



RBAC con VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Tabla de contenidos

RBAC con VMware vSphere	1
Entorno RBAC de vCenter Server con ONTAP tools for VMware vSphere 10	1
Ilustración de un permiso de vCenter Server	1
Componentes de un permiso de vCenter Server	2
Utilice vCenter Server RBAC con ONTAP tools for VMware vSphere 10	2
Roles de vCenter y la cuenta de administrador	2
Jerarquía de objetos de vSphere	2
Roles incluidos con las ONTAP tools for VMware vSphere 10	3
Objetos de vSphere y backends de almacenamiento ONTAP	3
Trabajar con vCenter Server RBAC	3

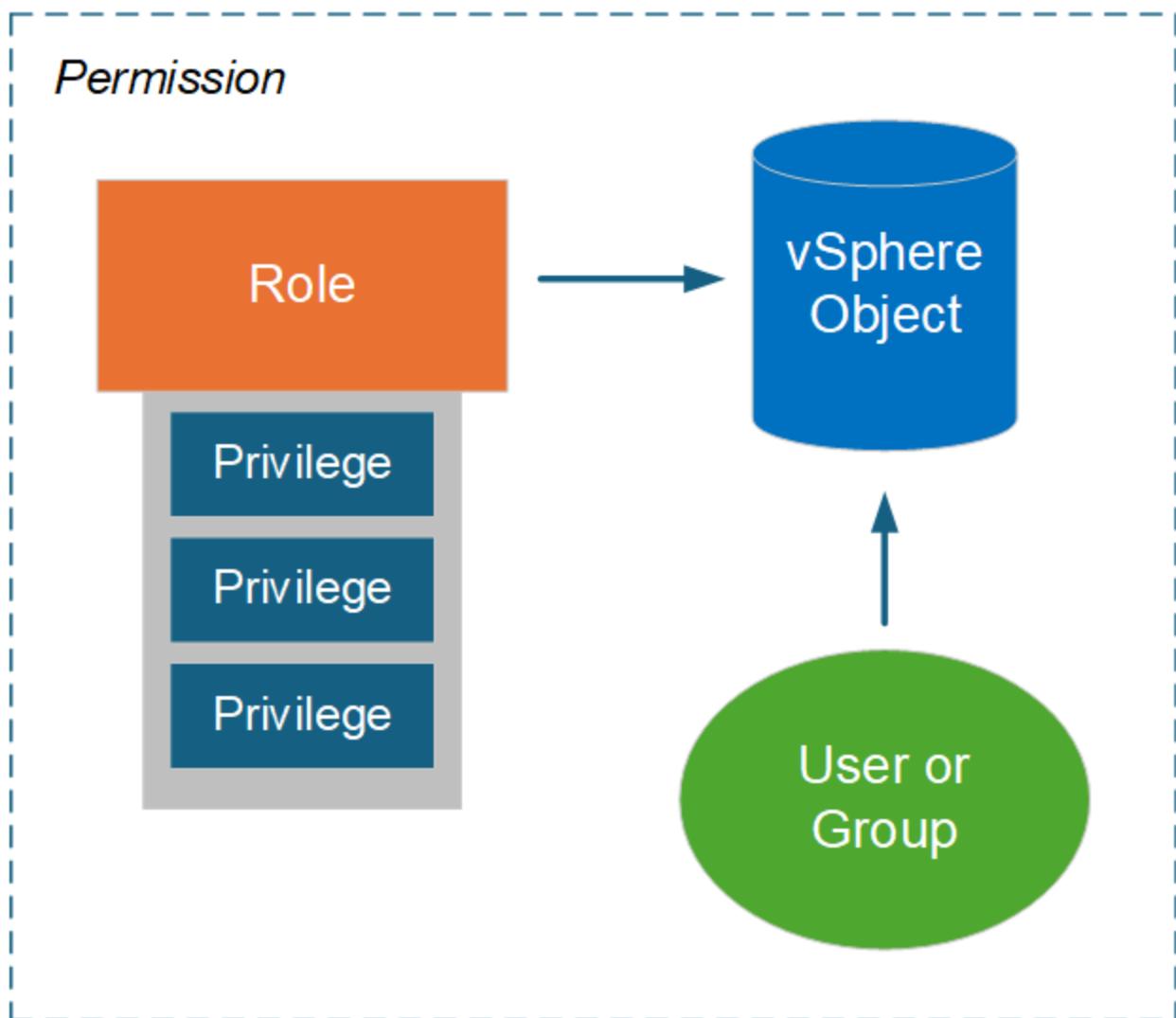
RBAC con VMware vSphere

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

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

Ilustración de un permiso de vCenter Server

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



Componentes de un permiso de vCenter Server

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

Objetos de vSphere

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

Privilegios y roles

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

- Privilegios nativos de vCenter Server

Estos son los privilegios que proporciona vCenter Server.

- Privilegios específicos de las herramientas ONTAP

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

Usuarios y grupos

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

Utilice vCenter Server RBAC con ONTAP tools for VMware vSphere 10

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

Roles de vCenter y la cuenta de administrador

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

Jerarquía de objetos de vSphere

El inventario de objetos de vSphere está organizado en una jerarquía. Por ejemplo, puede moverse hacia

abajo en la jerarquía de la siguiente manera:

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

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

Roles incluidos con las ONTAP tools for VMware vSphere 10

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



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

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

Herramientas NetApp ONTAP tools for VMware vSphere Administrator

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

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

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

Herramientas NetApp ONTAP tools for VMware vSphere Provision

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

- Crear nuevos almacenes de datos
- Administrar almacenes de datos

Objetos de vSphere y backends de almacenamiento ONTAP

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

Trabajar con vCenter Server RBAC

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

Privilegios requeridos

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

la interfaz de usuario.

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

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

Asignación de permisos

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



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

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

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

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

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.