Control de acceso basado en roles (RBAC)

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-learn-about.html on September 29, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Control de acceso basado en roles (RBAC) . . . 1
- Obtenga más información sobre las herramientas de ONTAP para el control de acceso basado en roles de VMware vSphere 10 . . . 1
  - Componentes de RBAC . . . 1
  - Dos entornos de RBAC . . . 2
- Control de acceso basado en roles con VMware vSphere . . . 2
  - Entorno RBAC de vCenter Server con herramientas de ONTAP para VMware vSphere 10 . . . 2
  - Utilice el control de acceso basado en roles de vCenter Server con herramientas de ONTAP para VMware vSphere 10 . . . 4
- RBAC con ONTAP . . . 6
  - Entorno RBAC de ONTAP con herramientas de ONTAP para VMware vSphere 10 . . . 6
  - Utilice el control de acceso basado en roles de ONTAP con herramientas de ONTAP para VMware vSphere 10 . . . 7

Control de acceso basado en roles (RBAC)

Obtenga más información sobre las herramientas de ONTAP para el control de acceso basado en roles de VMware vSphere 10

El control de acceso basado en roles (RBAC) es un marco de seguridad para controlar el acceso a los recursos de una organización. RBAC simplifica la administración definiendo roles con niveles de autoridad específicos para realizar acciones, en lugar de asignar autorización a usuarios individuales. Los roles definidos se asignan a los usuarios, lo que contribuye a reducir el riesgo de error y simplifica la gestión del control de acceso en toda la organización.

El modelo de estándar RBAC consta de varias tecnologías de implementación o fases que aumentan la complejidad. El resultado es que las puestas en marcha de control de acceso basado en roles reales, basadas en las necesidades de los proveedores de software y sus clientes, pueden variar y van de relativamente simples a muy complejas.

Componentes de RBAC

A nivel general, existen varios componentes que se incluyen en todas las implementaciones de RBAC. Estos componentes se unen de diferentes maneras como parte de la definición de los procesos de autorización.

Privilegios

Un *privilegio* es una acción o capacidad que se puede permitir o denegar. Puede ser algo simple, como leer un archivo, o una operación más abstracta, específica de un sistema de software. También se pueden definir Privileges para restringir el acceso a los puntos finales de la API REST y a los comandos de la CLI. Toda implementación de RBAC incluye privilegios predefinidos y puede permitir a los administradores crear privilegios personalizados.

Funciones

Un *role* es un contenedor que incluye uno o más Privileges. Los roles se definen generalmente en función de tareas o funciones de trabajo particulares. Cuando se asigna un rol a un usuario, se otorga al usuario toda la Privileges incluida en el rol. Y al igual que con Privileges, las implementaciones incluyen roles predefinidos y, en general, permiten la creación de roles personalizados.

Objetos

Un *OBJECT* representa un recurso real o abstracto identificado en el entorno de RBAC. Las acciones definidas mediante Privileges se realizan sobre o con los objetos asociados. Dependiendo de la implementación, Privileges se puede otorgar a un tipo de objeto o a una instancia de objeto específica.

Usuarios y grupos

Users se asignan o asocian a un rol aplicado después de la autenticación. Algunas implementaciones de RBAC permiten asignar solo un rol a un usuario, mientras que otras permiten varios roles por usuario, quizás con un solo rol activo a la vez. La asignación de roles a *groups* puede simplificar aún más la administración de seguridad.

Permisos

Un *permission* es una definición que enlaza un usuario o grupo junto con un rol a un objeto. Los permisos

pueden ser útiles con un modelo de objetos jerárquicos en el que, opcionalmente, pueden ser heredados por los hijos de la jerarquía.

Dos entornos de RBAC

Hay dos entornos distintos de control de acceso basado en roles que debes tener en cuenta al trabajar con herramientas de ONTAP para VMware vSphere 10.

Servidor VMware vCenter

La implementación de RBAC en VMware vCenter Server se utiliza para restringir el acceso a los objetos expuestos a través de la interfaz de usuario de vSphere Client. Como parte de la instalación de herramientas de ONTAP para VMware vSphere 10, el entorno de control de acceso basado en roles se amplía para incluir objetos adicionales que representen las funcionalidades de las herramientas de ONTAP. El acceso a estos objetos se proporciona a través del plug-in remoto. Consulte "Entorno de RBAC de vCenter Server" para obtener más información.

Clúster ONTAP

Las herramientas de ONTAP para VMware vSphere 10 se conectan a un clúster ONTAP mediante la API REST DE ONTAP para realizar operaciones relacionadas con el almacenamiento. El acceso a los recursos de almacenamiento se controla a través de un rol de ONTAP asociado con el usuario de ONTAP proporcionado durante la autenticación. Consulte "Entorno de RBAC de ONTAP" para obtener más información.

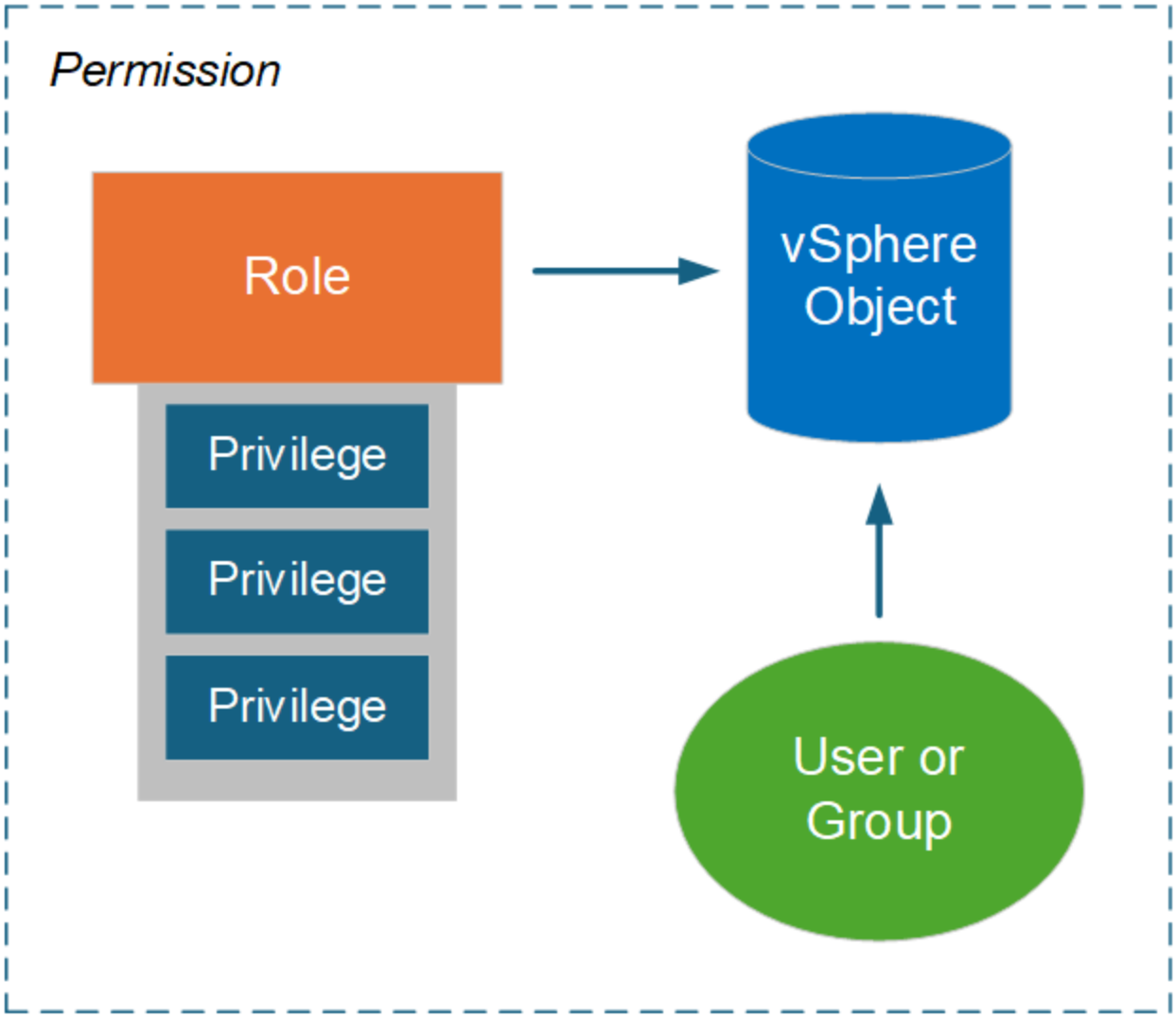
Control de acceso basado en roles con VMware vSphere

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

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 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.

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.