Conceptos

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Tabla de contenidos

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.

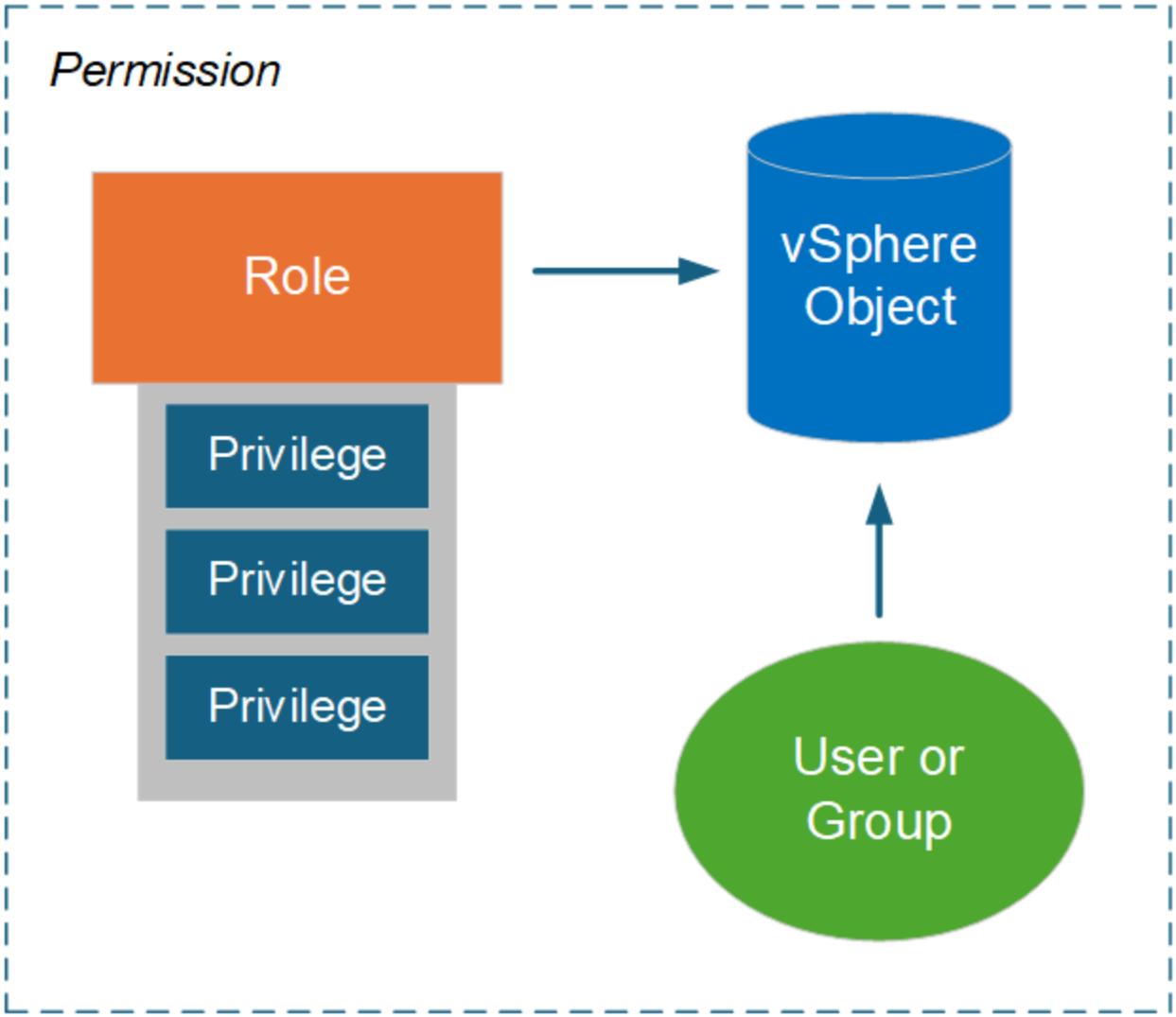
RBAC con VMware vSphere

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 edítalo 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
        - Suspender
    - 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 Privileges 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.