidos, como se describe a continuación.

Administrador de NetApp ONTAP tools for VMware vSphere

Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de ONTAP tools necesarios

para realizar las tareas principales de administrador de ONTAP tools for VMware vSphere.

NetApp ONTAP tools para VMware vSphere solo lectura

Proporciona acceso de solo lectura a las herramientas de ONTAP. Estos usuarios no pueden realizar ninguna acción de las herramientas de ONTAP para VMware vSphere que esté sujeta al control de acceso.

Aprovisionamiento de NetApp ONTAP tools for VMware vSphere

Ofrece algunos de los privilegios nativos de vCenter Server y los privilegios específicos de ONTAP tools que se requieren para aprovisionar almacenamiento. Puedes realizar las siguientes tareas:

- Crear nuevos almacenes de datos
- Gestiona almacenes de datos

vSphere objetos y backends de almacenamiento ONTAP

Los dos entornos RBAC funcionan conjuntamente. Al realizar una tarea en la interfaz de cliente de vSphere, primero se comprueban los roles de ONTAP tools definidos en vCenter Server. Si la operación está permitida por vSphere, se examinan los privilegios del rol de ONTAP. Este segundo paso se realiza según el rol de ONTAP asignado al usuario cuando se creó y configuró el backend de almacenamiento.

Trabajar con RBAC de vCenter Server

Hay algunos aspectos que debes tener en cuenta al trabajar con los privilegios y permisos de vCenter Server.

Privilegios necesarios

Para acceder a la interfaz de usuario de ONTAP tools for VMware vSphere 10, necesitas tener el privilegio *View* específico de ONTAP tools. Si inicias sesión en vSphere sin este privilegio y haces clic en el icono de NetApp, ONTAP tools for VMware vSphere muestra un mensaje de error y te impide 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 puedes acceder. Asignar el privilegio de Ver al objeto raíz te permite acceder a ONTAP tools for VMware vSphere haciendo clic en el icono de NetApp.

En su lugar, puedes asignar el privilegio View a otro nivel de objeto inferior de vSphere. Sin embargo, esto limitará los menús de ONTAP tools for VMware vSphere a los que puedes acceder y usar.

Asignación de permisos

Debes utilizar los permisos de vCenter Server si deseas limitar el acceso a los objetos y tareas de vSphere. El lugar en el que asignes los permisos dentro de la jerarquía de objetos de vSphere determina las tareas de ONTAP tools for VMware vSphere 10 que los usuarios pueden realizar.



A menos que necesites definir un acceso más restrictivo, por lo general es buena práctica asignar permisos a nivel del objeto raíz o de la carpeta raíz.

Los permisos disponibles con ONTAP tools for VMware vSphere 10 se aplican a objetos personalizados que no son de vSphere, como los sistemas de almacenamiento. Si es posible, deberías asignar estos permisos al objeto raíz de ONTAP tools for VMware vSphere porque no hay ningún objeto de vSphere al que puedas asignarlos. Por ejemplo, cualquier permiso que incluya un privilegio de ONTAP tools for VMware vSphere “Add/Modify/Remove storage systems” debería asignarse a nivel del objeto raíz.

Al definir un permiso en un nivel superior de la jerarquía de objetos, puedes configurarlo para que se transmita

y sea heredado por los objetos hijos. Si lo necesitas, puedes asignar permisos adicionales a los objetos hijos que anulen los permisos heredados del padre.

Puedes modificar un permiso en cualquier momento. Si modificas alguno de los privilegios de un permiso, los usuarios asociados a dicho permiso deben cerrar sesión en vSphere y volver a iniciar sesión para que el cambio surta efecto.

RBAC con ONTAP

Cómo funciona ONTAP RBAC con ONTAP tools

ONTAP ofrece un entorno RBAC robusto y ampliable. Puedes utilizar la funcionalidad RBAC para controlar el acceso a los recursos de almacenamiento y a las operaciones del sistema expuestas a través de la API de REST y la CLI. Es útil estar familiarizado con el entorno antes de usarlo con una implementación de ONTAP tools for VMware vSphere 10.

Resumen de las opciones administrativas

Existen varias opciones disponibles a la hora de utilizar el RBAC de ONTAP, en función de tu entorno y tus objetivos. A continuación se ofrece una visión general de las principales decisiones administrativas. También puedes ver ["Automatización de ONTAP: descripción general de la seguridad RBAC"](#) para más información.



El RBAC de ONTAP está diseñado específicamente para un entorno de almacenamiento y es más sencillo que la implementación de RBAC que ofrece vCenter Server. Con ONTAP, asignas un rol directamente al usuario. Configurar permisos explícitos, como los que se usan con vCenter Server, no es necesario con el RBAC de ONTAP.

Tipos de roles y privilegios

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

- REST

Los roles REST se introdujeron con ONTAP 9.6 y, por lo general, se aplican a los usuarios que acceden a ONTAP a través de la API de REST. Los privilegios incluidos en estos roles se definen en función del acceso a los endpoints de la API de REST de ONTAP y las acciones asociadas.

- Tradicional

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

Aunque los roles REST se introdujeron más recientemente, los roles tradicionales ofrecen algunas ventajas. Por ejemplo, se pueden incluir parámetros de consulta adicionales para que los Privilegios definan con mayor precisión los objetos a los que se aplican.

Ámbito

Las funciones de ONTAP pueden definirse con uno de dos ámbitos diferentes. Pueden aplicarse a un SVM de datos específico (nivel de SVM) o a todo el clúster de ONTAP (nivel de clúster).

Definiciones de funciones

ONTAP ofrece un conjunto de roles predefinidos tanto a nivel de clúster como de SVM. También puedes

definir roles personalizados.

Trabajar con los roles REST de ONTAP

Hay varios aspectos que hay que tener en cuenta al utilizar los roles REST de ONTAP incluidos en ONTAP tools for VMware vSphere 10.

Asignación de funciones

Tanto si usas un rol tradicional como uno REST, todas las decisiones de acceso de ONTAP se toman en función del comando CLI subyacente. Pero como los privilegios en un rol REST se definen en términos de los endpoints de la API de REST, ONTAP necesita crear un rol tradicional *asignado* para cada uno de los roles REST. Por eso, cada rol REST se asigna a un rol tradicional subyacente. Esto permite que ONTAP tome decisiones de control de acceso de manera coherente sin importar el tipo de rol. No puedes modificar los roles asignados en paralelo.

Definir un rol REST usando privilegios de la CLI

Dado que ONTAP siempre utiliza los comandos de la CLI para determinar el acceso a nivel básico, es posible definir un rol REST utilizando los privilegios de los comandos de la CLI en lugar de los endpoints REST. Una de las ventajas de este enfoque es la mayor granularidad que ofrecen los roles tradicionales.

Interfaz administrativa al definir roles de ONTAP

Puedes crear usuarios y roles mediante la CLI de ONTAP y la API de REST. Sin embargo, es más conveniente usar la interfaz de System Manager junto con el archivo JSON disponible a través de ONTAP tools Manager. Consulta ["Utiliza el RBAC de ONTAP con ONTAP tools for VMware vSphere 10"](#) para más información.

Consideraciones de ONTAP RBAC para ONTAP tools

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

Resumen del proceso de configuración

ONTAP tools para VMware vSphere incluye soporte para crear un usuario de ONTAP con un rol personalizado. Las definiciones están empaquetadas en un archivo JSON que puedes subir al clúster de ONTAP. Puedes crear el usuario y adaptar el rol a tu entorno y necesidades de seguridad.

A continuación se describen a grandes rasgos los principales pasos de configuración. Consulta ["Configura los roles y privilegios de los usuarios de ONTAP"](#) para más detalles.

1. Prepara

Debes disponer de credenciales de administrador tanto para ONTAP tools Manager como para el clúster ONTAP.

2. Descarga el archivo de definición JSON

Después de iniciar sesión en la interfaz de usuario de ONTAP tools Manager, puedes descargar el archivo JSON que contiene las definiciones de RBAC.

3. Crea un usuario de ONTAP con un rol

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

1. Selecciona **Cluster** a la izquierda y luego **Settings**.
2. Desplázate hacia abajo hasta **Usuarios y roles** y haz clic →.

3. Selecciona **Add** en **Users** y selecciona **Virtualization products**.
4. Selecciona el archivo JSON en tu estación de trabajo local y súbelo.

4. Configura el rol

Como parte de la definición del rol, debes tomar varias decisiones administrativas. Consulta [Configura el rol mediante System Manager](#) para obtener más detalles.

Configura el rol mediante System Manager

Una vez que hayas empezado a crear un nuevo usuario y un rol con System Manager y hayas cargado el archivo JSON, puedes personalizar el rol según tu entorno y necesidades.

Configuración básica de usuarios y roles

Las definiciones de RBAC se incluyen en varias funcionalidades del producto, entre las que se encuentran combinaciones de VSC, VASA Provider y SRA. Debes seleccionar el entorno o los entornos donde necesites compatibilidad con RBAC. Por ejemplo, si quieres que los roles sean compatibles con la funcionalidad de complemento remoto, selecciona VSC. También necesitas elegir el nombre de usuario y la contraseña asociada.

Privileges

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

- Descubrimiento

Este rol te permite añadir sistemas de almacenamiento.

- Crear almacenamiento

Este rol te permite crear almacenamiento. También incluye todos los privilegios asociados con el rol discovery.

- Modificar almacenamiento

Este rol te permite modificar el almacenamiento. También incluye todos los privilegios asociados con los roles discovery y create storage.

- Destruir almacenamiento

Este rol te permite destruir almacenamiento. También incluye todos los privilegios asociados con los roles de descubrimiento, creación de almacenamiento y modificación de almacenamiento.

Genera el usuario con un rol

Una vez que hayas seleccionado las opciones de configuración para tu entorno, haz clic en **Add** y ONTAP crea 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 has seleccionado
- Lista de conjuntos de privilegios.

Ejemplo

OTV_10_VSC_Discovery_Create

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

Implementa ONTAP tools para VMware vSphere

Guía de inicio rápido para ONTAP tools for VMware vSphere

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

Completa primero estas tareas básicas para que las herramientas de ONTAP estén operativas para la gestión y el aprovisionamiento desde el primer día. Luego completa las tareas opcionales según tu entorno y tus requisitos de protección.

Inicialmente, vas a implementar ONTAP tools for VMware vSphere como una configuración de un solo nodo de tamaño pequeño que proporciona los servicios principales para soportar los datastores NFS y VMFS. Para ampliar tu configuración y añadir contenedores adicionales por servicio, mejorar la resiliencia o usar datastores vVols y alta disponibilidad (HA), completa primero este flujo de trabajo y luego sigue los pasos de expansión. Para más información, consulta el ["Flujo de trabajo de implementación de HA"](#).

1

Planifica tu implementación

Comprueba que tu entorno esté preparado para una implementación compatible. Comprueba que tus versiones de vSphere, ONTAP y del host ESXi sean compatibles con la versión de ONTAP tools. Asigna suficiente CPU, memoria y espacio en disco. Según tus reglas de seguridad, puede que necesites configurar firewalls u otras herramientas de seguridad para permitir el tráfico de red.

Asegúrate de que el servidor vCenter esté instalado y sea accesible.

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

2

Implementa ONTAP tools para VMware vSphere

Implementa el appliance de ONTAP tools para establecer los servicios base para los datastores NFS y VMFS.

Al principio, vas a implementar ONTAP tools for VMware vSphere en una configuración de un solo nodo de tamaño pequeño. Si planeas ampliar tu configuración para usar almacenes de datos vVols y alta disponibilidad (HA), lo harás después de terminar este flujo de trabajo. Para ampliar a una configuración HA, asegúrate de que la incorporación en caliente de CPU y la memoria conectable en caliente estén habilitadas.

Durante la implementación, revisa con atención los campos de **Personalizar plantilla**, especialmente el nombre de host, el uso de la dirección IP de ONTAP tools y los requisitos de DNS.

- ["Implementa ONTAP tools para VMware vSphere"](#)

3

Regístrate e instala el complemento de cliente de vCenter

Añade una instancia de vCenter Server para registrar el complemento de cliente de vCenter y aplicar los privilegios y roles necesarios. Cuando añades una instancia de vCenter Server, ONTAP tools registra el complemento remoto, aplica privilegios personalizados del complemento y de la API, crea roles personalizados y añade un acceso directo al complemento en la interfaz de usuario de vSphere.

- ["Agrega instancias de vCenter Server a ONTAP tools"](#)

4

Configura los backends de almacenamiento

Conecta los recursos de almacenamiento de ONTAP para permitir que las ONTAP tools aprovisionen y gestionen los datastores. Añade un backend de almacenamiento a un clúster ONTAP. En entornos multitenant donde un servidor vCenter está asociado con un SVM de un tenant, usa ONTAP tools Manager para añadir el clúster. Luego asocia el backend de almacenamiento con el servidor vCenter para crear una asignación global para esa instancia de vCenter.

Añade los backends de almacenamiento local con credenciales de clúster o SVM usando la interfaz de usuario de ONTAP tools. Estos backends de almacenamiento están limitados a un solo vCenter. Cuando usas credenciales de clúster localmente, los SVM asociados se asignan automáticamente al vCenter para gestionar vVols o VMFS. Para la gestión de VMFS, incluido SRA, ONTAP tools admite credenciales de SVM sin necesidad de un clúster global.

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

Tareas siguientes opcionales

1

Configura los roles y privilegios de usuario de ONTAP

Configura roles personalizados de ONTAP para un acceso de mínimo privilegio en lugar de la cuenta de administrador predeterminada.

- ["Configura los roles y privilegios de los usuarios de ONTAP"](#)

2

Actualiza los certificados para varias instancias de vCenter Server

Actualiza los certificados para usar una comunicación fiable basada en certificados entre varias instancias de vCenter Server.

- ["Gestiona certificados"](#)

3

Configura la protección SRA

Activa la función SRA para configurar la protección de recuperación ante desastres para los almacenes de datos NFS y VMFS.

- ["Habilita ONTAP tools for VMware vSphere services"](#)
- ["Configura SRA en el dispositivo VMware Live Site Recovery"](#)

4

Habilita la protección de active sync de SnapMirror

Configura la protección de clústeres de host con la sincronización activa de SnapMirror para proteger los almacenes de datos VMFS. En los sistemas ONTAP, haz el emparejamiento del clúster y el SVM requeridos y luego configura la protección del clúster de hosts en ONTAP tools for VMware vSphere. Esta opción solo se aplica a los almacenes de datos VMFS.

- ["Proteger usando la protección de clúster de hosts"](#)

5

Configura la copia de seguridad y la recuperación para tu implementación de ONTAP tools

Configura las copias de seguridad y la recuperación para proteger la configuración de ONTAP tools y poder recuperarte rápidamente en caso de fallos.

La copia de seguridad está activada de forma predeterminada en ONTAP tools for VMware vSphere 10.5 y se realiza cada 10 minutos. Programa copias de seguridad de tu configuración de ONTAP tools for VMware vSphere que puedes usar para recuperar la configuración en caso de un fallo.

- ["Edita la configuración de backup"](#)
- ["Recupera la configuración de las herramientas de ONTAP"](#)

Flujo de trabajo de despliegue de alta disponibilidad para ONTAP tools

Para aumentar la resiliencia y admitir más contenedores por servicio, amplía tu implementación inicial de ONTAP tools a una configuración de alta disponibilidad (HA). Habilitar el servicio VASA Provider es necesario para los datastores de vVols en una configuración HA.

1

Ampliar la implementación

Puedes ampliar las ONTAP tools for VMware vSphere configuration para aumentar el número de nodos en el entorno y cambiar la configuración a una configuración HA.

- ["Cambiar la configuración de ONTAP tools for VMware vSphere"](#)

2

Activar servicios

Para configurar los almacenes de datos de vVols, debes habilitar el servicio VASA Provider. Registra el VASA provider en vCenter y asegúrate de que tus políticas de almacenamiento cumplen los requisitos de HA, incluidas las configuraciones adecuadas de red y almacenamiento.

Habilita los servicios SRA para usar ONTAP tools Storage Replication Adapter (SRA) para VMware Site Recovery Manager (SRM) o VMware Live Site Recovery (VLSR).

- ["Habilita los servicios de VASA Provider y SRA"](#)

3

Actualiza los certificados

Si utilizas almacenes de datos vVol con varias instancias de vCenter Server, actualiza el certificado autofirmado por uno firmado por una autoridad de certificación (CA).

- ["Gestiona certificados"](#)

Requisitos y límites de configuración de ONTAP tools for VMware vSphere

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

Puedes usar las herramientas ONTAP para VMware vSphere con VMware vCenter Server Virtual Appliance (vCSA). Debes implementar las herramientas ONTAP para VMware vSphere en un entorno vSphere compatible que incluya hosts ESXi.

Requisitos del sistema

- **Requisitos de espacio del paquete de instalación por nodo**
 - 15 GB para instalaciones con thin provisioning
 - 348 GB para instalaciones con aprovisionamiento fijo
- **Requisitos de dimensionamiento del sistema host** La tabla siguiente muestra la memoria recomendada para cada tamaño de implementación. Para implementaciones de alta disponibilidad (HA), necesitas tres veces el tamaño del dispositivo indicado.

Tipo de despliegue	CPU por nodo	Memoria (GB) por nodo	Espacio en disco (GB) aprovisionado de forma thick por nodo
Pequeño	9	18	350
Medio	13	26	350
NOTA IMPORTANTE: La implementación a gran escala es solo para la configuración HA.	17	34	350



Cuando la copia de seguridad está activada, cada clúster de ONTAP tools necesita otros 50 GB de espacio en el datastore donde se implementan las máquinas virtuales. Por lo tanto, non-HA requiere 400 GB y HA requiere 1100 GB de espacio en total.

Requisitos mínimos de almacenamiento y aplicaciones

Almacenamiento, host y aplicaciones	Requisitos de versión
ONTAP	9.15.1, 9.16.1 y 9.17.0
ONTAP tools compatibles con hosts ESXi	A partir de la versión 7.0.3
Herramientas de ONTAP compatibles con vCenter Server	A partir de la versión 7.0U3
Proveedor de VASA	3,0
Aplicación OVA	10,5

Almacenamiento, host y aplicaciones	Requisitos de versión
Host ESXi para implementar la máquina virtual de ONTAP tools	7.0U3 y 8.0U3
Servidor vCenter para implementar la máquina virtual de ONTAP tools	7.0 y 8.0



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

La herramienta Interoperability Matrix Tool (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 de puertos

En la siguiente tabla se detallan los puertos de red que utiliza NetApp y su finalidad. Hay tres tipos diferentes de puertos:

- Puertos externos: Estos puertos son accesibles desde fuera del clúster o nodo de Kubernetes. Permiten que los servicios se comuniquen con redes o usuarios externos, lo que permite la integración con sistemas fuera del entorno del clúster.
- Puertos entre nodos: Estos puertos permiten la comunicación entre los nodos dentro del clúster de Kubernetes. Son necesarios para tareas del clúster como compartir datos y trabajar juntos. Para implementaciones de un solo nodo, los puertos entre nodos solo se usan dentro del nodo y no necesitan acceso externo. Los puertos entre nodos pueden aceptar tráfico desde fuera del clúster. Bloquea el acceso a internet a los puertos entre nodos con reglas de firewall.
- Puertos internos: Estos puertos se comunican dentro del clúster de Kubernetes utilizando direcciones ClusterIP. No están expuestos al exterior y no es necesario añadirlos a las reglas del cortafuegos.



Asegúrate de que todos los nodos de las herramientas ONTAP se encuentren en la misma subred para garantizar una comunicación ininterrumpida entre ellos.

Haz clic para expandir o contraer la tabla de requisitos de puerto.

Nombre del servicio/componente	Puerto	Protocolo	Tipo de puerto	Descripción
ntv-gateway-svc (LB)	443, 8443	TCP	Externo	Puerto de paso para la comunicación entrante del servicio VASA Provider. El certificado autofirmado de VASA Provider y el certificado de la CA personalizada se alojan en este puerto.
SSH	22	TCP	Externo	Secure Shell para el inicio de sesión en el servidor remoto y la ejecución de comandos.
servidor rke2	9345	TCP	Entre nodos	API de supervisor de RKE2 (restringir a redes de confianza).
kube-apiserver	6443	TCP	Entre nodos	Puerto del servidor de la API de Kubernetes (limitar a redes de confianza).
rpcbind/portmapper	111	TCP/UDP	Entre nodos	Se utiliza para la comunicación RPC entre servicios.
coredns (DNS)	53	TCP/UDP	Entre nodos	Servicio DNS para la resolución de nombres dentro del clúster.
NTP	123	UDP	Entre nodos	Protocolo de tiempo de red (NTP) para la sincronización horaria.
etcd	2379, 2380, 2381	TCP	Entre nodos	Almacén de clave-valor para datos de clúster.

Nombre del servicio/componente	Puerto	Protocolo	Tipo de puerto	Descripción
kube-vip	2112	TCP	Entre nodos	Puerto del servidor de la API de Kubernetes.
kubelet	10248, 10250	TCP	Entre nodos	Componente de Kubernetes
kube-controller	10257	TCP	Entre nodos	Componente de Kubernetes
controlador de nube	10258	TCP	Entre nodos	Componente de Kubernetes
kube-scheduler	10259	TCP	Entre nodos	Componente de Kubernetes
kube-proxy	10249, 10256	TCP	Entre nodos	Componente de Kubernetes
calico-node	9091, 9099	TCP	Entre nodos	Componente de red Calico.
containerd	10010	TCP	Entre nodos	Servicio de daemon de contenedores.
VXLAN (Flannel)	8472	UDP	Entre nodos	Red superpuesta para la comunicación entre pods.



En las implementaciones de HA, asegúrate de que el puerto UDP 8472 esté abierto entre todos los nodos. Este puerto permite la comunicación entre pods de distintos nodos; bloquearlo interrumpirá la red entre nodos.

Límites de configuración para desplegar ONTAP tools for VMware vSphere para almacenes de datos vVols

Puedes usar la siguiente tabla como guía para configurar ONTAP tools for VMware vSphere.

Implementación	Tipo	Número de vVols	Número de hosts
No-HA	Pequeña (S)	hasta 12K	32
No-HA	Medio (M)	hasta 24K	64
Alta disponibilidad	Pequeña (S)	hasta 24K	64
Alta disponibilidad	Medio (M)	hasta 50k	128
Alta disponibilidad	Grande (L)	hasta 100k	256



Los recuentos de host en la tabla representan el total combinado de todos los vCenters conectados.

Límites de configuración para desplegar ONTAP tools for VMware vSphere para almacenes de datos VMFS y NFS

Los límites de configuración enumerados en esta sección están validados y respaldados por NetApp. Los límites reales pueden variar según tu entorno y carga de trabajo. Superar estos límites puede afectar el rendimiento o la capacidad de soporte y no se recomienda. Ten en cuenta lo siguiente al revisar la tabla:

- La recuperación ante desastres (DR) de la máquina virtual se configura usando políticas síncronas, asíncronas o de sincronización estricta. DR no es compatible con el protocolo NVMe.
- La protección de clústeres de hosts ESXi usa SnapMirror Active Sync, que no admite implementaciones multi-vCenter.
- ONTAP tools restringe únicamente el número de hosts ESXi y almacenes de datos según el tamaño del despliegue. No hay restricciones sobre la cantidad de servidores vCenter que se pueden conectar a ONTAP tools.
- ONTAP tools realiza el descubrimiento en paralelo de todos los objetos de almacenamiento. Los límites de configuración para los objetos de almacenamiento ONTAP se aplican independientemente del número de objetos en uso activo.
- ONTAP tools no impone un límite en el número de vCenter Servers que se pueden integrar. Los límites de configuración vienen determinados por el número de hosts y almacenes de datos compatibles, como se detalla en la siguiente tabla.

Despliegue	Número de almacenes de datos VMFS y NFS	Número de almacenes de datos VMFS con DR habilitado	Número de hosts
Small (sin HA)	200	80	32
Medio sin HA	250	100	32
HA pequeño	350	200	64
HA Medio	600	200	128
HA Grande	1024	250	256

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

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

vCenter Tamaño de la implementación	Pequeño	Medio
Número total de máquinas virtuales configuradas para protección usando replicación basada en arrays	2000	5000
Número total de grupos de protección de replicación basados en array	250	250

vCenter Tamaño de la implementación	Pequeño	Medio
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 el número de instancias de VMware Live Site Recovery y las herramientas ONTAP correspondientes para el tamaño de despliegue de VMware vSphere.

Número de instancias de VMware Live Site Recovery	Tamaño de la implementación de ONTAP tools
Hasta 4	Pequeño
4 a 8	Medio
Más de 8	Grande

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

Requisitos previos a la implementación de las ONTAP tools

Asegúrate de que se cumplen los siguientes requisitos antes de continuar con la implementación:

Requisitos	Tu estado
vSphere versión, versión de ONTAP y versión del host ESXi son compatibles con la versión de ONTAP tools.	☐ Sí ☐ No
vCenter Server environment está configurado e instalado	☐ Sí ☐ No
Se borró la caché del navegador	☐ Sí ☐ No
Tienes las credenciales del servidor principal vCenter	☐ Sí ☐ No
Tienes las credenciales de inicio de sesión para la instancia del servidor vCenter, a la que las ONTAP tools for VMware vSphere se conectarán después de la implementación para el registro	☐ Sí ☐ No
El nombre de dominio para el que se emite el certificado se asigna a la dirección IP virtual en una implementación multi-vCenter donde los certificados de CA personalizados son obligatorios.	☐ Sí ☐ No
Has realizado la comprobación con nslookup en el nombre de dominio para comprobar si el dominio se resuelve a la dirección IP prevista.	☐ Sí ☐ No

Requisitos	Tu estado
El certificado se crea con el nombre de dominio y la dirección IP de ONTAP tools.	☐ Sí ☐ No
Las aplicaciones y los servicios internos de ONTAP tools son accesibles desde el servidor vCenter.	☐ Sí ☐ No
Cuando usas SVM multi-tenant, tienes un LIF de gestión de SVM en cada SVM.	☐ Sí ☐ No

Hoja de trabajo de implementación

Para una implementación en un único nodo

Utiliza la siguiente hoja de trabajo para recopilar la información necesaria para la implementación inicial de ONTAP tools for VMware vSphere:

Requisito	Tu valor
Dirección IP de la aplicación ONTAP tools. Esta es la dirección IP para acceder a la interfaz web del ONTAP tools manager (load balancer) en <code>https://<ip>:8443/virtualization/ui/</code>	
Dirección IP virtual de ONTAP tools para la comunicación interna. Esta dirección IP se utiliza para la comunicación interna en una configuración con varias instancias de ONTAP tools. Esta dirección IP no debe ser la misma que la dirección IP de la aplicación ONTAP tools. (Plano de control de Kubernetes)	
Nombre de host DNS del nodo de gestión de ONTAP tools	
Servidor DNS primario	
Servidor DNS secundario	
Dominio de búsqueda DNS	
Dirección IPv4 para el nodo de gestión de ONTAP tools. Es una dirección IPv4 única para la interfaz de gestión del nodo en la red de gestión. Esto se usa para conectarte al appliance de ONTAP tools para acceso remoto de diagnóstico por SSH.	
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)	



Crea registros DNS para todas las direcciones IP anteriores. Antes de asignar nombres de host, asígnalos a las direcciones IP libres en DNS. Todas las direcciones IP deben estar en la misma VLAN seleccionada para el despliegue.

Para una implementación de alta disponibilidad (HA)

Además de los requisitos de implementación en un único nodo, necesitarás la siguiente información para la implementación de alta disponibilidad (HA):

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

Configuración del cortafuegos de red

Asegúrate de que los puertos necesarios del cortafuegos estén abiertos para todas las direcciones IP pertinentes. ONTAP tools requieren acceso al LIF a través del puerto 443. Para obtener una lista completa de los puertos necesarios, consulta la sección de requisitos de puertos en ["Requisitos y límites de configuración de ONTAP tools for VMware vSphere"](#).

Configuración del almacenamiento ONTAP

Para garantizar una integración perfecta del almacenamiento ONTAP con ONTAP tools for VMware vSphere, ten en cuenta los siguientes ajustes:

- Si utilizas Fibre Channel (FC) para la conectividad de almacenamiento, configura la división en zonas en tus switches FC para conectar los hosts ESXi con las LIF de FC del SVM. ["Infórmate sobre la división en zonas FC y FCoE con los sistemas ONTAP"](#)
- Para usar la replicación de SnapMirror gestionada por las ONTAP tools, el administrador de almacenamiento de ONTAP debe crear ["Relaciones de paridad entre clústeres de ONTAP"](#) y ["Relaciones entre iguales de SVM entre clústeres de ONTAP"](#) en ONTAP antes de usar SnapMirror.

Implementa las herramientas ONTAP

El appliance de ONTAP tools for VMware vSphere se implementa como un nodo único de pequeño tamaño con servicios principales para soportar los datastores NFS y VMFS. El proceso de implementación de ONTAP tools puede tardar hasta 45 minutos.

Antes de empezar

Si vas a implementar un único nodo pequeño, una biblioteca de contenidos es opcional. Para implementaciones de varios nodos o de alta disponibilidad (HA), una biblioteca de contenidos es obligatoria. En VMware, una biblioteca de contenidos almacena plantillas de máquinas virtuales, plantillas de vApp y otros

archivos. Implementar con una biblioteca de contenidos ofrece una experiencia fluida porque no depende de la conectividad de red.

Ten en cuenta lo siguiente antes de crear una biblioteca de contenidos:

- Crea la biblioteca de contenidos en un almacén de datos compartido para que todos los hosts del clúster puedan acceder a ella.
- Configura la biblioteca de contenidos antes de implementar las ONTAP tools for VMware vSphere OVA.
- Asegúrate de que la biblioteca de contenidos esté creada antes de configurar el appliance para HA.



No elimines la plantilla OVA de la biblioteca de contenidos tras la implementación.



Para permitir el despliegue de HA en el futuro, evita desplegar la máquina virtual de ONTAP tools directamente en un host ESXi. En su lugar, despliega la máquina virtual dentro de un clúster de hosts ESXi o pool de recursos.

Sigue estos pasos para crear una biblioteca de contenidos:

1. Descarga el archivo que contiene los binarios (.ova) y los certificados firmados para ONTAP tools for VMware vSphere desde ["Sitio de soporte de NetApp"](#).
2. Inicia sesión en el cliente de vSphere
3. Selecciona el menú del cliente vSphere y selecciona **biblioteca de contenidos**.
4. Selecciona **Crear** a la derecha de la página.
5. Introduce un nombre para la biblioteca y crea la biblioteca de contenidos.
6. Ve a la biblioteca de contenidos que has creado.
7. Selecciona **Acciones** a la derecha de la página, selecciona **Importar elemento** e importa el archivo OVA.



Para más información, consulta el ["Creación y uso de la biblioteca de contenidos"](#) blog.



Antes de proceder con el despliegue, configura el Programador de recursos distribuidos (DRS) del clúster en Conservador. Esto garantiza que las máquinas virtuales no se migren durante la instalación.

Las ONTAP tools for VMware vSphere se despliegan inicialmente como una configuración no HA. Para escalar a un despliegue HA, necesitarás habilitar la incorporación en caliente de CPU y la memoria conectable en caliente. Puedes realizar este paso como parte del proceso de despliegue o editar la configuración de la máquina virtual después del despliegue.

Pasos

1. Descarga el archivo que contiene los binarios (.ova) y los certificados firmados para ONTAP tools for VMware vSphere desde ["Sitio de soporte de NetApp"](#). Si ya has importado el archivo OVA a la biblioteca de contenidos, puedes saltarte este paso y continuar con el siguiente.
2. Inicia sesión en el servidor vSphere.
3. Ve al pool de recursos, clúster o host donde quieres implementar el OVA.



Nunca almacenes la máquina virtual de ONTAP tools for VMware vSphere en los almacenes de datos vVols que gestiona.

4. Puedes implementar el OVA desde la biblioteca de contenidos o desde el sistema local.

Desde el sistema local	De la biblioteca de contenidos
a. Haz clic con el botón derecho y selecciona Implementar plantilla OVF.... b. Elige el archivo OVA desde la URL o busca su ubicación, luego selecciona Siguiente .	a. Ve a tu biblioteca de contenidos y selecciona el elemento de la biblioteca que quieras implementar. b. Selecciona Acciones > Nueva máquina virtual a partir de esta plantilla

5. En el campo **Seleccionar un nombre y una carpeta**, introduce el nombre de la máquina virtual y elige su ubicación.

- Si estás usando la versión vCenter Server 8.0.3, selecciona la opción **Personalizar el hardware de esta máquina virtual**, lo que activará un paso adicional llamado **Personalizar hardware** antes de pasar a la ventana **Listo para finalizar**.
- Si estás usando la versión vCenter Server 7.0.3, sigue los pasos de la sección **¿Qué sigue?** al final de la implementación.

netapp-ontap-tools-for-vmware-vsphere-10.5-1740090540 - 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: demoov

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. Selecciona un recurso de computación y haz clic en **Siguiente**. Si lo deseas, marca la casilla para **Encender automáticamente la máquina virtual implementada**.

7. Revisa los detalles de la plantilla y selecciona **Siguiente**.

8. Lee y acepta el contrato de licencia y selecciona **Siguiente**.

9. Selecciona el almacenamiento para la configuración y el formato del disco, y selecciona **Siguiente**.
10. Selecciona la red de destino para cada red de origen y selecciona **Siguiente**.
11. En la ventana **Personalizar plantilla**, rellena los campos obligatorios.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template**
- Customize hardware
- Ready to complete

Customize template

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

vCenter Server configuration for ONTAP tools deployment 3 settings

vCenter Server hostname*

Enter the hostname of the target vCenter Server for ONTAP tools deployment.

vCenter Server username (user@domain.com)*

Enter the user principal name of the vCenter Server account (for example, username@vsphere.local).
backup@vsphere.local

vCenter Server password*

Enter the vCenter Server password to authenticate your login.

Password

Confirm Password

CANCEL BACK NEXT

Los valores de la página **Personalizar plantilla** son obligatorios para que la implementación sea exitosa.

Presta especial atención a estos campos:



- **Nombre de host:** Introduce el nombre de host de la máquina virtual de ONTAP tools. Utiliza un formato de nombre de host válido.
- **Dirección IP de ONTAP tools:** Esta es la interfaz de gestión principal que se usa para acceder a ONTAP tools.
- **Dirección IPv4:** Esta es la dirección IP del nodo que se usa para el shell de diagnóstico y el acceso SSH para la resolución de problemas y el mantenimiento.

Si utilizas nombres DNS para el host o vCenter, asegúrate de que esos nombres se resuelvan correctamente en DNS.



El nombre de host de vCenter es el nombre de la instancia de servidor vCenter donde se implementa el appliance de ONTAP tools.

Si estás desplegando herramientas ONTAP en una topología de dos vCenter Server, donde el appliance está alojado en una instancia de vCenter y gestiona otra, puedes asignar un rol restringido para la instancia de vCenter que aloja las herramientas ONTAP. Puedes crear un usuario y un rol dedicados de vCenter con solo los permisos necesarios para el despliegue de plantillas OVF. Para más detalles, consulta los roles listados en ["Roles incluidos con ONTAP tools for VMware vSphere 10"](#).

Para la instancia de vCenter que será gestionada por ONTAP tools, asegúrate de que la cuenta de usuario de vCenter tenga privilegios de administrador.

- Los nombres de host deben incluir letras (A-Z, a-z), dígitos (0-9) y guiones (-). Para configurar la pila dual, especifica el nombre de host asociado a la dirección IPv6.



No se admite IPv6 puro. Se admite el modo mixto con una VLAN que contenga direcciones tanto IPv6 como IPv4.

- La dirección IP de ONTAP tools es la interfaz principal para comunicarse con ONTAP tools.
- IPv4 es el componente de la dirección IP de la configuración del nodo, que puede utilizarse para habilitar el shell de diagnóstico y el acceso SSH en el nodo con fines de depuración y mantenimiento.

12. Cuando utilices la versión vCenter Server 8.0.3, en la ventana **Personalizar hardware**, activa las opciones **CPU incorporación en caliente** y **Memoria conectable en caliente** para permitir la funcionalidad de HA.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - 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 Customize hardware**
- 9 Ready to complete

Customize hardware

Configure the virtual machine hardware

Virtual Hardware VM Options Advanced Parameters

[ADD NEW DEVICE](#)

CPU * 9 ⓘ

Cores per Socket 1 ⌵
Sockets: 9

CPU Hot Plug ☒ Enable CPU Hot Add

Reservation 10305 ⌵ 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 ⓘ

CANCEL BACK NEXT

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - 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 Customize hardware

9 Ready to complete

Customize hardware

Limit

Unlimited

MIN

Shares

Normal

1000

Hardware virtualization

☐

Expose hardware assisted virtualization to the guest OS

Performance Counters

☐

Enable virtualized CPU performance counters

Scheduling Affinity

I/O MMU

☐

Enabled

Memory *

18

GB

Reservation

9

GB

☐

Reserve all guest memory (All locked)

Limit

Unlimited

MB

Shares

Normal

368640

Memory Hot Plug

☒

Enable

Hard disks *

5 total | 348 GB

CANCEL

BACK

NEXT

13. Revisa los detalles en la ventana **Listo para finalizar** y selecciona **Finalizar**.

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

14. Enciende la máquina virtual después de completar la tarea si no seleccionaste la opción de encenderla automáticamente.

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

Si hay discrepancias en el formulario OVF, aparecerá un cuadro de diálogo solicitando que tomes medidas correctivas. Usa la tecla Tab para navegar, haz los cambios necesarios y selecciona **OK**. Tienes 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.

¿Y ahora qué?

Si has desplegado ONTAP tools for VMware vSphere con vCenter Server 7.0.3, entonces sigue estos pasos después del despliegue.

1. Inicia sesión en el cliente de vCenter
2. Apaga el nodo de ONTAP tools.
3. Ve a las ONTAP tools for VMware vSphere máquina virtual en **Inventarios** y selecciona la opción **Editar configuración**.
4. En las opciones de **CPU**, marca la casilla **Enable CPU hot add**
5. En las opciones de **Memoria**, marca la casilla **Habilitar** junto a **Incorporación en caliente de memoria**.

Soluciona errores de despliegue de ONTAP tools

Si tienes problemas con la implementación, revisa los registros y los códigos de error para diagnosticar y resolver problemas. A partir de ONTAP tools for VMware vSphere 10.5, los paquetes de registros recopilados de los pods incluyen registros de MongoDB, RabbitMQ y Vault, junto con el estado y las descripciones de todos los pods. Estos se proporcionan además de los registros de servicio existentes de ONTAP tools, mejorando la capacidad de soporte y la resolución de problemas.

Recopila los archivos de registro

Puedes recopilar los archivos de registro de ONTAP tools for VMware vSphere desde las opciones disponibles en la interfaz de usuario de ONTAP tools Manager. El soporte técnico podría pedirte que recopiles los archivos de registro para ayudar a solucionar un problema.



La generación de registros desde el administrador de ONTAP tools 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 vCenter Server seleccionado.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona **Paquetes de registros** en la barra lateral.

Esta operación puede tardar varios minutos.

4. Selecciona **Generar** para generar los archivos de registro.
5. Introduce la etiqueta del paquete de registros y selecciona **Generar**.

Descarga el archivo tar.gz y envíalo al soporte técnico.

Sigue los pasos que se indican a continuación para generar un paquete de registros mediante la interfaz de usuario del cliente de vCenter:

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Desde la página de inicio del vSphere Client, ve a **Soporte > Paquete de registros > Generar**.
3. Introduce la etiqueta del paquete de registros y genera el paquete de registros. Puedes ver la opción de descarga cuando se generan los archivos. La descarga puede tardar un rato.



El paquete de registros generado sustituye al paquete de registros que se generó en los últimos 3 días o 72 hrs.

Códigos de error de implementación

Es posible que encuentres códigos de error durante las operaciones de implementación, reinicio y

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

Todos los registros de errores se guardan en el archivo `ansible-perl-errors.log`, ubicado en el directorio `/var/log`, para facilitar el seguimiento y la resolución de problemas. Este archivo de registro contiene el código de error y la tarea de Ansible que falló.



Los códigos de error proporcionados en esta página son solo de referencia. Contacta al equipo de soporte si el error persiste o si no se menciona una resolución.

En la siguiente tabla se enumeran los códigos de error y los nombres de archivo correspondientes.

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

Los tres últimos dígitos del código de error indican el error concreto del flujo de trabajo 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 claves SSH	Reinicia la máquina virtual (VM) principal.
053	Error al instalar RKE2	Ejecuta lo siguiente y reinicia la máquina virtual principal o vuelve a implementarlas: <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	Reimplementar

055	Error al implementar el registro	Si el pod de registro está presente, espera a que el pod esté listo y luego reinicia la máquina virtual principal o vuelve a desplegar.
059	KubeVip la implementación ha fallado	Asegúrate de que la dirección IP virtual para el plano de control de Kubernetes y la dirección IP de ONTAP tools proporcionadas durante el despliegue pertenezcan a la misma VLAN y sean direcciones IP libres. Reinicia si todos los puntos anteriores son correctos. Si no, vuelve a desplegar.
060	El despliegue del operador ha fallado	Reiniciar
061	Error en la implementación de los servicios	Realiza tareas básicas de depuración de Kubernetes como get pods, get rs, get svc, etc., en el espacio de nombres ntv-system para obtener más detalles y consultar los registros de errores en /var/log/ansible-perl-errors.log y /var/log/ansible-run.log y vuelve a implementar.
062	Error en la implementación de los servicios de ONTAP tools	Consulta los registros de errores en /var/log/ansible-perl-errors.log para obtener más detalles y vuelve a realizar la implementación.
065	No se puede acceder a la URL de la página de Swagger	Reimplementar
066	Los pasos posteriores a la implementación para el certificado de la pasarela han fallado	Haz lo siguiente para recuperar/completar la actualización: • Habilita el shell de diagnóstico. • Ejecuta el comando 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'. • Revisa los registros en /var/log/post-deploy-upgrade.log.

088	Error al configurar la rotación de registros para journald	Comprueba que la configuración de red de la máquina virtual sea compatible con el host en el que está alojada. Puedes intentar migrar a otro host y reiniciar la máquina virtual.
089	Error al cambiar el propietario del archivo de configuración de rotación del registro de resumen	Reinicia la máquina virtual principal.
096	Instala el proveedor de almacenamiento dinámico	-
108	El script de seeding ha fallado	-
114	Falló la actualización interna del certificado en la colección MongoDB	Si el despliegue falla con el código de error 114, completa los siguientes pasos: • Habilita el shell de diagnóstico. • Ejecuta el siguiente comando: <pre>sudo perl /home/maint/scripts/post- t-deploy-upgrade.pl --internal_cert_update_ collection</pre> • Revisa los registros en <pre>/var/log/otvng/post- deploy-upgrade.log</pre>

Código de error de reinicio	Flujo de trabajo	Resolución
067	Se agotó el tiempo de espera para rke2-server.	-
101	No se pudo restablecer la contraseña del usuario Maint/Console.	-
102	No se pudo eliminar el archivo de contraseñas durante el restablecimiento de la contraseña del usuario Maint/Console.	-
103	No se pudo actualizar la contraseña del nuevo usuario Maint/Console en el almacén.	-
088	Error al configurar la rotación de registros para journald.	Comprueba que la configuración de red de la máquina virtual sea compatible con el host en el que está alojada. Puedes intentar migrar a otro host y reiniciar la máquina virtual.

089	No se pudo cambiar el propietario del archivo de configuración de rotación del registro de resumen.	Reinicia la máquina virtual.
-----	---	------------------------------

Configura ONTAP tools para VMware vSphere

Agrega instancias de vCenter Server a ONTAP tools

Añade instancias de vCenter Server a ONTAP tools for VMware vSphere para configurar, gestionar y proteger tus almacenes de datos virtuales en tu entorno de vCenter Server. Cuando añades varias instancias de vCenter Server, se requieren certificados CA personalizados para una comunicación segura entre ONTAP tools y cada vCenter Server.

Acerca de esta tarea

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

Al añadir una instancia de vCenter Server a ONTAP tools, se activan automáticamente las siguientes acciones:

- ONTAP tools registra el complemento de cliente vCenter como un complemento remoto.
- Los privilegios personalizados para los complementos y las API se aplican a la instancia de vCenter Server.
- Los roles personalizados se crean para gestionar a los usuarios.
- El complemento aparece como un acceso directo en la interfaz de usuario de vSphere.

Antes de empezar

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

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

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

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



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

Pasos

1. Abre un navegador web y ve a la URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona **vCenters** > **Add** para integrar las instancias de vCenter Server. Introduce tu dirección IP o nombre de host de vCenter, nombre de usuario, contraseña y detalles del puerto.
4. En las opciones avanzadas, descarga automáticamente el certificado del servidor vCenter (autorízalo) o súbelo manualmente.



No necesitas una cuenta de administrador para añadir instancias de vCenter a ONTAP tools. Puedes crear un rol personalizado sin la cuenta de administrador, con permisos limitados. Consulta "[Usa RBAC de vCenter Server con ONTAP tools for VMware vSphere 10](#)" para más detalles.

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

Utiliza ONTAP tools for VMware vSphere para registrar el VASA Provider con una instancia de vCenter Server. Esto permite la gestión basada en políticas de almacenamiento, compatibilidad con vVols y la integración con los appliances VMware Live Site Recovery en sistemas ONTAP.

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

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Selecciona **Accesos directos** > **NetApp ONTAP tools** en la sección de complementos.
3. Selecciona **Configuración** > **Configuración del proveedor VASA**. ONTAP tools muestra el estado de registro del proveedor VASA como no registrado.
4. Pulsa el botón **Registrar** para registrar el proveedor VASA.
5. Introduce un nombre y credenciales para el VASA Provider. El nombre de usuario solo puede contener letras, números y guiones bajos. La contraseña debe tener entre 8 y 256 caracteres.
6. Selecciona **Register**.
7. Después de un registro exitoso y de actualizar la página, las herramientas de ONTAP muestran el estado, el nombre y la versión del VASA Provider registrado.

Qué sigue

Comprueba que el proveedor VASA incorporado esté en la lista de proveedores VASA desde el cliente vCenter:

Pasos

1. Ve a la instancia de vCenter Server.

2. Inicia sesión con las credenciales de administrador.
3. Selecciona **Proveedores de almacenamiento > Configurar**. Comprueba que el proveedor VASA integrado aparezca correctamente en la lista.

Instala el complemento NFS VAAI usando ONTAP tools

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

Antes de empezar

- Descarga el paquete de instalación "[NetApp Complemento NFS para VMware VAAI](#)".
- Asegúrate de que tienes hosts ESXi con vSphere 7.0 U3 (último parche o posterior) y ONTAP 9.14.1 o posterior.
- Monta un almacén de datos NFS.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Selecciona **Accesos directos > NetApp ONTAP tools** en la sección de complementos.
3. Selecciona **Configuración > Herramientas NFS VAAI**.
4. Si ya has subido el complemento VAAI a vCenter Server, selecciona **Cambiar** en **Versión existente**. Si aún no lo has hecho, selecciona **Subir**.
5. Busca y selecciona el archivo `.vib` y selecciona **Subir** para cargar el archivo en ONTAP tools.
6. Selecciona **Install on ESXi host**, selecciona el host ESXi en el que quieres instalar el complemento NFS VAAI y luego selecciona **Install**.

El vSphere Web Client muestra únicamente los hosts ESXi en los que se puede instalar el complemento. Puedes supervisar el progreso de la instalación en la sección de tareas recientes.

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

Después de reiniciar el host ESXi, ONTAP tools for VMware vSphere detecta y habilita automáticamente el complemento NFS VAAI.

¿Qué sigue?

Una vez que instales el complemento NFS VAAI y reinicies tu host ESXi, configura las políticas de exportación NFS para la copia de datos descargados mediante VAAI. Asegúrate de que las reglas de las políticas de exportación cumplan estos requisitos:

- El volumen ONTAP correspondiente permite llamadas NFSv4.
- El usuario raíz sigue siendo root y se permite NFSv4 en todos los volúmenes principales de los enlaces de unión.
- La opción de compatibilidad con VAAI se configura en el servidor NFS correspondiente.

Para obtener más información, consulta el artículo de la base de conocimientos en "[Configura las políticas de exportación NFS correctas para la copia de datos descargados VAAI](#)" KB.

Información relacionada

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

["Activar o desactivar NFSv4.0"](#)

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

Configura los ajustes del host ESXi en ONTAP tools

La configuración de los parámetros de multivía y tiempo de espera del servidor ESXi ayuda a mantener la disponibilidad y la integridad de los datos. Permite la conmutación automática por error a una ruta de almacenamiento de backup si la ruta principal deja de estar disponible.

Configura los parámetros de multivía y tiempo de espera del servidor ESXi

ONTAP tools for VMware vSphere comprueba y configura los ajustes de multivía del host ESXi y los ajustes de tiempo de espera del HBA que mejor funcionan con los sistemas de almacenamiento NetApp.

Acerca de esta tarea

Este proceso puede tardar un tiempo, dependiendo de tu configuración y de la carga del sistema. Puedes ver el progreso en el panel Tareas recientes.

Pasos

1. Desde la página de inicio del cliente web de VMware vSphere, selecciona **Hosts and Clusters**.
2. En la página de accesos directos del cliente web de VMware vSphere, selecciona **NetApp ONTAP tools** en la sección de complementos.
3. Accede a la ficha **Cumplimiento del host ESXi** en la vista general (panel de control) del complemento ONTAP tools for VMware vSphere.
4. Selecciona el enlace **Aplicar la configuración recomendada**.
5. En la ventana **Aplicar la configuración recomendada para los hosts**, selecciona los hosts que quieres actualizar para que usen la configuración recomendada por NetApp y selecciona **Siguiente**.



Puedes expandir el host ESXi para ver los valores actuales.

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

Configura los valores del host ESXi

Utiliza ONTAP tools for VMware vSphere para configurar los tiempos de espera y otros valores en los hosts ESXi para un rendimiento y una conmutación de sitios óptimos. Establece estos valores según las pruebas de NetApp.

Puedes configurar los siguientes valores en un host ESXi:

Configuración del adaptador HBA/CNA

Establece los siguientes parámetros en sus valores predeterminados:

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

Configuración de MPIO

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

En entornos de alto rendimiento o al realizar pruebas con un único almacén de datos LUN, ajusta la configuración de equilibrio de carga de la política de selección de ruta round-robin (VMW_PSP_RR) para mejorar el rendimiento. Establece el valor predeterminado de IOPS de 1000 a 1.



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

Configuración de NFS

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

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

Utiliza esta sección para configurar los roles y privilegios de usuario de ONTAP para los backends de almacenamiento con ONTAP tools for VMware vSphere y ONTAP System Manager. Puedes asignar roles utilizando los archivos JSON proporcionados, crear usuarios y roles manualmente y aplicar los privilegios mínimos necesarios para las cuentas que no sean de administrador.

Antes de empezar

- Descarga el archivo de Privileges de ONTAP desde ONTAP tools for VMware vSphere usando https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip. Después de descargar el archivo zip, encontrarás dos archivos JSON. Usa el archivo JSON específico de ASA r2 cuando configures

un sistema ASA r2.



Puedes crear usuarios a nivel de clúster o directamente a nivel de las máquinas virtuales de almacenamiento (SVM). Si no utilizas el archivo `user_roles.json`, asegúrate de que el usuario tenga los permisos mínimos requeridos para las SVM.

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

Pasos

1. Extrae el archivo `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip` que descargaste.
2. Accede a ONTAP System Manager usando la dirección IP de gestión del clúster.
3. Inicia sesión en el clúster con privilegios de administrador. Para configurar un usuario:
 - a. Para configurar un usuario de ONTAP tools del clúster, selecciona **Cluster > Settings > el panel Users and Roles**.
 - b. Para configurar un usuario de ONTAP tools en una SVM, selecciona **Storage SVM > Settings > el panel Users and Roles**.
 - c. Selecciona **Add** en Usuarios.
 - d. En el cuadro de diálogo **Add User**, selecciona **Virtualization products**.
 - e. **Navega** para seleccionar y cargar el archivo JSON de Privileges de ONTAP. Para los sistemas que no sean ASA r2, selecciona el archivo `users_roles.json` y para los sistemas ASA r2, selecciona el archivo `users_roles_ASAr2.json`.

ONTAP tools rellena automáticamente el campo **Producto**.

- f. Selecciona la funcionalidad del producto **VSC, VASA Provider y SRA** en el menú desplegable.

ONTAP tools rellena automáticamente el campo **Role** según la capacidad del producto que selecciones.

- g. Introduce el nombre de usuario y la contraseña requeridos.
- h. Selecciona los privilegios (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) que necesita el usuario y luego selecciona **Add**.

ONTAP tools añade el nuevo rol y el nuevo usuario. Puedes ver los privilegios bajo el rol que configuraste.

Requisitos de mapeo de agregados de SVM

Al aprovisionar almacenes de datos utilizando las credenciales de usuario de SVM, ONTAP tools for VMware vSphere crea volúmenes en el agregado especificado en la API POST de los almacenes de datos. ONTAP impide que los usuarios de SVM creen volúmenes en agregados que no estén asignados al SVM. Asigna el SVM a los agregados necesarios usando la API de REST de ONTAP o la CLI antes de crear volúmenes.

API de REST:

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

CLI de ONTAP:

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

Crear usuario y rol de ONTAP manualmente

Crea usuarios y roles manualmente sin el archivo JSON.

1. Accede a ONTAP System Manager usando la dirección IP de gestión del clúster.
2. Inicia sesión en el clúster con privilegios de administrador.
 - a. Para configurar las funciones de las herramientas ONTAP del clúster, selecciona **Cluster > Settings > Users and Roles**.
 - b. Para configurar los roles de las herramientas SVM ONTAP del clúster, selecciona **Storage SVM > Settings > Users and Roles**.
3. Crear roles:
 - a. Selecciona **Add** en la tabla **Roles**.
 - b. Introduce los datos de **Nombre del rol** y **Atributos del rol**.

Agrega la **ruta de la API de REST** y elige el tipo de acceso en la lista desplegable.

- c. Agrega todas las API necesarias y guarda los cambios.
4. Crear usuarios:
 - a. Selecciona **Add** en la tabla **Users**.
 - b. En el cuadro de diálogo **Añadir usuario**, selecciona **System Manager**.
 - c. Introduce el **nombre de usuario**.
 - d. Selecciona **Rol** entre las opciones creadas en el paso **Crear Roles** anterior.
 - e. Introduce las aplicaciones a las que quieres dar acceso y el método de autenticación. ONTAPI y HTTP son las aplicaciones requeridas, y el tipo de autenticación es **Password**.
 - f. Establece la **contraseña del usuario** y **guarda** el usuario.

Lista de privilegios mínimos necesarios para un usuario del clúster sin derechos de administrador y con ámbito global

En esta página se enumeran los privilegios mínimos necesarios para un usuario del clúster de ámbito global que no sea administrador y que no disponga de un archivo JSON. Si el clúster tiene ámbito local, utiliza el archivo JSON para crear usuarios porque ONTAP tools for VMware vSphere necesita algo más que los privilegios de lectura para el aprovisionamiento en ONTAP.

Puedes acceder a las funciones mediante las API:

API	Nivel de acceso	Se utiliza para
-----	-----------------	-----------------

/api/cluster	Solo lectura	Detección de la configuración del clúster
/api/cluster/licensing/licenses	Solo lectura	Comprobación de licencias específicas del protocolo
/api/cluster/nodes	Solo lectura	Detección del tipo de plataforma
/api/security/accounts	Solo lectura	Detección de privilegios
/api/security/roles	Solo lectura	Detección de privilegios
/api/storage/aggregates	Solo lectura	Comprobación del espacio del agregado durante el aprovisionamiento del almacén de datos o volumen
/api/storage/cluster	Solo lectura	Para obtener los datos sobre el espacio y la eficiencia a nivel de clúster
/api/storage/disks	Solo lectura	Para obtener los discos asociados en un agregado
/api/storage/qos/policies	Leer/Crear/Modificar	Gestión de políticas de QoS y de VM
/api/svm/svms	Solo lectura	Para obtener la configuración de SVM cuando se añade el clúster de forma local.
/api/network/ip/interfaces	Solo lectura	Agregar backend de almacenamiento: para identificar que el ámbito del LIF de gestión es clúster/SVM
/api/storage/availability-zones	Solo lectura	Descubrimiento de SAZ. Aplicable a la versión ONTAP 9.16.1 en adelante y a los sistemas ASA r2.
/api/cluster/metrocluster	Solo lectura	Obtiene el estado y los detalles de configuración de MetroCluster.

Crear herramientas ONTAP para VMware vSphere usuario con ámbito de clúster basado en la API de ONTAP



Para las operaciones PATCH y la reversión automática en los almacenes de datos se requieren privilegios de discovery, create, modify y destroy. La falta de permisos podría causar problemas en el flujo de trabajo y en la limpieza.

Un usuario basado en la API de ONTAP con privilegios para detectar, crear, modificar y eliminar puede gestionar los flujos de trabajo de las herramientas de ONTAP.

Para crear un usuario con ámbito de clúster que cuente con todos los privilegios mencionados anteriormente, ejecuta 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

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

```

Además, para las versiones de ONTAP 9.16.0 y superiores, ejecuta el siguiente comando:

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

Para sistemas ASA r2 en versiones de ONTAP 9.16.1 y superiores, ejecuta el siguiente comando:

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

Crear herramientas ONTAP para VMware vSphere usuario con ámbito SVM basado en la API de ONTAP

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

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

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

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

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

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

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

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

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

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

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

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

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

```

Además, para las versiones de ONTAP 9.16.0 y superiores, ejecuta 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 usando los roles basados en API creados previamente, ejecuta 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_
```

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

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

Ejemplo:

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

Actualiza ONTAP tools for VMware vSphere usuario 10.1 a usuario 10.3

Los usuarios de ONTAP tools for VMware vSphere 10.1 que tengan un usuario con ámbito de clúster creado mediante el archivo JSON deben usar los siguientes comandos de la CLI de ONTAP con privilegios de admin para actualizar a la versión 10.3.

Para las capacidades del producto:

- VSC
- VSC y VASA Provider
- VSC y SRA
- VSC, VASA Provider y SRA.

Privilegios del clúster:

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

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

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

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

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access
```

all

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

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

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

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

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

Para los usuarios de ONTAP tools for VMware vSphere 10.1 con un usuario con ámbito SVM creado usando el archivo json, usa los comandos de la CLI de ONTAP con privilegios de usuario admin para actualizar a la versión 10.3.

Privilegios de SVM:

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

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

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

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

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

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

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

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

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

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

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

Para habilitar los siguientes comandos, añade los comandos *vserver nvme namespace show* y *vserver nvme*

subsystem show al rol existente.

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

Actualiza ONTAP tools for VMware vSphere 10.3 user a 10.4 user

A partir de ONTAP 9.16.1, actualiza el usuario de ONTAP tools for VMware vSphere 10.3 a usuario 10.4.

Para los usuarios de ONTAP tools for VMware vSphere 10.3 con un usuario con ámbito de clúster creado usando el archivo JSON y ONTAP versión 9.16.1 o superior, usa el comando de la CLI de ONTAP con privilegios de usuario admin para actualizar a la versión 10.4.

Para las capacidades del producto:

- VSC
- VSC y VASA Provider
- VSC y SRA
- VSC, VASA Provider y SRA.

Privilegios del clúster:

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

Agrega un backend de almacenamiento a ONTAP tools

Utiliza las herramientas ONTAP para VMware vSphere para añadir y gestionar backends de almacenamiento para tus hosts ESXi. Puedes integrar clústeres o SVM, habilitar la compatibilidad con MetroCluster y validar certificados para garantizar una conectividad segura. Puedes configurar backends de almacenamiento mediante ONTAP tools Manager o el cliente vSphere, supervisar el estado de los certificados y volver a detectar manualmente los recursos tras los cambios en el clúster.

Para añadir un backend de almacenamiento de forma local, utiliza las credenciales del clúster o del SVM en la interfaz de usuario de ONTAP tools. Los backends de almacenamiento locales solo están disponibles para el vCenter Server seleccionado. ONTAP tools asigna los SVM al vCenter Server para la gestión de vVols o almacenes de datos VMFS. Para los almacenes de datos VMFS y los flujos de trabajo SRA, puedes usar las credenciales del SVM sin asignar un clúster globalmente.

Para añadir un backend de almacenamiento global, utiliza las credenciales del clúster ONTAP en ONTAP tools

Manager. Los backends de almacenamiento global permiten que los flujos de trabajo de detección identifiquen los recursos del clúster necesarios para la gestión de vVol. En entornos multitenant, puedes añadir un usuario SVM localmente para gestionar los almacenes de datos de vVols.

Consulta el artículo de KB: ["OTV 10: ¿Qué es el ámbito global y local del backend de almacenamiento?"](#) para obtener más información sobre los backends de almacenamiento global y local.

Si la compatibilidad con MetroCluster está habilitada en ONTAP, incorpora tanto el clúster de origen como el de destino como backends de almacenamiento locales o globales.

Antes de empezar

Comprueba que el certificado incluya un campo «Subject Alternative Name» (SAN) válido. Los sistemas ONTAP utilizan el campo SAN para identificar las LIF de gestión de clúster y SVM.

Uso de ONTAP tools Manager



En una configuración multi-tenant, puedes añadir un clúster de almacenamiento de forma global y un SVM de forma local para utilizar las credenciales de usuario del SVM.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona **Storage Backends** en la barra lateral.
4. Añade el backend de almacenamiento y proporciona la dirección IP o el FQDN del servidor, el nombre de usuario y los detalles de la contraseña.



Se admiten LIF de gestión de direcciones IPv4 e IPv6.

5. Obtén automáticamente los certificados del clúster ONTAP y autoriza el certificado, o súbelo manualmente buscando su ubicación.



Si es necesario, puedes desactivar la validación del nombre alternativo del sujeto (SAN) desde la consola de mantenimiento. Para obtener instrucciones, consulta ["Cambiar el indicador de validación del certificado"](#).

6. Si el backend de almacenamiento que añades forma parte de una configuración de MetroCluster, ONTAP tools Manager muestra un mensaje emergente para añadir el clúster emparejado. Selecciona **Add** e introduce los detalles para el backend de almacenamiento peer de MetroCluster.



Después de que el sistema ONTAP realice una conmutación de sitios y una reversión, ejecuta manualmente el descubrimiento de las ONTAP tools.

Uso de la interfaz de usuario del cliente vSphere



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

1. Inicia sesión en el cliente de vSphere.
2. En la página de accesos directos, selecciona **NetApp ONTAP tools** en la sección de complementos.
3. Selecciona **Storage Backends** en la barra lateral.
4. Añade el backend de almacenamiento e introduce la dirección IP del servidor, el nombre de usuario, la contraseña y los datos del puerto.



Puedes añadir un backend de almacenamiento utilizando credenciales basadas en clúster con LIF de gestión IPv4 o IPv6. Para añadir un usuario SVM directamente, proporciona credenciales basadas en SVM junto con un LIF de gestión SVM. Si un clúster ya está integrado, no puedes volver a integrar un usuario SVM de ese clúster.

5. Obtén automáticamente los certificados del clúster ONTAP y autoriza el certificado, o súbelo manualmente buscando su ubicación.

6. Si el backend de almacenamiento añadido forma parte de la configuración de MetroCluster, ONTAP tools muestra la pantalla **Add MetroCluster peer**. Selecciona **Add peer** para añadir el backend de almacenamiento peer.



Después de que el sistema ONTAP realice una conmutación de sitios y una reversión, ejecuta manualmente el descubrimiento de las ONTAP tools.

ONTAP tools muestra el backend de almacenamiento recién añadido en la página **Storage backends**. Si un certificado caduca en 30 días o menos, ONTAP tools muestra una advertencia en la columna de la fecha de caducidad del certificado. Después de la caducidad, ONTAP tools marca el backend de almacenamiento como desconocido porque no puede conectarse al sistema de almacenamiento.

Información relacionada

["OTV 10: ¿Qué es el ámbito global y local del backend de almacenamiento?"](#)

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

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

Asocia un backend de almacenamiento con una instancia de vCenter Server para habilitar el acceso para todas las instancias de vCenter Server. Para la configuración de MetroCluster, cuando asocies un clúster de backend de almacenamiento, asegúrate de asociar también su clúster par con el vCenter Server.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona vCenter en la barra lateral.
4. Selecciona los puntos suspensivos verticales junto a la instancia de vCenter Server a la que quieres conectar los backends de almacenamiento.
5. En el menú desplegable, selecciona el backend de almacenamiento que desees asociar a la instancia de vCenter Server seleccionada.

Configura el acceso a la red en ONTAP tools

De forma predeterminada, todas las direcciones IP detectadas desde el host ESXi se añaden automáticamente a la política de exportación a menos que configures el acceso a la red. Puedes modificar la política de exportación para permitir el acceso solo desde direcciones IP específicas. Si un host ESXi excluido intenta realizar una operación de montaje, la operación falla.

Pasos

1. Inicia sesión en el cliente de vSphere.

2. Selecciona **NetApp ONTAP tools** en la página de accesos directos, dentro de la sección de complementos.
3. En el panel izquierdo de ONTAP tools, ve a **Configuración > Gestionar acceso a la red > Editar**.

Para añadir varias direcciones IP, separa la lista con comas, rango, Classless Inter-Domain Routing (CIDR) o una combinación de los tres.

4. Selecciona **Guardar**.

Crear un almacén de datos en ONTAP tools

Cuando creas un almacén de datos a nivel del clúster de hosts, ONTAP tools lo monta en todos los hosts de destino y solo permite la acción si tienes los privilegios necesarios.

Interoperabilidad entre los almacenes de datos nativos con vCenter Server y los almacenes de datos gestionados por ONTAP tools

A partir de ONTAP tools para VMware vSphere 10.4, ONTAP tools crea igroups anidados para los datastores, con igroups principales específicos para los datastores e igroups secundarios asignados a los hosts. Puedes crear igroups planos desde ONTAP System Manager y usarlos para crear datastores VMFS sin usar ONTAP tools. Consulta ["Gestiona iniciadores SAN y igroups"](#) para más información.

Después de incorporar el almacenamiento y ejecutar el descubrimiento de almacenes de datos, ONTAP tools cambia los igroups planos en los almacenes de datos VMFS a igroups anidados. No puedes usar los igroups planos anteriores para crear nuevos almacenes de datos. Usa la interfaz de ONTAP tools o la API de REST para reutilizar los igroups anidados.

Crea un almacén de datos vVols

A partir de ONTAP tools for VMware vSphere 10.3, puedes crear un datastore de vVols en sistemas ASA r2 con eficiencia de espacio como thin.vVol. El VASA Provider crea un contenedor y los endpoints de protocolo deseados al crear el datastore de vVol. El VASA Provider no asigna ningún volumen de respaldo a este contenedor.

Antes de empezar

- Asegúrate de que los agregados raíz no están asignados a la SVM.
- Asegúrate de que el proveedor VASA esté registrado con el vCenter seleccionado.
- En el sistema de almacenamiento ASA r2, la SVM debe asignarse al agregado para el usuario de la SVM.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Haz clic con el botón derecho en un sistema host, un clúster de hosts o un centro de datos y selecciona **NetApp ONTAP tools > Crear almacén de datos**.
3. Selecciona vVols como **tipo de almacén de datos**.
4. Introduce el **nombre del almacén de datos** y la información de **protocolo**.



El sistema ASA r2 es compatible con los protocolos iSCSI y FC para vVols.

5. Selecciona la máquina virtual de almacenamiento donde quieres crear el almacén de datos.
6. En las opciones avanzadas:
 - Si seleccionas la **Política de exportación personalizada**, asegúrate de ejecutar el proceso de detección en vCenter para todos los objetos. Se recomienda que no uses esta opción.
 - Puedes seleccionar un nombre de **grupo iniciador personalizado** para los protocolos iSCSI y FC.



En el sistema de almacenamiento ASA r2 de tipo SVM, no se crean unidades de almacenamiento (LUN/namespace), ya que el datastore es solo un contenedor lógico.

7. En el panel **Atributos de almacenamiento**, puedes crear nuevos volúmenes o utilizar los volúmenes existentes. Sin embargo, no puedes combinar estos dos tipos de volúmenes para crear un datastore de vVols.

Al crear un nuevo volumen, puedes activar QoS en el almacén de datos. Por defecto, se crea un volumen por cada solicitud de creación de LUN. Omite este paso para los almacenes de datos vVols en los sistemas de almacenamiento ASA r2.

8. Revisa tu selección en el panel **Resumen** y selecciona **Finalizar**.

Crear un almacén de datos NFS

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

Pasos

1. Inicia sesión en el cliente de vSphere.

2. Haz clic con el botón derecho en un sistema host, un clúster de hosts o un centro de datos y selecciona **NetApp ONTAP tools > Create datastore**.
3. Selecciona NFS en el campo **Tipo de almacén de datos**.
4. Introduce el nombre del almacén de datos, el tamaño y la información del protocolo en el panel **Nombre y protocolo**. Selecciona **Datastore cluster** y **Kerberos authentication** en las opciones avanzadas.



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

5. Selecciona **Platform y Storage VM** en el panel **Storage**.
6. Si seleccionas **Política de exportación personalizada** en las opciones avanzadas, ejecuta el análisis en vCenter para todos los objetos. Se recomienda que no uses esta opción.



No puedes crear un almacén de datos NFS usando la política predeterminada o la política de volumen raíz del SVM.

- En las opciones avanzadas, el botón de selección **Asimétrico** solo aparece si seleccionas rendimiento o capacidad en el menú desplegable de la plataforma.
 - Al seleccionar la opción **Cualquiera** en el menú desplegable de plataformas, puedes ver todas las SVM en el vCenter. La plataforma y el indicador asimétrico no afectan la visibilidad.
7. Selecciona el agregado para la creación del volumen en el panel **Atributos de almacenamiento**. En las opciones avanzadas, elige **Reserva de espacio** y **Habilitar QoS** según sea necesario.
 8. Revisa las opciones del panel **Resumen** y selecciona **Finalizar**.

ONTAP tools crea el almacén de datos NFS y lo monta en todos los hosts.

Crear un almacén de datos VMFS

VMFS es un sistema de archivos en clúster para almacenar archivos de máquinas virtuales. Varios hosts ESXi pueden acceder a los mismos archivos de máquinas virtuales al mismo tiempo para vMotion y las funciones de alta disponibilidad.

En un clúster protegido:

- Solo puedes crear almacenes de datos VMFS. Al añadir un almacén de datos VMFS a un clúster protegido, este se protege automáticamente.
- No puedes crear un almacén de datos en un centro de datos con uno o más clústeres de hosts protegidos.
- No puedes crear un almacén de datos en un host ESXi si el clúster de hosts principal está protegido por una "Automated Failover Duplex policy" (configuración uniforme o no uniforme).
- Solo puedes crear un almacén de datos VMFS en un host ESXi protegido por una relación asíncrona. No puedes crear ni montar un almacén de datos en un host ESXi que forme parte de un clúster de hosts protegido por la política "Automated Failover Duplex".

Antes de empezar

- Activa los servicios y las LIF para cada protocolo en el lado de almacenamiento de ONTAP.
- Asigna SVM a la agregada para el usuario SVM en el sistema de almacenamiento ASA r2.
- Configura el host ESXi si utilizas el protocolo NVMe/TCP:

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



VMware vSphere 7.0 U3 y versiones posteriores son compatibles con el protocolo NVMe/TCP. Sin embargo, se recomienda VMware vSphere 8.0 y versiones posteriores.

- b. Comprueba si el fabricante de la tarjeta de interfaz de red (NIC) es compatible con la NIC de ESXi con el protocolo NVMe/TCP.
 - c. Configura la NIC de ESXi para NVMe/TCP según las especificaciones del proveedor de la NIC.
 - d. Cuando uses la versión VMware vSphere 7, sigue las instrucciones en el sitio de VMware ["Configura la vinculación de VMkernel para el adaptador NVMe sobre TCP"](#) para configurar la vinculación de puertos NVMe/TCP. Cuando uses la versión VMware vSphere 8, sigue ["Configurar NVMe sobre TCP en ESXi"](#) para configurar la vinculación de puertos NVMe/TCP.
 - e. Para la versión vSphere 7 de VMware, sigue las instrucciones de la página ["Habilita los adaptadores de software NVMe sobre RDMA o NVMe sobre TCP"](#) para configurar los adaptadores de software NVMe/TCP. Para la versión vSphere 8 de VMware, sigue ["Agregar adaptadores de software NVMe over RDMA o NVMe over TCP"](#) para configurar los adaptadores de software NVMe/TCP.
 - f. Ejecuta la acción ["Descubre los sistemas de almacenamiento y los hosts"](#) en el host ESXi. Para obtener más información, consulta ["Cómo configurar NVMe/TCP con vSphere 8.0 Update 1 y ONTAP 9.13.1 para almacenes de datos VMFS"](#).
- Si utilizas el protocolo NVMe/FC, sigue estos pasos para configurar el host ESXi:
 - a. Si aún no está habilitado, habilita NVMe over Fabrics (NVMe-oF) en tus hosts ESXi.
 - b. Completa la división en zonas SCSI.
 - c. Asegúrate de que los hosts ESXi y el sistema ONTAP estén conectados tanto a nivel físico como lógico.

Para configurar un SVM de ONTAP para el protocolo FC, consulta ["Configura un SVM para FC"](#).

Para obtener más información sobre el uso del protocolo NVMe/FC con VMware vSphere 8.0, consulta ["Configuración del host NVMe-oF para ESXi 8.x con ONTAP"](#).

Para obtener más información sobre el uso de NVMe/FC con VMware vSphere 7.0, consulta ["Guía de configuración del host ONTAP NVMe/FC"](#) y ["TR-4684"](#).

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Haz clic con el botón derecho en un sistema host, un clúster de hosts o un centro de datos y selecciona **NetApp ONTAP tools > Crear almacén de datos**.
3. Selecciona el tipo de almacén de datos VMFS.
4. Introduce el nombre del almacén de datos, el tamaño y la información sobre el protocolo en el panel **Nombre y protocolo**. Para añadir el nuevo almacén de datos a un clúster VMFS ya existente, selecciona el clúster de almacenes de datos en Opciones avanzadas.
5. Selecciona una VM de almacenamiento en el panel **Almacenamiento**. Introduce el **nombre personalizado del grupo de iniciadores** en la sección **Opciones avanzadas** según sea necesario. Puedes elegir un igroup ya existente para el datastore 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 que se usa para la asignación de espacios de nombres. ONTAP tools crea el subsistema de espacio de nombres usando el nombre generado automáticamente que incluye el nombre del datastore. Puedes cambiar el nombre del subsistema de espacio de nombres en el campo **custom namespace subsystem name** en las opciones avanzadas del panel **Storage**.

6. Desde el panel **atributos de almacenamiento**:

- a. Selecciona **Aggregate** en el menú desplegable.



En los sistemas de almacenamiento ASA r2, la opción **Agregado** no aparece porque el almacenamiento está desagregado. Cuando eliges un SVM del tipo de sistema de almacenamiento ASA r2, la página de atributos de almacenamiento muestra las opciones para habilitar QoS.

- b. ONTAP tools crea una unidad de almacenamiento (LUN/espacio de nombres) con una reserva de espacio thin según el protocolo seleccionado.



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

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

«Any» es el valor predeterminado del nivel de servicio de rendimiento (PSL). Esta configuración crea la unidad de almacenamiento utilizando el algoritmo de colocación equilibrada de ONTAP. Sin embargo, puedes seleccionar la opción performance o extreme según lo necesites.

- d. Selecciona **Usar volumen existente, Habilitar QoS** según sea necesario, y proporciona los detalles.



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



No puedes usar el volumen existente para crear un almacén de datos VMFS con el protocolo NVMe/FC o NVMe/TCP. Crea un nuevo volumen para el almacén de datos VMFS.

7. Revisa los detalles del almacén de datos en el panel **Resumen** y selecciona **Finalizar**.



Si creas el almacén de datos en un clúster protegido, puedes ver un mensaje de solo lectura: «El almacén de datos se está montando en un clúster protegido».

Resultado

ONTAP tools crea el almacén de datos VMFS y lo monta en todos los hosts.

Protege los almacenes de datos y las máquinas virtuales

Protege un clúster de hosts en ONTAP tools

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

Antes de empezar

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

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

Pasos

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

El tipo de política puede ser Asynchronous o AutomatedFailOverDuplex.

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

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

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

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

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

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



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

Información relacionada

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

Proteger usando la protección SRA

Configura SRA en ONTAP tools para proteger los datastores

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

Antes de empezar

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

Pasos

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



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



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

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

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

Información relacionada

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

Configura SRA en ONTAP tools para entornos SAN y NAS

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

Configurar SRA para entornos SAN



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

Antes de empezar

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

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

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

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

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

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

Pasos

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

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

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

Configura SRA para entornos NAS



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

Antes de empezar

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

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

Pasos

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

Configura SRA en ONTAP tools para entornos altamente escalados

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

Configuración del proveedor de almacenamiento

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

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

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

También deberías activar la opción `StorageProvider.autoResignatureMode`.

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

Configuración de almacenamiento

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



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

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

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

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

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

Antes de empezar

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



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

Pasos

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

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

Actualiza las credenciales de SRA en ONTAP tools

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

Antes de empezar

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

Pasos

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

e. `rm -rf *`

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

a. `cd ..`

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

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

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

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

Pasos

1. Reconfigura vCenter en el dispositivo VMware Live Site Recovery

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

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

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

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

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

Configura sitios protegidos y de recuperación en ONTAP tools

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

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

Empareja los sitios protegidos y los de recuperación

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



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

Antes de empezar

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

Pasos

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

Resultado

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

Configura grupos de protección

Antes de empezar

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

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

Pasos

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

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

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

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

Configura los recursos del sitio protegido y del sitio de recuperación

Configura las asignaciones de red en ONTAP tools

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

Debes realizar las siguientes configuraciones de recursos:

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

Antes de empezar

Ya deberías haber conectado los sitios protegidos y de recuperación.

Pasos

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

Resultado

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

Configura las asignaciones de carpetas en ONTAP tools

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

Antes de empezar

Ya deberías haber conectado los sitios protegidos y de recuperación.

Pasos

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

Resultado

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

Configura las asignaciones de recursos en ONTAP tools

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

Antes de empezar

Ya deberías haber conectado los sitios protegidos y de recuperación.



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

Pasos

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

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

Resultado

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

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

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

Antes de empezar

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

Pasos

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



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

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

Configura SRA usando el gestor de arrays en ONTAP tools

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

Antes de empezar

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

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

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

Pasos

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



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

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

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

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

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

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

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

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

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

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

Verifica los sistemas de almacenamiento replicados en ONTAP tools

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

Antes de empezar

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

Pasos

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

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

Protección fan-out en las herramientas ONTAP

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



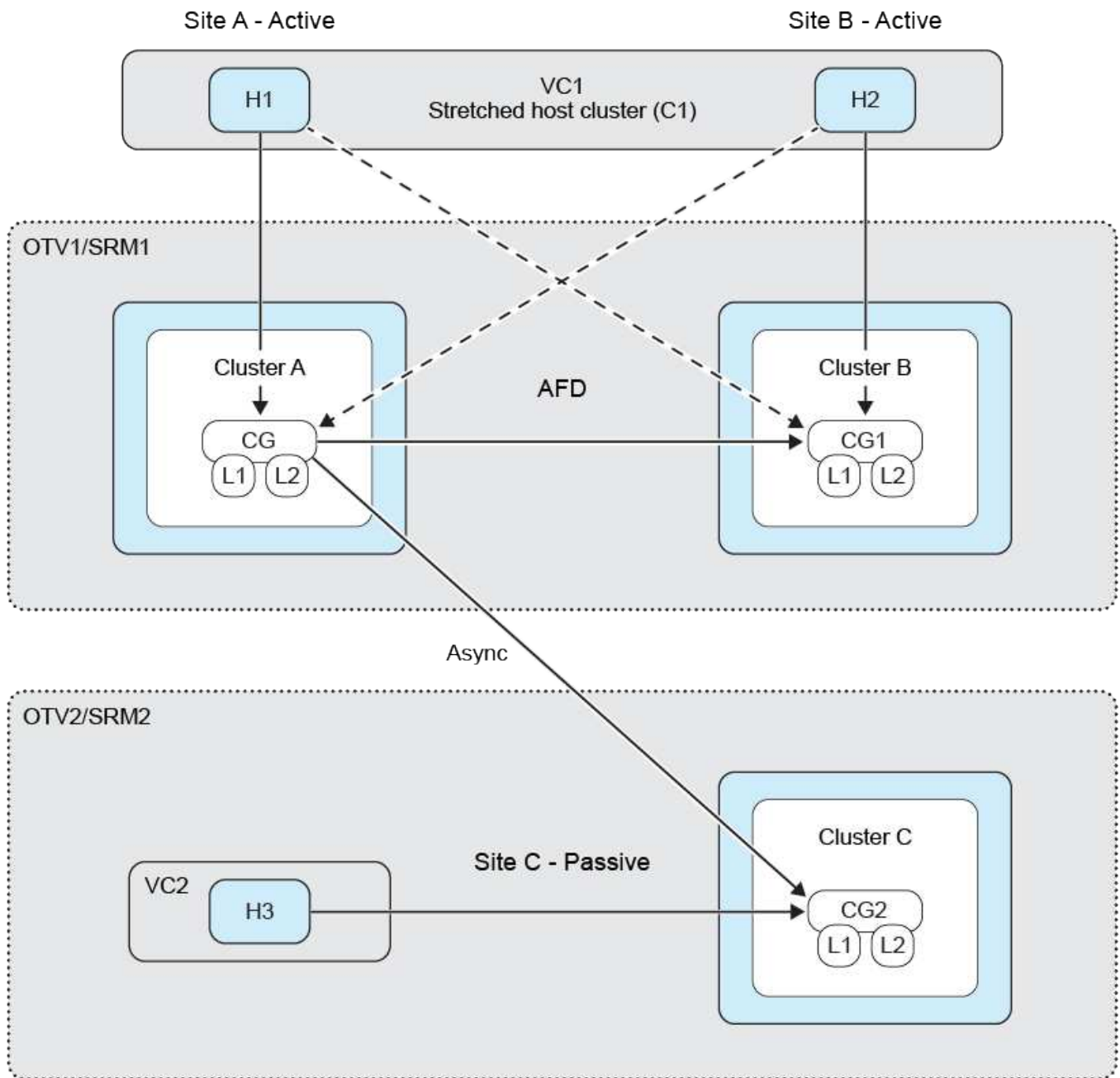
La salida en abanico no es compatible para los usuarios de SVM.

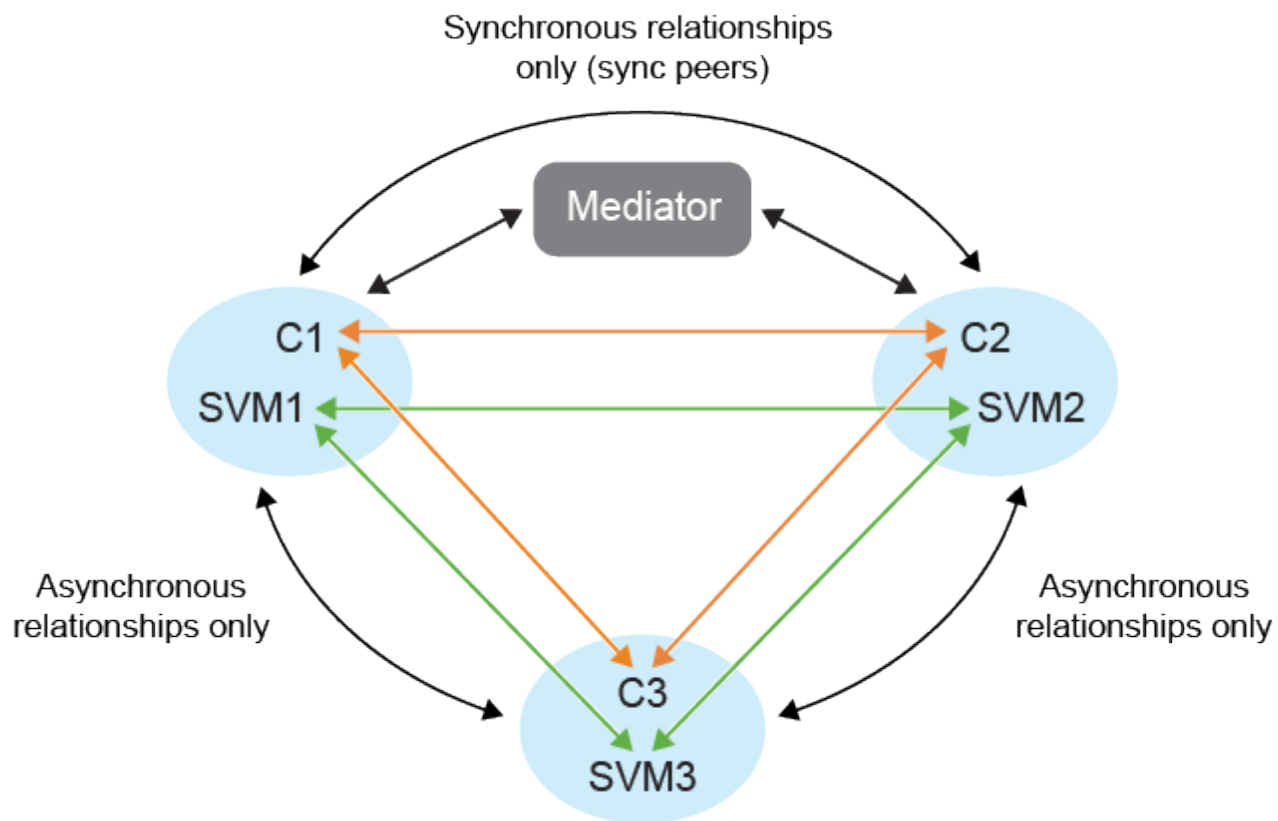
Para configurar la protección contra la dispersión, haz peer entre los tres clústeres de los sitios y las SVM.

Ejemplo:

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

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





Pasos

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

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

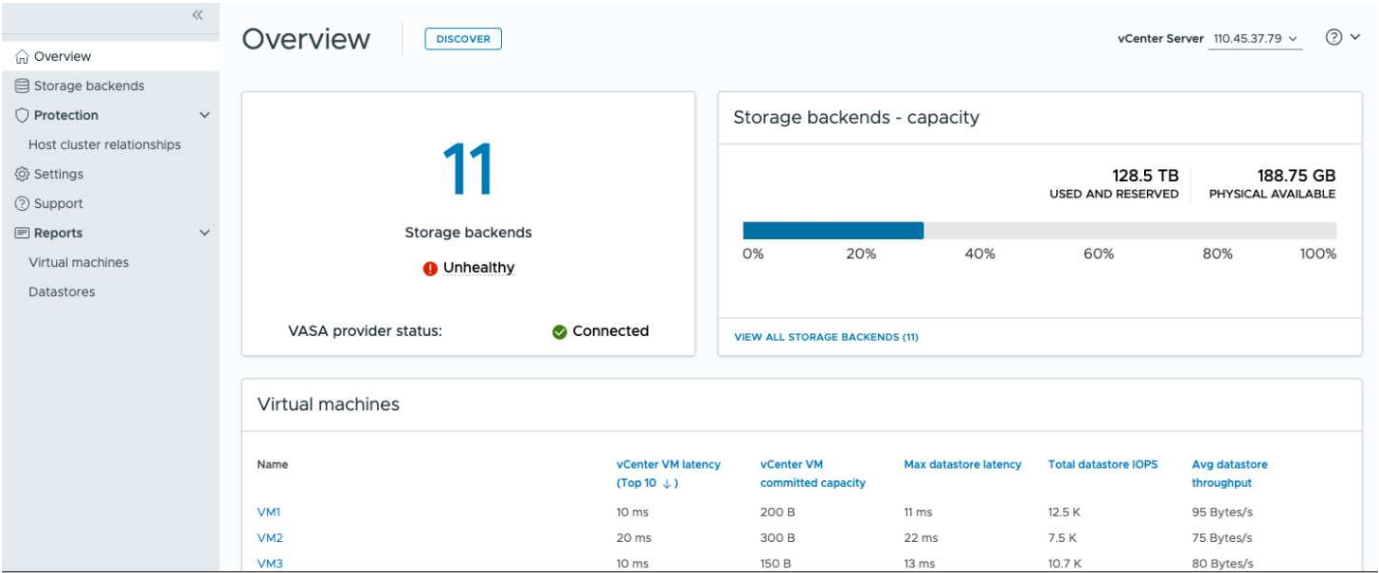
2. Agrega los datastores a la protección del clúster de hosts siguiendo ["Modificar el clúster de hosts protegidos"](#). Agrega ambos tipos de políticas: asíncronas y síncronas.

Administra ONTAP tools for VMware vSphere

Conoce el panel de ONTAP tools

Al seleccionar el icono del complemento ONTAP tools for VMware vSphere en la sección de accesos directos del cliente vCenter, se abre la página de resumen. Este panel de control ofrece un resumen del complemento ONTAP tools for VMware vSphere.

En Enhanced Linked Mode (ELM), aparece el menú desplegable vCenter Server. Elige un vCenter Server para ver sus datos. El menú desplegable está disponible en todas las vistas de listado del complemento. Cuando seleccionas un vCenter Server en una página, permanece igual cuando cambias de pestaña en el complemento.



Desde la página de resumen, puedes ejecutar la acción **Discovery**. La acción de detección identifica los backends de almacenamiento, los hosts, los almacenes de datos añadidos o actualizados recientemente y el estado de protección o las relaciones a nivel de vCenter. Ejecuta una detección bajo demanda sin esperar a la detección programada.



El botón **Detección** solo se activa si tienes el privilegio necesario para realizar la detección.

Después de enviar la solicitud de descubrimiento, puedes seguir el progreso de la acción en el panel de tareas recientes.

El panel de control cuenta con varias fichas que muestran distintos elementos del sistema. La siguiente tabla muestra las diferentes fichas y lo que representan.

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

Estado	La tarjeta de estado muestra el número de backends de almacenamiento y el estado de salud general de los backends de almacenamiento y del VASA Provider. El estado de los backends de almacenamiento muestra Saludable cuando todos los estados de los backends de almacenamiento son normales y muestra No saludable si algún backend de almacenamiento tiene un problema (estado desconocido/inaccesible/degradado). Selecciona el tool tip para abrir los detalles del estado de los backends de almacenamiento. Puedes seleccionar cualquier backend de almacenamiento para ver más detalles. El enlace Other VASA Provider states muestra el estado actual del VASA Provider que está registrado en el servidor vCenter.
Sistemas de almacenamiento - Capacidad	Esta tarjeta muestra la capacidad agregada utilizada y disponible de todos los backends de almacenamiento para la instancia de vCenter Server seleccionada. Para los sistemas de almacenamiento ASA r2, los datos de capacidad no se muestran porque el almacenamiento está desagregado.
Máquinas virtuales	Esta ficha muestra las 10 máquinas virtuales principales ordenadas según un indicador de rendimiento. Puedes seleccionar el encabezado para ver las 10 máquinas virtuales principales según el indicador seleccionado, ordenadas en orden ascendente o descendente. Los cambios de ordenación y filtrado realizados en la ficha se mantienen hasta que cambies o borres la caché del navegador.
Almacenes de datos	Esta tarjeta muestra los 10 almacenes de datos principales ordenados según una métrica de rendimiento. Puedes seleccionar el encabezado para ver los 10 almacenes de datos principales para la métrica seleccionada, ordenados en orden ascendente o descendente. Los cambios de ordenación y filtrado realizados en la tarjeta se mantienen hasta que cambies o borres la caché del navegador. Hay un menú desplegable de tipo de almacén de datos para seleccionar el tipo de los almacenes de datos: NFS, VMFS o vVols.
Ficha de cumplimiento del host ESXi	Esta tarjeta muestra si todos los hosts ESXi (para el vCenter seleccionado) siguen la configuración recomendada de host NetApp por grupo o categoría. Puedes seleccionar el enlace Aplicar configuración recomendada para aplicar la configuración recomendada. Puedes seleccionar el estado de cumplimiento de los hosts para ver la lista de hosts.

Cómo las herramientas de ONTAP gestionan los igroups y las políticas de exportación

Los grupos de iniciadores (igroups) son tablas que contienen los nombres de puerto global (WWPN) de los hosts del protocolo FC o los nombres de nodo calificados de los hosts iSCSI. Puedes definir igroups y asignarlos a LUN para controlar qué iniciadores tienen acceso a los LUN.

En las herramientas de ONTAP para VMware vSphere 9.x, los igroups se creaban y gestionaban en una estructura plana, donde cada almacén de datos en vCenter se asociaba con un único igroup. Este modelo limitaba la flexibilidad y la reutilización de los igroups en varios almacenes de datos. Las herramientas ONTAP para VMware vSphere introducen igroups anidados, donde cada almacén de datos en vCenter está asociado a un igroup padre, mientras que cada host está vinculado a un igroup hijo bajo ese padre. Puedes definir igroups padre personalizados con nombres definidos por el usuario para reutilizarlos en distintos almacenes de datos y así facilitar la gestión de los igroups. Conoce el flujo de trabajo de los igroups para gestionar LUN y almacenes de datos en las herramientas ONTAP para VMware vSphere. Los diferentes flujos de trabajo generan configuraciones de igroups variables, como se muestra en los siguientes ejemplos:



Los nombres mencionados son meramente ilustrativos y no hacen referencia a nombres reales de igroups. Los igroups gestionados por ONTAP tools usan el prefijo “otv_”. A los igroups personalizados se les puede dar cualquier nombre.

Término	Descripción
DS<number>	Almacén de datos
iqn<number>	Iniciador IQN
host<number>	MoRef de host
lun<number>	ID de LUN
<DSName>Igroup<number>	Igroup principal predeterminado (gestionado por ONTAP tools)
<Host-Moref>Igroup<number>	Subgrupo hijo
CustomIgroup<number>	Grupo principal de igroup personalizado definido por el usuario
ClassicIgroup<number>	Igroup utilizado en las versiones 9.x de ONTAP tools.

Ejemplo 1:

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

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

Resultado:

- DS1Igroup:
 - host1Igroup → (iqn1: lun1)

ONTAP crea el igroup principal DS1Igroup para DS1 y asigna el igroup secundario host1Igroup a lun1. El sistema siempre asigna los LUN a los igroups secundarios.

Ejemplo 2:

Montar un almacén de datos existente en un host adicional

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

Resultado:

- DS1lgroup:
 - host1lgroup → (iqn1: lun1)
 - host2lgroup → (iqn2: lun1)

ONTAP tools for VMware vSphere crean un igroup secundario host2lgroup y lo añaden al igroup principal existente DS1lgroup.

Ejemplo 3:

Desmontar un almacén de datos de un host

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

Resultado:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

ONTAP tools for VMware vSphere elimina host1lgroup de la jerarquía. El sistema no elimina explícitamente los igroups secundarios. Los elimina cuando se dan estas dos condiciones:

- Si no hay ningún LUN asignado, el sistema ONTAP elimina el igroup secundario.
- Una tarea de limpieza programada elimina los igroups «suspensos» que no tienen asignaciones de LUN. Estos casos solo se aplican a los igroups gestionados por ONTAP tools, no a los creados de forma personalizada.

Ejemplo 4:

Eliminar almacén de datos

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

Resultado:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

Los igroups padres e hijos se eliminan, a menos que otro almacén de datos reutilice el igroup padre. Los igroups hijos no se eliminan de forma explícita

Ejemplo 5:

Crear varios 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:

- CustomIgroup1:
 - host1Igroup → (iqn1: lun2, lun3)
 - host2Igroup → (iqn2: lun2)
 - host3Igroup → (iqn3: lun3)

Se crea CustomIgroup1 para DS2 y se reutiliza para DS3. Los child igroups se crean o actualizan bajo el parent compartido, y cada child igroup 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:

- CustomIgroup1:
 - host1Igroup → (iqn1: lun3)
 - host3Igroup → (iqn3: lun3)
- Aunque CustomIgroup1 no se vuelve a utilizar, no se elimina.
- Si no hay ningún LUN asignado, el sistema ONTAP elimina host2Igroup.
- host1Igroup no se elimina porque está asignado a lun3 de DS3. Los igroups personalizados nunca se eliminan, independientemente del estado de reutilización.

Ejemplo 7:

Ampliar vVols datastore (Agregar volumen)

Flujo de trabajo:

Antes de la expansión:

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

- DS4Igroup: host4Igroup → (iqn4: lun4)

Después de la ampliación:

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

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Se crea un nuevo LUN y se asigna al igroup secundario existente host4Igroup.

Ejemplo 8:

Reducir el almacén de datos vVols (Eliminar volumen)

Flujo de trabajo:

Antes de la reducción:

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

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

Después de la contracción:

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

- DS4lgroup: host4lgroup → (iqn4: lun4)

El LUN especificado (lun5) se ha desasignado del igroup secundario. El igroup permanece activo siempre que tenga al menos un LUN asignado.

Ejemplo 9:

Migración de ONTAP tools de la versión 9 a la 10 (normalización de igroup)

Flujo de trabajo

ONTAP tools for VMware vSphere 9.x versions no admiten igroups jerárquicos. Durante la migración a 10.3 o versiones superiores, los igroups deben normalizarse en la estructura jerárquica.

Antes de la migración:

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

La lógica de ONTAP tools 9.x permite tener varios iniciadores por igroup sin imponer una correspondencia uno a uno con los hosts.

Después de la migración:

[Migración] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classiclgroup1: otv_Classiclgroup1 (iqn6 & iqn7 : lun6, lun7)

Durante la migración:

- Se crea un nuevo grupo principal (Classiclgroup1).
- El igroup original se renombra con el prefijo otv_ y se convierte en un igroup secundario.

Esto garantiza el cumplimiento del modelo jerárquico.

A partir de ONTAP tools 10.5P2, los igroups migrados se eliminan cuando ya no se utilizan. En versiones anteriores, los igroups migrados nunca se eliminaban. Ten en cuenta lo siguiente:

- Los grupos migrados no se pueden reutilizar en distintos almacenes de datos.
- Los igroups personalizados (definidos por el usuario) nunca se eliminan y pueden seguir reutilizándose.

Temas relacionados

["Acerca de igroups"](#)

Políticas de exportación

Las políticas de exportación controlan el acceso a los datastores NFS y los permisos de los clientes en ONTAP tools for VMware vSphere. Las políticas de exportación se crean y gestionan en los sistemas ONTAP y pueden usarse con datastores NFS para aplicar el control de acceso. Cada política de exportación consta de

reglas que especifican los clientes (direcciones IP o subredes) que tienen permitido el acceso y los permisos otorgados (solo lectura o lectura y escritura).

Al crear un almacén de datos NFS en ONTAP tools for VMware vSphere, puedes seleccionar una política de exportación ya existente o crear una nueva. Luego, la política de exportación se aplica al almacén de datos, asegurando que solo los clientes autorizados puedan acceder a él.

Al montar un almacén de datos NFS en un nuevo host ESXi, ONTAP tools for VMware vSphere añade la dirección IP del host a la política de exportación existente asociada al almacén de datos. Esto permite que el nuevo host acceda al almacén de datos sin crear una nueva política de exportación.

Al eliminar o desmontar un almacén de datos NFS de un host ESXi, las herramientas ONTAP para VMware vSphere eliminan la dirección IP del host de la política de exportación. Si ningún otro host está utilizando esa política de exportación, esta se eliminará. Al eliminar un almacén de datos NFS, las herramientas ONTAP para VMware vSphere eliminan la política de exportación asociada a dicho almacén de datos si no la reutiliza ningún otro almacén de datos. Si la política de exportación se reutiliza, conserva la dirección IP del host y no cambia. Al eliminar los almacenes de datos, la política de exportación desasigna 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 cuando se reutiliza en diferentes almacenes de datos. Al reutilizar la política de exportación, puedes añadir la nueva dirección IP del host a la política. Al eliminar o desmontar un almacén de datos que utilice una política de exportación compartida, la política no se eliminará. Permanece sin cambios y la dirección IP del host no se elimina, ya que se comparte con los demás almacenes de datos. No se recomienda reutilizar las políticas de exportación, ya que puede provocar problemas de acceso y latencia.

Temas relacionados

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

Cómo las herramientas de ONTAP gestionan los igroups

Si gestionas tanto máquinas virtuales con herramientas ONTAP como sistemas de almacenamiento ONTAP, es importante que entiendas cómo se comportan los igroups, especialmente al mover almacenes de datos desde entornos no gestionados por herramientas ONTAP a los que sí lo están. En esta página se explica cómo ONTAP tools for VMware vSphere representa y gestiona los igroups. Es información conceptual para entender las diferencias de comportamiento entre versiones anteriores y el modelo actual de igroups anidados.

A partir de ONTAP tools for VMware vSphere 10.4, ONTAP tools crea y mantiene automáticamente objetos ONTAP y vCenter, lo que simplifica la gestión de datastores en entornos de centros de datos VMware. A partir de ONTAP tools for VMware vSphere 10.5 P2, los igroups migrados también se eliminan automáticamente cuando ya no están en uso.

Resumen rápido del comportamiento

- Los almacenes de datos VMFS gestionados con ONTAP tools utilizan igroups anidados: un igroup padre por contexto de almacén de datos e igroups hijos por host.
- Las asignaciones LUN se aplican a los igroups hijos.
- Los igrupos padre personalizados pueden reutilizarse en todos los datastores.

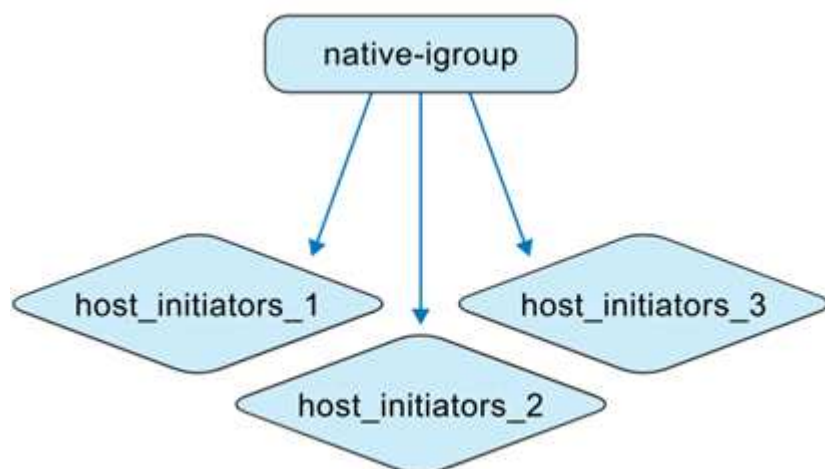
- Los igroups migrados de ONTAP tools 9.x no se pueden reutilizar.

Contextos de igroup

Las herramientas ONTAP para VMware vSphere manejan igroups en dos contextos.

Igroups gestionados por herramientas ajenas a ONTAP

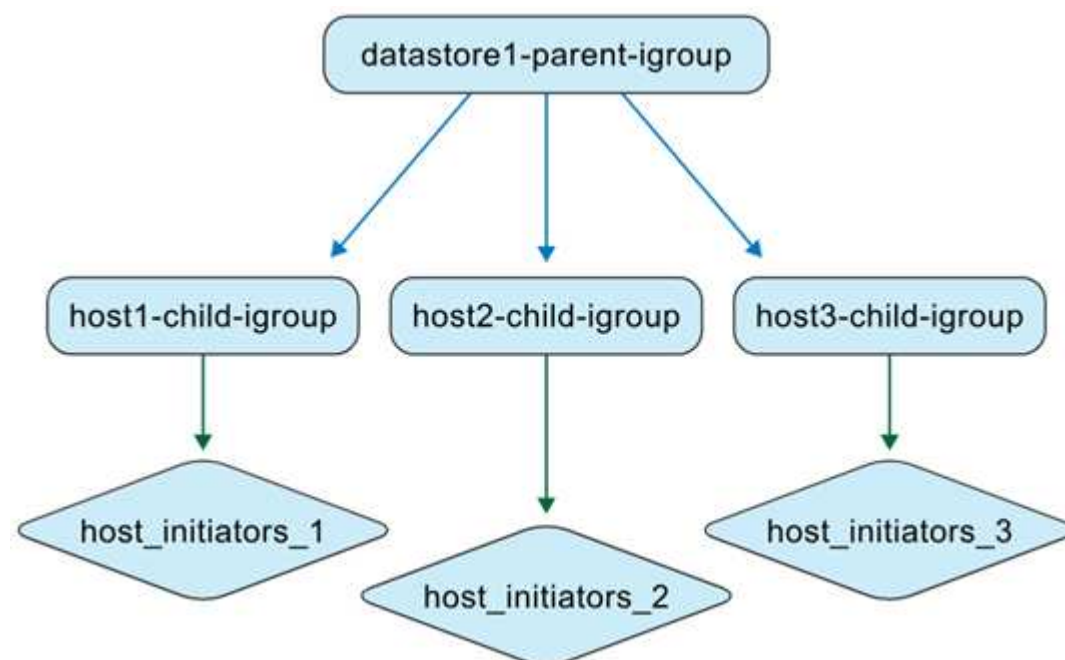
Como administrador de almacenamiento, puedes crear igroups en el sistema ONTAP como estructuras planas o anidadas. La siguiente ilustración muestra un igroup plano creado directamente en ONTAP.

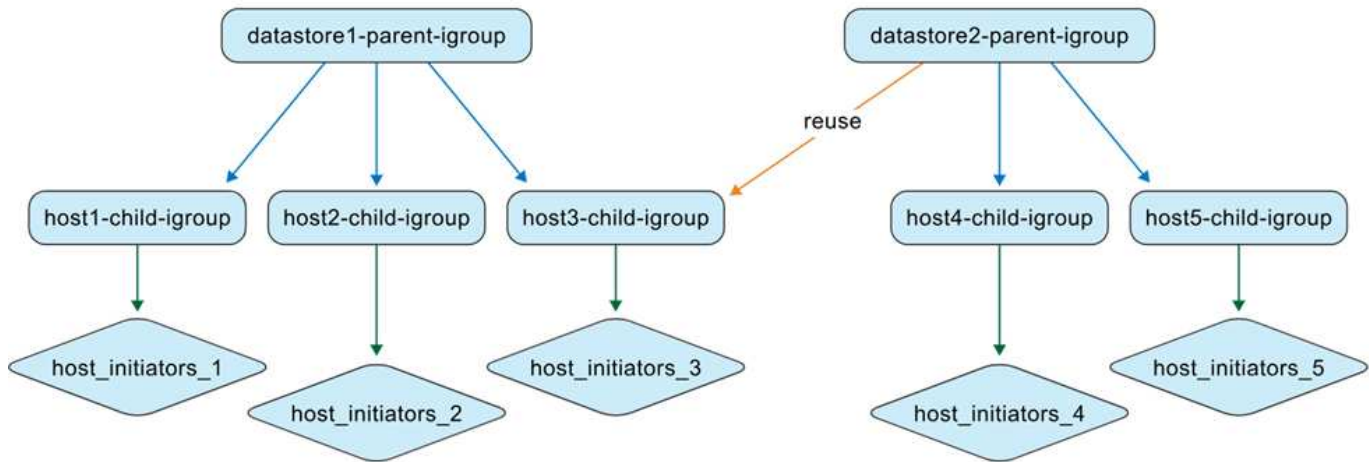


Igroups gestionados por ONTAP tools

Cuando creas almacenes de datos, ONTAP tools for VMware vSphere crea igroups en una estructura anidada.

Por ejemplo, cuando se crea el almacén de datos datastore1 y se monta en los hosts 1, 2 y 3, y se crea un nuevo almacén de datos (datastore2) y se monta en los hosts 3, 4 y 5, ONTAP tools reutiliza el igroup a nivel de host para una gestión eficiente.





Comportamiento de la nomenclatura

Cuando creas un almacén de datos y dejas el campo igroup en blanco, ONTAP tools crea una estructura igroup anidada por defecto.

- Patrón de nomenclatura de los igroup parentales:
otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>
- Patrón de nomenclatura de igroup infantil: otv_<hostMoref>_<vcguid>

La interfaz de sistemas de ONTAP muestra la relación entre los igroups padre e hijo en el campo **Parent Initiator Group**.

Comportamiento por escenario

Escenario	Comportamiento del igroup parental	Comportamiento de igroup secundario	Asignación y visibilidad de LUN
Datastore creado con la configuración igroup por defecto	Se crea un igroup padre por defecto gestionado por ONTAP tools.	Los igrupos hijo a nivel de host se crean según sea necesario.	Los LUN se asignan a igroups secundarios. El almacén de datos aparece en el inventario de vCenter Server.
Datastore creado con nombre de igroup personalizado	Se crea un igroup padre personalizado con el nombre especificado.	Los igrupos hijos existentes a nivel de host se reutilizan cuando los hosts se solapan.	El nuevo LUN del almacén de datos se asigna al igroup hijo reutilizado o recién creado. El datastore aparece en vCenter Server.
Igroup personalizado existente reutilizado durante la creación del almacén de datos	Se selecciona y reutiliza un igroup padre personalizado existente.	Los igrupos hijos se reutilizan o amplían en función de la pertenencia al host.	El nuevo LUN del datastore se mapea a través del igroup hijo asociado. El datastore aparece en vCenter Server.

Escenario	Comportamiento del igroup parental	Comportamiento de igroup secundario	Asignación y visibilidad de LUN
Datastore e igroup creados de forma nativa en ONTAP y vCenter, luego descubiertos por ONTAP tools	ONTAP tools crea un igroup padre en su contexto de gestión y mantiene el nombre original del igroup.	ONTAP tools renombran el igroup original con el prefijo <code>otv_</code> y lo representan como un igroup hijo en la jerarquía.	Las asignaciones de iniciadores no se modifican. Durante el descubrimiento solo se convierten los igroups asignados a los datastores.

Reutilización personalizada de igroups y comportamiento de la API

En la interfaz de usuario de las ONTAP tools, puedes reutilizar un igroup padre personalizado existente de la lista desplegable mientras creas un datastore.

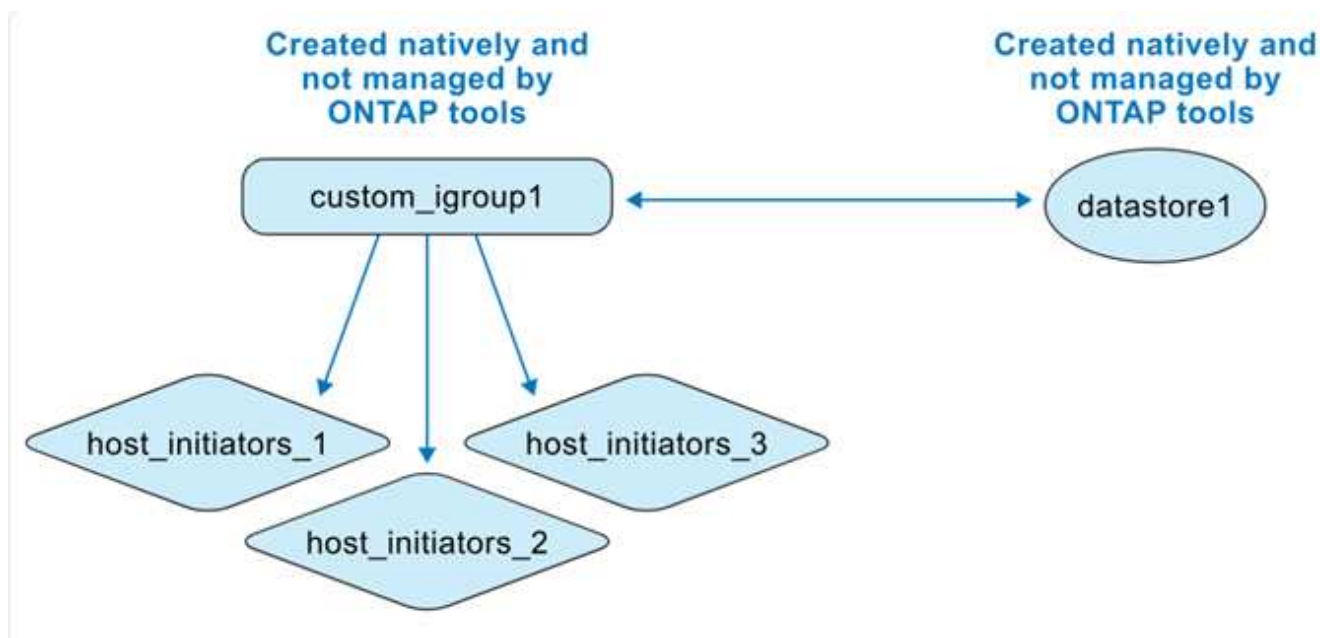
El mismo comportamiento se admite a través de la API. Para reutilizar un igroup existente durante la creación del almacén de datos, proporciona el UUID del igroup en la carga útil de la solicitud de API.



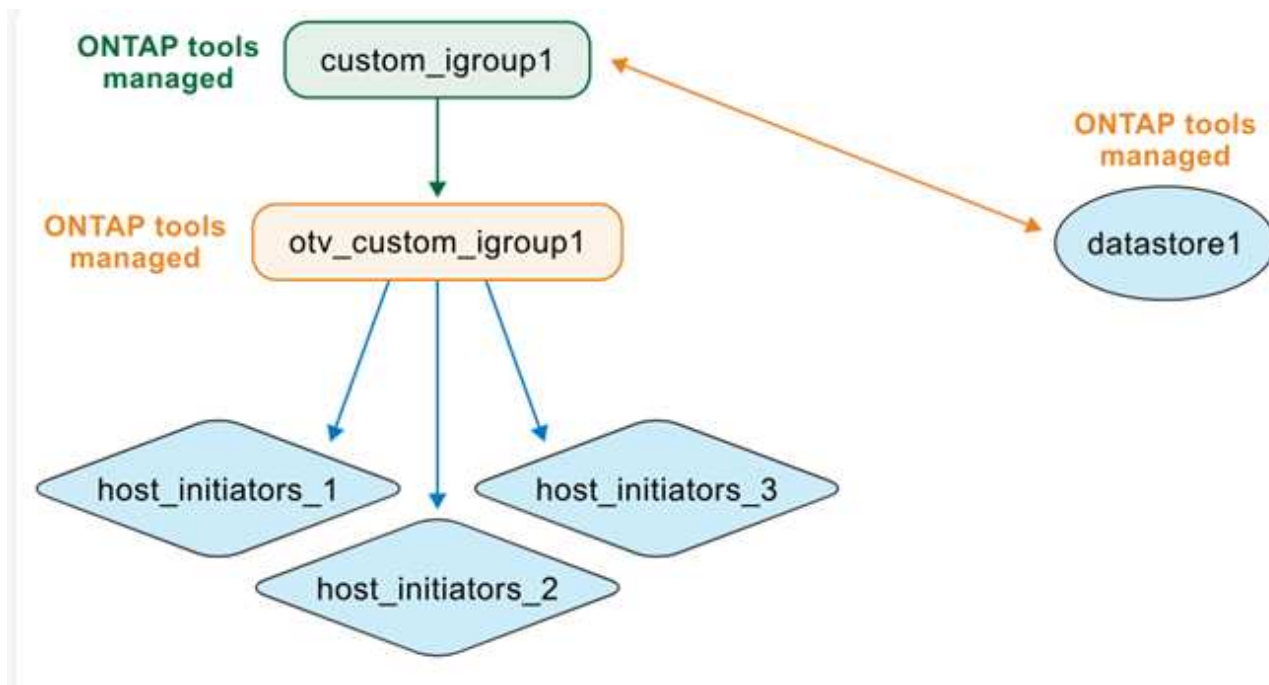
Sólo se pueden reutilizar los igroups personalizados. Los igroups migrados de ONTAP tools 9.x no se pueden reutilizar y, a partir de ONTAP tools 10.5 P2, se eliminan automáticamente cuando ya no se utilizan.

Vista de conversión de nativo a gestionado

Si creas el igroup y el datastore directamente en sistemas ONTAP y entornos VMware, ONTAP tools no gestiona estos objetos inicialmente. Esto da como resultado una estructura de igroup plana.



Tras el descubrimiento del almacén de datos, ONTAP tools identifica y registra los igroups mapeados por el almacén de datos y luego los representa en un modelo anidado. El igroup padre se representa en el nivel del almacén de datos, el igroup existente se renombra con el prefijo `otv_` como igroup hijo y las asignaciones del iniciador permanecen sin cambios.



ONTAP tools for VMware vSphere no detecta ni gestiona los igroups que se crean en los sistemas ONTAP pero que no están asignados a un datastore ni vinculados a ONTAP tools. Durante el descubrimiento, ONTAP tools solo convierte los igroups que están asignados a los datastores descubiertos; los demás igroups permanecen sin gestionar.

Reutilización de los igroups nativos descubiertos

Después de que ONTAP tools gestione un igroup nativo descubierto, ese igroup estará disponible en la lista desplegable de nombres de grupos de iniciadores personalizados para la creación de datastores.

El nuevo LUN del datastore se asigna al igroup hijo normalizado, por ejemplo, `otv_NativeIgroup1`.

ONTAP tools for VMware vSphere no detecta ni utiliza igroups creados en sistemas ONTAP que no están gestionados por ONTAP tools o que no están vinculados a un datastore.

Conoce la interfaz de usuario de ONTAP tools Manager

ONTAP tools for VMware vSphere admite multi-tenancy, lo que te permite gestionar varias instancias de vCenter Server.

ONTAP tools Manager es una consola basada en web para gestionar ONTAP tools for VMware vSphere, vCenter Server instances, storage backends y la configuración del appliance, como la alta disponibilidad (HA) y el escalado de nodos.

ONTAP tools Manager ofrece las siguientes funciones:

- Gestiona alertas: ve y filtra las alertas generadas por ONTAP tools for VMware vSphere.
- Gestiona los backends de almacenamiento: añade y gestiona clústeres de almacenamiento ONTAP, y asígnalos a instancias de vCenter Server a nivel global.
- Administra instancias de vCenter Server: agrega y administra instancias de vCenter Server dentro de ONTAP tools.

- Supervisa trabajos: supervisa y depura trabajos asíncronos iniciados tanto desde la interfaz del complemento de ONTAP tools como desde la interfaz de ONTAP tools Manager. Puedes filtrar trabajos por periodo de tiempo, ajustar el tamaño de página y ver los detalles del trabajo, incluidos errores y subtareas. Haz clic en el estado de error para ver los detalles del error. Para trabajos con subtareas, expande la fila para ver descripciones y estados. Para subtrabajos, usa el desglose del trabajo para ver los detalles.
- Descargar paquetes de registros: recopila archivos de registro para solucionar problemas de ONTAP tools for VMware vSphere.
- Gestiona certificados: reemplaza el certificado autofirmado por un certificado de CA personalizado y renueva o actualiza los certificados para VASA Provider y ONTAP tools.
- Restablecer contraseñas: cambia la contraseña para el VASA Provider y SRA.
- Gestiona la configuración del appliance: configura el appliance de ONTAP tools, incluyendo habilitar HA y aumentar el tamaño de los nodos.

Para acceder a ONTAP tools Manager, abre <https://<ONTAPtoolsIP>:8443/virtualization/ui/> desde el navegador e inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.

The screenshot displays the ONTAP tools Manager interface. The top navigation bar includes the ONTAP tools Manager logo and a user profile dropdown for 'admin'. The left sidebar lists navigation options: Overview, Alerts, Storage backends, vCenters, Jobs, 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 a table of configuration details: Size (Small), HA (Enabled), VASA Provider (Enabled), and SRA (Enabled). The 'Alerts' section shows 'No alerts' for the last 24 hours. The 'vCenters' section shows '1 Healthy' vCenter. The 'Storage backends' section shows 'No storage backends added'. The 'ONTAP tools nodes' section displays three nodes: vee-lab3-vm41, vee-lab3-vm184, and vee-lab3-vm187, all with 'Healthy' status and a 'Deploy_OVA_b29c029_998' task. Each node has a 'VIEW DETAILS' link.

Tarjeta	Descripción
Tarjeta del appliance	La ficha Appliance muestra el estado general del appliance de ONTAP tools, los detalles de la configuración y el estado de los servicios habilitados. Para ver más información, selecciona el enlace Ver detalles . Si cambias una configuración del appliance, la ficha muestra el estado y los detalles del trabajo hasta que se complete el cambio.
Tarjeta de alertas	La ficha «Alertas» muestra las alertas de ONTAP tools clasificadas por tipo, incluidas las alertas a nivel de nodo HA. Puedes ver alertas detalladas haciendo clic en el enlace del recuento, que te lleva a la página de alertas filtrada por el tipo de alerta seleccionado.
tarjeta de vCenters	La tarjeta de vCenters muestra el estado de salud de todas las instancias de vCenter Server gestionadas por ONTAP tools. Puedes ver los detalles de cada vCenter seleccionando el enlace correspondiente, que te lleva a una página con más información sobre la instancia seleccionada.
Tarjeta de backends de almacenamiento	La tarjeta de backends de almacenamiento muestra el estado de salud y conectividad de todos los clústeres de almacenamiento ONTAP configurados en ONTAP tools. Puedes ver los detalles de cada backend de almacenamiento seleccionando el enlace correspondiente, que te lleva a una página con más información sobre el clúster seleccionado.
Tarjeta de nodos de ONTAP tools	La tarjeta de nodos de ONTAP tools muestra todos los nodos del appliance, incluyendo el nombre de nodo, el nombre de la VM, el estado y la información de red. Selecciona Ver detalles para ver más detalles de un nodo específico. [NOTA] En una configuración que no es HA, solo aparece un nodo. En una configuración HA, se muestran tres nodos.

Gestiona la configuración de ONTAP tools Manager

Editar la configuración de AutoSupport de ONTAP tools

Cuando configuras por primera vez ONTAP tools for VMware vSphere, AutoSupport está habilitado de forma predeterminada. Envía mensajes al soporte técnico 24 horas después de estar habilitado.

Desactivar AutoSupport

Cuando desactivas AutoSupport, ya no recibes soporte y supervisión proactivos.



Se recomienda mantener AutoSupport activado, ya que ayuda a acelerar la detección y resolución de problemas. Incluso cuando AutoSupport está desactivado, el sistema sigue recopilando y almacenando información localmente, pero no envía informes por la red.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la opción **Configuración > Telemetría > Editar**.
4. Desmarca la opción **AutoSupport** y guarda los cambios.

Actualizar la URL del proxy de AutoSupport

Actualiza la URL del proxy de AutoSupport para que la función AutoSupport envíe los datos a través del servidor proxy para una transmisión segura.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona **Configuración** en la barra lateral.
4. Selecciona la opción **Configuración > Telemetría > Editar**.
5. Introduce una **URL de proxy** válida y guarda los cambios.

Si desactivas AutoSupport, la URL del proxy también se desactiva.

Agrega servidores NTP a las herramientas ONTAP

Introduce los datos del servidor NTP para sincronizar los relojes del dispositivo ONTAP tools.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la opción **Settings > NTP server > Edit**.
4. Introduce el nombre de dominio completo (FQDN), o las direcciones IPv4 o IPv6 separadas por comas.

Actualiza la pantalla para ver los valores actualizados.

Restablece las credenciales de VASA Provider y SRA en ONTAP tools

Si olvidas tus credenciales de VASA Provider o SRA, puedes restablecerlas a una nueva contraseña usando la interfaz de ONTAP tools Manager. La nueva contraseña debe tener entre 8 y 256 caracteres.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la opción **Configuración > Credenciales de VASA Provider / SRA > Restablecer contraseña**.
4. Introduce la nueva contraseña y confírmala.
5. Selecciona **Guardar** para aplicar los cambios.

Editar la configuración de copia de seguridad de ONTAP tools

A partir de ONTAP tools for VMware vSphere 10.5, la función de copia de seguridad está activada de forma predeterminada y se crea una copia de seguridad cada 10 minutos. Puedes desactivar la copia de seguridad o modificar la frecuencia de la copia de seguridad.

No desactives la copia de seguridad, ya que esto impide que las herramientas de ONTAP mantengan un RPO bajo. Al desactivar la copia de seguridad no se eliminan los archivos de copia de seguridad existentes. Puedes cambiar la frecuencia de la copia de seguridad a un valor comprendido entre 10 y 60 minutos.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la opción **Configuración > Copia de seguridad > Editar**.
4. En la ventana de edición, puedes desactivar la copia de seguridad o editar la frecuencia de la copia de seguridad.

Habilitar los servicios de ONTAP tools

Puedes cambiar la contraseña de administrador usando ONTAP tools Manager para habilitar servicios como VASA Provider, la importación de la configuración de vVols y la recuperación ante desastres (SRA) usando ONTAP tools Manager.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la opción **Editar configuración del dispositivo** en la sección de resumen.
4. En la sección **Servicios**, puedes activar servicios opcionales como VASA Provider, la importación de la configuración de vVols y la recuperación ante desastres (SRA) según sea necesario.

Al habilitar los servicios por primera vez, debes crear las credenciales del proveedor VASA y de SRA. Estas se utilizan para registrar o habilitar los servicios del proveedor VASA y de SRA en el servidor vCenter. El nombre de usuario solo puede contener letras, números y guiones bajos. La longitud de la

contraseña debe estar comprendida entre 8 y 256 caracteres.



Antes de desactivar cualquier servicio opcional, asegúrate de que los servidores vCenter gestionados por ONTAP tools no los usen.

La opción **Permitir la importación de la configuración de vVols** solo se muestra cuando el servicio VASA Provider está habilitado. Esta opción permite la migración de datos de vVols desde ONTAP tools 9.xx a ONTAP tools 10.5.

Cambiar la configuración del dispositivo ONTAP tools

Utiliza ONTAP tools Manager para ampliar la configuración de ONTAP tools for VMware vSphere, ya sea aumentando el número de nodos o activando la conmutación automática al respaldo (HA). De forma predeterminada, el appliance ONTAP tools for VMware vSphere se implementa como una configuración de un solo nodo, sin conmutación automática al respaldo.

Antes de empezar

- Asegúrate de que tu 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.
- Asegúrate de que la incorporación en caliente de la CPU y la incorporación en caliente de la memoria estén habilitadas.
- En el vCenter Server, configura el nivel de automatización del Disaster Recovery Service (DRS) en parcialmente automatizado. Después de implementar HA, vuelve a configurarlo en totalmente automatizado.
- Los nombres de host de los nodos en la configuración de alta disponibilidad deben estar en minúsculas.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la opción **Editar configuración del dispositivo** en la sección de resumen.
4. En la sección **Configuración**, aumenta el tamaño del nodo y activa la configuración de alta disponibilidad (HA). Utiliza las credenciales del servidor vCenter para realizar los cambios.

En la configuración de HA, puedes cambiar los detalles de la biblioteca de contenidos. Proporciona la contraseña para cada edición.



En ONTAP tools for VMware vSphere, solo se permite aumentar el tamaño del nodo; no puedes reducir el tamaño del nodo. En una configuración sin HA, solo se admite la configuración de tamaño medio. En una configuración con HA, se admiten las configuraciones de tamaño medio y grande.

5. Utiliza el botón de activación/desactivación de HA para habilitar la configuración de HA. En la página **Configuración de HA**, asegúrate de que:
 - La biblioteca de contenidos pertenece al mismo servidor vCenter donde se ejecutan las máquinas virtuales del nodo de ONTAP tools. Las credenciales del servidor vCenter se usan para validar y

descargar la plantilla OVA para los cambios en el appliance.

- La máquina virtual que aloja las ONTAP tools no se implementa directamente en un host ESXi. La máquina virtual debe implementarse en un clúster o en un pool de recursos.



Después de habilitar la configuración HA, no puedes volver a una configuración de un solo nodo sin HA.

6. En la sección **Configuración de HA** de la ventana **Editar configuración del dispositivo**, puedes introducir los datos de los nodos 2 y 3. ONTAP tools for VMware vSphere admite tres nodos en una configuración de HA.



Las herramientas de ONTAP rellenan automáticamente la mayoría de las opciones de entrada con los detalles de red del nodo 1 para simplificar el flujo de trabajo. Puedes editar los datos de entrada antes de ir a la última página del asistente. Solo puedes introducir los detalles de la dirección IPv6 de los otros dos nodos cuando la dirección IPv6 está habilitada en el nodo de gestión de ONTAP tools.

Asegúrate de que cada host ESXi contiene solo una VM de ONTAP tools. Las entradas se validan cada vez que pasas a la siguiente ventana.

7. Revisa los detalles en la sección **Resumen** y **Guarda** los cambios.

¿Qué sigue?

La página **Resumen** muestra el estado de la implementación. También puedes realizar un seguimiento del estado de la tarea de edición de la configuración del dispositivo desde la vista de tareas utilizando el ID de la tarea.

Si falla la implementación de HA y el estado del nuevo nodo es «Nuevo», elimina la nueva máquina virtual en vCenter antes de volver a intentar habilitar HA.

La pestaña **Alertas** del panel izquierdo muestra las alertas de ONTAP tools for VMware vSphere.

Agrega hosts de VMware vSphere a las ONTAP tools

Añade nuevos hosts de VMware vSphere a ONTAP tools for VMware vSphere para gestionar y proteger los datastores en los hosts.

Pasos

1. Agrega un host a tu clúster de VMware vSphere siguiendo el flujo de trabajo en la página: ["Cómo añadir un host ESX a tu clúster de vSphere usando el flujo de trabajo de inicio rápido"](#)
2. Después de añadir el host, ve al menú principal de ONTAP tools y selecciona **Discover** en el panel de resumen. Espera a que termine el proceso de descubrimiento. O bien, puedes esperar a que se complete la detección programada del host.

Resultado

El nuevo host ya ha sido detectado y ahora es gestionado por ONTAP tools for VMware vSphere. Puedes proceder a gestionar el datastore en el nuevo host.

Temas relacionados

- ["Monta un datastore de vVols"](#) en nuevos hosts.

- ["Montar almacén de datos NFS y VMFS" en nuevos servidores.](#)

Gestiona almacenes de datos

Monta almacenes de datos NFS y VMFS en ONTAP tools

Montar un almacén de datos permite el acceso al almacenamiento a hosts adicionales. Puedes montar el almacén de datos en los hosts adicionales después de añadir los hosts a tu entorno VMware.



Cuando añadas un nuevo host ESXi usando el ["Agrega un host ESX a tu flujo de trabajo de clúster de vSphere"](#), espera a que finalice la detección programada del host antes de que aparezca en ONTAP tools. O bien, puedes ejecutar manualmente la detección desde la pantalla de resumen de NetApp ONTAP tools.

Acerca de esta tarea

- Algunas acciones del botón derecho del ratón están desactivadas o no disponibles dependiendo de la versión del cliente de vSphere y del tipo de almacén de datos seleccionado.
 - Si utilizas el cliente vSphere 8.0 o versiones posteriores, algunas de las opciones del menú contextual están ocultas.
 - Desde vSphere 7.0U3 hasta vSphere 8.0, aunque aparezcan las opciones, la acción estará desactivada.
- vSphere desactiva la opción de montar el almacén de datos cuando el clúster de hosts está protegido con configuraciones uniformes.

Pasos

1. Desde la página de inicio del vSphere Client, selecciona **Hosts and Clusters**.
2. En el panel de navegación de la izquierda, selecciona los centros de datos que contienen los hosts.
3. Para montar almacenes de datos NFS/VMFS en un host o en un clúster de hosts, haz clic con el botón derecho y selecciona **NetApp ONTAP tools > Montar almacenes de datos**.
4. Selecciona los almacenes de datos que quieras montar y selecciona **Montar**.

¿Qué sigue?

Puedes seguir el progreso en el panel de tareas recientes.

Tema relacionado

["Agrega nuevos hosts de VMware vSphere"](#)

Desmonta los almacenes de datos NFS y VMFS en ONTAP tools

La acción «Desmontar almacén de datos» elimina un almacén de datos NFS o VMFS de los hosts ESXi. Está disponible para los almacenes de datos detectados o gestionados por ONTAP tools for VMware vSphere.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Haz clic con el botón derecho del ratón en un objeto de almacén de datos NFS o VMFS y selecciona

Desmontar almacén de datos.

El cliente de vSphere abre un cuadro de diálogo y muestra una lista de los hosts ESXi que tienen montado el almacén de datos. Cuando la operación se realiza en un almacén de datos protegido, aparece un mensaje de advertencia en pantalla.

3. Selecciona uno o varios hosts ESXi para desmontar el almacén de datos.

No puedes desmontar el almacén de datos de todos los hosts. La interfaz de usuario sugiere que uses la operación de eliminar almacén de datos en su lugar.

4. Selecciona el botón **Desmontar**.

Si el almacén de datos forma parte de un clúster de hosts protegido, aparece un mensaje de advertencia.



Si se desmonta el almacén de datos protegido, la configuración de protección actual podría dar lugar a una protección parcial. Consulta ["Modificar el clúster de hosts protegidos"](#) para habilitar la protección completa.

¿Qué sigue?

Puedes seguir el progreso en el panel de tareas recientes.

Monta un almacén de datos vVols en ONTAP tools

Puedes montar un almacén de datos de VMware Virtual Volumes (vVols) en uno o varios hosts adicionales para proporcionar acceso al almacenamiento a hosts adicionales. Solo puedes desmontar un almacén de datos de vVols a través de las API.



Cuando añadas un nuevo host ESXi usando el ["Agrega un host ESX a tu flujo de trabajo de clúster de vSphere"](#), espera a que finalice la detección programada del host antes de que aparezca en ONTAP tools. O bien, puedes ejecutar manualmente la detección desde la pantalla de resumen de NetApp ONTAP tools.

Pasos

1. Desde la página de inicio del vSphere Client, selecciona **Hosts and Clusters**.
2. En el panel de navegación, selecciona el centro de datos que contiene el datastore.
3. Haz clic con el botón derecho del ratón en el almacén de datos y selecciona **NetApp ONTAP tools > Montar almacén de datos**.
4. En el cuadro de diálogo **Montar almacenes de datos en hosts**, selecciona los hosts en los que deseas montar el almacén de datos y luego selecciona **Montar**.

El panel de tareas reciente muestra el progreso.

Tema relacionado

["Agrega nuevos hosts de VMware vSphere"](#)

Redimensiona los almacenes de datos NFS y VMFS en ONTAP tools

Al cambiar el tamaño de un almacén de datos, puedes aumentar el espacio de almacenamiento para los archivos de tu máquina virtual. Puedes cambiar el tamaño de

un almacén de datos a medida que cambian los requisitos de tu infraestructura.

Acerca de esta tarea

Puedes aumentar el tamaño de los almacenes de datos NFS y VMFS. Un volumen FlexVol en estos almacenes de datos no puede reducirse por debajo de su tamaño actual, pero puede crecer hasta un 120%.

Pasos

1. Desde la página de inicio del vSphere Client, selecciona **Hosts and Clusters**.
2. En el panel de navegación, selecciona el centro de datos que contiene el datastore.
3. Haz clic con el botón derecho del ratón en el almacén de datos NFS o VMFS y selecciona **NetApp ONTAP tools > Cambiar el tamaño del almacén de datos**.
4. En el cuadro de diálogo «Cambiar tamaño», introduce un nuevo tamaño para el datastore y selecciona **OK**.

Amplía los datastores vVols en ONTAP tools

Cuando haces clic con el botón derecho en el objeto datastore en la vista de objetos de vCenter, la sección del complemento muestra las acciones compatibles para ONTAP tools for VMware vSphere. Las acciones específicas se habilitan según el tipo de datastore y los privilegios actuales del usuario.



La operación de ampliación del datastore vVols no es aplicable para los datastores vVols basados en el sistema ASA r2.

Pasos

1. Desde la página de inicio del vSphere Client, selecciona **Hosts and Clusters**.
2. En el panel de navegación, selecciona el centro de datos que contiene el datastore.
3. Haz clic con el botón derecho del ratón en el almacén de datos y selecciona **NetApp ONTAP tools > Add storage to datastore**.
4. En la ventana **Crear o seleccionar volúmenes**, puedes crear nuevos volúmenes o elegir entre los ya existentes. Sigue las instrucciones que aparecen en pantalla para realizar tu selección.
5. En la ventana **Resumen**, revisa las selecciones y selecciona **Expand**. Puedes seguir el progreso en el panel de tareas recientes.

Reduce un almacén de datos vVols en ONTAP tools

Esta página explica cómo eliminar volúmenes de un almacén de datos de vVols.

Utiliza la acción eliminar almacenamiento del almacén de datos en cualquier almacén de datos vVols gestionado por ONTAP tools en vCenter Server.

No puedes eliminar almacenamiento de un volumen si contiene vVols; la opción de eliminar estará desactivada para esos volúmenes. Al eliminar volúmenes del almacén de datos, también tienes la opción de eliminar los volúmenes seleccionados del almacenamiento ONTAP.



La operación de reducción del almacén de datos vVols no es compatible con los almacenes de datos vVols basados en sistemas ASA r2.

Pasos

1. Desde la página de inicio del vSphere Client, selecciona **Hosts and Clusters**.
2. En el panel de navegación, selecciona el centro de datos que contiene el datastore.
3. Haz clic con el botón derecho en el almacén de datos vVol y selecciona **NetApp ONTAP tools > Eliminar almacenamiento del almacén de datos**.
4. Selecciona los volúmenes que no tengan vVols y selecciona **Eliminar**.



La opción para seleccionar el volumen en el que se encuentra vVols está desactivada.

5. En la ventana emergente **Eliminar almacenamiento**, marca la casilla **Eliminar volúmenes del clúster ONTAP** para eliminar los volúmenes del almacén de datos y del almacenamiento ONTAP y selecciona **Eliminar**.

Eliminar almacenes de datos en ONTAP tools

Esta página describe cómo eliminar almacenes de datos NFS, VMFS o vVols usando ONTAP tools en el vCenter Server.

Al eliminar un almacén de datos, se realizan las siguientes acciones según el tipo de almacén de datos:

- El contenedor vVol está desmontado.
- Si el igroup no está en uso, sus iniciadores se eliminan del igroup.
- El contenedor vVol se elimina.
- Los volúmenes Flex permanecen en la matriz de almacenamiento.

Solo puedes eliminar el almacén de datos si no hay ningún vVols en el almacén de datos seleccionado.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Haz clic con el botón derecho en un sistema host, un clúster de hosts o un centro de datos y selecciona **NetApp ONTAP tools > Eliminar datastore**.



No puedes eliminar un almacén de datos que está siendo usado por máquinas virtuales. Mueve las máquinas virtuales a otro almacén de datos antes de eliminarlo. No puedes eliminar el volumen si forma parte de un clúster de hosts 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 usan el almacén de datos.
- b. Si no hay máquinas virtuales asociadas a un almacén de datos VMFS, verás un cuadro de diálogo de confirmación. Si la protección de clústeres de hosts está habilitada y existe una relación AFD, puedes limpiar los elementos de almacenamiento secundario.
- c. En el caso de los almacenes de datos VMFS protegidos en sistemas ASA r2, desactiva la protección antes de eliminarlos. A partir de ONTAP 9.17.1 y ONTAP tools for VMware vSphere 10.5, puedes eliminar un almacén de datos protegido. Si es el único almacén de datos en el grupo de protección, la protección del clúster de hosts se elimina automáticamente.
- d. Para los almacenes de datos vVols, solo puedes eliminar el almacén de datos si no hay ningún vVols presente. El cuadro de diálogo **Eliminar almacén de datos** incluye una opción para eliminar volúmenes del clúster ONTAP.

- e. Para los almacenes de datos vVols en sistemas ASA r2, no puedes eliminar los volúmenes de soporte desde ONTAP usando la opción **Eliminar almacén de datos**.
3. Para eliminar los volúmenes de respaldo en el almacenamiento ONTAP, selecciona **Eliminar volúmenes en el clúster ONTAP**.



En el caso de los almacenes de datos VMFS en un sistema de almacenamiento ONTAP unificado que formen parte de un clúster de hosts protegido, no es posible eliminar el volumen del clúster ONTAP.

Cuando eliminas un almacén de datos NFS, VMFS o vVols, los igroups principales permanecen en el sistema ONTAP. Los igroups secundarios que no están asignados a ningún LUN se eliminan automáticamente. Las herramientas de ONTAP realizan una limpieza diaria para eliminar los igroups principales predeterminados no asignados. Elimina manualmente los igroups principales personalizados en ONTAP. Las herramientas de ONTAP no pueden reutilizar los igroups principales obsoletos.

Vistas de almacenamiento ONTAP para datastores en ONTAP tools

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

Pasos

1. Desde el cliente vSphere, ve al almacén de datos.
2. Selecciona la pestaña **Configurar** en el panel de la derecha.
3. Selecciona **NetApp ONTAP tools > ONTAP Storage**. La vista varía según el tipo de almacén de datos. Consulta la tabla siguiente:

Tipo de almacén de datos	Información disponible
Almacén de datos NFS	La página Detalles de almacenamiento contiene backends de almacenamiento, información de agregados y de volúmenes. La página Detalles de NFS contiene datos relacionados con el datastore NFS.
Almacenes de datos VMFS	La página Detalles de almacenamiento contiene información sobre el backend de almacenamiento, el agregado, el volumen y la zona de disponibilidad de almacenamiento (SAZ). La página Detalles de la unidad de almacenamiento contiene información sobre la unidad de almacenamiento.
vVols almacenes de datos	Muestra una lista de todos los volúmenes. Puedes ampliar o eliminar espacio de almacenamiento desde el panel de almacenamiento de ONTAP. Las herramientas de ONTAP no admiten esta vista para los almacenes de datos basados en el sistema ASA r2 vVols.

Vista de almacenamiento de máquinas virtuales en ONTAP tools

La vista de almacenamiento muestra la lista de vVols que crea la máquina virtual.



Esta vista se aplica a las VM con al menos un disco de un datastore de vVols gestionado por ONTAP tools for VMware vSphere.

Pasos

1. Desde el vSphere Client, ve a la máquina virtual.
2. Selecciona la pestaña **Monitor** en el panel de la derecha.
3. Selecciona **NetApp ONTAP tools > Storage**. Los detalles de **Storage** aparecen en el panel derecho. Puedes ver la lista de vVols que están en la VM.

Puedes utilizar la opción 'Gestionar columnas' para ocultar o mostrar diferentes columnas.

Administra los umbrales de almacenamiento en ONTAP tools

Puedes configurar el umbral para recibir notificaciones en vCenter Server cuando el volumen y la capacidad del agregado alcancen ciertos niveles.

Pasos:

1. Inicia sesión en el cliente de vSphere.
2. En la página de accesos directos, selecciona **NetApp ONTAP tools** en la sección de complementos.
3. En el panel izquierdo de ONTAP tools, ve a **Configuración > Configuración de umbrales > Editar**.
4. En la ventana **Editar umbral**, introduce los valores deseados en los campos **Casi lleno** y **Lleno** y selecciona **Guardar**. Puedes restablecer los valores de umbral a los valores predeterminados recomendados: 80 para **Casi lleno** y 90 para **Lleno**.

Administra los backends de almacenamiento en ONTAP tools

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

Descubre almacenamiento

Puedes ejecutar la detección de un backend de almacenamiento bajo demanda sin esperar a que una detección programada actualice los detalles del almacenamiento de forma inmediata. Para configuraciones de MetroCluster, ejecuta manualmente la detección de ONTAP tools después de una conmutación de sitios.

Sigue los pasos que se indican a continuación para descubrir los backends de almacenamiento.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. En la página de accesos directos, selecciona **NetApp ONTAP tools** en la sección de complementos.
3. En el panel izquierdo de ONTAP tools, ve a **Storage Backends** y selecciona un storage backend.
4. Selecciona el menú de los tres puntos verticales y selecciona **Descubrir almacenamiento**

Puedes seguir el progreso en el panel de tareas recientes.

Modificar los backends de almacenamiento

Puedes modificar las credenciales del backend de almacenamiento o el nombre del puerto. También puedes modificar el backend de almacenamiento para los clústeres globales de ONTAP usando ONTAP tools Manager. Si el certificado va a caducar en 30 días o menos, ONTAP tools muestra una advertencia. Modifica el backend de almacenamiento y sube el nuevo certificado desde el administrador de ONTAP.

Cuando modificas el backend de almacenamiento, ONTAP tools for VMware vSphere realiza un descubrimiento del backend de almacenamiento para actualizar los detalles de almacenamiento.

Sigue los pasos que se indican en esta sección para modificar un backend de almacenamiento.

1. Inicia sesión en el cliente de vSphere.
2. En la página de accesos directos, selecciona **NetApp ONTAP tools** en la sección de complementos.
3. En el panel izquierdo de ONTAP tools, ve a **Storage Backends** y selecciona un storage backend.
4. Selecciona el menú de los tres puntos verticales y elige **Modificar** para modificar las credenciales o el nombre del puerto. Puedes seguir el progreso en el panel de tareas recientes.

Modifica los clústeres globales de ONTAP con ONTAP tools Manager de la siguiente manera.

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona los backends de almacenamiento en la barra lateral.
4. Selecciona el backend de almacenamiento que deseas modificar.
5. Selecciona el menú de los tres puntos verticales y selecciona **Modificar**.
6. Puedes modificar las credenciales o el puerto. Introduce el **nombre de usuario** y la **contraseña** para modificar el backend de almacenamiento.

Eliminar backends de almacenamiento

Debes eliminar todos los almacenes de datos asociados al backend de almacenamiento antes de eliminarlo. Sigue los pasos que se indican a continuación para eliminar un backend de almacenamiento.

1. Inicia sesión en el cliente de vSphere.
2. En la página de accesos directos, selecciona **NetApp ONTAP tools** en la sección de complementos.
3. En el panel izquierdo de ONTAP tools, ve a **Storage Backends** y selecciona un storage backend.
4. Selecciona el menú de los tres puntos verticales y elige **Eliminar**. Asegúrate de que el backend de almacenamiento no contenga ningún datastore. Puedes seguir el progreso en el panel de tareas recientes.

Puedes eliminar clústeres ONTAP globales usando ONTAP tools Manager.

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona **Storage Backends** en la barra lateral.

4. Selecciona el backend de almacenamiento que deseas eliminar
5. Selecciona el menú de los tres puntos verticales y selecciona **Eliminar**.

Vista detallada del backend de almacenamiento

La página de backends de almacenamiento muestra una lista de todos los backends de almacenamiento. Puedes realizar operaciones de detección, modificación y eliminación en los backends de almacenamiento que hayas añadido, pero no en las SVM secundarias individuales bajo el clúster.

Selecciona el clúster principal o el secundario para ver el resumen de los componentes. Para el clúster principal, usa el menú desplegable de acciones para descubrir almacenamiento, modificar o quitar el backend de almacenamiento.

La página de resumen ofrece los siguientes datos:

- Estado del sistema de almacenamiento subyacente
- Información sobre la capacidad
- Información básica sobre la máquina virtual
- Detalles del certificado, como el estado del certificado y la fecha de caducidad.
- Información de red, como la dirección IP y el puerto de la red. Para el SVM secundario, la información es la misma que la del backend de almacenamiento principal.
- Privilegios permitidos y restringidos para el backend de almacenamiento. Para el SVM hijo, la información es la misma que para el backend de almacenamiento padre. ONTAP tools muestra los privilegios solo en los backends de almacenamiento basados en cluster. Si añades SVM como backend de almacenamiento, no se muestra la información de privilegios.
- La vista detallada del clúster del sistema ASA r2 no incluye la pestaña "Niveles locales" cuando la propiedad `disaggregated` está configurada como `"true"` para el SVM o el clúster.
- En los sistemas SVM de ASA r2, no se muestra el panel de capacidad. El panel de capacidad solo es necesario cuando la propiedad `"disaggregated"` está configurada como `"true"` para el SVM o el clúster.
- En el caso de los sistemas SVM de ASA r2, la sección de información básica muestra el tipo de plataforma.

La pestaña de interfaz ofrece información detallada sobre la interfaz.

La pestaña «Niveles locales» ofrece información detallada sobre la lista de agregados.

Administra instancias de vCenter Server en ONTAP tools

Las instancias de vCenter Server son plataformas de gestión centralizadas que te permiten controlar hosts, máquinas virtuales y backends de almacenamiento.

Desvincula los backends de almacenamiento de la instancia de vCenter Server

La página de listado de vCenter Server muestra el número de backends de almacenamiento asociados. Cada instancia de vCenter Server tiene la opción de asociar o desasociar un backend de almacenamiento.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la instancia de vCenter Server que necesites en la barra lateral.
4. Selecciona los puntos suspensivos verticales junto al vCenter Server que quieres asociar o desasociar con los storage backends.
5. Selecciona **Desvincular el backend de almacenamiento**.

Modifica una instancia de vCenter Server

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

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona la instancia correspondiente de vCenter Server en la barra lateral
4. Selecciona los puntos suspensivos verticales junto al servidor vCenter que quieres modificar y selecciona **Modificar**.
5. En la ventana **Modificar vCenter**, introduce el nombre de usuario, la contraseña y los detalles del puerto.
6. Sube el certificado y selecciona **Modificar**.

Eliminar una instancia de vCenter Server

Elimina todos los backends de almacenamiento del vCenter Server antes de eliminarlo.

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona las instancias de vCenter Server correspondientes desde la barra lateral
4. Selecciona los puntos suspensivos verticales junto al vCenter Server que quieres quitar y selecciona **Eliminar**.



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

Cuando eliminas instancias de vCenter Server en ONTAP tools, se realizan automáticamente las siguientes acciones:

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

Renueva el certificado del servidor vCenter

ONTAP tools te avisa cuando el certificado vCenter está a punto de caducar o ya ha caducado. Después de renovar el certificado vCenter, sube el nuevo certificado a ONTAP tools siguiendo estos pasos:

1. Inicia sesión en el shell de diagnóstico remoto de ONTAP tools.
2. Obtén el certificado renovado de vCenter desde el shell de diagnóstico:

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Asegúrate de que el certificado esté en formato Base 64 ASCII e incluya las líneas inicial y final, por ejemplo:

```
---{}BEGIN CERTIFICATE{}---
MIIIFUzCCA7ugAwIBAgIJANOGlapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMqwwCgYD
VQQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKZImiZPyLGBGRYF
bG9jYWwxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WHcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcml5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZ0ZXRBcHAXDDAKBgNVBAsMA0xPRDCCAAIwDQYJ
KoZIHvcNAQEBBQADgGgPADCCAYoCggGBALU8OCWmtA2gvIC/OTw/7xucvPVuM+b8
DhZvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaDloi2u
ZDW0CaF0QhLopNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVlZiIQ
TIWpdQMbEEzFIkrLfc70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoXleRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+ttZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIhV02
WWDQRLiuVFAcDAyvCrO9Irx0Gk1RyRShKYakdWxZ3hhMdLuGq0yvRXqo1Ib94zwO
JfBJHjFTtoA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsgA1UdDwQEAwIF
4DA7BgNVHREENDAYgRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMC0AB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVRO0BBYEFJ0V0zY+JRpFrEt31ovAY4BLFXmAMB8G
A1UdIwQYMBaAFENf6fRxWF3OJQNTPIduPk6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWZl
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfK7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienbl6copzUNwtqh+m9Ifow74Gf+ulRzEC0EAVO1X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJD1N2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMHlgmXP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI3lD7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZNi/QTMh/MkWW2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJA1cI7ak=
---{}END CERTIFICATE{}---
```

4. Copia el resultado y guárdalo como un archivo de texto con una extensión .pem en tu escritorio.
5. Inicia ONTAP tools Manager desde un navegador web:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>

6. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
7. Selecciona la instancia correspondiente de vCenter Server en la barra lateral
8. Selecciona los puntos suspensivos verticales junto al servidor vCenter que quieres modificar y selecciona **Modificar**.
9. En la ventana **Modificar vCenter**, introduce el nombre de usuario, la contraseña y los detalles del puerto.
10. Sube el certificado y selecciona **Modificar**.

Información relacionada

["Configura el acceso al diagnóstico remoto"](#)

Administra los certificados de ONTAP tools

Durante la implementación, se genera de forma predeterminada un certificado autofirmado para ONTAP tools y VASA Provider. Puedes usar la interfaz de ONTAP tools Manager para renovar este certificado o reemplazarlo por un certificado CA personalizado. En implementaciones multi-vCenter, es obligatorio usar certificados CA personalizados.

Antes de empezar

Debes tener lo siguiente antes de empezar:

- El nombre de dominio asociado a la dirección IP virtual.
- Consulta nslookup del nombre de dominio realizada correctamente, confirmando que se resuelve en la dirección IP correcta.
- Certificados creados con el nombre de dominio y la dirección IP de ONTAP tools.



La dirección IP de ONTAP tools debe estar asociada a un nombre de dominio completo (FQDN). Los certificados deben contener el mismo FQDN asociado a la dirección IP de ONTAP tools en el campo sujeto o en los nombres alternativos del sujeto.



No puedes cambiar de un certificado firmado por una autoridad de certificación a uno autofirmado.

Actualizar el certificado de ONTAP tools

La pestaña ONTAP tools muestra detalles como el tipo de certificado (autofirmado o firmado por una CA) y el nombre de dominio. Durante la implementación, se genera de forma predeterminada un certificado autofirmado. Puedes renovar el certificado o actualizarlo a uno firmado por una CA.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona **Certificados > ONTAP tools > Renovar** para renovar los certificados.

Puedes renovar el certificado si ha caducado o está a punto de caducar. La opción de renovación está disponible cuando el tipo de certificado está firmado por una CA. En la ventana emergente, introduce los datos del certificado del servidor, la clave privada, la CA raíz y el certificado intermedio.



El sistema estará fuera de línea hasta que se renueve el certificado, y se te cerrará la sesión de la interfaz de usuario de ONTAP tools Manager.

4. Para actualizar el certificado autofirmado a un certificado de CA personalizado, selecciona **Certificates > ONTAP tools > la opción Upgrade to CA**.
 - a. En la ventana emergente, sube los archivos del certificado del servidor, la clave privada del certificado del servidor, el certificado de la CA raíz y el certificado intermedio.
 - b. Introduce el FQDN de la dirección IP del Load Balancer para el que generaste este certificado y actualiza el certificado.



El sistema estará fuera de línea hasta que termine la actualización y se te cerrará la sesión de la interfaz de usuario de ONTAP tools Manager.

Actualizar el certificado de VASA Provider

ONTAP tools for VMware vSphere se implementa con un certificado autofirmado para VASA Provider. Con esto, solo se puede gestionar una instancia de vCenter Server para los datastores de vVols. Cuando gestionas varias instancias de vCenter Server y quieres habilitar la capacidad de vVols en ellas, necesitas cambiar el certificado autofirmado por un certificado CA personalizado.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con las credenciales de administrador de ONTAP tools for VMware vSphere que proporcionaste durante la implementación.
3. Selecciona **Certificates > VASA Provider o ONTAP tools > Renew** para renovar los certificados.
4. Selecciona **Certificados > Proveedor VASA o ONTAP tools > Actualizar a CA** para actualizar el certificado autofirmado a un certificado de CA personalizado.
 - a. En la ventana emergente, sube los archivos del certificado del servidor, la clave privada del certificado del servidor, el certificado de la CA raíz y el certificado intermedio.
 - b. Introduce el FQDN de la dirección IP del Load Balancer para el que generaste este certificado y actualiza el certificado.



El sistema estará fuera de línea hasta que termine la actualización y se te cerrará la sesión de la interfaz de usuario de ONTAP tools Manager.

Accede a las herramientas de ONTAP para VMware vSphere consola de mantenimiento

Conoce la consola de mantenimiento de las herramientas ONTAP

La consola de mantenimiento de ONTAP tools for VMware vSphere te permite gestionar la configuración de la aplicación, el sistema y la red. Puedes actualizar las contraseñas de administrador y de mantenimiento, generar paquetes de soporte, configurar los niveles de registro, gestionar la configuración de TLS y habilitar el diagnóstico remoto.

Tras implementar ONTAP tools para VMware vSphere, si no puedes acceder a la consola de mantenimiento, instala VMware tools desde el vCenter Server. Inicia sesión usando el `maint` nombre de usuario y la contraseña que configuraste durante la implementación. Usa **nano** para editar archivos en la consola de mantenimiento o en la consola de inicio de sesión root.



Debes establecer una contraseña para el usuario `diag` al habilitar el diagnóstico remoto.

Debes utilizar la pestaña **Resumen** de tus herramientas ONTAP implementadas para VMware vSphere para acceder a la consola de mantenimiento. Cuando seleccionas , la consola de mantenimiento se inicia.

Menú de la consola	Opciones
Configuración de la aplicación	1. Mostrar resumen del estado del servidor 2. Cambiar el nivel de registro para los servicios de ONTAP tools 3. Cambiar el indicador de validación del certificado
Configuración del sistema	1. Reiniciar la máquina virtual 2. Apagar la máquina virtual 3. Cambiar la contraseña del usuario «maint» 4. Cambiar la zona horaria 5. Aumenta el tamaño del disco de la jaula (/jail) 6. Actualizar 7. Instalar VMware Tools

Configuración de red	1. Mostrar la configuración de la dirección IP 2. Mostrar la configuración de búsqueda de nombre de dominio 3. Cambiar la configuración de búsqueda de nombre de dominio 4. Mostrar rutas estáticas 5. Cambiar rutas estáticas 6. Confirmar cambios 7. Hacer ping a un host 8. Restablecer la configuración predeterminada
Soporte y diagnóstico	1. Accede al shell de diagnóstico 2. Habilita el acceso al diagnóstico remoto 3. Proporciona las credenciales de vCenter para la copia de seguridad 4. Haz una copia de seguridad

Configura el acceso remoto de diagnóstico para las herramientas ONTAP

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

Antes de empezar

Activa la extensión VASA Provider para tu instancia de vCenter Server.

Acerca de esta tarea

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

- Solo se permite una cuenta de inicio de sesión por cada activación de SSH.
- El acceso SSH a la cuenta de usuario «diag» se desactiva cuando ocurre una de las siguientes situaciones:

- Se agota el tiempo.

La sesión de inicio de sesión caduca a medianoche del día siguiente.

- Vuelves a iniciar sesión como usuario «diag» mediante SSH.

Pasos

1. Desde el servidor vCenter, abre una consola para VASA Provider.
2. Inicia sesión como usuario de mantenimiento.
3. Introduce 4 para seleccionar **Asistencia técnica y diagnóstico**.
4. Introduce 2 para seleccionar **Habilitar acceso remoto para diagnósticos**.
5. Escribe `y` en el cuadro de diálogo de confirmación para habilitar el acceso al diagnóstico remoto.

6. Introduce una contraseña para acceder al diagnóstico remoto.

Inicia SSH en otros nodos de ONTAP tools

Debes iniciar SSH en los demás nodos antes de realizar la actualización.

Antes de empezar

Activa la extensión VASA Provider para tu instancia de vCenter Server.

Acerca de esta tarea

Repite este procedimiento en cada nodo antes de actualizar.

Pasos

1. Desde el servidor vCenter, abre una consola para VASA Provider.
2. Inicia sesión como usuario de mantenimiento.
3. Introduce 4 para seleccionar Soporte y diagnóstico.
4. Escribe 1 para seleccionar Access diagnostic shell.
5. Introduce `y` para continuar.
6. Ejecuta el comando `sudo systemctl restart ssh`.

Actualiza las credenciales de vCenter Server en ONTAP tools

Puedes actualizar las credenciales de la instancia de vCenter Server usando la consola de mantenimiento.

Antes de empezar

Debes disponer de las credenciales de acceso de usuario de mantenimiento.

Acerca de esta tarea

Si cambiaste las credenciales de vCenter Server después de la implementación, actualízalas usando este procedimiento.

Pasos

1. Desde el servidor vCenter, abre una consola para VASA Provider.
2. Inicia sesión como usuario de mantenimiento.
3. Teclea 2 para seleccionar el menú de configuración del sistema.
4. Introduce 8 para cambiar las credenciales de vCenter.

Cambia el indicador de validación de certificados en ONTAP tools

De forma predeterminada, el indicador de validación de certificados está activado (establecido en "true"). Puedes establecer el indicador de validación de certificados del backend de almacenamiento ONTAP en "false" si necesitas omitir las comprobaciones de certificados SAN. Esta configuración no es aplicable a los certificados de vCenter Server.

Antes de empezar

Debes disponer de las credenciales de acceso de usuario de mantenimiento.

Pasos

1. Desde el servidor vCenter, abre una consola para ONTAP tools.
2. Inicia sesión como usuario de mantenimiento.
3. Introduce 1 para seleccionar el menú **Configuración de la aplicación**.
4. Introduce 3 para cambiar el indicador de validación del certificado.

La consola de mantenimiento muestra el estado del indicador de validación del certificado y te pide que lo cambies.

5. Teclea «y» para activar o desactivar la opción o «n» para cancelar.

Al habilitar el indicador de validación de certificados (establecido en true), ONTAP tools comprueba que todos los backends de almacenamiento usen certificados con un Subject Alternative Name (SAN). Si algún backend usa un certificado sin un SAN, no puedes habilitar la validación de certificados. Antes de habilitar este indicador, verifica que todos los backends de almacenamiento usen certificados basados en SAN. Si desactivas el indicador de validación de certificados (establecido en false), ONTAP tools omite la validación de certificados para todos los backends de almacenamiento configurados.

Verifica los certificados basados en SAN para backends de almacenamiento

Para garantizar una comunicación segura y una validación adecuada, verifica que todos los backends de almacenamiento usen certificados basados en SAN:

1. Verifica que el certificado de gestión de ONTAP incluya una entrada Subject Alternative Name (SAN).
2. Confirma que las entradas SAN coinciden con la dirección IP de gestión de ONTAP, el nombre DNS o ambos.
3. Asegúrate de que los datos usados para incorporar ONTAP coincidan con la dirección IP o el nombre DNS en la entrada SAN del certificado.

Seguir estos pasos ayuda a evitar problemas de validación de certificados y asegura que el sistema ONTAP esté integrado de forma segura.

El siguiente ejemplo de certificado muestra la información descodificada:

```
HG8u6GK r2JJonWe/kjoKTUnkjwW7feDI747RUuFrthcvTDqhBNWL76jihNp1VX7
v0SDWMaVdecTeU1X/1X3qMxIL+tU4p9SbKVpQw6hJM/zi0LNC784EYIOSQ7qVob
6f21mfP0JHbqs5fLim9NFFUu2DQIDAQA8oQw0jBABgNVHREEEOT43hwShsSHdKXsgi9z
dGkyMjAtdnNpbS1zcjA1MWUtY2OuY2Rs LmdkbC5lbmdsYWJuZKThcPHauY29nt
BgkqhkiG9wQBAQsFAAOCCAQAEEagptz11RN7PLuJUo-SSQExBsF5/3JHr0+sSIMZDzm
4P24kxbQZbfryy68itKGF4LeAid0hgyxc3y9iv4zK1x85fLNgiTnVqAe8'KYNoyD6
IEWppDUE0eVNZIZQjrz9QjUAAF9ifjq8+SKr'lphoXnYYUiM6utvobPMG8cR8Gca
jiLibiMM01K6rD7Ng+7+ydUCAwBQwMDDwdn8+7RIRdKgwqx9QDLegcC5IL5WFLwbMc
2GBv8VM839m0KUAKXSDGwJBZ5nSHQdNi7MU3AES7Nzkv63kGEQJT/5Wr1DmOwlf
osl4qeeeMRigrAbFL6EHMsOMSP0521rtTrJrjBooB22r0tyDA--
-----END CERTIFICATE-----
```

Certificate Information:

- ✓ Common Name: **test.xyz.com**
- ✓ Subject Alternative Names: IP Address: **xxx.xx.xxx.xxx**, **test.xyz.com**
- ✓ Organization: Self-signed-certificate
- ✓ Organization Unit:
- ✓ Locality: N/A
- ✓ State: N/A
- ✓ Country: XX
- ✓ Valid From: March 8, 2026
- ✓ Valid To: March 7, 2028
- ✓ Issuer: **test.xyz.com**, Self-signed-certificate
- ✓ Serial Number: 640c2752bd2c972c5775180070cfdd2120809ee

Informes de ONTAP tools

El complemento ONTAP tools for VMware vSphere proporciona informes sobre máquinas virtuales y almacenes de datos. Cuando seleccionas el icono del complemento NetApp ONTAP tools for VMware vSphere en la sección de accesos directos del cliente vCenter, la interfaz de usuario te lleva a la página de resumen. Selecciona la pestaña de informes para ver el informe de máquinas virtuales y almacenes de datos.

El informe «Máquinas virtuales» muestra la lista de máquinas virtuales detectadas (que deben tener al menos un disco procedente de almacenes de datos basados en ONTAP) junto con métricas de rendimiento. Al desplegar el registro de la máquina virtual, la interfaz muestra toda la información del almacén de datos relacionada con el disco.

El informe de almacenes de datos enumera los almacenes de datos detectados o reconocidos por ONTAP tools for VMware vSphere que utilizan cualquier almacenamiento ONTAP, con métricas de rendimiento.

Puedes utilizar la opción Gestionar columnas para ocultar o mostrar diferentes columnas.

Gestiona máquinas virtuales

Consideraciones sobre la migración y clonación de máquinas virtuales para ONTAP tools

ONTAP tools for VMware vSphere admiten todos los tipos principales de migración de máquinas virtuales, incluida la migración solo de cómputo (vMotion), solo de almacenamiento (Storage vMotion) y la migración combinada de cómputo y almacenamiento en todos los datastores. Este tema describe las consideraciones clave y las mejores prácticas para garantizar el éxito de la migración y la clonación de máquinas virtuales, independientemente del tipo de datastore subyacente.

Migrar máquinas virtuales protegidas

Puedes migrar máquinas virtuales protegidas a:

- El mismo almacén de datos en un host ESXi diferente
- Un datastore compatible diferente en el mismo host ESXi
- Un datastore compatible diferente en un host ESXi diferente

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

Para obtener información sobre la migración de máquinas virtuales, consulta la documentación de Broadcom: ["vSphere Migración de máquinas virtuales"](#)

Clonar máquinas virtuales protegidas

Puedes clonar máquinas virtuales protegidas en los siguientes destinos:

- El mismo contenedor del mismo volumen FlexVol utilizando un 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 volumen FlexVol diferente utilizando un grupo de replicación

En el volumen FlexVol donde se encuentra la máquina virtual clonada, el archivo de metadatos se actualiza con los detalles de la máquina virtual clonada.

- Un contenedor diferente o almacén de datos vVols

En el volumen FlexVol donde se encuentra la máquina virtual clonada, el archivo de metadatos se actualiza con los detalles de la máquina virtual.

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

Se admite un clon de un clon de una máquina virtual protegida.

Consulta la documentación de Broadcom: ["Creación de una máquina virtual para clonar"](#) para más detalles.

Instantáneas de máquinas virtuales

Las herramientas ONTAP admiten instantáneas de máquinas virtuales a través de flujos de trabajo estándar de VMware. Las instantáneas son puntos de reversión a corto plazo pensados para casos de uso como pruebas y preparación de parches. No sustituyen la protección de datos basada en copias de seguridad o replicación. Ejecutar una máquina virtual en una instantánea durante periodos prolongados puede provocar inestabilidad y pérdida de datos.

Puedes tomar snapshots consistentes con fallos (snapshots sin estado de memoria, que pueden usarse para reiniciar la máquina virtual a un estado consistente) en todos los tipos de datastore compatibles. También se admiten snapshots en reposo, que usan VMware Tools para volcar los datos en memoria al disco antes de capturar. Para una visión general de los tipos de snapshots y su comportamiento, consulta ["Visión general de las instantáneas de máquinas virtuales en vSphere"](#).



Las instantáneas de memoria capturan el estado de la memoria en ejecución y aturden temporalmente la máquina virtual. No están soportadas en los flujos de trabajo de ONTAP tools. Si una máquina virtual tiene una instantánea de memoria, debes eliminarla antes de que la máquina virtual pueda incluirse en un grupo de consistencia o en una relación de clúster de host gestionada por ONTAP tools.

En los sistemas de almacenamiento ASA r2, el comportamiento de las instantáneas de máquinas virtuales difiere de otros tipos de almacenamiento. Las instantáneas son de solo lectura. Cuando enciendes la máquina virtual, VASA Provider crea un LUN a partir de la instantánea de solo lectura y habilita las IOPS. Cuando apagas la máquina virtual, VASA Provider elimina el LUN y deshabilita las IOPS.

Para obtener información sobre la gestión de instantáneas de máquinas virtuales, consulta la documentación de Broadcom ["Administra máquinas virtuales con instantáneas"](#).

Migra máquinas virtuales a almacenes de datos vVols en ONTAP tools

Puedes migrar máquinas virtuales desde almacenes de datos NFS y VMFS a almacenes de datos de Virtual Volumes (vVols) para aprovechar la gestión de máquinas virtuales basada en políticas y otras capacidades de vVols. Los almacenes de datos de vVols te permiten satisfacer los crecientes requisitos de las cargas de trabajo.

Antes de empezar

Asegúrate de que VASA Provider no se esté ejecutando en ninguna de las máquinas virtuales que tengas previsto migrar. Si migras una máquina virtual en la que se está ejecutando VASA Provider a un almacén de datos vVols, no podrás realizar ninguna operación de gestión, incluido encender las máquinas virtuales que estén en almacenes de datos vVols.

Acerca de esta tarea

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

Pasos

1. Haz clic con el botón derecho del ratón en la máquina virtual que quieras migrar y selecciona **Migrar**.
2. Selecciona **Solo cambiar almacenamiento** y luego selecciona **Siguiente**.
3. Selecciona un formato de disco virtual, una política de almacenamiento de máquinas virtuales y un almacén de datos vVol que se ajuste a las características del almacén de datos que vas a migrar.

4. Revisa la configuración y selecciona **Finalizar**.

Limpia las configuraciones VASA en ONTAP tools

Para completar el proceso de limpieza de VASA, sigue estos pasos.



Se recomienda eliminar cualquier almacén de datos de vVols antes de iniciar la limpieza de VASA.

Pasos

1. Desregistra el complemento entrando en https://OTV_IP:8143/Register.html
2. Comprueba que el complemento ya no esté disponible en el servidor vCenter.
3. Apaga las ONTAP tools for VMware vSphere VM.
4. Elimina ONTAP tools for VMware vSphere VM.

Conectar o desconectar un disco de datos de una máquina virtual en ONTAP tools

Sigue estos pasos para conectar o desconectar discos de datos de máquinas virtuales en vSphere y gestionar sus recursos de almacenamiento.

Conectar un disco de datos a una máquina virtual

Conecta un disco de datos a una máquina virtual para añadir más almacenamiento.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Haz clic con el botón derecho del ratón sobre una máquina virtual en el inventario y selecciona **Editar configuración**.
3. En la pestaña **Hardware virtual**, selecciona **Disco duro existente**.
4. Selecciona la máquina virtual en la que se encuentra el disco.
5. Selecciona el disco que quieras conectar y selecciona el botón **OK**.

Resultado

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

Desconectar un disco de datos de la máquina virtual

Desconecta un disco de datos de una máquina virtual cuando ya no lo necesites. El disco no se elimina; permanece en el sistema de almacenamiento ONTAP.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Haz clic con el botón derecho del ratón sobre una máquina virtual en el inventario y selecciona **Editar configuración**.
3. Pasa el puntero por encima del disco y selecciona **Eliminar**.



El disco se retira de la máquina virtual. Si hay otras máquinas virtuales que compartan el disco, los archivos del disco no se eliminan.

Información relacionada

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

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

Descubre sistemas de almacenamiento y hosts en las herramientas ONTAP

Cuando se inicia por primera vez ONTAP tools for VMware vSphere en el vSphere Client, detecta automáticamente los hosts ESXi, sus LUN y exportaciones NFS asociadas, así como los sistemas de almacenamiento NetApp que poseen estos recursos.

Antes de empezar

- Asegúrate de que todos los hosts ESXi estén encendidos y conectados.
- Asegúrate de que todas las máquinas virtuales de almacenamiento (SVM) que se vayan a detectar estén en funcionamiento y de que cada nodo del clúster tenga configurada al menos una LIF de datos para el protocolo de almacenamiento que se utilice (NFS o iSCSI).

Acerca de esta tarea

Puedes descubrir nuevos sistemas de almacenamiento o actualizar los ya existentes para obtener la información más reciente sobre capacidad y configuración. También puedes cambiar las credenciales de ONTAP tools for VMware vSphere para acceder al sistema de almacenamiento.

Mientras detecta los sistemas de almacenamiento, ONTAP tools for VMware vSphere recopila información de los hosts ESXi gestionados por la instancia de vCenter Server.

Pasos

1. Desde la página de inicio del vSphere Client, selecciona **Hosts and Clusters**.
2. Haz clic con el botón derecho en el centro de datos que necesites y selecciona **NetApp ONTAP tools > Update Host Data**.

En el cuadro de diálogo **Confirmar**, confirma tu elección.

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

Una vez finalizado el proceso de descubrimiento, realiza las siguientes acciones:

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

Modificar la configuración del host ESXi usando ONTAP tools

Utiliza el panel de herramientas de ONTAP en VMware vSphere para identificar problemas de configuración, seleccionar hosts ESXi, revisar los ajustes recomendados de NetApp y aplicarlos.

Antes de empezar

El portlet de sistemas host ESXi muestra los problemas relacionados con la configuración de los hosts ESXi. Selecciona un problema para ver el nombre de host o la dirección IP.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. En la página de accesos directos, selecciona **NetApp ONTAP tools** en la sección de complementos.
3. Accede al portlet **Cumplimiento del host ESXi** en la vista general (panel de control) del complemento ONTAP tools for VMware vSphere.
4. Selecciona el enlace **Aplicar la configuración recomendada**.
5. En la ventana **Aplicar la configuración recomendada para los hosts**, selecciona los hosts para los que quieras usar la configuración recomendada de NetApp y selecciona **Siguiente**.



Puedes expandir el host ESXi para ver los valores actuales.

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

Información relacionada

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

Gestionar contraseñas

Cambiar la contraseña de ONTAP tools Manager

Puedes cambiar la contraseña de administrador usando ONTAP tools Manager.

Pasos

1. Inicia ONTAP tools Manager desde un navegador web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Inicia sesión con tus credenciales de administrador de ONTAP tools for VMware vSphere.
3. Selecciona el icono **administrador** en la esquina superior derecha de la pantalla y selecciona **Cambiar contraseña**.
4. En la ventana emergente para cambiar la contraseña, introduce la contraseña antigua y la nueva. La pantalla de la interfaz de usuario muestra los requisitos de la contraseña.
5. Selecciona **Cambiar** para aplicar los cambios.

Restablecer la contraseña de ONTAP tools Manager

Si olvidas la contraseña de ONTAP tools Manager, puedes recuperar el acceso de administrador utilizando un token de restablecimiento generado desde la consola de mantenimiento de ONTAP tools for VMware vSphere.

Pasos

1. Abre un navegador web y ve a <https://<ONTAPtoolsIP>:8443/virtualization/ui/> para acceder a ONTAP tools Manager.
2. En la página de inicio de sesión, selecciona **Restablecer contraseña**.
3. Genera un token de restablecimiento de contraseña usando las ONTAP tools for VMware vSphere maintenance console:
 - a. Inicia sesión en el servidor vCenter y abre la consola de mantenimiento.
 - b. Introduce 2 para seleccionar **Configuración del sistema**.
 - c. Introduce 3 para seleccionar **Cambiar la contraseña del usuario «maint»**.
4. En el cuadro de diálogo de restablecimiento de contraseña, introduce el código de restablecimiento, el nombre de usuario y la nueva contraseña.
5. Selecciona **Restablecer** para actualizar las credenciales.
6. Inicia sesión en ONTAP tools Manager con la nueva contraseña.

Restablecer la contraseña de usuario de la aplicación en ONTAP tools

Sigue estos pasos para restablecer la contraseña de usuario de la aplicación necesaria para el registro de SRA y VASA Provider con vCenter Server usando ONTAP tools for VMware vSphere.

Pasos

1. Abre un navegador web y ve a: <https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Inicia sesión con las credenciales de administrador configuradas durante la implementación de ONTAP tools.
3. En la barra lateral, selecciona **Configuración**.
4. En la página **Credenciales de VASA/SRA**, selecciona **Restablecer contraseña**.
5. Introduce y confirma la nueva contraseña.
6. Selecciona **Restablecer** para aplicar la nueva contraseña.

Restablece la contraseña de la consola de mantenimiento de las ONTAP tools

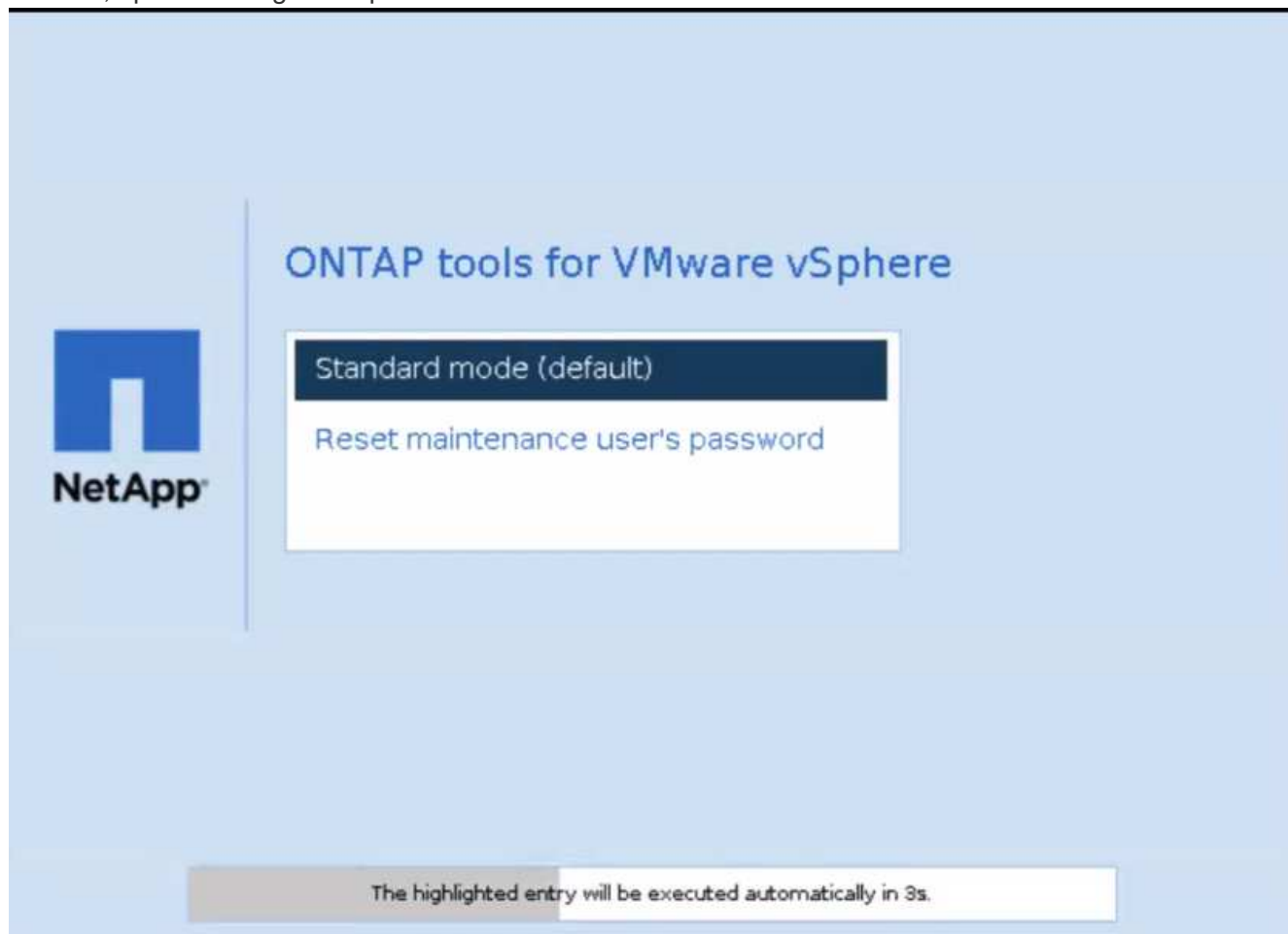
Durante una operación de reinicio del SO huésped, el menú GRUB muestra una opción para restablecer la contraseña de usuario de la consola de mantenimiento. Usa esta opción para actualizar la contraseña de usuario de la consola de mantenimiento en la VM. Después de restablecer la contraseña, la VM se reinicia para establecer la nueva contraseña. En un escenario de implementación en HA, después del reinicio de la VM, la contraseña se actualiza automáticamente en las otras dos VMs.



Para la implementación HA de ONTAP tools for VMware vSphere, debes cambiar la contraseña de usuario de la consola de mantenimiento en el nodo de gestión de ONTAP tools, que es node1.

Pasos

1. Inicia sesión en tu servidor vCenter
2. Haz clic con el botón derecho en la VM y selecciona **Power > Restart Guest OS**. Durante el reinicio del sistema, aparece la siguiente pantalla:



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

3. Selecciona la opción **Restablecer la contraseña del usuario de mantenimiento**. Se abre la consola de mantenimiento.
4. En la consola, introduce y confirma la nueva contraseña. Tienes tres intentos. El sistema se reinicia después de que introduzcas correctamente la nueva contraseña.
5. Pulsa **Intro** para continuar. El sistema actualiza la contraseña en la máquina virtual.



Aparece el mismo menú GRUB cuando enciendes la máquina virtual. Sin embargo, deberías usar la opción de restablecer contraseña solo con la opción **Restart Guest OS**.

Gestiona la protección del clúster de hosts

Modifica un clúster de hosts protegidos en ONTAP tools

Puedes modificar la configuración de protección de un clúster de hosts en un único flujo de trabajo. Se admiten los siguientes cambios:

- Agrega nuevos almacenes de datos o hosts al clúster protegido.
- Agrega nuevas relaciones de SnapMirror a la configuración de protección.
- Elimina las relaciones existentes de SnapMirror de la configuración de protección.
- Modifica una relación existente de SnapMirror.



Necesitas realizar una detección de almacenamiento después de crear, editar o eliminar la protección de un clúster de hosts para reflejar los cambios. Si no realizas la detección de almacenamiento, los cambios se reflejarán después de que se active la detección periódica de almacenamiento.

Supervisar la protección del clúster de hosts

Supervisa el estado de protección, las relaciones de SnapMirror, los datastores y el estado de SnapMirror de cada clúster de hosts protegidos.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Ve a **NetApp ONTAP tools > Protección > Relaciones entre clústeres de hosts**.

La columna de protección muestra un icono que indica el estado de la protección.

3. Pasa el cursor por encima del icono para ver más detalles.

Agrega nuevos almacenes de datos o hosts

Añade hosts o crea almacenes de datos en el clúster protegido usando la interfaz de usuario de vCenter.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Para editar las propiedades de un clúster protegido, puedes
 - a. Ve a **NetApp ONTAP tools > Protección > Relaciones entre clústeres de hosts**, selecciona el menú de tres puntos situado junto al clúster y selecciona **Editar** o
 - b. Haz clic con el botón derecho en un clúster de hosts y selecciona **NetApp ONTAP tools > Protect Cluster**.
3. Si creas un almacén de datos en la interfaz de usuario de vCenter, aparece como desprotegido. Puedes ver todos los almacenes de datos del clúster y su estado de protección en un cuadro de diálogo. Selecciona el botón **Proteger** para activar la protección.



Tras crear un almacén de datos en la interfaz de usuario de vCenter Server, selecciona **Detectar** en la página de resumen para que el almacén de datos aparezca como candidato a protección en el clúster de hosts. El estado de protección se actualiza a protegido después de la siguiente detección periódica de protección.

4. Si añades un nuevo host ESXi, el estado de protección se muestra como parcialmente protegido. Selecciona el menú de los tres puntos debajo de la configuración de SnapMirror y selecciona **Editar** para establecer la proximidad del host ESXi recién añadido.



En el caso de las relaciones asíncronas, la edición no es compatible en ONTAP tools porque el SVM de destino de un sitio terciario no se puede añadir a la misma instancia. Para modificar la configuración de la relación, usa System Manager o la CLI en el SVM de destino.

5. Después de hacer cambios, selecciona **Guardar**.
6. Puedes ver los cambios en la ventana **Protect Cluster**.

ONTAP tools crea una tarea de vCenter, y puedes seguir su progreso en el panel **Tareas recientes**.

Agrega una nueva relación de SnapMirror

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Para editar las propiedades de un clúster protegido, puedes
 - a. Ve a **NetApp ONTAP tools > Protección > Relaciones entre clústeres de hosts**, selecciona el menú de puntos suspensivos junto al clúster y selecciona **Editar** o
 - b. Haz clic con el botón derecho en un clúster de hosts y selecciona **NetApp ONTAP tools > Protect Cluster**.
3. Selecciona **Add relationship**.
4. Agrega una nueva relación como tipo de política **Asynchronous** o **AutomatedFailOverDuplex**.
5. Selecciona **Protect**.

Puedes ver los cambios en la ventana **Protect Cluster**.

ONTAP tools crea una tarea de vCenter, y puedes seguir su progreso en el panel **Tareas recientes**.

Eliminar una relación existente de SnapMirror

Para eliminar una relación asíncrona de SnapMirror, asegúrate de que el SVM o clúster del sitio secundario esté añadido como backend de almacenamiento en ONTAP tools for VMware vSphere. No puedes eliminar todas las relaciones de SnapMirror a la vez. Al eliminar una relación, también se elimina la relación correspondiente del clúster ONTAP. Cuando eliminas una relación Automated Failover Duplex SnapMirror, el sistema desasigna los datastores de destino y elimina el grupo de consistencia, los LUN, los volúmenes y los igroups del clúster ONTAP de destino.

Al eliminar la relación, el sistema vuelve a escanear el sitio secundario para eliminar el LUN no asignado como ruta activa de los hosts.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Para editar las propiedades de un clúster protegido, puedes
 - a. Ve a **NetApp ONTAP tools > Protección > Relaciones entre clústeres de hosts**, selecciona el menú de puntos suspensivos junto al clúster y selecciona **Editar** o
 - b. Haz clic con el botón derecho en un clúster de hosts y selecciona **NetApp ONTAP tools > Protect Cluster**.
3. Selecciona el menú de los tres puntos debajo de la configuración de SnapMirror y selecciona **Eliminar**.
 - Si eliminas una relación asíncrona basada en políticas de un clúster de hosts protegidos, debes eliminar manualmente los elementos de almacenamiento del clúster de almacenamiento terciario. Los elementos de almacenamiento incluyen grupos de consistencia, volúmenes (para sistemas ONTAP), unidades de almacenamiento (LUN/Namespaces) e instantáneas.
 - Si eliminas una relación basada en políticas de conmutación automática al respaldo (AFD) de un clúster de hosts protegidos, puedes optar por eliminar los elementos de almacenamiento asociados en el almacenamiento secundario directamente desde la interfaz.
 - Si eliminas una relación basada en políticas de Automated Failover Duplex (AFD) y el grupo de consistencia ahora es jerárquico para las copias de seguridad a nivel de aplicación, aparece una advertencia sobre el impacto en las copias de seguridad. Confirma para continuar. Después de confirmar, elimina los elementos de almacenamiento asociados en el almacenamiento secundario. Si no los eliminas, permanecen en el sitio secundario.

ONTAP tools crea una tarea de vCenter, y puedes seguir su progreso en el panel **Tareas recientes**.

Modificar una relación existente de SnapMirror

Para modificar una relación asíncrona de SnapMirror, asegúrate de que el SVM o clúster del sitio secundario esté añadido como backend de almacenamiento en ONTAP tools for VMware vSphere. Para las relaciones Automated Failover Duplex SnapMirror, puedes actualizar la proximidad del host para configuraciones uniformes o el acceso al host para configuraciones no uniformes. No se admite cambiar entre los tipos de política Asynchronous y Automated Failover Duplex. Puedes configurar los ajustes de proximidad o acceso para los hosts recién detectados en el clúster.



No puedes editar una relación asíncrona existente de SnapMirror.

Pasos

1. Inicia sesión en el cliente de vSphere.
2. Para editar las propiedades de un clúster protegido, puedes
 - a. Ve a **NetApp ONTAP tools > Protección > Relaciones entre clústeres de hosts**, selecciona el menú de puntos suspensivos junto al clúster y selecciona **Editar** o
 - b. Haz clic con el botón derecho en un clúster de hosts y selecciona **NetApp ONTAP tools > Protect Cluster**.
3. Si se selecciona el tipo de política AutomatedFailOverDuplex, añade los datos de proximidad o de acceso al host.
4. Selecciona el botón **Proteger**.

Las herramientas de ONTAP crean una tarea de vCenter. Sigue su progreso en el panel **Tareas recientes**.

Eliminar la protección de clúster de host en ONTAP tools

Al desactivar la protección del clúster de hosts, los almacenes de datos quedan desprotegidos.

Pasos

1. Para ver la lista de clústeres de hosts protegidos, ve a **NetApp ONTAP tools > Protección > Relaciones de clústeres de hosts**.

En esta página, puedes supervisar los clústeres de host protegidos, el estado de protección, la relación SnapMirror y el estado. Selecciona los grupos de coherencia para ver la capacidad, los almacenes de datos asociados y los grupos secundarios.

2. En la ventana **Protección del clúster de host**, selecciona el menú de puntos suspensivos junto al clúster y selecciona **Eliminar protección**.
 - Si quitas la protección de un clúster de hosts que solo tiene una relación asíncrona de SnapMirror, debes eliminar manualmente los elementos de almacenamiento. Los elementos de almacenamiento incluyen grupos de consistencia, volúmenes (para sistemas ONTAP), unidades de almacenamiento (LUN) e instantáneas.
 - Si quitas la protección de un clúster de hosts que solo tiene una relación de políticas de SnapMirror basada en dúplex con conmutación automática al respaldo y un grupo de consistencia no jerárquico, puedes eliminar los elementos de almacenamiento asociados en el almacenamiento secundario directamente desde la misma pantalla.
 - Si quitas la protección de un clúster de hosts que tiene tanto políticas de SnapMirror como un grupo de consistencia jerárquico para copias de seguridad, aparecerá una advertencia sobre los impactos en las copias de seguridad. Confirma para continuar. Después de confirmar, elimina los elementos de almacenamiento asociados en el almacenamiento secundario. Si no limpias, los elementos de almacenamiento permanecerán en el sitio secundario.

Recupera la configuración de las herramientas de ONTAP

A partir de ONTAP tools for VMware vSphere 10.5, la función de copia de seguridad está activada de forma predeterminada.

El almacén de datos donde implementas ONTAP tools for VMware vSphere máquinas virtuales almacena los archivos de copia de seguridad. Una carpeta con el nombre de la dirección IP de ONTAP tools (los puntos se reemplazan por guiones bajos y se añade el sufijo *OTV_backup*) guarda los dos archivos de copia de seguridad más recientes (*OTV_backup_1.tar.enc* y *OTV_backup_2.tar.enc*) y un archivo de información (*OTV_backup_info.txt*) que contiene el nombre de la copia de seguridad más reciente.

Asegúrate de que la nueva máquina virtual utilice la misma dirección IP de ONTAP tools y coincida con la configuración inicial del sistema, incluidos los servicios habilitados, el tamaño del nodo y el modo HA.

Pasos

1. Descarga los archivos de copia de seguridad del almacén de datos de la máquina virtual original a tu sistema local.
 - a. Ve a la sección de almacenamiento y elige el almacén de datos que contiene los archivos de copia de seguridad de la máquina virtual.
 - b. Selecciona la sección **Archivos**.
 - c. Descarga el directorio de copia de seguridad necesario.

2. Apaga la máquina virtual actual. Luego, implementa una nueva máquina virtual usando el mismo archivo OVA que en la implementación original.
3. Desde el servidor vCenter, abre la consola de mantenimiento.
4. Inicia sesión como usuario de mantenimiento.
5. Introduce 4 para seleccionar **Asistencia técnica y diagnóstico**.
6. Accede a 2 para seleccionar la opción **Habilitar acceso de diagnóstico remoto** y crear una nueva contraseña para el acceso de diagnóstico.
7. Selecciona un archivo de copia de seguridad del directorio de descargas. Consulta el archivo `OTV_backup_info.txt` para identificar la copia de seguridad más reciente.
8. Utiliza el siguiente comando para transferir el archivo de copia de seguridad a la nueva máquina virtual. Cuando se te solicite, introduce la contraseña de diagnóstico.

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



No modifies la ruta de destino ni el nombre del archivo (/home/diag/system_recovery.tar.enc) que se mencionan en el comando.

9. Una vez transferido el archivo de copia de seguridad, inicia sesión en el shell de diagnóstico y ejecuta el siguiente comando:

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

Los registros se guardan en el archivo `/var/log/post-deploy-upgrade.log`.

Después de completar la recuperación, ONTAP tools restaura los servicios y los objetos de vCenter.

Desinstala ONTAP tools

Al desinstalar las herramientas de ONTAP para VMware vSphere, se eliminan todos los datos de las herramientas.

Pasos

1. Elimina o mueve todas las máquinas virtuales de los almacenes de datos gestionados por ONTAP tools for VMware vSphere.
 - Para eliminar las máquinas virtuales, consulta ["Eliminar y volver a registrar máquinas virtuales y plantillas de máquinas virtuales"](#)
 - Para moverlos a un almacén de datos no gestionado, consulta ["Cómo migrar tu máquina virtual con almacenamiento vMotion"](#)
2. ["Eliminar almacenes de datos"](#) creado en ONTAP tools for VMware vSphere.
3. Si has habilitado el proveedor VASA, selecciona **Configuración > Configuración del proveedor VASA > Darse de baja** en ONTAP tools para dar de baja a los proveedores VASA de todos los servidores vCenter.
4. Desvincula todos los backends de almacenamiento de la instancia de vCenter Server. Consulta

["Desvincula los backends de almacenamiento de la instancia de vCenter Server"](#).

5. Elimina todos los backends de almacenamiento. Consulta ["Gestiona los sistemas de almacenamiento subyacentes"](#).
6. Elimina el adaptador SRA de VMware Live Site Recovery:
 - a. Inicia sesión como admin en la interfaz de gestión del dispositivo VMware Live Site Recovery usando el puerto 5480.
 - b. Selecciona **Adaptadores de replicación de almacenamiento**.
 - c. Selecciona la tarjeta SRA correspondiente y, en el menú desplegable, selecciona **Eliminar**.
 - d. Confirma que conoces los resultados de eliminar el adaptador y selecciona **Eliminar**.
7. Elimina las instancias del servidor vCenter integradas en ONTAP tools for VMware vSphere. Consulta ["Gestiona instancias de vCenter Server"](#).
8. Apaga las ONTAP tools for VMware vSphere VMs desde el vCenter Server y elimina las VMs.

¿Y ahora qué?

["Eliminar volúmenes FlexVol"](#)

Elimina los volúmenes FlexVol después de desinstalar ONTAP tools

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

Pasos

1. Consulta el tipo de implementación de ONTAP tools for VMware vSphere desde la máquina virtual del nodo de gestión de ONTAP tools. Ejecuta el siguiente comando para comprobar el tipo de implementación:
`cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol`

Si se trata de una implementación iSCSI, elimina también los igroups.
2. Obtén la lista de volúmenes FlexVol. `kubectl describe persistentvolumes | grep internalName | awk -F'=' '{print $2}'`
3. Retira las máquinas virtuales del vCenter Server. Consulta ["Eliminar y volver a registrar máquinas virtuales y plantillas de máquinas virtuales"](#).
4. Elimina volúmenes FlexVol. Consulta ["Eliminar un volumen FlexVol"](#). Introduce el nombre exacto del volumen FlexVol en el comando de la CLI para eliminar un volumen.
5. Elimina los grupos SAN del sistema de almacenamiento ONTAP en caso de despliegue iSCSI. Consulta ["Ver y gestionar iniciadores SAN e igroups"](#).

Actualiza ONTAP tools para VMware vSphere

Actualiza desde ONTAP tools for VMware vSphere 10.x a 10.5

Puedes actualizar desde ONTAP tools for VMware vSphere 10.3 o 10.4 a 10.5. Sin embargo, para actualizar desde ONTAP tools 10.0, 10.1 o 10.2 a 10.5, primero debes actualizar a 10.3 o 10.4 antes de pasar a 10.5.



- En los sistemas ASA r2, asegúrate de actualizar ONTAP tools for VMware vSphere a la versión 10.5 y ONTAP a la 9.16.1 antes de configurar más zonas de disponibilidad de almacenamiento (SAZ).
- Si la actualización de ONTAP tools for VMware vSphere 10.3 o 10.4 a 10.5 falla, no puedes revertirla. Usa un RPO bajo o la recuperación por instantánea para restaurar la configuración. Para ONTAP tools for VMware vSphere 10.2 y anteriores, usa RPO cero para restaurar la configuración.

Antes de empezar

- Asegúrate de que todos los nodos estén activos.
- Asegúrate de que el certificado del sistema ONTAP y los certificados de vCenter integrados sean válidos por al menos 5 días. Si los certificados caducan antes, la actualización falla.
- Asegúrate de que todos los nodos tengan un quinto disco con una capacidad de 100 GB.
- Comprueba que la configuración del nodo se ajuste a las especificaciones que figuran en la tabla siguiente.

Tipo de implementación	CPU (núcleo) por nodo	Memoria (GB) por nodo	Espacio en disco (GB) por nodo	Total de CPU (núcleos)	Memoria (GB)	Espacio total en disco (GB)
Small (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

- Asegúrate de que la función de conexión en caliente para la CPU y la RAM esté activada.
- Activa la copia de seguridad con un RPO bajo y asegúrate de que haya una copia de seguridad visible en la interfaz de usuario de vCenter Client. Descarga la carpeta de copia de seguridad antes de la actualización.
- Se recomienda realizar una copia de seguridad con un RPO bajo. Sin embargo, en una implementación sin HA, puedes tomar una instantánea en estado de reposo de la máquina virtual de ONTAP tools antes de actualizar.

Consulta ["Editar la configuración de backup"](#) y ["Recupera la configuración de las herramientas de ONTAP"](#) para obtener más información sobre las copias de seguridad y la recuperación.

Pasos

1. Sube la ISO de actualización de ONTAP tools for VMware vSphere a la biblioteca de contenidos.
2. En la página de la máquina virtual principal, selecciona **Acciones > Editar configuración**. Para identificar el nombre de la máquina virtual principal:
 - a. Habilita el shell de diagnóstico en cualquier nodo
 - b. Ejecuta el siguiente comando:

```
grep sourceHost /opt/netapp/meta/ansible_vars.yaml
```
3. Selecciona el **archivo ISO de la biblioteca de contenidos** en la ventana de configuración, en el campo **CD/DVD drive**.
4. Selecciona el archivo ISO, marca la casilla **Conectado** en el campo **CD/DVD drive** y haz clic en **OK**.
5. Desde el servidor vCenter, abre una consola para ONTAP tools.
6. Inicia sesión como usuario de mantenimiento.
7. Teclea **2** para seleccionar el menú **Configuración del sistema**.
8. Teclea **6** para seleccionar la opción **Upgrade**.
9. Proporciona las credenciales de vCenter cuando se te solicite. Esta es la instancia de vCenter donde se alojan las ONTAP tools.

Si estás usando las herramientas ONTAP en una topología de dos vCenter Server, donde el appliance se aloja en una instancia de vCenter y gestiona otra, puedes asignar un rol restringido para la instancia de vCenter que aloja las herramientas ONTAP. Puedes crear un usuario y un rol dedicados de vCenter con solo los permisos necesarios para el despliegue de plantillas OVF. Para más detalles, consulta los roles listados en "[Roles incluidos con ONTAP tools for VMware vSphere 10](#)".

Para la instancia de vCenter que será gestionada por ONTAP tools, asegúrate de que la cuenta de usuario de vCenter tenga privilegios de administrador.

Durante la actualización, si alguno de los certificados del backend de almacenamiento integrado carece de entradas de «Nombre alternativo del sujeto» (SAN), aparecerá un mensaje indicando el SAN que falta. Si decides continuar sin validar el SAN, la actualización seguirá adelante, pero no es recomendable debido a los posibles riesgos de seguridad.

10. Al actualizar, se realizan automáticamente las siguientes acciones:
 - a. El certificado de la puerta de enlace se renueva con un periodo de validez de un año. Al eliminar el adaptador SRA anterior y subir el nuevo adaptador 10.5, la validez del certificado SRA pasa de 10 años a 1 año.
 - b. Se ha actualizado el complemento remoto
 - c. Se validan los certificados de ONTAP y del servidor vCenter y se añaden a ONTAP tools
 - d. La copia de seguridad está activada

Qué sigue

Después de actualizar a ONTAP tools for VMware vSphere 10.5:

- Supervisa las alertas del sistema y planifica renovar el certificado de la pasarela antes de que caduque dentro de un año.
- Elimina el adaptador SRA de ONTAP tools 10.4 o 10.3 y carga el archivo tar del adaptador SRA 10.5.
- Ejecuta el comando de instalación después de cargar el archivo tar del adaptador SRA. Luego, vuelve a escanear los adaptadores SRA para actualizar la página de Adaptadores de replicación de

Tras la actualización, podrás:

- Desactiva los servicios desde la interfaz de usuario del manager
- Pasar de una configuración sin alta disponibilidad (HA) a una configuración con alta disponibilidad (HA)
- Amplía una configuración pequeña sin alta disponibilidad (HA) a una configuración mediana sin alta disponibilidad (HA), o a una configuración mediana o grande con alta disponibilidad (HA).

Información relacionada

["Migra desde ONTAP tools for VMware vSphere 9.xx a 10.5"](#)

Códigos de error de actualización de ONTAP tools

Es posible que aparezcan códigos de error durante la operación de actualización de ONTAP tools for VMware vSphere. Los códigos de error constan de cinco dígitos, donde los dos primeros indican el script en el que se produjo el problema y los tres últimos representan el flujo de trabajo específico dentro de ese script.

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



Los códigos de error proporcionados en esta página son solo de referencia. Contacta al equipo de soporte si el error persiste o si no se menciona una resolución.

En la siguiente tabla se enumeran los códigos de error y los nombres de archivo correspondientes.

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

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

Código de error de actualización	Flujo de trabajo	Resolución
052	La versión ISO puede ser la misma que la actual o estar dos versiones por encima de la actual.	Utiliza una versión ISO compatible para actualizar desde tu versión actual.
068	Ha fallado la reversión de los paquetes de Debian	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
069	Error al restaurar los archivos	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
070	No se pudo eliminar la copia de seguridad	-
071	El clúster de Kubernetes no estaba en buen estado	-
074	Error al montar el archivo ISO	Comprueba el archivo <code>/var/log/upgrade-run.log</code> y vuelve a intentar la actualización.
075	Las comprobaciones previas a la actualización han fallado	Vuelve a intentar la actualización.
076	La actualización del registro ha fallado	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
077	La reversión del registro ha fallado	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
078	La actualización del operador ha fallado	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
079	Error al revertir el operador	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
080	La actualización de los servicios ha fallado	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
081	La reversión de los servicios ha fallado	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
082	No se pudieron eliminar las imágenes antiguas del contenedor	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
083	No se ha podido eliminar la copia de seguridad	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.

Código de error de actualización	Flujo de trabajo	Resolución
084	No se pudo cambiar JobManager de nuevo a Production	Sigue estos pasos para recuperar o completar la actualización. 1. Activa el shell de diagnóstico 2. Ejecuta el comando: <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Revisa los registros en /var/log/post-deploy-upgrade.log
087	Los pasos posteriores a la actualización fallaron.	Sigue estos pasos para recuperar o completar la actualización. 1. Activa el shell de diagnóstico 2. Ejecuta el comando <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Revisa los registros en /var/log/post-deploy-upgrade.log
088	Error al configurar la rotación de registros para journald	Verifica la configuración de red de la VM compatible con el host en el que está alojada la VM. Puedes intentar migrar la VM a otro host y reiniciarla.
089	Error al cambiar el propietario del archivo de configuración de rotación del registro de resumen	Vuelve a intentar la actualización.
095	Error en la actualización del sistema operativo	No hay recuperación tras la actualización del sistema operativo. Los servicios de ONTAP tools se actualizan y se ejecutarán nuevos pods.
096	Instala el proveedor de almacenamiento dinámico	Consulta los registros de actualización y vuelve a intentar la actualización.
097	Error al desinstalar los servicios para la actualización	Utiliza una recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
098	Error al copiar el secreto "dockercred" de "ntv-system" al espacio de nombres del proveedor de almacenamiento dinámico	Consulta los registros de actualización y vuelve a intentar la actualización.
099	No se pudo validar la incorporación del nuevo disco duro	Agrega el nuevo HDD a todos los nodos en caso de HA y a un solo nodo en caso de una implementación sin HA.
109	Error al hacer copia de seguridad de los datos del volumen persistente	Consulta los registros de actualización y vuelve a intentar la actualización.

Código de error de actualización	Flujo de trabajo	Resolución
110	Error al restaurar los datos del volumen persistente	Utiliza la recuperación con RPO cero o basada en instantáneas y vuelve a intentar la actualización.
111	Error al actualizar los parámetros de tiempo de espera de etcd para RKE2	Consulta los registros de actualización y vuelve a intentar la actualización.
112	Error al desinstalar el proveedor de almacenamiento dinámico	-
113	Error al actualizar los recursos en los nodos secundarios	Consulta los registros de actualización y vuelve a intentar la actualización.
104	Ha fallado el reinicio del nodo secundario	Reinicia los nodos manualmente, uno por uno.
100	La reversión del kernel ha fallado	-
051	Ha fallado la actualización del proveedor de almacenamiento dinámico	Comprueba los registros de actualización y vuelve a intentar la actualización.
056	Error al eliminar la copia de seguridad de la migración	NA
090	La validación de certificados para los backends de almacenamiento y vCenter falló	Comprueba los registros de actualización y el archivo de registro en <code>/var/log/cert_validation_error.log</code> y vuelve a intentar la actualización.

Código de error de actualización	Flujo de trabajo	Resolución
114	Falló la actualización interna del certificado en la colección MongoDB	Si la actualización falla con el código de error 114, realiza los siguientes pasos: 1. Conéctate a la ISO de actualización en el nodo primario y activa el shell de diagnóstico. 2. Monta la ISO desde la sesión SSH al nodo primario: <pre> sudo mount /dev/cdrom sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade </pre> 3. Instala paquetes Debian: <pre> sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vplatform.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vpupgrader.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vmware-tools.deb </pre> 4. Copia el archivo de información de construcción: <pre> sudo cp /upgrade/APPLIANCE_BUILD / </pre> Agrega certificados a la colección habilitando el shell de diagnóstico y ejecutando:



A partir de ONTAP tools for VMware vSphere 10.3 no se admite ⁵RPO cero.

Más información ["Cómo restaurar ONTAP tools for VMware vSphere si falla la actualización de la versión 10.0 a la 10.1"](#)

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

Consulta los registros en
/var/log/otvng/post-
deploy-upgrade.log.

6. Reinicia los nodos:

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. Realiza los pasos posteriores a la actualización:

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

Migra ONTAP tools for VMware vSphere 9.xx a 10.5

Migra desde ONTAP tools for VMware vSphere 9.xx a 10.5

Mover la configuración de NetApp ONTAP tools for VMware vSphere de la versión 9.xx a la 10.5 requiere un proceso de migración debido a las importantes actualizaciones y mejoras del producto entre las versiones.

Puedes migrar desde ONTAP tools for VMware vSphere 9.12D1, 9.13D2 y 9.13P2 a ONTAP tools for VMware vSphere 10.5.

Si tienes almacenes de datos NFS y VMFS y no tienes almacenes de datos vVols en tu configuración, simplemente desinstala ONTAP tools 9.xx y despliega ONTAP tools 10.5. Sin embargo, si tu configuración contiene almacenes de datos vVols, debes pasar por un proceso de migración del VASA Provider y del SRA.

La siguiente tabla resume 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. "Migrar el proveedor VASA" 2. "Crear políticas de almacenamiento para máquinas virtuales"	Pasos: 1. Elimina ONTAP tools 9.xx de tu entorno. Consulta el artículo de base de conocimientos "Cómo eliminar OTV 9.xx de tu entorno" NetApp. 2. "Implementa y configura ONTAP tools for VMware vSphere 10.5" 3. "Actualizar la SRA" 4. "Crear políticas de almacenamiento para máquinas virtuales"



Después de migrar de ONTAP tools for VMware vSphere 9.xx a 10.5, los almacenes de datos vVols que usan el protocolo NVMe/FC dejan de funcionar porque ONTAP tools 10.5 solo admite el protocolo NVMe-oF con almacenes de datos VMFS.

Migra el proveedor VASA y actualiza el SRA en ONTAP tools

Sigue los pasos que se indican en esta sección para migrar el VASA Provider de ONTAP tools for VMware vSphere 9.xx a ONTAP tools for VMware vSphere 10.5 y actualizar el Storage Replication Adapter (SRA) en el appliance VMware Live Site Recovery.

Pasos para migrar el proveedor VASA

1. Para habilitar el puerto 1527 de Derby en las herramientas existentes de ONTAP para VMware vSphere, habilita el usuario raíz e inicia sesión en la CLI a través de SSH. A continuación, ejecuta el siguiente comando:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Implementa el archivo OVA de ONTAP tools for VMware vSphere 10.5.

- Añade la instancia de vCenter Server que quieres migrar a ONTAP tools for VMware vSphere 10.5 release. Consulta ["Agrega una instancia de vCenter Server"](#) para más información.
- "Habilitar VASA Provider" servicio en ONTAP tools for VMware vSphere 10.5. Verifica que se haya completado correctamente consultando los registros:
- Incorpora el backend de almacenamiento localmente desde las API del servicio vCenter para el complemento ONTAP tools. Consulta ["Agrega un backend de almacenamiento usando la interfaz del cliente de vSphere"](#) para obtener más información.

- Obtén un token de acceso para autenticar las solicitudes de la API de REST. Utiliza el siguiente ejemplo, sustituyendo las variables por los valores específicos de tu entorno.

```
tail -f
/var/log/post-
deploy-upgrade.log
```

```
curl --request POST \
  --location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/vcenter-
login" \
  --header "Content-Type: application/json" \
  --header "Accept: */*" \
  -d '{"username": "$MYUSER", "password": "$MYPASSWORD", "vcenter
hostname": "$MYVCENTER"}'
```

Copia y guarda el token de acceso que aparece en la respuesta.

- Emite la siguiente API desde Swagger o Postman para migrar.

```
/upgrade
sudo umount -l -f
/dev/cdrom
sudo eject
```

```
curl -X POST
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

Puedes acceder a Swagger a través de esta URL: `https://$FQDN_IP_PORT/`, por ejemplo: `https://10.67.25.33:8443/`.

```
sudo reboot -f
```

Método HTTP y endpoint

Esta llamada a la API de REST utiliza el siguiente método y endpoint.

Método HTTP	Ruta
POST	/api/v1

Tipo de procesamiento

Asíncrono

Ejemplo de Curl

```
curl -X POST 'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <auth_token>' \
--header 'Content-Type: application/json' \
--data '{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*****"
  },
  "database_password": "*****"
}'
```

Cuerpo de la solicitud para la migración a otra versión:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*****"
  }
}
```

Ejemplo de salida en formato JSON

El sistema devuelve un objeto de trabajo. Guarda el identificador del trabajo para utilizarlo en el siguiente paso.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Utiliza el siguiente URI en Swagger para comprobar el estado:

```
curl
`https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobId
>?includeSubJobsAndTasks=true`
```

Usa el valor 'id' devuelto por el trabajo de migración en el paso anterior. Después de que el trabajo termine, revisa el informe de migración en la respuesta del trabajo.

9. Registra el proveedor VASA con ONTAP tools for VMware vSphere. Para obtener instrucciones, consulta ["Registra el proveedor de VASA"](#).
10. Verifica el registro del proveedor VASA:
 - a. En el vSphere Client, ve al vCenter Server.
 - b. Selecciona **Configurar > Proveedores de almacenamiento**.
 - c. Confirma que el VASA Provider registrado en el paso anterior aparece en línea.
11. Detén el servicio VASA Provider de ONTAP tools for VMware vSphere storage provider 9.10/9.11/9.12/9.13 usando estos pasos:
 - a. En ONTAP tools 9.x, abre la consola web.
 - b. Accede a la consola de mantenimiento.
 - c. Introduce 1 para seleccionar el menú **Configuración de la aplicación**.
 - d. Introduce 5 para detener los servicios VASA Provider y SRA.
 - e. En el vSphere Client, ve al vCenter Server y selecciona **Configurar > Proveedores de almacenamiento**.
 - f. Selecciona el VASA Provider offline para ONTAP tools 9.x y selecciona **Remove**.

Después de que se detiene el antiguo proveedor VASA, el servidor vCenter realiza una conmutación por error a ONTAP tools for VMware vSphere. Todos los datastores y las máquinas virtuales quedan accesibles y se sirven desde ONTAP tools for VMware vSphere.
12. Los almacenes de datos NFS y VMFS migrados aparecen en ONTAP tools for VMware vSphere 10.5 después de la tarea de detección de almacenes de datos, que puede tardar hasta 30 minutos. Comprueba su visibilidad en la página de resumen.
13. Realiza la migración de parches utilizando la siguiente API en Swagger o en Postman:

Método HTTP y endpoint

Esta llamada a la API de REST utiliza el siguiente método y endpoint.

Método HTTP	Ruta
PATCH	/api/v1

Tipo de procesamiento

Asíncrono

Utiliza el siguiente URI en Swagger:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Método HTTP y endpoint

Esta llamada a la API de REST utiliza el siguiente método y endpoint.

Método HTTP	Ruta
PATCH	/api/v1

Tipo de procesamiento

Asíncrono

Utiliza el siguiente URI en Swagger:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Ejemplo de Curl

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-4ce66f802c35`
```

Ejemplo de salida en formato JSON

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```



Usa el valor 'migration_id' devuelto en el paso 7 como <migration_id> en la llamada a la API PATCH. El cuerpo de la solicitud está vacío para la operación patch.



El UUID es el UUID de la migración devuelto en la respuesta a la API post-migrate.

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 ONTAP tools 10.5 en el servidor vCenter, sigue estos pasos:

- Espera a que finalice el proceso de **Discovery** y el sistema actualiza automáticamente los certificados en todos los hosts.
- Espera antes de iniciar operaciones en el almacén de datos y en las máquinas virtuales. El tiempo de espera depende del número de hosts, almacenes de datos y máquinas virtuales. Si no esperas, es posible que se produzcan fallos ocasionales.

Tras la actualización, si el estado de cumplimiento de la máquina virtual está desactualizado, vuelve a aplicar la política de almacenamiento siguiendo estos pasos:

1. Ve al almacén de datos y selecciona **Resumen > Políticas de almacenamiento de VM**.
2. El sistema muestra el estado de cumplimiento en **Cumplimiento de la política de almacenamiento de VM** como **Desactualizado**.
3. Selecciona la política de la Storage VM y la máquina virtual correspondiente.
4. Selecciona **Aplicar**.
5. El estado de cumplimiento en **Cumplimiento de la política de almacenamiento de VM** se muestra como conforme.

Información relacionada

- ["Conoce las ONTAP tools for VMware vSphere 10 RBAC"](#)
- ["Actualiza desde ONTAP tools for VMware vSphere 10.x a 10.5"](#)

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 las máquinas virtuales están ejecutándose actualmente, mientras que el sitio de recuperación es donde se recuperarán las máquinas virtuales. La interfaz del dispositivo VMware Live Site Recovery muestra el estado del plan de recuperación con detalles sobre los sitios protegido y de recuperación. En el plan de recuperación, los botones CLEANUP y REPROTECT están deshabilitados, mientras que los botones TEST y RUN siguen habilitados. Esto indica que

el sitio está preparado para la recuperación de datos. Antes de migrar el SRA, verifica que un sitio esté en estado protegido y el otro en estado de recuperación.



No inicies la migración si la conmutación por error se ha completado pero la reprotección está pendiente. Asegúrate de que el proceso de reprotección se haya completado antes de proceder con la migración. Si hay una conmutación por error de prueba en curso, limpia la conmutación por error de prueba e inicia la migración.

1. Sigue estos pasos para eliminar el adaptador SRA de ONTAP tools para VMware vSphere 9.xx en VMware Site Recovery:
2. Ve a la página de gestión de la configuración de VMware Live Site Recovery.
 - a. Ve a la sección **Storage Replication Adapter**.
 - b. En el menú de los tres puntos, selecciona **Restablecer configuración**.
 - c. En el menú de los tres puntos, selecciona **Delete**.
3. Sigue estos pasos tanto en el sitio de protección como en el de recuperación.
 - a. ["Habilita ONTAP tools for VMware vSphere services"](#)
 - b. Configura ONTAP tools for VMware vSphere 10.5 SRA adapter usando los pasos en ["Configura SRA en el dispositivo VMware Live Site Recovery"](#).
 - c. En la interfaz de VMware Live Site Recovery, ejecuta **Detectar matrices** y **Detectar dispositivos**. Confirma que los dispositivos se muestren como antes de la migración.

Automatiza usando la API de REST

Conoce la API de REST de las herramientas ONTAP

ONTAP tools for VMware vSphere 10 es un conjunto de herramientas para la gestión del ciclo de vida de las máquinas virtuales. Incluye una robusta API de REST que puedes usar como parte de tus procesos de automatización.

Fundamentos de los servicios web REST

La Transferencia de Estado Representacional (REST) es un estilo para crear aplicaciones web distribuidas, incluido 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 de estado

Los recursos son los componentes fundamentales de una aplicación de servicios web REST. Hay dos tareas iniciales importantes a la hora de diseñar una API de REST:

- Identifica los recursos del sistema o del servidor
- Define los estados de los recursos y las operaciones de transición de estado asociadas

Las aplicaciones cliente pueden mostrar y modificar el estado de los recursos mediante flujos de mensajes bien definidos.

Mensajes de HTTP

El Protocolo de Transferencia de Hipertexto (HTTP) es el protocolo que utilizan el cliente y el servidor de los servicios web para intercambiar mensajes sobre los recursos. Sigue el modelo CRUD, basado en las operaciones genéricas de 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

Aunque existen varios formatos de mensajes disponibles, la opción más popular es la Notación de Objetos de JavaScript (JSON). JSON es un estándar del sector para representar estructuras de datos sencillas en texto sin formato 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 de REST. Además del protocolo Transport Layer Security (TLS) que se utiliza para proteger el tráfico HTTP en la red, la API de REST de ONTAP tools for VMware vSphere 10 también utiliza tokens de acceso para la autenticación. Necesitas obtener un token de acceso y usarlo en las siguientes llamadas a la API.

Compatibilidad con solicitudes asíncronas

Las ONTAP tools for VMware vSphere 10 API de REST ejecutan la mayoría de las solicitudes de forma sincrónica, devolviendo un código de estado cuando la operación ha finalizado. También admite el procesamiento asíncrono para tareas que requieren más tiempo para completarse.

Entorno de ONTAP tools Manager

Hay varios aspectos del entorno de ONTAP tools Manager que debes tener en cuenta.

Máquina virtual

Las herramientas de ONTAP para VMware vSphere 10 se implementan usando la arquitectura de complementos remotos de vSphere. El software, incluido el soporte para la API de REST, se ejecuta en una máquina virtual independiente.

Dirección IP de ONTAP tools

Las herramientas ONTAP para VMware vSphere 10 exponen una única dirección IP que actúa como puerta de enlace a las capacidades de la máquina virtual. Necesitas proporcionar la dirección durante la configuración inicial y se asigna a un componente interno del equilibrador de carga. La dirección es utilizada por la interfaz de usuario de ONTAP tools Manager, así como para acceder directamente a la página de documentación de Swagger y a la API de REST.

Dos API de REST

Además de las ONTAP tools for VMware vSphere 10 API de REST, el clúster de ONTAP tiene su propia API de REST. ONTAP tools Manager utiliza la API de 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 obtener más información, consulta ["Automatización de ONTAP"](#).

Detalles de implementación de la API de REST de ONTAP tools

Aunque REST establece un conjunto común de tecnologías y buenas prácticas, la implementación concreta de cada API puede variar en función de las decisiones de diseño. Deberías familiarizarte con cómo está diseñada la API de REST de ONTAP tools for VMware vSphere 10 antes de usarla.

La API de REST incluye varias categorías de recursos, como vCenters y Aggregates. Consulta la ["Referencia sobre API"](#) para obtener más información.

Cómo acceder a la API de REST

Puedes acceder a las ONTAP tools for VMware vSphere 10 API de REST a través de la dirección IP de las ONTAP tools junto con el puerto. La URL completa consta de varias partes, entre las que se incluyen:

- Dirección IP y puerto de ONTAP tools
- Versión de API
- Categoría de recursos
- `${post_edited_translations.segment}`

Debes configurar la dirección IP durante la configuración inicial, mientras que el puerto se mantiene fijo en 8443. La primera parte de la URL es la misma para cada instancia de ONTAP tools for VMware vSphere 10; solo la categoría de recurso y el recurso específico cambian entre los distintos endpoints.



Los valores de la dirección IP y del puerto que aparecen en los ejemplos siguientes son meramente ilustrativos. Debes modificar estos valores para adaptarlos a tu entorno.

Ejemplo para acceder a los 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 usar para solicitar una lista de las instancias definidas del servidor vCenter usando el método GET.

Detalles de HTTP

La API de REST de ONTAP tools for VMware vSphere 10 utiliza HTTP y los parámetros correspondientes para actuar sobre las instancias y colecciones de recursos. A continuación se detallan los aspectos de la implementación de HTTP.

Métodos HTTP

En la tabla siguiente se muestran los métodos o verbos HTTP compatibles con la API de REST.

Método	CRUD	Descripción
GET	Leer	Recupera las propiedades de un objeto para una instancia de recurso o una colección. Se considera una operación de lista cuando se utiliza con una colección.
POST	Crear	Crea una nueva instancia de recurso basándose en los parámetros de entrada.
<code>\${post_edited_translations.segment}</code>	Actualización	Actualiza toda una instancia de recurso con el cuerpo de la solicitud JSON proporcionado. Se conservan los valores de las claves que no se pueden modificar por el usuario.
PATCH	Actualización	Solicita que se apliquen a la instancia del recurso un conjunto de cambios seleccionados en la solicitud.
ELIMINAR	Borrar	Elimina una instancia de recurso existente.

Encabezados de solicitud y respuesta

La siguiente tabla resume los encabezados HTTP más importantes que se utilizan con la API de REST.

Encabezado	Tipo	Notas de uso
Aceptar	Solicitud	Este es el tipo de contenido que puede aceptar la aplicación cliente. Entre los valores válidos se incluyen <code>'/'</code> o <code>application/json</code> .
x-auth	Solicitud	Contiene un token de acceso que identifica al usuario que realiza la solicitud a través de la aplicación cliente.
Tipo de contenido	Respuesta	Lo devuelve el servidor según el encabezado de solicitud <code>Accept</code> .

Códigos de estado HTTP

A continuación se describen los códigos de estado HTTP que utiliza la API de REST.

Código	Significado	Descripción
200	OK	Indica éxito para las llamadas que no crean una nueva instancia de recurso.
201	Creado	Se ha creado correctamente un objeto con un identificador único para la instancia del recurso.
202	Aceptado	La solicitud ha sido aceptada y se ha creado una tarea en segundo plano para ejecutarla.
204	Sin contenido	La solicitud se realizó correctamente, aunque no se devolvió ningún contenido.
400	Solicitud incorrecta	La solicitud introducida no se reconoce o es inapropiada.
401	No autorizado	El usuario no está autorizado y debe autenticarse.
403	Prohibido	El acceso está denegado debido a un error de autorización.
404	No encontrado	El recurso al que se hace referencia en la solicitud no existe.
409	Conflicto	Se ha producido un intento de crear un objeto, pero el objeto ya existe.
500	Error interno	Se ha producido un error interno general en el servidor.

Autenticación

La autenticación de un cliente en la API de REST se realiza usando 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 de ONTAP tools Manager (nombre de usuario y contraseña).
- Los tokens tienen el formato de un JSON Web Token (JWT).
- Cada token caduca al cabo de 60 minutos.
- Las solicitudes a la API desde un cliente deben incluir el token en el encabezado de la solicitud `x-auth`.

Consulta ["Tu primera llamada a la API de REST"](#) para ver un ejemplo de cómo solicitar y utilizar un token de acceso.

Solicitudes síncronas y asíncronas

La mayoría de las llamadas a la API de REST se completan rápidamente y, por lo tanto, se ejecutan de forma síncrona. Es decir, devuelven un código de estado (como 200) después de que se haya completado la solicitud. Las solicitudes que tardan más en completarse se ejecutan de forma asíncrona usando una tarea en segundo plano.

Tras realizar una llamada a la API que se ejecuta de forma asíncrona, el servidor devuelve un código de estado HTTP 202. Esto indica que la solicitud ha sido aceptada pero aún no se ha completado. Puedes consultar el trabajo en segundo plano para determinar su estado, incluyendo si se ha completado con éxito o ha fallado.

El procesamiento asíncrono se utiliza para varios tipos de operaciones de larga duración, incluidas las operaciones con el almacén de datos y las de vVol. Consulta la categoría job manager de la API de REST en la página de Swagger para más información.

Haz tu primera llamada a la API de REST de ONTAP tools

Puedes realizar una llamada a la API de REST mediante curl para empezar a utilizar las ONTAP tools for VMware vSphere 10 API de REST.

Antes de empezar

Deberías revisar la información y los parámetros necesarios en los ejemplos de curl.

Información obligatoria

Necesitas lo siguiente:

- ONTAP tools for VMware vSphere 10: dirección IP o dominio completo (FQDN), así como el puerto
- Credenciales para el administrador de ONTAP tools Manager (nombre de usuario y contraseña)

Parámetros y variables

Los ejemplos de curl que se muestran a continuación incluyen variables al estilo de Bash. Puedes configurar estas variables en el entorno de Bash o actualizarlas manualmente antes de ejecutar los comandos. Si configuras las variables, el shell sustituirá los valores en cada comando antes de que se ejecute. Las variables se describen en la tabla siguiente.

Variable	Descripción
\$FQDN_IP_PORT	El nombre de dominio completo o la dirección IP de ONTAP tools Manager junto con el número de puerto.
\$MYUSER	Nombre de usuario para la cuenta de ONTAP tools Manager.
\$MYPASSWORD	Contraseña asociada con el nombre de usuario de ONTAP tools Manager.
\$ACCESS_TOKEN	El token de acceso emitido por ONTAP tools Manager.

Los siguientes comandos y resultados en la línea de comandos de Linux muestran cómo se puede establecer y visualizar 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

Para utilizar la API de REST, debes obtener un token de acceso. A continuación se muestra un ejemplo de cómo solicitar un token de acceso. Debes sustituir los valores por los correspondientes a 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"}'
```

Copia y guarda el token de acceso proporcionado en la respuesta.

Paso 2: Realizar la llamada a la API de REST

Una vez que tengas un token de acceso, puedes utilizar curl para realizar una llamada a la API de REST. Incluye el token de acceso obtenido en el primer paso.

Ejemplo de Curl

```
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 ONTAP tools Manager.

Referencia de la API de REST de ONTAP tools

La referencia de la API de REST de ONTAP tools for VMware vSphere 10 contiene detalles sobre todas las llamadas a la API. Esta referencia es útil cuando desarrollas aplicaciones de automatización.

Puedes acceder a la documentación en línea de la API de REST de ONTAP tools for VMware vSphere 10 a través de la interfaz de usuario de Swagger. Necesitas la dirección IP o el dominio completo de ONTAP tools for VMware vSphere 10 gateway service, así como el puerto.

Pasos

1. Escribe la siguiente URL en tu navegador, sustituyendo la variable por la dirección IP y la combinación de puerto adecuada, y pulsa **Intro**.

```
https://$FQDN_IP_PORT/
```

Ejemplo

```
https://10.61.25.33:8443/
```

2. Como ejemplo de una llamada individual a la API, desplázate hacia abajo hasta la categoría **vCenters** y selecciona **GET** junto al endpoint `/virtualization/api/v1/vcenters`

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas registradas, patentes y más.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas registradas

NETAPP, el logotipo de NETAPP y las marcas que aparecen en la página de NetApp Trademarks 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

Una lista actual de patentes propiedad de NetApp se puede encontrar 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 los derechos de autor y las licencias de terceros utilizadas en el software NetApp.

["Aviso sobre ONTAP tools for VMware vSphere 10.5"](#)

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.