Control de acceso basado en roles (RBAC) de SnapCenter

SnapCenter Software 5.0

NetApp
July 18, 2024

Tabla de contenidos

Control de acceso basado en roles (RBAC) de SnapCenter

Tipos de RBAC

El control de acceso basado en roles (RBAC) de SnapCenter y los permisos de ONTAP permiten que los administradores de SnapCenter delegen el control de los recursos de SnapCenter a diferentes usuarios o grupos de usuarios. Este acceso con gestión central otorga a los administradores de aplicaciones la posibilidad de trabajar con seguridad dentro de entornos delegados.

Es posible crear y modificar roles, y añadir acceso a recursos para usuarios en cualquier momento, pero cuando configura SnapCenter por primera vez, debe añadir al menos usuarios o grupos de Active Directory a roles, y luego añadir acceso a recursos para esos usuarios o grupos.

> No se puede usar SnapCenter para cuentas de usuarios o grupos. Creó cuentas de usuario o de grupo en Active Directory mediante el sistema operativo o la base de datos.

SnapCenter usa los siguientes tipos de control de acceso basado en roles:

- RBAC de SnapCenter
- RBAC para plugin de SnapCenter (para algunos plugins)
- RBAC en el nivel de aplicaciones
- Permisos de ONTAP

RBAC de SnapCenter

Roles y permisos

SnapCenter incluye roles predefinidos con permisos ya asignados. Es posible asignar usuarios o grupos de usuarios a estos roles. También es posible crear nuevos roles y gestionar los permisos y los usuarios.

Asignación de permisos a usuarios o grupos

Es posible asignar permisos a usuarios o grupos para que tengan acceso a objetos de SnapCenter, como hosts, conexiones de almacenamiento y grupos de recursos. No es posible cambiar los permisos del rol SnapCenterAdmin.

Se pueden asignar permisos de RBAC a usuarios y grupos dentro del mismo bosque y a usuarios de distintos bosques. No es posible asignar permisos de RBAC a usuarios que pertenecen a grupos anidados en diferentes bosques.

> Si se crea un rol personalizado, este debe contener todos los permisos del rol SnapCenter Admin. Si solo se copian algunos de los permisos, como Host add o Host remove, no se pueden ejecutar tales operaciones.

Autenticación

Los usuarios deben proporcionar autenticación durante el inicio de sesión, ya sea desde la interfaz gráfica de usuario o mediante cmdlets de PowerShell. Si un usuario es parte de más de un rol, después de introducir las credenciales de inicio de sesión, se le solicita que especifique el rol que desea usar. Los usuarios también deben proporcionar autenticación para ejecutar las API.

RBAC en el nivel de aplicaciones

SnapCenter usa credenciales para verificar que los usuarios de SnapCenter autorizados también tengan permisos en el nivel de aplicaciones.

Por ejemplo, para ejecutar operaciones de Snapshot y protección de datos en un entorno de SQL Server, se deben configurar las credenciales con las credenciales de Windows o SQL correspondientes. El servidor de SnapCenter autentica el conjunto de credenciales con cualquiera de estos métodos. Para ejecutar operaciones de Snapshot y protección de datos en un entorno de sistema de archivos de Windows sobre almacenamiento ONTAP, el rol SnapCenter Admin debe tener privilegios de administrador en el host de Windows.

Del mismo modo, si se desean ejecutar operaciones de protección de datos en una base de datos de Oracle y la autenticación del sistema operativo está deshabilitada en el host de base de datos, se deben configurar las credenciales con la base de datos de Oracle o las credenciales de ASM de Oracle. El servidor de SnapCenter autentica el conjunto de credenciales mediante uno de estos métodos, según la operación.

Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere

Cuando se utiliza el plugin de SnapCenter VMware para protección de datos coherente con máquinas virtuales, vCenter Server ofrece un nivel adicional de control de acceso basado en roles. El plugin de SnapCenter de VMware es compatible con el control de acceso basado en roles de vCenter Server y de Data ONTAP.

Para obtener más información, consulte "Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere"

Permisos de ONTAP

Es necesario crear una cuenta de vsadmin con los permisos requeridos para acceder al sistema de almacenamiento.

Para obtener información sobre cómo crear la cuenta y asignar permisos, consulte "Cree un rol de clúster de ONTAP con privilegios mínimos"

Permisos y roles de RBAC

El control de acceso basado en roles de SnapCenter permite crear roles y asignar permisos a esos roles para luego asignar usuarios o grupos de usuarios a ellos. Esto permite que los administradores de SnapCenter creen un entorno gestionado de manera centralizada, mientras que los administradores de aplicaciones pueden gestionar trabajos de protección de datos. SnapCenter se envía con algunos roles y permisos predefinidos.

Roles de SnapCenter

SnapCenter se envía con los siguientes roles predefinidos. Es posible asignar usuarios y grupos a estos roles, o bien crear roles nuevos.

Cuando se asigna un rol a un usuario, solo los trabajos relevantes para ese usuario son visibles en la página Jobs, a menos que se haya asignado el rol SnapCenter Admin.

- App Backup y Clone Admin
- Backup y Clone Viewer
- Administrador de infraestructuras
- Administrador de SnapCenter

Roles del plugin de SnapCenter para VMware vSphere

Para gestionar la protección de datos coherente con las máquinas virtuales de máquinas virtuales, VMDK y almacenes de datos, el plugin de SnapCenter para VMware vSphere crea los siguientes roles en vCenter:

- Administrador de SCV
- Vista de VCS
- Backup de SCV
- Restauración de SCV
- Restauración de archivos invitados de SCV

Para obtener más información, consulte "Tipos de RBAC para usuarios del plugin de SnapCenter para VMware vSphere"

Mejor práctica: NetApp recomienda crear un rol de ONTAP para las operaciones del plugin de SnapCenter para VMware vSphere y asignarle todos los privilegios necesarios.

Permisos de SnapCenter

SnapCenter otorga los siguientes permisos:

- Grupo de recursos
- Política
- Backup
- Host
- Conexión de almacenamiento
- Clonar
- Aprovisionamiento (solo para bases de datos Microsoft SQL)
- Consola
- Leídos
- Restaurar
    - Restauración de volúmenes completa (solo para plugins personalizados)

- Recurso

  El administrador debe otorgar privilegios de plugins para que los no administradores realicen operaciones de detección de recursos.

- Instalar o desinstalar plugins

  Cuando habilita los permisos de instalación de plugins, también debe modificar el permiso del host para permitir lecturas y actualizaciones.

- Migración
- Montaje (solo para bases de datos de Oracle)
- Desmontaje (solo para bases de datos de Oracle)
- Monitor de trabajos

  El permiso Monitor de trabajo permite a los miembros de diferentes roles ver las operaciones en todos los objetos a los que están asignados.

Roles y permisos predefinidos de SnapCenter

SnapCenter incluye de forma predeterminada varios roles predefinidos, cada uno con un conjunto de permisos ya habilitados. Al configurar y administrar el control de acceso basado en roles, se pueden usar estos roles predefinidos o crear roles nuevos.

SnapCenter incluye los siguientes roles predefinidos:

- SnapCenter Admin
- App Backup and Clone Admin
- Backup and Clone Viewer
- Infrastructure Admin

Cuando se agrega un usuario a un rol, se le debe asignar el permiso StorageConnection para permitir la comunicación con Storage Virtual Machine (SVM) o asignarle una SVM al usuario para habilitar su uso. El permiso Storage Connection permite que los usuarios creen conexiones de SVM.

Por ejemplo, un usuario con el rol SnapCenter Admin puede crear conexiones de SVM y asignarlas a un usuario con el rol App Backup and Clone Admin, cuyos permisos predeterminados no incluyen la creación o edición de SVM. Si no hay una conexión de SVM, los usuarios no pueden ejecutar ninguna operación de backup, clonado o restauración.

SnapCenter Admin

El rol SnapCenter Admin tiene todos los permisos habilitados. No es posible modificar los permisos de este rol. Se pueden agregar usuarios y grupos al rol o quitarlos.

App Backup and Clone Admin

El rol App Backup and Clone Admin tiene los permisos necesarios para ejecutar acciones administrativas para tareas vinculadas con el backup y la clonado de aplicaciones. Este rol no tiene permisos para gestión de

hosts, aprovisionamiento, gestión de conexiones de almacenamiento o instalación remota.

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	Sí	Sí	Sí	Sí
Backup	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	No	Sí	No	No
Clonar	No aplicable	Sí	Sí	Sí	Sí
Provisionamiento	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Leídos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Recurso	Sí	Sí	Sí	Sí	Sí
Instalar/desinstalar plugins	No	No aplicable		No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montaje	Sí	Sí	No aplicable	No aplicable	No aplicable
Desmontar	Sí	Sí	No aplicable	No aplicable	No aplicable
Restaurar volumen completo	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Backup and Clone Viewer

El rol Backup and Clone Viewer tiene una vista de solo lectura de todos los permisos. Este rol también tiene permisos habilitados para detección, generación de informes y acceso a la consola.

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Grupo de recursos	No aplicable	No	Sí	No	No
Política	No aplicable	No	Sí	No	No
Backup	No aplicable	No	Sí	No	No
Host	No aplicable	No	Sí	No	No
Conexión de almacenamiento	No aplicable	No	Sí	No	No
Clonar	No aplicable	No	Sí	No	No
Provisionamiento	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Leídos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar	No	No	No aplicable	No aplicable	No aplicable
Recurso	No	No	Sí	Sí	No
Instalar/desinstalar plugins	No	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montaje	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar volumen completo	No	No aplicable	No aplicable	No aplicable	No aplicable
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Infrastructure Admin

El rol Infrastructure Admin tiene permisos habilitados para gestión de hosts, administración del almacenamiento, aprovisionamiento, grupos de recursos, informes de instalación remota, Y acceso a la consola.

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	No	Sí	Sí	Sí
Backup	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	Sí	Sí	Sí	Sí
Clonar	No aplicable	No	Sí	No	No
Provisionamiento	No aplicable	Sí	Sí	Sí	Sí
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Leídos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Recurso	Sí	Sí	Sí	Sí	Sí
Instalar/desinstalar plugins	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montaje	No	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	No	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar volumen completo	No	No	No aplicable	No aplicable	No aplicable

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable