Control de acceso basado en roles

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

Tabla de contenidos

Control de acceso basado en roles

Información general del control de acceso basado en roles en herramientas de ONTAP para VMware vSphere

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 utilizan en permisos para asignar roles desde Active Directory (AD). VCenter Server tiene sus propios usuarios y grupos locales que se pueden utilizar.
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 tener los roles de RBAC de vCenter Server apropiados. Durante una tarea, las herramientas de ONTAP para VMware vSphere 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 las herramientas de ONTAP para usuarios de VMware vSphere 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.

Cuando se asigna un rol, determina las herramientas de ONTAP para las tareas de VMware vSphere 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.

Roles estándar incluidos con las herramientas de ONTAP para VMware vSphere

Para simplificar el uso de privilegios de vCenter Server y el control de acceso basado en roles, las herramientas de ONTAP para VMware vSphere proporcionan herramientas estándar de ONTAP para roles de VMware vSphere que permiten realizar herramientas de ONTAP clave para tareas de VMware vSphere. También hay un rol de solo lectura que permite ver la información, pero no ejecutar tareas.

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

Rol	Descripción
Herramientas de NetApp ONTAP para administrador de VMware vSphere	Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de las herramientas de ONTAP que se requieren para ejecutar algunas de las herramientas de ONTAP para tareas de VMware vSphere.
Herramientas de NetApp ONTAP para VMware vSphere Read Only	Ofrece acceso de solo lectura a herramientas de ONTAP. Estos usuarios no pueden ejecutar ninguna herramienta ONTAP para acciones de VMware vSphere controladas por acceso.
Herramientas de NetApp ONTAP para el aprovisionamiento de VMware vSphere	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: • Crear nuevos almacenes de datos • Gestionar almacenes de datos

La función de administrador de ONTAP tools no está registrada en vCenter Server. Esta función es específica del Administrador de herramientas de ONTAP.

Si su empresa requiere la implantación de funciones más restrictivas que las herramientas estándar de ONTAP para funciones de VMware vSphere, puede utilizar las herramientas de ONTAP para funciones de VMware vSphere para crear nuevas funciones.

En este caso, debe clonar las herramientas de ONTAP necesarias para los roles de VMware vSphere 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 para VMware vSphere comprueban los privilegios de control de acceso basado en roles 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 requieren las herramientas de ONTAP para la tarea de VMware vSphere en ese back-end de almacenamiento. Si tiene los privilegios de ONTAP correctos, puede acceder a Back-ends de almacenamiento y realizar herramientas de ONTAP para tareas de VMware vSphere. Los roles ONTAP determinan las herramientas de ONTAP para tareas de VMware vSphere que se pueden realizar en el back-end del almacenamiento.

Componentes de permisos de vCenter Server

El servidor de vCenter reconoce permisos, no privilegios. Cada permiso de vCenter Server consta de tres componentes.

El servidor vCenter tiene los siguientes componentes:

- Uno o más privilegios (el rol)

  Los privilegios definen las tareas que un usuario puede realizar.

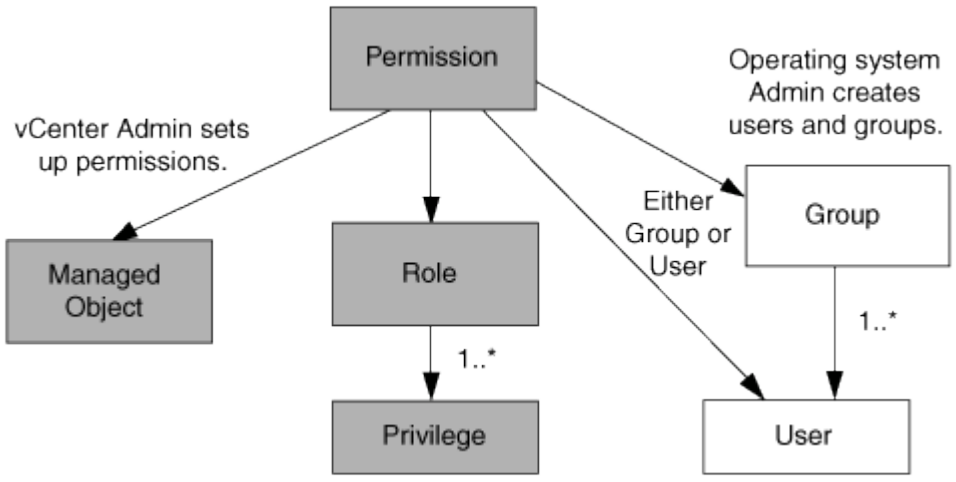
- Un objeto de vSphere

  El objeto es el destino de las tareas.

- Un usuario o grupo

  El usuario o grupo define quién puede realizar la tarea.

En este diagrama, los cuadros grises indican los componentes que existen en vCenter Server y los recuadros blancos indican componentes que existen en el sistema operativo donde se ejecuta vCenter Server.



Privilegios

Existen dos tipos de privilegios asociados con las herramientas de ONTAP para VMware vSphere:

- Privilegios nativos de vCenter Server

  Estos privilegios vienen con vCenter Server.

- Privilegios específicos de herramientas de ONTAP

  Estos privilegios se definen para tareas de ONTAP específicas para tareas de VMware vSphere. Son exclusivas de las herramientas de ONTAP para VMware vSphere.

Las herramientas de ONTAP para las tareas de VMware vSphere requieren privilegios específicos para las herramientas de ONTAP y privilegios nativos de vCenter Server. Estos privilegios constituyen el "'rol'" del usuario. Un permiso puede tener varios privilegios. Estos privilegios corresponden a un usuario que ha iniciado sesión en vCenter Server.

> Para simplificar el uso del control de acceso basado en roles de vCenter Server, las herramientas de ONTAP para VMware vSphere proporcionan varios roles estándar que contienen todos los privilegios nativos y específicos de las herramientas de ONTAP necesarios para ejecutar tareas de ONTAP para VMware vSphere.

Si cambia los privilegios dentro de un permiso, el usuario asociado a ese permiso debe cerrar sesión y, a continuación, iniciar sesión para activar el permiso actualizado.

Objetos de vSphere

Los permisos se asocian con objetos de vSphere, como vCenter Server, hosts ESXi, máquinas virtuales, almacenes de datos, centros de datos, y carpetas. Puede asignar permisos a cualquier objeto de vSphere. Según el permiso que se asigna a un objeto de vSphere, vCenter Server determina quién puede ejecutar qué tareas en ese objeto. En el caso de las herramientas de ONTAP para tareas específicas de VMware vSphere, los permisos se asignan y validan solo en el nivel de carpeta raíz (vCenter Server) y no en ninguna otra entidad. Excepto para la operación del plugin VAAI, donde los permisos se validan en el host ESXi afectado.

Usuarios y grupos

Es posible usar Active Directory (o la máquina local de vCenter Server) para configurar usuarios y grupos de usuarios. Luego, puede utilizar permisos de vCenter Server para otorgar acceso a estos usuarios o grupos para permitirles ejecutar herramientas de ONTAP específicas para tareas de VMware vSphere.

> Estos permisos de vCenter Server se aplican a las herramientas de ONTAP para usuarios de VMware vSphere vCenter, no a las herramientas de ONTAP para administradores de VMware vSphere. De forma predeterminada, las herramientas de ONTAP para administradores de VMware vSphere tienen acceso completo al producto y no requieren permisos que se les asignen.

Los usuarios y grupos no tienen roles asignados. Estos obtienen acceso a un rol mediante el permiso de vCenter Server.

Asigne y modifique permisos para vCenter Server

Hay varios puntos clave que se deben tener en cuenta cuando se trabaja con permisos de vCenter Server. Si una tarea de las herramientas de ONTAP para VMware vSphere se complete correctamente, puede depender de la ubicación en la que se haya asignado un

permiso o de las acciones que haya realizado un usuario después de modificar un permiso.

Asignación de permisos

Solo debe configurar permisos de vCenter Server si desea limitar el acceso a los 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 permiso determina las herramientas de ONTAP para las tareas de VMware vSphere que puede realizar un usuario.

A veces, para garantizar la finalización de una tarea, debe asignar permiso a un nivel superior, como el objeto raíz. Es así cuando una tarea requiere un privilegio que no se aplica a un objeto de vSphere específico (por ejemplo, un seguimiento de la tarea) o cuando un privilegio requerido se aplica a un objeto que no es vSphere (por ejemplo, un sistema de almacenamiento).

En estos casos, puede configurar un permiso para que sea heredado por las entidades secundarias. También puede asignar otros permisos a las entidades secundarias. El permiso asignado a una entidad hijo siempre anula el permiso heredado de la entidad padre. Esto significa que puede otorgar permisos a una entidad secundaria para restringir el ámbito de un permiso asignado a un objeto raíz y heredado por la entidad secundaria.

A menos que las políticas de seguridad de la empresa requieran permisos más restrictivos, es recomendable asignar permisos al objeto raíz (también denominado carpeta raíz).

Permisos y objetos que no son de vSphere

El permiso que cree se aplica a un objeto que no sea de vSphere. Por ejemplo, un sistema de almacenamiento no es un objeto de vSphere. Si un privilegio se aplica a un sistema de almacenamiento, debe asignar el permiso que incluye ese privilegio a las herramientas de ONTAP para el objeto raíz de VMware vSphere porque no existe ningún objeto de vSphere al que pueda asignarlo.

Por ejemplo, cualquier permiso que incluya un privilegio, como ONTAP tools for VMware vSphere privilege «Añadir/modificar/omitir sistemas de almacenamiento», se debe asignar al nivel de objeto raíz.

Modificar permisos

Puede modificar un permiso en cualquier momento.

Si cambia los privilegios dentro de un permiso, el usuario asociado con ese permiso debe cerrar la sesión y, a continuación, volver a iniciar la sesión para habilitar el permiso actualizado.

Privilegios requeridos para las herramientas de ONTAP para tareas de VMware vSphere

Las diferentes herramientas de ONTAP para las tareas de VMware vSphere requieren diferentes combinaciones de privilegios específicos de las herramientas de ONTAP para VMware vSphere y los privilegios nativos de vCenter Server.

Para acceder a las herramientas de ONTAP para la interfaz gráfica de usuario de VMware vSphere, tiene que

contar con el privilegio View específico para las herramientas de ONTAP para el producto asignado en el nivel de objeto de vSphere correspondiente. Si se inicia sesión sin este privilegio, las herramientas de ONTAP para VMware vSphere muestran un mensaje de error cuando se hace clic en el icono de NetApp y no puede acceder a las herramientas de ONTAP.

En el privilegio **View**, puede acceder a las herramientas de ONTAP para VMware vSphere. Este privilegio no le permite realizar tareas dentro de las herramientas de ONTAP para VMware vSphere. Para ejecutar tareas en las herramientas de ONTAP para VMware vSphere, es necesario contar con los privilegios específicos para las herramientas de ONTAP y los privilegios nativos del servidor de vCenter correspondientes a esas tareas.

El nivel de asignación determina qué porciones de la interfaz de usuario se muestran. Al asignar el privilegio View al objeto raíz (carpeta), es posible ingresar a las herramientas de ONTAP para VMware vSphere haciendo clic en el icono de NetApp.

Es posible asignar el privilegio View a otro nivel de objeto de vSphere. No obstante, de esta forma se limitan las herramientas de ONTAP para menús de VMware vSphere que se pueden ver y usar.

El objeto raíz es el lugar recomendado para asignar cualquier permiso que contiene el privilegio View.

Roles de ONTAP recomendados para 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 ONTAP necesarios para realizar las operaciones de almacenamiento que ejecutan las herramientas ONTAP para tareas de VMware vSphere.

Para crear roles de usuario nuevos, debe iniciar sesión como administrador de los sistemas de almacenamiento que ejecutan ONTAP. Se pueden crear roles de ONTAP con ONTAP System Manager 9.8P1 o posterior.

Cada rol de ONTAP tiene una pareja asociada de nombre de usuario y contraseña, 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, las herramientas de ONTAP para las funciones de ONTAP específicas de VMware vSphere se ordenan jerárquicamente. Esto significa que el primer rol es el más restrictivo y solo tiene los privilegios asociados al conjunto más básico de herramientas ONTAP para operaciones de almacenamiento de VMware vSphere. El siguiente rol incluye sus propios privilegios y todos los privilegios asociados con el rol anterior. Cada rol adicional es menos restrictivo con respecto a 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 herramientas de ONTAP para VMware vSphere. Después de crear estos roles, puede asignarlos a usuarios que deban realizar tareas relacionadas con el almacenamiento, como el aprovisionamiento de máquinas virtuales.

Rol	privilegios
Detección	Este rol le permite añadir sistemas de almacenamiento.

Cree almacenamiento	Este rol le permite crear almacenamiento. Este rol también incluye todos los privilegios asociados con el rol de detección.
Modificar almacenamiento	Este rol permite modificar almacenamiento. Este rol también incluye todos los privilegios asociados con el rol de detección y el rol de creación de almacenamiento.
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 herramientas de ONTAP para VMware vSphere, 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

Información de la marca comercial