Control de acceso basado en roles con VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Tabla de contenidos

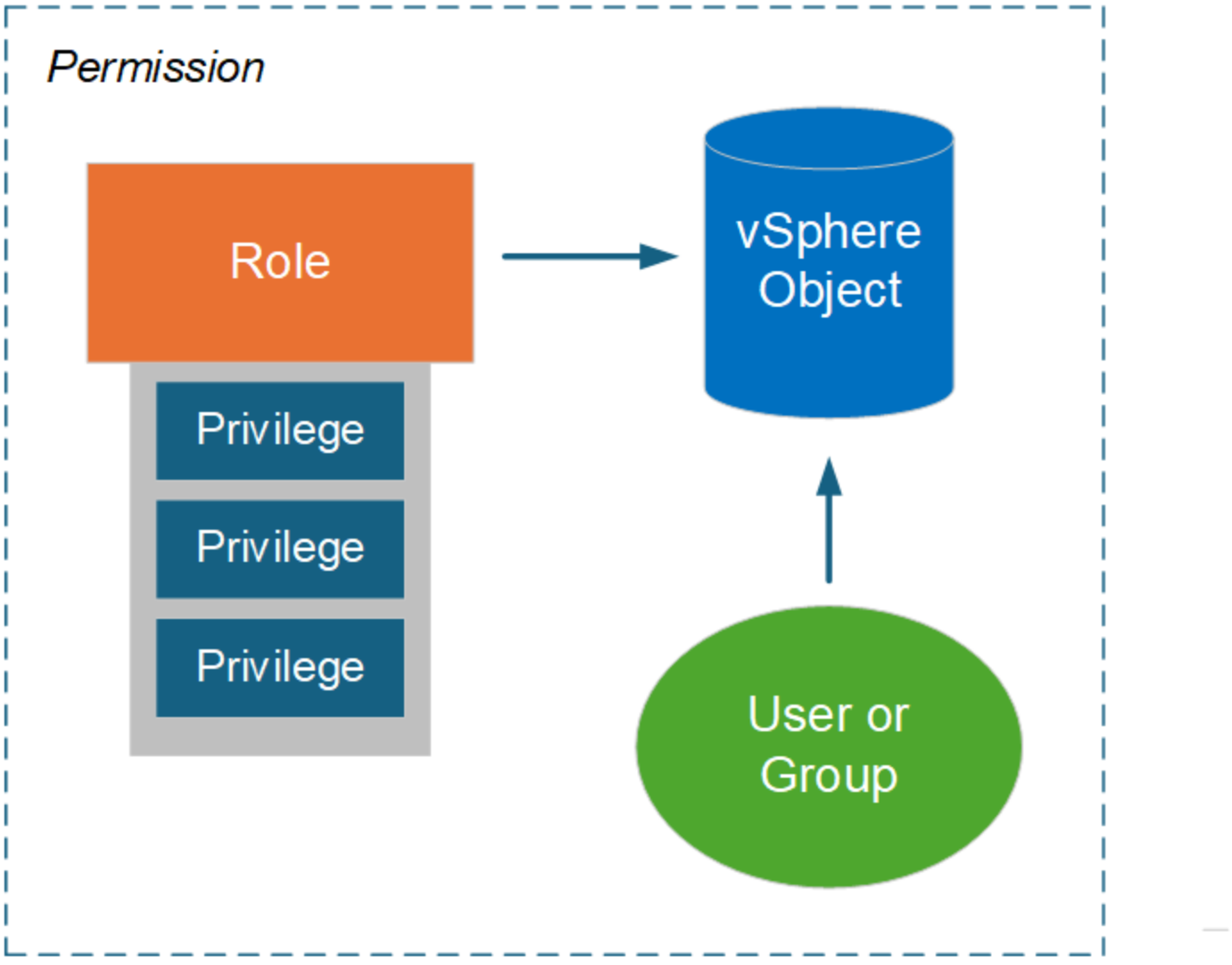
Control de acceso basado en roles con VMware vSphere

Entorno RBAC de vCenter Server con herramientas de ONTAP para VMware vSphere 10

VMware vCenter Server proporciona una funcionalidad de control de acceso basado en roles que 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 vCenter Server. Se aplica a un objeto de vSphere con un usuario o grupo incluido con la definición de permiso. En la siguiente figura, se proporciona una ilustración general 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 al crear el permiso.

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. Según los permisos asignados al objeto, vCenter Server determina qué acciones o tareas se pueden ejecutar en el objeto por cada usuario o grupo. Para las tareas específicas de las herramientas de ONTAP para VMware vSphere, todos los permisos se asignan y se validan en el nivel de carpeta raíz o raíz de vCenter Server. Consulte "Utilice RBAC con vCenter Server" para obtener más información.

Privileges y roles

Existen dos tipos de vSphere Privileges usados con las herramientas de ONTAP para VMware vSphere 10. Para simplificar el uso del control de acceso basado en roles en este entorno, ONTAP Tools proporciona funciones que contienen la Privileges nativa y personalizada necesaria. El Privileges incluye:

- Privilegios nativos de vCenter Server

  Estas son las Privileges que proporciona vCenter Server.

- Privilegios específicos de herramientas de ONTAP

  Se trata de herramientas Privileges personalizadas únicas de ONTAP para VMware vSphere.

Usuarios y grupos

Se pueden 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 basado en el Privileges en el rol asociado. Tenga en cuenta que los roles no se asignan directamente a los usuarios de forma aislada. En su lugar, los usuarios y los grupos obtienen acceso a un objeto a través del rol Privileges como parte del permiso más grande de vCenter Server.

Utilice el control de acceso basado en roles de vCenter Server con herramientas de ONTAP para VMware vSphere 10

Existen varios aspectos de las herramientas de ONTAP para la implementación de control de acceso basado en roles de VMware vSphere 10 con vCenter Server que debería tener en cuenta antes de su uso en un entorno de producción.

Los roles de vCenter y la cuenta de administrador

Solo es necesario definir y utilizar los roles personalizados de vCenter Server si desea limitar el acceso a los objetos de vSphere y a las tareas administrativas asociadas. Si no se requiere 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 los añadidos por las herramientas de ONTAP para VMware vSphere 10.

Jerarquía de objetos de vSphere

El inventario de objetos de vSphere está organizado en una jerarquía. Por ejemplo, puede bajar la jerarquía de la siguiente manera:

```
vCenter Server --> Datacenter --> Cluster --> --Virtual Machine> ESXi host
```

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

Roles incluidos con las herramientas de ONTAP para VMware vSphere 10

Para simplificar el uso del control de acceso basado en roles de vCenter Server, las herramientas de ONTAP para 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 de ONTAP existentes y editarlo según sea necesario. Después de realizar cambios en la configuración, los usuarios del cliente vSphere afectados deben cerrar la sesión y volver a iniciarla para activar los cambios.

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

Herramientas de NetApp ONTAP para administrador de VMware vSphere

Ofrece todas las Privileges nativas de las herramientas de vCenter Server Privileges y ONTAP necesarias para realizar las herramientas principales de ONTAP para las tareas de administrador 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

Objetos de vSphere y back-ends de almacenamiento de ONTAP

Los dos entornos de RBAC funcionan juntos. Cuando se realiza una tarea en la interfaz del cliente de vSphere, primero se comprueban los roles de las herramientas de ONTAP definidas en vCenter Server. Si vSphere permite la operación, se examina el Privileges de rol ONTAP. Este segundo paso se realiza según el rol ONTAP asignado al usuario cuando se creó y configuró el back-end de almacenamiento.

Trabajar con RBAC de vCenter Server

Hay algunos aspectos que hay que tener en cuenta cuando se trabaja con la Privileges y los permisos de vCenter Server.

Privilegios requeridos

Para acceder a la interfaz de usuario de las herramientas de ONTAP para VMware vSphere 10, es necesario tener el privilegio *View* específico de ONTAP tools. Si inicia sesión en vSphere sin este privilegio y hace clic en el icono de NetApp, las herramientas de ONTAP para VMware vSphere muestran un mensaje de error y no permite acceder a la interfaz de usuario.

El nivel de asignación en la jerarquía de objetos de vSphere determina a qué porciones de la interfaz de usuario puede acceder. Al asignar el privilegio View al objeto raíz, puede acceder a las herramientas de ONTAP para VMware vSphere haciendo clic en el icono de NetApp.

En su lugar, es posible asignar el privilegio View a otro nivel de objeto de vSphere inferior. Sin embargo, esto limitará las herramientas de ONTAP para los menús de VMware vSphere a los que puede acceder y usar.

Asignación de permisos

Se deben usar permisos de vCenter Server si desea limitar el acceso a los objetos y las tareas de vSphere. Donde se asigna permiso en la jerarquía de objetos de vSphere determina las herramientas de ONTAP para VMware vSphere 10 tareas que los usuarios pueden realizar.

A menos que necesite definir un acceso más restrictivo, por lo general es recomendable asignar permisos en el nivel de objeto raíz o carpeta raíz.

Los permisos disponibles con las herramientas de ONTAP para VMware vSphere 10 se aplican a objetos personalizados que no son de vSphere, como sistemas de almacenamiento. Si es posible, debería asignar estos permisos a las herramientas de ONTAP para el objeto raíz de VMware vSphere porque no hay ningún objeto de vSphere al que pueda asignarlo. Por ejemplo, cualquier permiso que incluya un privilegio de «Añadir/modificar/quitar sistemas de almacenamiento» de ONTAP tools for VMware vSphere se debería asignar en el nivel de objeto raíz.

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

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

Información de copyright

Información de la marca comercial