



Control de acceso basado en roles

ONTAP tools for VMware vSphere 10

NetApp

September 30, 2025

This PDF was generated from https://docs.netapp.com/es-es/ontap-tools-vmware-vsphere-100/concepts/concept_vcenter_server_role_based_access_control_features_in_vsc_for_vmware_vsphere.html on September 30, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Control de acceso basado en roles 1
 - Información general sobre el control de acceso basado en roles en las herramientas de ONTAP 1
 - Puntos clave sobre la asignación y modificación de roles para vCenter Server 2
 - Funciones estándar incluidas en las herramientas de ONTAP 2
 - Permisos para back-ends de almacenamiento de ONTAP y objetos de vSphere 3
 - Roles de ONTAP recomendados al usar herramientas de ONTAP para VMware vSphere 3

Control de acceso basado en roles

Información general sobre el control de acceso basado en roles en las herramientas de ONTAP

VCenter Server proporciona un control de acceso basado en roles (RBAC) que permite controlar el acceso a los objetos de vSphere. VCenter Server proporciona servicios de autenticación y autorización centralizados en muchos niveles diferentes dentro de su inventario mediante derechos de usuario y grupo con roles y privilegios. VCenter Server cuenta con cinco componentes principales para la gestión de RBAC:

Componentes	Descripción
Privilegios	Un privilegio habilita o deniega el acceso para realizar acciones en vSphere.
Funciones	Un rol contiene uno o más privilegios del sistema donde cada privilegio define un derecho administrativo para un determinado objeto o tipo de objeto del sistema. Al asignar un rol a un usuario, el usuario hereda las capacidades de los privilegios definidos en ese rol.
Usuarios y grupos	Los usuarios y grupos se usan en permisos para asignar roles desde Active Directory (AD) o, potencialmente, usuarios/grupos de Windows locales también (no se recomienda)
Permisos	Los permisos permiten asignar privilegios a usuarios o grupos para realizar ciertas acciones y realizar cambios en objetos dentro de vCenter Server. Los permisos de vCenter Server afectan solo a los usuarios que inician sesión en vCenter Server en lugar de a los usuarios que inician sesión en un host ESXi directamente.
Objeto	Una entidad sobre la que se realizan las acciones. Los objetos de VMware vCenter son centros de datos, carpetas, pools de recursos, clústeres, hosts, y máquinas virtuales

Para completar correctamente una tarea, debe contar con los roles de RBAC de vCenter Server correspondientes. Durante una tarea, las herramientas de ONTAP comprueban los roles de vCenter Server de un usuario antes de comprobar los privilegios de ONTAP del usuario.



Los roles de vCenter Server se aplican a los usuarios de las herramientas de ONTAP de vCenter, no a los administradores. De forma predeterminada, los administradores tienen acceso completo al producto y no requieren roles asignados a ellos.

Los usuarios y los grupos obtienen acceso a un rol formando parte de un rol de vCenter Server.

Puntos clave sobre la asignación y modificación de roles para vCenter Server

Solo debe configurar roles de vCenter Server si desea limitar el acceso a objetos y tareas de vSphere. De lo contrario, puede iniciar sesión como administrador. Este inicio de sesión permite acceder automáticamente a todos los objetos de vSphere.

Donde se asigna un rol, determina las tareas de las herramientas de ONTAP que puede realizar un usuario. Puede modificar un rol en cualquier momento. Si cambia los privilegios dentro de un rol, el usuario asociado a ese rol debe cerrar la sesión y, a continuación, volver a iniciar sesión para activar el rol actualizado.

Funciones estándar incluidas en las herramientas de ONTAP

Para simplificar el trabajo con los privilegios de vCenter Server y el control de acceso basado en roles, las herramientas de ONTAP ofrecen funciones de herramientas estándar de ONTAP que permiten realizar tareas de herramientas clave de ONTAP. También hay un rol de solo lectura que permite ver la información, pero no ejecutar tareas.

Puede ver las funciones estándar de las herramientas de ONTAP haciendo clic en **Roles** en la página inicial del cliente de vSphere. Los roles que las herramientas de ONTAP proporcionan le permiten realizar las siguientes tareas:

Rol	Descripción
Administrador de herramientas de NetApp ONTAP	Ofrece todos los privilegios nativos de vCenter Server y privilegios específicos de las herramientas de ONTAP que se requieren para ejecutar algunas de las tareas de herramientas de ONTAP.
Herramientas de NetApp ONTAP Sólo lectura	Ofrece acceso de solo lectura a herramientas de ONTAP. Estos usuarios no pueden realizar ninguna acción de las herramientas de ONTAP que esté controlada por acceso.
Aprovisionamiento de herramientas de NetApp ONTAP	Ofrece algunos privilegios nativos de vCenter Server y privilegios específicos de las herramientas de ONTAP que se requieren para aprovisionar el almacenamiento. Es posible realizar las siguientes tareas: <ul style="list-style-type: none">• Crear nuevos almacenes de datos• Gestionar almacenes de datos

El rol de administrador de la interfaz de usuario de administrador no está registrado en vCenter. Este rol es específico de la interfaz de usuario del administrador.

Si su empresa requiere que implemente funciones que son más restrictivas que las funciones de herramientas estándar de ONTAP, puede utilizar las funciones de herramientas de ONTAP para crear nuevas funciones.

En este caso, debe clonar los roles de herramientas ONTAP necesarios y, a continuación, editar el rol clonado para que solo tenga los privilegios que necesite el usuario.

Permisos para back-ends de almacenamiento de ONTAP y objetos de vSphere

Si el permiso de vCenter Server es suficiente, las herramientas de ONTAP luego comprueba los privilegios de RBAC de ONTAP (el rol de ONTAP) asociados con las credenciales de back-ends de almacenamiento (el nombre de usuario y la contraseña). para determinar si tiene suficientes privilegios para realizar las operaciones de almacenamiento que requiere la tarea de herramientas de ONTAP en ese back-end de almacenamiento. Si tiene los privilegios de ONTAP correctos, puede acceder a Almacenamiento back-ends y realizar la tarea de herramientas ONTAP. Los roles ONTAP determinan las tareas de herramientas de ONTAP que se pueden realizar en el back-end de almacenamiento.

Roles de ONTAP recomendados al usar herramientas de ONTAP para VMware vSphere

Es posible configurar varios roles de ONTAP recomendados para trabajar con las herramientas de ONTAP para VMware vSphere y el control de acceso basado en roles (RBAC). Estos roles contienen los privilegios de la ONTAP que se requieren para ejecutar las operaciones de almacenamiento requeridas que ejecutan las tareas de las herramientas de ONTAP.

Para crear roles de usuario nuevos, debe iniciar sesión como administrador en sistemas de almacenamiento que ejecutan ONTAP. Se pueden crear roles de ONTAP con ONTAP System Manager 9.8P1 o posterior. Consulte ["Lista de privilegios mínimos necesarios para el usuario de cluster de ámbito global no administrativo"](#) si quiere más información.

Cada rol de ONTAP tiene asociado un nombre de usuario y una pareja de contraseñas que constituyen las credenciales del rol. Si no inicia sesión con estas credenciales, no podrá acceder a las operaciones de almacenamiento que están asociadas con el rol.

Como medida de seguridad, los roles ONTAP específicos de las herramientas de ONTAP se ordenan jerárquicamente. Esto significa que el primer rol es el más restrictivo y solo tiene los privilegios asociados al conjunto más básico de operaciones de almacenamiento de herramientas de ONTAP. El siguiente rol incluye sus propios privilegios y todos los privilegios asociados con el rol anterior. Cada puesto adicional resulta menos restrictivo en relación con las operaciones de almacenamiento admitidas.

A continuación se muestran algunos de los roles de control de acceso basado en roles recomendados de ONTAP cuando se utilizan las herramientas de ONTAP. Después de crear estos roles, es posible asignar los roles a los usuarios que deben realizar tareas relacionadas con el almacenamiento, como el aprovisionamiento de máquinas virtuales.

1. Detección

Este rol le permite añadir sistemas de almacenamiento.

2. Cree almacenamiento

Este rol le permite crear almacenamiento. Este rol también incluye todos los privilegios asociados con el rol de detección.

3. Modificar almacenamiento

Este rol permite modificar almacenamiento. Este rol también incluye todos los privilegios asociados con el rol de detección y creación de almacenamiento.

4. Destruya el almacenamiento

Este rol le permite destruir almacenamiento. Este rol también incluye todos los privilegios asociados con el rol Discovery, el rol Create Storage y el rol Modify Storage.

Si utiliza VASA Provider para ONTAP, también debe configurar un rol de gestión basada en políticas (PBM). Este rol le permite gestionar el almacenamiento mediante políticas de almacenamiento. Esta función requiere que usted también establezca el papel de «recuperación».

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.