RBAC con ONTAP

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/es-es/ontap-tools-vmware-vsphere-10/concepts/rbac-ontap-environment.html on September 29, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

RBAC con ONTAP . . . 1
Entorno RBAC de ONTAP con herramientas de ONTAP para VMware vSphere 10 . . . 1
Descripción general de las opciones administrativas . . . 1
Trabajar con roles de REST DE ONTAP . . . 2
Utilice el control de acceso basado en roles de ONTAP con herramientas de ONTAP para VMware vSphere 10 . . . 2
Descripción general del proceso de configuración . . . 2
Configure el rol mediante System Manager . . . 3

RBAC con ONTAP

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

ONTAP proporciona un entorno de control de acceso basado en roles sólido y ampliable. Es posible usar la funcionalidad de RBAC para controlar el acceso al almacenamiento y las operaciones del sistema tal y como se expone mediante la API DE REST y la CLI. Es conveniente familiarizarse con el entorno antes de usarlo con una herramienta de ONTAP para la puesta en marcha de VMware vSphere 10.

Descripción general de las opciones administrativas

Hay varias opciones disponibles cuando se utiliza el control de acceso basado en roles de ONTAP en función de su entorno y sus objetivos. A continuación se presenta una visión general de las principales decisiones administrativas. Consulte también "Automatización ONTAP: Información general sobre la seguridad de control de acceso basado en roles" para obtener más información.

> ONTAP RBAC está diseñado para un entorno de almacenamiento y es más simple que la implementación de RBAC proporcionada con vCenter Server. Con ONTAP, asignas un rol directamente al usuario. No es necesario configurar permisos explícitos, como los que se usan con vCenter Server, con ONTAP RBAC.

Tipos de roles y Privileges

Al definir un usuario ONTAP, se requiere un rol ONTAP. Existen dos tipos de roles de ONTAP:

- DESCANSO

  Los roles DE REST se introdujeron con ONTAP 9.6 y se aplican generalmente a los usuarios que acceden a ONTAP a través de la API DE REST. El Privileges incluido en estos roles se define en términos de acceso a los extremos de la API DE REST DE ONTAP y las acciones asociadas.

- Tradicional

  Estas son las funciones heredadas que se incluyen antes de ONTAP 9.6. Siguen siendo un aspecto fundamental del RBAC. Los Privileges se definen en términos de acceso a los comandos de la CLI de la ONTAP.

Mientras que los roles REST se introdujeron más recientemente, los roles tradicionales tienen algunas ventajas. Por ejemplo, se pueden incluir parámetros de consulta adicionales de forma opcional para que Privileges defina con mayor precisión los objetos a los que se aplican.

Ámbito

Los roles de ONTAP pueden definirse con uno o dos ámbitos diferentes. Se pueden aplicar a una SVM de datos específico (nivel de SVM) o a todo el clúster de ONTAP (nivel de clúster).

Definiciones de roles

ONTAP proporciona un conjunto de roles predefinidos tanto a nivel de clúster como de SVM. También puede definir roles personalizados.

Trabajar con roles de REST DE ONTAP

Hay varias consideraciones cuando se usan los roles DE REST DE ONTAP que se incluyen con las herramientas de ONTAP para VMware vSphere 10.

Asignación de roles

Tanto si se utiliza un rol tradicional como DE REST, todas las decisiones de acceso a la ONTAP se toman basándose en el comando de la CLI subyacente. Sin embargo, como la Privileges de un rol REST se define en términos de los extremos de la API REST, ONTAP debe crear un rol tradicional *mapped* para cada uno de los roles REST. Por lo tanto, cada rol REST se asigna a un rol tradicional subyacente. Esto permite a ONTAP tomar decisiones de control de acceso de manera coherente, independientemente del tipo de rol. No es posible modificar los roles asignados paralelos.

Definición de un rol DE REST mediante CLI Privileges

Como ONTAP siempre utiliza los comandos de la CLI para determinar el acceso en un nivel base, es posible expresar un rol REST con el comando de la CLI Privileges en lugar de los extremos REST. Una de las ventajas de este método es la granularidad adicional disponible con los roles tradicionales.

Interfaz administrativa al definir roles de ONTAP

Es posible crear usuarios y roles con la interfaz de línea de comandos de ONTAP y la API DE REST. Sin embargo, es más cómodo usar la interfaz de System Manager junto con el archivo JSON disponible a través del Administrador de herramientas de ONTAP. Consulte "Utilice el control de acceso basado en roles de ONTAP con herramientas de ONTAP para VMware vSphere 10" para obtener más información.

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

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

Descripción general del proceso de configuración

Las ONTAP tools for VMware vSphere incluyen soporte para crear un usuario ONTAP con un rol personalizado. Las definiciones están empaquetadas en un archivo JSON que puedes cargar en el clúster ONTAP . Puede crear el usuario y adaptar el rol a su entorno y necesidades de seguridad.

Los pasos de configuración principales se describen a un nivel superior a continuación. Consulte "Configure los roles y privilegios de usuario de ONTAP"si desea obtener más información.

1. Prepare

Debe disponer de credenciales administrativas para el Administrador de herramientas de ONTAP y el clúster de ONTAP.

2. Descargue el archivo de definición JSON

Después de iniciar sesión en la interfaz de usuario del Administrador de herramientas de ONTAP, puede descargar el archivo JSON que contiene las definiciones de RBAC.

3. Crear un usuario ONTAP con un rol

Después de iniciar sesión en System Manager, puede crear el usuario y el rol:

1. Selecciona **Cluster** a la izquierda y luego **Settings**.
2. Desplácese hacia abajo hasta **Usuarios y roles** y haga clic en −→.
3. Seleccione **Agregar** en **Usuarios** y seleccione **Productos de virtualización**.
4. Seleccione el archivo JSON en su estación de trabajo local y cárguelo.

4. Configure el rol

Como parte de la definición del rol, debe tomar varias decisiones administrativas. Consulte Configure el rol mediante System Manager para obtener más información.

Configure el rol mediante System Manager

Después de comenzar a crear un usuario y un rol nuevos con System Manager y haber cargado el archivo JSON, puede personalizar el rol según el entorno y las necesidades.

Configuración de rol y usuario principal

Las definiciones de RBAC se empaquetan como varias funcionalidades de producto, como las combinaciones de VSC, VASA Provider y SRA. Debe seleccionar el entorno o los entornos donde necesite compatibilidad con RBAC. Por ejemplo, si desea que los roles admitan la funcionalidad de plugin remoto, seleccione VSC. También debe elegir el nombre de usuario y la contraseña asociada.

Privilegios

El rol Privileges se distribuye en cuatro conjuntos según el nivel de acceso necesario al almacenamiento ONTAP. La Privileges en la que se basan los roles incluye:

- Detección

  Este rol le permite añadir sistemas de almacenamiento.

- Crear almacenamiento

  Este rol le permite crear almacenamiento. También incluye todos los Privileges asociados con el rol de detección.

- Modifique el almacenamiento

  Este rol permite modificar almacenamiento. También incluye todos los Privileges asociados con la detección y crear los roles de almacenamiento.

- Destruya el almacenamiento

  Este rol le permite destruir almacenamiento. También incluye todas las Privileges asociadas con la detección, crear almacenamiento y modificar los roles de almacenamiento.

Generar el usuario con un rol

Después de haber seleccionado las opciones de configuración para su entorno, haga clic en **Agregar** 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 ha seleccionado

- Lista de juegos de privilegios.

Ejemplo

```
OTV_10_VSC_Discovery_Create
```

El nuevo usuario se agregará a la lista de la página “Usuarios y roles”. Tenga en cuenta que tanto los métodos de inicio de sesión de usuario HTTP como ONTAPI son compatibles.

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.