Privilegios necesarios para las tareas de VSC

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

Tabla de contenidos

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.	El nivel de asignación determina qué porciones de la interfaz de usuario se muestran. Al asignar el privilegio View en el objeto raíz (carpeta), es posible ingresar a VSC 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 los menús de VSC que se pueden ver y usar. El objeto raíz es el lugar recomendado para asignar cualquier permiso que contiene el privilegio View.

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`.
- 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` 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.