



# **Funciones de control de acceso basado en roles de vCenter Server en VSC para VMware vSphere**

**VSC, VASA Provider, and SRA 9.7**

NetApp  
March 21, 2024

This PDF was generated from <https://docs.netapp.com/es-es/vsc-vasa-provider-sra-97/deploy/reference-components-that-make-up-vcenter-server-permissions.html> on March 21, 2024. Always check docs.netapp.com for the latest.

# Tabla de contenidos

- Funciones de control de acceso basado en roles de vCenter Server en VSC para VMware vSphere . . . . . 1
  - Componentes de permisos de vCenter Server . . . . . 1
  - Puntos clave sobre la asignación y modificación de permisos para vCenter Server. . . . . 3
  - Roles estándar que se incluyen en el dispositivo virtual para VSC, proveedor VASA y SRA . . . . . 4
  - Privilegios necesarios para las tareas de VSC . . . . . 6

# Funciones de control de acceso basado en roles de vCenter Server en VSC para VMware vSphere

VCenter Server proporciona un control de acceso basado en roles (RBAC) que permite controlar el acceso a los objetos de vSphere. En Virtual Storage Console para VMware vSphere, el control de acceso basado en roles de vCenter Server funciona con ONTAP para determinar qué tareas de VSC puede ejecutar un usuario específico en objetos de un sistema de almacenamiento específico.

Para completar correctamente una tarea, debe tener los permisos de control de acceso basado en roles de vCenter Server correspondientes. Durante una tarea, VSC comprueba los permisos de vCenter Server de un usuario antes de comprobar los privilegios de ONTAP del usuario.

Es posible establecer los permisos de vCenter Server para el objeto raíz (también denominado carpeta raíz). Posteriormente, es posible refinar la seguridad aplicando restricciones a entidades secundarias que no necesitan los mismos permisos.

## 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.

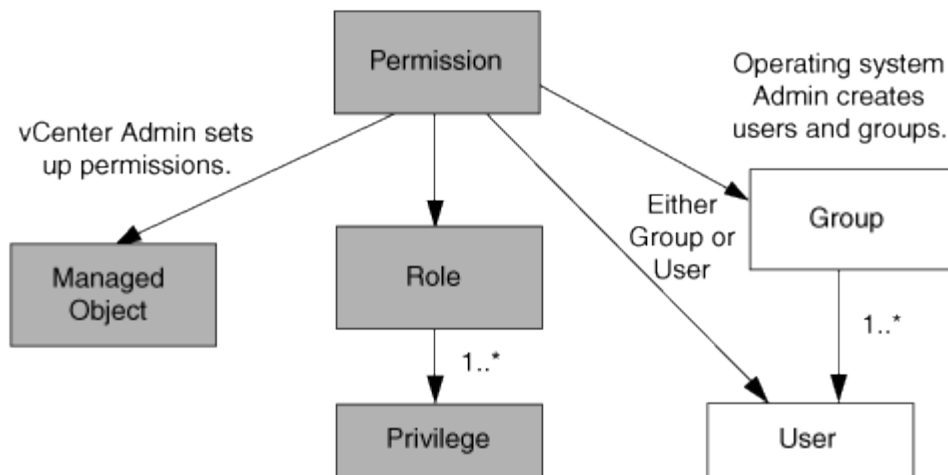
- Un usuario o grupo

El usuario o grupo define quién puede realizar la tarea.

Como se muestra en el siguiente diagrama, debe tener los tres elementos para tener un permiso.



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 Virtual Storage Console para VMware vSphere:

- Privilegios nativos de vCenter Server

Estos privilegios vienen con vCenter Server.

- Privilegios específicos de VSC

Estos privilegios se definen para tareas de VSC específicas. Son exclusivos de VSC.

Las tareas de VSC requieren privilegios específicos de VSC 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, VSC ofrece varias funciones estándar que contienen todos los privilegios nativos y específicos de VSC necesarios para ejecutar tareas de VSC.

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.

Privilegio	Funciones	Tareas
Menú:consola de almacenamiento virtual de NetApp[View]	<ul style="list-style-type: none"> <li>• Administrador de VSC</li> <li>• Aprovisionamiento de VSC</li> <li>• Solo lectura de VSC</li> </ul>	Todas las tareas específicas de VSC y VASA Provider requieren el privilegio View.
Menu:NetApp Virtual Storage Console[Administración basada en políticas > Gestión] o <b>privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label &gt; Management</b>	Administrador de VSC	Tareas de VSC y VASA Provider relacionadas con los perfiles de funcionalidad de almacenamiento y la configuración de umbral.

## 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. Para tareas específicas de VSC, los permisos se asignan y validan solo en el nivel de carpeta raíz (vCenter Server), no en ninguna otra entidad. Excepto para la operación del complemento VAAI, donde se validan los permisos en ESXi en cuestión.

## Usuarios y grupos

Es posible usar Active Directory (o la máquina local de vCenter Server) para configurar usuarios y grupos de usuarios. A continuación, es posible usar permisos de vCenter Server para otorgar acceso a estos usuarios o grupos con el fin de permitirles ejecutar tareas VSC específicas.



Estos permisos de vCenter Server se aplican a los usuarios de VSC vCenter, no a los administradores de VSC. De forma predeterminada, los administradores de VSC tienen acceso completo al producto y no requieren permisos asignados.

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

## Puntos clave sobre la asignación y modificación de 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 Virtual Storage Console para VMware vSphere se realiza correctamente puede depender de la ubicación en la que se asignó un permiso o de las acciones que realizó 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 tareas de VSC que puede ejecutar un usuario.

A veces, para garantizar la finalización de una tarea, debe asignar el 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 tener permisos para una entidad secundaria como una manera de restringir el ámbito de un permiso que se asignó a un objeto raíz y que la entidad secundaria hereda.



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 crea se aplica a un objeto que no sea de vSphere. Por ejemplo, un sistema de almacenamiento no es un objeto de vSphere. Si se aplica un privilegio a un sistema de almacenamiento, debe asignar el permiso que contiene ese privilegio al objeto raíz de VSC porque no hay ningún objeto de vSphere al cual pueda asignarlo.

Por ejemplo, todos los permisos que incluyan un privilegio, como el privilegio VSC "Add/Modify/Skip Storage systems", se deben asignar en el nivel de objetos 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.

## Roles estándar que se incluyen en el dispositivo virtual para VSC, proveedor VASA y SRA

Para simplificar el uso de los privilegios de vCenter Server y el control de acceso basado en roles (RBAC), (VSC) ofrece roles estándar de VSC que permiten ejecutar tareas clave de VSC. También hay un rol de solo lectura que le permite ver la información de VSC, pero no ejecutar tareas.

Los roles estándar de VSC tienen privilegios específicos requeridos de VSC y los privilegios nativos de vCenter Server necesarios para que los usuarios ejecuten tareas de VSC. Además, los roles están configurados para contar con todos los privilegios necesarios en todas las versiones compatibles de vCenter Server.

El administrador puede asignar estos roles a los usuarios, según sea necesario.



Cuando actualiza VSC a la versión más reciente, los roles estándar se actualizan automáticamente para que funcionen con la nueva versión de VSC.

Para ver los roles estándar de VSC, haga clic en **roles** en la página **Inicio** de vSphere Client.

Los roles que ofrece VSC permiten realizar las siguientes tareas:

Función	Descripción
Administrador de VSC	Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de VSC requeridos para ejecutar todas las tareas de VSC.
Solo lectura de VSC	Proporciona acceso de solo lectura a VSC.  Estos usuarios no pueden realizar ninguna acción VSC que esté controlada por el acceso.

Función	Descripción
Aprovisionamiento de VSC	<p>Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de VSC necesarios para aprovisionar almacenamiento.</p> <p>Es posible realizar las siguientes tareas:</p> <ul style="list-style-type: none"> <li>• Crear nuevos almacenes de datos</li> <li>• Destrucción de almacenes de datos</li> <li>• Ver información sobre los perfiles de funcionalidad del almacenamiento</li> </ul>

## Directrices para usar roles estándar de VSC

Cuando trabaja con roles estándar de Virtual Storage Console para VMware vSphere, hay ciertas directrices que debe seguir.

No debe modificar directamente los roles estándar. Si lo hace, VSC sobrescribirá los cambios cada vez que actualice VSC. El instalador actualiza las definiciones de rol estándar cada vez que actualiza VSC. Si hace esto, se garantiza que los roles sean actuales para la versión de VSC, así como para todas las versiones compatibles de vCenter Server.

Sin embargo, puede usar los roles estándar para crear roles que se ajusten a su entorno. Para ello, debe copiar el rol estándar de VSC y editar el rol copiado. Al crear un rol nuevo, puede mantener esta función incluso al reiniciar o actualizar el servicio VSC Windows.

Algunas de las formas de utilizar las funciones estándar de VSC incluyen las siguientes:

- Utilice los roles estándar de VSC para todas las tareas de VSC.

En esta situación, los roles estándar ofrecen todos los privilegios que un usuario necesita para realizar las tareas de VSC.

- Combinar roles para expandir las tareas que un usuario puede realizar.

Si los roles estándar de VSC proporcionan demasiada granularidad en el entorno, puede ampliar los roles creando grupos de nivel superior que contengan varias funciones.

Si un usuario tiene que ejecutar otras tareas que no son de VSC y requieren privilegios nativos de vCenter Server adicionales, puede crear una función que incluya esos privilegios y también añadirla al grupo.

- Cree funciones más detalladas.

Si su empresa necesita implementar funciones más restrictivas que las funciones estándar de VSC, puede usar los roles de VSC para crear nuevas funciones.

En este caso, debe clonar los roles de VSC necesarios y editar el rol clonado para que solo tenga los privilegios que requiere el usuario.

# Privilegios necesarios para las tareas de VSC

Las diferentes tareas de Virtual Storage Console para VMware vSphere requieren diferentes combinaciones de privilegios específicas de (VSC) y los privilegios nativos de vCenter Server.

Puede encontrar información sobre los privilegios necesarios para las tareas de VSC en el artículo 1032542 de la base de conocimientos de NetApp.

["Cómo configurar RBAC para Virtual Storage Console"](#)

## Privilegios a nivel de producto que requiere VSC para VMware vSphere

Para acceder a la interfaz gráfica de usuario de Virtual Storage Console para VMware vSphere, es necesario contar con el privilegio View específico de VSC para el producto asignado en el nivel de objeto de vSphere correspondiente. Si se inicia sesión sin este privilegio, VSC muestra un mensaje de error al hacer clic en el icono de NetApp y no le permite acceder a VSC.

En la siguiente tabla, se describe el privilegio View en el nivel de producto de VSC:

Privilegio	Descripción	Nivel de asignación
Ver	Puede acceder a la interfaz gráfica de usuario de VSC. Este privilegio no le permite realizar tareas en VSC. Para realizar cualquier tarea de VSC, debe tener los privilegios correctos específicos de VSC y nativos de vCenter Server para esas tareas.	<p>El nivel de asignación determina qué porciones de la interfaz de usuario se muestran.</p> <p>Al asignar el privilegio View en el objeto raíz (carpeta), es posible ingresar a VSC haciendo clic en el icono de NetApp.</p> <p>Es posible asignar el privilegio View a otro nivel de objeto de vSphere. No obstante, de esta forma se limitan los menús de VSC que se pueden ver y usar.</p> <p>El objeto raíz es el lugar recomendado para asignar cualquier permiso que contiene el privilegio View.</p>

## Control de acceso basado en roles de ONTAP para el dispositivo virtual para VSC, proveedor VASA y SRA

El control de acceso basado en roles de ONTAP permite controlar el acceso a sistemas de almacenamiento específicos y controlar las acciones que un usuario puede ejecutar en esos sistemas de almacenamiento. En Virtual Storage Console para VMware vSphere, el control de acceso basado en roles de ONTAP funciona con el control de



acceso basado en roles de vCenter Server para determinar qué tareas de VSC (Virtual Storage Console) puede ejecutar un usuario específico en los objetos de un sistema de almacenamiento específico.

VSC usa las credenciales (nombre de usuario y contraseña) configuradas en VSC para autenticar cada sistema de almacenamiento y determinar qué operaciones de almacenamiento se pueden ejecutar en ese sistema de almacenamiento. VSC usa un conjunto de credenciales para cada sistema de almacenamiento. Estas credenciales determinan qué tareas de VSC se pueden ejecutar en ese sistema de almacenamiento, es decir, las credenciales se aplican a VSC, no a un usuario individual de VSC.

El control de acceso basado en roles de ONTAP se aplica únicamente al acceso a sistemas de almacenamiento y a la ejecución de tareas de VSC relacionadas con el almacenamiento, como el aprovisionamiento de máquinas virtuales. Si no se cuenta con los privilegios de control de acceso basado en roles de ONTAP correspondientes a un sistema de almacenamiento específico, no es posible ejecutar ninguna tarea en un objeto de vSphere que se encuentre alojado en ese sistema de almacenamiento. Es posible utilizar el control de acceso basado en roles de ONTAP junto con los privilegios específicos de VSC para controlar qué tareas de VSC puede ejecutar un usuario:

- Supervisar y configurar objetos de almacenamiento o de vCenter Server que residen en un sistema de almacenamiento
- Aprovisionamiento de objetos de vSphere que residen en un sistema de almacenamiento

El uso de RBAC de ONTAP con los privilegios específicos de VSC ofrece una capa de seguridad orientada al almacenamiento que puede gestionar el administrador de almacenamiento. Como resultado, dispone de un control de acceso más detallado del que admite RBAC de ONTAP o RBAC de vCenter Server por sí solo. Por ejemplo, con RBAC de vCenter Server, puede permitir que vCenterUserB aprovisione un almacén de datos con el almacenamiento, mientras impide que vCenterUserA aprovisione almacenes de datos. Si las credenciales del sistema de almacenamiento para un sistema de almacenamiento específico no admiten la creación de almacenamiento, ni vCenterUserB ni vCenterUserA pueden aprovisionar un almacén de datos en ese sistema de almacenamiento.

Cuando se inicia una tarea VSC, VSC primero comprueba si tiene el permiso correcto de vCenter Server para esa tarea. Si el permiso de vCenter Server no es suficiente para permitir ejecutar la tarea, VSC no tiene que comprobar los privilegios de ONTAP de ese sistema de almacenamiento debido a que no ha superado la comprobación de seguridad inicial de vCenter Server. Como resultado, no podrá acceder al sistema de almacenamiento.

Si el permiso de vCenter Server es suficiente, VSC comprueba los privilegios de RBAC de ONTAP (su rol de ONTAP) asociados con las credenciales del sistema de almacenamiento (el nombre de usuario y la contraseña) Determinar si tiene privilegios suficientes para realizar las operaciones de almacenamiento que requiere esa tarea de VSC en ese sistema de almacenamiento. Si cuenta con los privilegios de ONTAP correctos, puede acceder al sistema de almacenamiento y ejecutar la tarea de VSC. Los roles de ONTAP determinan las tareas de VSC que se pueden ejecutar en el sistema de almacenamiento.

Cada sistema de almacenamiento está asociado con un conjunto de privilegios de ONTAP.

Usar el control de acceso basado en roles de ONTAP y de vCenter Server ofrece los siguientes beneficios:

- Seguridad

El administrador puede controlar qué usuarios pueden realizar qué tareas a nivel de objeto de vCenter Server específico y a nivel de sistema de almacenamiento.

- Información de auditoría

En muchos casos, VSC ofrece un seguimiento de auditoría del sistema de almacenamiento que permite asociar los eventos con el usuario de vCenter Server que aplicó el cambio en el almacenamiento.

- Facilidad de uso

Es posible conservar todas las credenciales de la controladora en un mismo lugar.

## **Roles de ONTAP recomendados cuando se usa VSC para VMware vSphere**

Puede configurar varios roles de ONTAP recomendados para trabajar con la consola de almacenamiento virtual para VMware vSphere y el control de acceso basado en roles (RBAC). Estos roles contienen los privilegios de ONTAP necesarios para ejecutar las operaciones de almacenamiento necesarias que ejecutan las tareas de (VSC).

Para crear roles de usuario nuevos, debe iniciar sesión como administrador en sistemas de almacenamiento que ejecutan ONTAP. Es posible crear roles de ONTAP mediante uno de los siguientes:

- 9.7 o posterior

["Configure los roles y privilegios de usuario"](#)

- Herramienta de creación de usuarios de RBAC para ONTAP (si se usa ONTAP 9.6 o una versión anterior)

["Herramienta RBAC User Creator para VSC, proveedor VASA y Storage Replication Adapter 7.0 para VMware vSphere"](#)

Cada rol de ONTAP tiene asociado un nombre de usuario y una pareja de contraseñas 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, los roles de ONTAP específicos de VSC se ordenan jerárquicamente. Esto significa que la primera función es la más restrictiva y que sólo tiene los privilegios asociados con el conjunto más básico de operaciones de almacenamiento VSC. El siguiente rol incluye sus propios privilegios y todos los privilegios asociados con el rol anterior. Cada puesto adicional resulta menos restrictivo en relación con las operaciones de almacenamiento admitidas.

A continuación, se enumeran algunos de los roles de control de acceso basado en roles de ONTAP recomendados cuando se usa VSC. Después de crear estos roles, es posible asignar los roles a los usuarios que deben realizar tareas relacionadas con el almacenamiento, como el aprovisionamiento de máquinas virtuales.

### **1. Detección**

Este rol le permite añadir sistemas de almacenamiento.

### **2. Cree almacenamiento**

Este rol le permite crear almacenamiento. Este rol también incluye todos los privilegios asociados con el rol de detección.

### **3. Modificar almacenamiento**

Este rol permite modificar almacenamiento. Este rol también incluye todos los privilegios asociados con el

rol de detección y creación de almacenamiento.

#### 4. 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 VASA Provider para ONTAP, 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».

## Cómo configurar el control de acceso basado en roles de ONTAP para VSC para VMware vSphere

Debe configurar el control de acceso basado en roles de ONTAP en el sistema de almacenamiento si desea utilizar el control de acceso basado en roles con Virtual Storage Console para VMware vSphere (VSC). Es posible crear una o varias cuentas de usuario personalizadas con privilegios de acceso limitados mediante la función RBAC de ONTAP.

VSC y SRA pueden acceder a los sistemas de almacenamiento a nivel de clúster o de. Si va a añadir sistemas de almacenamiento en el nivel del clúster, debe proporcionar las credenciales del usuario administrador para proporcionar todas las funcionalidades necesarias. Si va a añadir sistemas de almacenamiento agregando detalles directamente, debe ser consciente de que el usuario "vsadmin" no tiene todos los roles y capacidades requeridos para realizar ciertas tareas.

EL proveedor DE VASA puede acceder a los sistemas de almacenamiento únicamente en el nivel del clúster. Si se requiere un proveedor de VASA para una controladora de almacenamiento en particular, debe añadir el sistema de almacenamiento a VSC en el nivel del clúster aunque utilice VSC o SRA.

Para crear un usuario nuevo y conectar un clúster o un a VSC, proveedor VASA y SRA, debe realizar lo siguiente:

- Cree un administrador de clúster o un rol de administrador



Es posible usar uno de los siguientes para crear estos roles:

- ONTAP System Manager 9.7 o posterior

["Configure los roles y privilegios de usuario"](#)

- Herramienta de creación de usuarios de RBAC para ONTAP (si se usa ONTAP 9.6 o una versión anterior)

["Herramienta RBAC User Creator para VSC, proveedor VASA y Storage Replication Adapter 7.0 para VMware vSphere"](#)

- Cree usuarios con el rol asignado y el conjunto de aplicaciones adecuado mediante ONTAP

Es necesario contar con estas credenciales del sistema de almacenamiento para configurar los sistemas de almacenamiento para VSC. Puede configurar sistemas de almacenamiento para VSC introduciendo las credenciales en VSC. Cada vez que inicie sesión en un sistema de almacenamiento con estas credenciales, tendrá permisos sobre las funciones VSC que haya configurado en ONTAP al crear las

credenciales.

- Añada el sistema de almacenamiento a VSC y proporcione las credenciales del usuario que acaba de crear

## Roles de VSC

VSC clasifica los privilegios de ONTAP en el siguiente conjunto de funciones de VSC:

- Detección

Permite la detección de todas las controladoras de almacenamiento conectadas

- Cree almacenamiento

Permite la creación de volúmenes y número de unidad lógica (LUN).

- Modificar almacenamiento

Permite redimensionar y deduplicar los sistemas de almacenamiento

- Destruya el almacenamiento

Permite la destrucción de volúmenes y LUN

## Roles del proveedor DE VASA

Solo puede crear gestión basada en políticas en el nivel de clúster. Este rol permite la gestión basada en políticas del almacenamiento mediante perfiles de capacidades de almacenamiento.

## Roles SRA

El SRA clasifica los privilegios del ONTAP en un rol DE SAN o NAS a nivel de clúster o de. Esto permite a los usuarios ejecutar operaciones de SRM.



Debe consultar los artículos de la base de conocimientos si desea configurar manualmente roles y privilegios mediante comandos ONTAP.

- ["Configuración de RBAC de ONTAP para VSC, VASA y SRA 7.0"](#)
- ["Implementación de todos los comandos para VSC y SRA en nivel de SVM"](#)

VSC realiza una validación de privilegios inicial de los roles de control de acceso basado en roles de ONTAP cuando se añade el clúster a VSC. Si ha añadido una IP de almacenamiento directo, VSC no realizará la validación inicial. VSC comprueba y aplica los privilegios más adelante en el flujo de trabajo de las tareas.

## Configure los roles y privilegios de usuario

Es posible configurar roles de usuario nuevos para gestionar los sistemas de almacenamiento mediante el archivo JSON que se proporciona con el dispositivo virtual para VSC, proveedor VASA y SRA y System Manager de ONTAP.

### Antes de empezar

- Debe haber descargado el archivo de privilegios de ONTAP del dispositivo virtual para VSC, proveedor VASA y SRA con  
[https://{virtual\\_appliance\\_IP}:9083/vsc/config/VSC\\_ONTAP\\_User\\_Privileges.zip](https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip).
- Debe haber configurado ONTAP 9.7 System Manager.
- Inició sesión con privilegios de administrador del sistema de almacenamiento.

## pasos

1. Descomprima el archivo descargado  
[https://{virtual\\_appliance\\_IP}:9083/vsc/config/VSC\\_ONTAP\\_User\\_Privileges.zip](https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip)  
 archivo.
2. Acceda a ONTAP System Manager.
3. Haga clic en **CLUSTER › Configuración › usuarios y roles**.
4. Haga clic en **Agregar usuario**.
5. En el cuadro de diálogo **Agregar usuario**, seleccione **Productos de virtualización**.
6. Haga clic en **examinar** para seleccionar y cargar el archivo JSON de privilegios de ONTAP.

El campo DE PRODUCTO se completa automáticamente.

7. Seleccione la capacidad necesaria en el menú desplegable **CAPACIDAD DEL PRODUCTO**.

El campo **ROL** se rellena automáticamente en función de la capacidad del producto seleccionada.

8. Introduzca el nombre de usuario y la contraseña necesarios.
9. Seleccione los privilegios (Discovery, Create Storage, Modify Storage, Destroy Storage) necesarios para el usuario y, a continuación, haga clic en **Add**.

## Resultados

Se añaden el nuevo rol y el usuario, y se pueden ver los privilegios detallados en el rol que se configuró.

## Información de copyright

Copyright © 2024 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.