Utilice usuarios y grupos locales para autenticación y autorización

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/smb-admin/local-users-groups-concepts-concept.html on April 20, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Utilice usuarios y grupos locales para autenticación y autorización . . . 1
Cómo utiliza ONTAP usuarios y grupos locales . . . 1
Qué privilegios locales son . . . 5
Directrices para el uso de grupos BUILTIN y la cuenta de administrador local . . . 7
Requisitos para las contraseñas de usuario local . . . 7
Grupos BUILTIN predefinidos y privilegios predeterminados . . . 8
Habilite o deshabilite la funcionalidad de grupos y usuarios locales . . . 9
Permite gestionar cuentas de usuario local . . . 12
Administrar grupos locales . . . 16
Gestione los privilegios locales . . . 23

Utilice usuarios y grupos locales para autenticación y autorización

Cómo utiliza ONTAP usuarios y grupos locales

Conceptos de usuarios locales y grupos

Debe saber cuáles son los usuarios y grupos locales, así como alguna información básica sobre ellos, antes de determinar si configurar y utilizar usuarios y grupos locales en su entorno.

- **Usuario local**

  Una cuenta de usuario con un identificador de seguridad único (SID) que solo tiene visibilidad en la máquina virtual de almacenamiento (SVM) donde se crea. Las cuentas de usuario local tienen un conjunto de atributos, incluidos el nombre de usuario y el SID. Una cuenta de usuario local autentica de forma local en el servidor CIFS mediante la autenticación NTLM.

  Las cuentas de usuario tienen varios usos:

  - Se utiliza para otorgar privilegios *User Rights Management* a un usuario.
  - Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Grupo local**

  Un grupo con un SID exclusivo tiene visibilidad solo en la SVM donde se crea. Los grupos contienen un conjunto de miembros. Los miembros pueden ser usuarios locales, usuarios de dominio, grupos de dominio y cuentas de equipos de dominio. Los grupos se pueden crear, modificar o eliminar.

  Los grupos tienen varios usos:

  - Se utiliza para otorgar privilegios *User Rights Management* a sus miembros.
  - Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Dominio local**

  Un dominio que tiene un alcance local, delimitado por la SVM. El nombre del dominio local es el nombre del servidor CIFS. Los usuarios y grupos locales se encuentran dentro del dominio local.

- **Identificador de seguridad (SID)**

  Un SID es un valor numérico de longitud variable que identifica los principios de seguridad de estilo Windows. Por ejemplo, un SID típico toma la siguiente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticación NTLM**

  Un método de seguridad de Microsoft Windows que se utiliza para autenticar usuarios en un servidor CIFS.

- **Base de datos replicada en cluster (RDB)**

  Base de datos replicada con una instancia en cada nodo de un clúster. Los objetos de usuario local y de grupo se almacenan en el RDB.

Motivos para crear usuarios locales y grupos locales

Hay varias razones para crear usuarios locales y grupos locales en la máquina virtual de almacenamiento (SVM). Por ejemplo, puede tener acceso a un servidor SMB utilizando una cuenta de usuario local si los controladores de dominio (DC) no están disponibles, es posible que desee utilizar grupos locales para asignar privilegios o que el servidor SMB esté en un grupo de trabajo.

Es posible crear una o varias cuentas de usuario locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los usuarios del dominio no están disponibles.

  Los usuarios locales son necesarios en configuraciones de grupos de trabajo.

- Puede autenticar e iniciar sesión en el servidor SMB si las controladoras de dominio no están disponibles.

  Los usuarios locales pueden autenticarse con el servidor SMB mediante la autenticación NTLM cuando el controlador de dominio está inactivo o cuando los problemas de red impiden que el servidor SMB se ponga en contacto con el controlador de dominio.

- Desea asignar privilegios *User Rights Management* a un usuario local.

  User Rights Management es la capacidad de un administrador de servidor SMB para controlar los derechos que tienen los usuarios y los grupos en la SVM. Puede asignar privilegios a un usuario asignando los privilegios a la cuenta del usuario o haciendo que el usuario sea miembro de un grupo local que tenga esos privilegios.

Se pueden crear uno o varios grupos locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los grupos de dominio no están disponibles.

  Los grupos locales no son necesarios en las configuraciones de grupos de trabajo, pero pueden ser útiles para administrar privilegios de acceso para los usuarios de grupos de trabajo locales.

- Desea controlar el acceso a los recursos de archivos y carpetas mediante grupos locales para controlar el uso compartido y el acceso a archivos.
- Desea crear grupos locales con privilegios *User Rights Management* personalizados.

  Algunos grupos de usuarios integrados tienen privilegios predefinidos. Para asignar un conjunto personalizado de privilegios, puede crear un grupo local y asignar los privilegios necesarios a ese grupo. A continuación, puede agregar usuarios locales, usuarios de dominio y grupos de dominio al grupo local.

Información relacionada

Cómo funciona la autenticación de usuarios locales

Lista de privilegios compatibles

Cómo funciona la autenticación de usuarios locales

Para que un usuario local pueda acceder a los datos en un servidor CIFS, el usuario debe crear una sesión autenticada.

Debido a que el bloque de mensajes del servidor se basa en sesiones, la identidad del usuario se puede determinar una sola vez cuando se configura la sesión por primera vez. El servidor CIFS utiliza autenticación basada en NTLM al autenticar usuarios locales. Se admiten tanto NTLMv1 como NTLMv2.

ONTAP utiliza autenticación local en tres casos de uso. Cada caso de uso depende de si la parte del dominio del nombre de usuario (con el formato de DOMINIO\usuario) coincide con el nombre de dominio local del servidor CIFS (el nombre del servidor CIFS):

- La parte del dominio coincide

  Los usuarios que proporcionan credenciales de usuario local al solicitar acceso a los datos se autentican localmente en el servidor CIFS.

- La parte del dominio no coincide

  ONTAP intenta utilizar la autenticación NTLM con un controlador de dominio del dominio al que pertenece el servidor CIFS. Si la autenticación se realiza correctamente, se completa el inicio de sesión. Si no se realiza correctamente, lo que sucede a continuación depende de por qué la autenticación no se ha realizado correctamente.

  Por ejemplo, si el usuario existe en Active Directory pero la contraseña no es válida o ha caducado, ONTAP no intenta utilizar la cuenta de usuario local correspondiente en el servidor CIFS. En su lugar, la autenticación genera errores. Hay otros casos en los que ONTAP utiliza la cuenta local correspondiente en el servidor CIFS, si existe, para la autenticación, aunque los nombres de dominio NetBIOS no coincidan. Por ejemplo, si existe una cuenta de dominio coincidente pero está deshabilitada, ONTAP utiliza la cuenta local correspondiente en el servidor CIFS para la autenticación.

- No se ha especificado la parte del dominio

  ONTAP intenta primero la autenticación como usuario local. Si la autenticación como usuario local falla, ONTAP autentica al usuario con una controladora de dominio en el dominio al que pertenece el servidor CIFS.

Una vez que la autenticación de usuario local o de dominio se ha completado correctamente, ONTAP crea un token de acceso de usuario completo, que tiene en cuenta la pertenencia a grupos locales y los privilegios.

Para obtener más información acerca de la autenticación NTLM para usuarios locales, consulte la documentación de Microsoft Windows.

Información relacionada

Habilitar o deshabilitar la autenticación de usuario local

Cómo se construyen los tokens de acceso de usuario

Cuando un usuario asigna un recurso compartido, se establece una sesión SMB autenticada y se crea un token de acceso de usuario que contiene información acerca del usuario, la pertenencia al grupo del usuario y los privilegios acumulativos, así como el usuario UNIX asignado.

A menos que la funcionalidad esté deshabilitada, la información de grupo y de usuario local también se agrega al token de acceso de usuario. La forma en que se crean los tokens de acceso depende de si el inicio de sesión es para un usuario local o un usuario de dominio de Active Directory:

- Inicio de sesión de usuario local

  Aunque los usuarios locales pueden ser miembros de diferentes grupos locales, los grupos locales no pueden ser miembros de otros grupos locales. El token de acceso de usuario local se compone de una unión de todos los privilegios asignados a grupos a los que pertenece un usuario local determinado.

- Inicio de sesión de usuario de dominio

  Cuando un usuario de dominio inicia sesión, ONTAP obtiene un token de acceso de usuario que contiene el SID y SID de usuario para todos los grupos de dominio a los que pertenece el usuario. ONTAP utiliza la unión del token de acceso de usuario de dominio con el token de acceso proporcionado por las membresías locales de los grupos de dominio del usuario (si los hay), así como todos los privilegios directos asignados al usuario de dominio o cualquiera de sus pertenencias a grupos de dominio.

Tanto para el inicio de sesión local como para el usuario de dominio, el RID de grupo principal también está configurado para el token de acceso de usuario. EL RID predeterminado es `Domain Users` (RID 513). No puede cambiar el valor predeterminado.

El proceso de asignación de nombres de Windows a UNIX y UNIX a Windows sigue las mismas reglas para las cuentas locales y de dominio.

> No hay ningún mapeo implícito y automático de un usuario UNIX a una cuenta local. Si es necesario, se debe especificar una regla de asignación explícita mediante los comandos de asignación de nombres existentes.

Directrices para usar SnapMirror en SVM que contienen grupos locales

Debe tener en cuenta las directrices al configurar SnapMirror en los volúmenes que son propiedad de las SVM que contienen grupos locales.

No se pueden utilizar grupos locales en ACE aplicados a archivos, directorios o recursos compartidos replicados por SnapMirror en otra SVM. Si utiliza la función SnapMirror para crear un reflejo de recuperación ante desastres en un volumen en otra SVM y el volumen tiene una ACE para un grupo local, la ACE no es válida en el reflejo. Si los datos se replican en una SVM diferente, estos se cruzan realmente en un dominio local diferente. Los permisos concedidos a los usuarios y grupos locales solo son válidos dentro del ámbito de la SVM en la que se crearon originalmente.

Lo que sucede a los usuarios locales y los grupos al eliminar servidores CIFS

El conjunto predeterminado de usuarios y grupos locales se crea cuando se crea un servidor CIFS y está asociado con las máquinas virtuales de almacenamiento (SVM) que alojan el servidor CIFS. Los administradores de SVM pueden crear usuarios y grupos locales en cualquier momento. Debe saber qué sucede con los usuarios locales y los grupos al eliminar el servidor CIFS.

Los usuarios y grupos locales están asociados a las SVM; por lo tanto, no se eliminan cuando los servidores CIFS se eliminan debido a consideraciones de seguridad. Aunque los usuarios y grupos locales no se eliminan al eliminar el servidor CIFS, sí se ocultan. No se pueden ver ni gestionar usuarios y grupos locales

hasta que se vuelva a crear un servidor CIFS en la SVM.

> El estado administrativo del servidor CIFS no afecta a la visibilidad de los grupos o usuarios locales.

Cómo puede utilizar Microsoft Management Console con usuarios y grupos locales

Puede ver información acerca de los usuarios y grupos locales desde la Consola de administración de Microsoft. Con esta versión de ONTAP, no puede realizar otras tareas de administración para usuarios y grupos locales desde la Consola de administración de Microsoft.

Directrices para revertir

Si piensa revertir el clúster a una versión de ONTAP que no da soporte a usuarios y grupos locales y se están utilizando grupos y usuarios locales para gestionar los derechos de usuario o el acceso a los archivos, debe tener en cuenta ciertas consideraciones.

- Debido a motivos de seguridad, no se elimina la información sobre usuarios locales, grupos y privilegios configurados cuando ONTAP se revierte a una versión que no admite la funcionalidad de usuarios y grupos locales.
- Al volver a una versión principal anterior de ONTAP, ONTAP no utiliza usuarios ni grupos locales durante la autenticación ni la creación de credenciales.
- Los usuarios y grupos locales no se quitan de las ACL de archivos y carpetas.
- Se deniegan las solicitudes de acceso a archivos que dependen de que se conceda el acceso debido a los permisos concedidos a los usuarios o grupos locales.

  Para permitir el acceso, debe volver a configurar los permisos de archivo para permitir el acceso basado en objetos de dominio en lugar de objetos de usuario local y de grupo.

Qué privilegios locales son

Lista de privilegios compatibles

ONTAP tiene un conjunto predefinido de privilegios admitidos. Algunos grupos locales predefinidos tienen algunos de estos privilegios añadidos de forma predeterminada. También puede agregar o quitar privilegios de los grupos predefinidos o crear nuevos usuarios o grupos locales y agregar privilegios a los grupos que creó o a los usuarios y grupos de dominio existentes.

En la siguiente tabla se enumeran los privilegios admitidos en la máquina virtual de almacenamiento (SVM) y se proporciona una lista de los grupos BUILTIN con privilegios asignados:

Nombre del privilegio	Configuración de seguridad predeterminada	Descripción
`SeTcbPrivilege`	Ninguno	Actuar como parte del sistema operativo
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Realice copias de seguridad de archivos y directorios, anulando cualquier ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restaurar archivos y directorios, anulando cualquier ACL establecer cualquier SID de usuario o grupo válido como propietario del archivo
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Tomar posesión de archivos u otros objetos
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gestionar auditoría Esto incluye ver, volcar y borrar el registro de seguridad.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Comprobación de desvío transversal No es necesario que los usuarios con este privilegio tengan permisos de desplazamiento (x) para recorrer carpetas, vínculos simbólicos o uniones.

Información relacionada

- Asigne privilegios locales
- Configuración de la comprobación de recorrido de derivación

Asigne privilegios

Es posible asignar privilegios directamente a usuarios locales o a usuarios de dominio. También puede asignar usuarios a grupos locales cuyos privilegios asignados coincidan con las capacidades que desea que tengan esos usuarios.

- Puede asignar un conjunto de privilegios a un grupo que cree.

  A continuación, agregue un usuario al grupo que tenga los privilegios que desea que tenga ese usuario.

- También puede asignar usuarios locales y usuarios de dominio a grupos predefinidos cuyos privilegios predeterminados coincidan con los privilegios que desea conceder a esos usuarios.

Información relacionada

- Adición de privilegios a usuarios o grupos locales o de dominio
- Quitar privilegios de usuarios o grupos locales o de dominio
- Restableciendo privilegios para usuarios y grupos locales o de dominio
- Configuración de la comprobación de recorrido de derivación

Directrices para el uso de grupos BUILTIN y la cuenta de administrador local

Hay ciertas pautas que debe tener en cuenta cuando utilice los grupos BUILTIN y la cuenta de administrador local. Por ejemplo, puede cambiar el nombre de la cuenta de administrador local, pero no puede eliminar esta cuenta.

- Se puede cambiar el nombre de la cuenta Administrador, pero no se puede eliminar.
- La cuenta de administrador no se puede quitar del grupo BUILTIN\Administrators.
- Se puede cambiar el nombre de los grupos INTEGRADOS, pero no se pueden eliminar.

  Después de cambiar el nombre del grupo BUILTIN, se puede crear otro objeto local con el nombre bien conocido; sin embargo, al objeto se le asigna UN NUEVO RID.

- No hay una cuenta de invitado local.

Información relacionada

Grupos BUILTIN predefinidos y privilegios predeterminados

Requisitos para las contraseñas de usuario local

De manera predeterminada, las contraseñas de usuario local deben cumplir con los requisitos complejos. Los requisitos de complejidad de la contraseña son similares a los que se definen en la directiva de seguridad local de Microsoft Windows.

La contraseña debe cumplir los siguientes criterios:

- Debe tener al menos seis caracteres de longitud
- No se debe contener el nombre de cuenta de usuario
- Debe contener caracteres de al menos tres de las siguientes cuatro categorías:
  - Caracteres en mayúsculas (De La A a la Z)
  - Caracteres en minúscula (de la a a la z)
  - Base de 10 dígitos (de 0 a 9)
  - Caracteres especiales:

    ~ ! @ # $ % ^ & * _ - + = ' \ | ( ) [ ] : ; " < > , . ? /

Información relacionada

Habilitar o deshabilitar la complejidad de contraseña necesaria para los usuarios locales de la SMB

Mostrar información acerca de la configuración de seguridad del servidor CIFS

Grupos BUILTIN predefinidos y privilegios predeterminados

Puede asignar la pertenencia de un usuario local o un usuario de dominio a un conjunto predefinido de grupos BUILTIN proporcionados por ONTAP. Los grupos predefinidos tienen privilegios predefinidos asignados.

En la siguiente tabla se describen los grupos predefinidos:

Grupo BUILTIN predefinido	Privilegios predeterminados
`BUILTIN\Administrators`RID 544 Cuando se crea por primera vez, el local `Administrator` La cuenta, CON UN RID de 500, se hace automáticamente miembro de este grupo. Cuando la máquina virtual de almacenamiento (SVM) se une a un dominio, el `domain\Domain Admins` el grupo se agrega al grupo. Si la SVM sale del dominio, el `domain\Domain Admins` el grupo se elimina del grupo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo tienen las siguientes características: • Puede crear y administrar usuarios y grupos locales. • No se pueden agregar a sí mismos ni a ningún otro objeto `BUILTIN\Administrators` grupo.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo pueden anular los permisos de lectura y escritura en archivos o carpetas si se abren con la intención de copia de seguridad.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`

Grupo BUILTIN predefinido	Privilegios predeterminados
`BUILTIN\Users`RID 545 Cuando se crea por primera vez, este grupo no tiene ningún miembro (además del implícito `Authenticated Users` grupo especial). Cuando la SVM se une a un dominio, el `domain\Domain Users` el grupo se agrega a este grupo. Si la SVM sale del dominio, el `domain\Domain Users` el grupo se elimina de este grupo.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Este grupo incluye a todos los usuarios, incluidos invitados (pero no usuarios anónimos). Este es un grupo implícito con una membresía implícita.	`SeChangeNotifyPrivilege`

Información relacionada

Directrices para el uso de grupos BUILTIN y la cuenta de administrador local

Lista de privilegios compatibles

Configuración de la comprobación de recorrido de derivación

Habilite o deshabilite la funcionalidad de grupos y usuarios locales

Habilite o deshabilite la descripción general de la funcionalidad de los usuarios locales y los grupos

Antes de poder utilizar usuarios y grupos locales para controlar el acceso a los datos del estilo de seguridad NTFS, se debe habilitar la funcionalidad de usuario local y grupo. Además, si desea utilizar usuarios locales para la autenticación SMB, se debe habilitar la funcionalidad de autenticación de usuarios locales.

La funcionalidad de grupos y usuarios locales y la autenticación de usuarios locales están habilitadas de forma predeterminada. Si no están habilitadas, debe habilitarlas para poder configurar y utilizar usuarios y grupos locales. La funcionalidad de grupos y usuarios locales se puede deshabilitar en cualquier momento.

Además de deshabilitar explícitamente la funcionalidad de grupo y usuario local, ONTAP deshabilita la funcionalidad de grupo y usuario local si algún nodo del clúster se revierte a una versión de ONTAP que no admite la funcionalidad. La funcionalidad de usuario local y de grupo no está habilitada hasta que todos los nodos del clúster ejecuten una versión de ONTAP que la admita.

Información relacionada

Modifique las cuentas de usuario local

Modificar grupos locales

Añada privilegios a usuarios o grupos locales o de dominio

Habilite o deshabilite usuarios y grupos locales

Puede habilitar o deshabilitar usuarios y grupos locales para el acceso SMB en máquinas virtuales de almacenamiento (SVM). La funcionalidad de grupos y usuarios locales está activada de forma predeterminada.

Acerca de esta tarea

Puede usar usuarios y grupos locales al configurar los permisos de archivos NTFS y compartidos de SMB, y puede usar, opcionalmente, usuarios locales para la autenticación al crear una conexión SMB. Para usar usuarios locales para la autenticación, también debe habilitar la opción de autenticación de grupos y usuarios locales.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que los grupos y usuarios locales sean…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo habilita la funcionalidad de grupos y usuarios locales en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

Habilite o deshabilite la autenticación de usuario local

Habilite o deshabilite la autenticación de usuario local

Puede habilitar o deshabilitar la autenticación de usuario local para el acceso SMB en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es permitir la autenticación de usuario local, que resulta útil cuando la SVM no puede ponerse en contacto con un controlador de dominio o si decide no utilizar controles de acceso a nivel de dominio.

Antes de empezar

La funcionalidad de grupos y usuarios locales debe estar habilitada en el servidor CIFS.

Acerca de esta tarea

Es posible habilitar o deshabilitar la autenticación de usuario local en cualquier momento. Si desea usar usuarios locales para la autenticación al crear una conexión SMB, también debe habilitar la opción de grupos y usuarios locales del servidor CIFS.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que la autenticación local sea…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo habilita la autenticación de usuario local en SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

Cómo funciona la autenticación de usuarios locales

Habilitar o deshabilitar usuarios y grupos locales

Permite gestionar cuentas de usuario local

Modifique las cuentas de usuario local

Puede modificar una cuenta de usuario local si desea cambiar el nombre completo o la descripción de un usuario existente y si desea habilitar o deshabilitar la cuenta de usuario. También puede cambiar el nombre de una cuenta de usuario local si el nombre del usuario está en peligro o si se necesita un cambio de nombre con fines administrativos.

Si desea…	Introduzca el comando…
Modifique el nombre completo del usuario local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Si el nombre completo contiene un espacio, debe estar entre comillas dobles.
Modifique la descripción del usuario local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Si la descripción contiene un espacio, debe estar entre comillas dobles.
Habilite o deshabilite la cuenta de usuario local	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	Cambie el nombre de la cuenta de usuario local

Ejemplo

En el siguiente ejemplo, se cambia el nombre del usuario local «'CIFS_SERVER\sue'» a «'CIFS_SERVER\sue_new» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Habilite o deshabilite cuentas de usuario locales

Es posible habilitar una cuenta de usuario local si desea que el usuario pueda acceder a los datos contenidos en la máquina virtual de almacenamiento (SVM) a través de una

conexión de SMB. También puede deshabilitar una cuenta de usuario local si no desea que ese usuario acceda a los datos de SVM mediante SMB.

Acerca de esta tarea

Para habilitar un usuario local, debe modificar la cuenta de usuario.

Paso

1. Ejecute la acción adecuada:

Si desea…	Introduzca el comando…
Habilite la cuenta de usuario	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`
Desactive la cuenta de usuario	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

Cambiar las contraseñas de la cuenta de usuario local

Es posible cambiar la contraseña de la cuenta de un usuario local. Esto puede ser útil si la contraseña del usuario está en peligro o si el usuario ha olvidado la contraseña.

Paso

1. Realice la acción correspondiente para cambiar la contraseña: `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

Ejemplo

En el siguiente ejemplo, se establece la contraseña del usuario local "'CIFS_SERVER\sue'" asociada con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Información relacionada

Habilitar o deshabilitar la complejidad de contraseña necesaria para los usuarios locales de la SMB

Mostrar información acerca de la configuración de seguridad del servidor CIFS

Muestra información acerca de los usuarios locales

Puede mostrar una lista de todos los usuarios locales en un formulario de resumen. Si desea determinar qué configuración de cuenta está configurada para un usuario específico, puede mostrar información detallada de la cuenta para ese usuario, así como la información de la cuenta para varios usuarios. Esta información puede ayudarle a determinar si necesita modificar la configuración de un usuario y también a resolver problemas de autenticación o acceso a archivos.

Acerca de esta tarea

Nunca se muestra información sobre la contraseña de un usuario.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Mostrar información sobre todos los usuarios de la máquina virtual de almacenamiento (SVM)	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Muestra información detallada de la cuenta de un usuario	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

Hay otros parámetros opcionales que puede elegir cuando ejecuta el comando. Consulte la página del manual para obtener más información.

Ejemplo

El siguiente ejemplo muestra información sobre todos los usuarios locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- --------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Muestra información acerca de las pertenencias a grupos de usuarios locales

Puede mostrar información sobre los grupos locales a los que pertenece un usuario local. Puede utilizar esta información para determinar qué acceso debe tener el usuario a los archivos y carpetas. Esta información puede ser útil para determinar qué derechos de acceso debe tener el usuario a los archivos y carpetas o al solucionar problemas de acceso a archivos.

Acerca de esta tarea

Puede personalizar el comando para que muestre solo la información que desea ver.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Muestra información de pertenencia de usuario local para un usuario local específico	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
Mostrar información de pertenencia al usuario local para el grupo local del que forma parte este usuario local	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Mostrar información de pertenencia al usuario para los usuarios locales que están asociados a una máquina virtual de almacenamiento (SVM) especificada	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Mostrar información detallada para todos los usuarios locales en una SVM especificada	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo se muestra la información de pertenencia de todos los usuarios locales de SVM vs1; el usuario «'CIFS_SERVER\Administrator'» es miembro del grupo «'BUILTIN\Administrators'» y «'CIFS_SERVER\sue'» es miembro del grupo «'CIFS_SERVER\g1'»:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Eliminar cuentas de usuario locales

Es posible eliminar cuentas de usuario locales de la máquina virtual de almacenamiento (SVM) si ya no son necesarias para la autenticación local de SMB en el servidor CIFS o para determinar los derechos de acceso a los datos incluidos en la SVM.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar usuarios locales:

- El sistema de archivos no se ha modificado.

Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este usuario no están ajustados.

- Todas las referencias a los usuarios locales se eliminan de las bases de datos de pertenencia y privilegios.
- No se pueden eliminar los usuarios estándar conocidos, como el Administrador.

Pasos

1. Determine el nombre de la cuenta de usuario local que desea eliminar: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Elimine el usuario local: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Compruebe que la cuenta de usuario se ha eliminado: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo se elimina el usuario local "'CIFS_SERVER\sue'" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Administrar grupos locales

Modificar grupos locales

Puede modificar los grupos locales existentes cambiando la descripción de un grupo local existente o cambiando el nombre del grupo.

Si desea…	Usar el comando…
Modifique la descripción del grupo local	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` Si la descripción contiene un espacio, debe estar entre comillas dobles.
Cambie el nombre del grupo local	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Ejemplos

En el ejemplo siguiente se cambia el nombre del grupo local "'CIFS_SERVER\engineering'" a "'CIFS_SERVER\engineering_new'":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

En el siguiente ejemplo se modifica la descripción del grupo local "'CIFS_SERVER\engineering'":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Muestra información acerca de los grupos locales

Es posible mostrar una lista de todos los grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) específica. Esta información puede ser útil para solucionar problemas de acceso a los archivos en la SVM o problemas de derechos de usuario (privilegios) en la SVM.

Paso

1. Ejecute una de las siguientes acciones:

Si desea información acerca de…	Introduzca el comando…
Todos los grupos locales del clúster	`vserver cifs users-and-groups local-group show`
Todos los grupos locales en la SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Consulte la página del

manual para obtener más información.

Ejemplo

En el siguiente ejemplo, se muestra información sobre todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Administrar la pertenencia a grupos locales

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

Acerca de esta tarea

Directrices para agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.
- El grupo local debe existir antes de poder añadir un usuario.
- El usuario debe existir antes de poder agregar el usuario a un grupo local.
- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, Data ONTAP debe poder resolver el nombre a un SID.

Directrices para eliminar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- El grupo del que desea quitar un miembro debe existir.
- ONTAP debe poder resolver los nombres de los miembros que desea quitar del grupo a un SID correspondiente.

Paso

1. Agregar o quitar un miembro de un grupo.

Si desea…	A continuación, se usa el comando…
Agregar un miembro a un grupo	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee agregar al grupo local especificado.
Quitar un miembro de un grupo	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee quitar del grupo local especificado.

En el siguiente ejemplo, se agrega un usuario local "MB_SERVER\sue" y un grupo de dominios "'AD_DOM\dom_eng'" al grupo local "MB_SERVER\engineering" en SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

En el siguiente ejemplo se eliminan los usuarios locales «MB_SERVER\sue» y «MB_SERVER\james» del grupo local «MB_SERVER\engineering» de SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Información relacionada

Mostrar información acerca de los miembros de los grupos locales

Muestra información acerca de los miembros de los grupos locales

Es posible mostrar una lista de todos los miembros de grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ser útil para solucionar problemas de acceso a archivos o problemas de derechos de usuario (privilegios).

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Miembros de todos los grupos locales del cluster	`vserver cifs users-and-groups local-group show-members`
Miembros de todos los grupos locales en la SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo, se muestra información acerca de los miembros de todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Eliminar un grupo local

Es posible eliminar un grupo local de la máquina virtual de almacenamiento (SVM) si ya no es necesario para determinar los derechos de acceso a los datos asociados con esa SVM o si ya no es necesario para asignar los derechos de usuario (privilegios) de SVM a los miembros del grupo.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar grupos locales:

- El sistema de archivos no se ha modificado.

  Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este grupo no se ajustan.

- Si el grupo no existe, se devuelve un error.
- El grupo especial *Everyone* no se puede eliminar.
- Los grupos integrados como *BUILTIN\Administrators BUILTIN\Users* no se pueden eliminar.

Pasos

1. Determine el nombre del grupo local que desea eliminar mostrando la lista de grupos locales de la SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`

2. Elimine el grupo local: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Compruebe que el grupo se ha eliminado: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo se elimina el grupo local "'CIFS_SERVER\sales'" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

Actualizar nombres de usuario y grupo de dominio en bases de datos locales

Puede agregar usuarios y grupos de dominio a los grupos locales de un servidor CIFS. Estos objetos de dominio se registran en bases de datos locales en el clúster. Si se cambia el nombre de un objeto de dominio, las bases de datos locales deben actualizarse manualmente.

Acerca de esta tarea

Debe especificar el nombre de la máquina virtual de almacenamiento (SVM) en la que desea actualizar los nombres de dominio.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`

2. Ejecute la acción adecuada:

Si desea actualizar usuarios y grupos de dominio y…	Se usa este comando…
Muestra usuarios y grupos de dominio que se han actualizado correctamente y que no se han podido actualizar	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*
Muestra los usuarios y grupos de dominio que se han actualizado correctamente	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only false`
Muestra sólo los usuarios y grupos de dominio que no se pueden actualizar	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only true`
Suprimir toda la información de estado acerca de las actualizaciones	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-suppress -all-output true`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

En el siguiente ejemplo se actualizan los nombres de los usuarios y grupos de dominio asociados con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Para la última actualización, hay una cadena de nombres dependiente que se debe actualizar:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Gestione los privilegios locales

Añada privilegios a usuarios o grupos locales o de dominio

Puede administrar los derechos de usuario para usuarios o grupos locales o de dominio mediante la adición de privilegios. Los privilegios agregados anulan los privilegios predeterminados asignados a cualquiera de estos objetos. Esto proporciona una seguridad mejorada al permitirle personalizar qué privilegios tiene un usuario o grupo.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio al que se añadirán privilegios.

Acerca de esta tarea

Al agregar un privilegio a un objeto se reemplazan los privilegios predeterminados para ese usuario o grupo. Al añadir un privilegio, no se quitan los privilegios añadidos anteriormente.

Debe tener en cuenta lo siguiente al agregar privilegios a usuarios o grupos locales o de dominio:

- Puede añadir uno o varios privilegios.
- Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

  Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Agregue uno o más privilegios a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Compruebe que los privilegios deseados se aplican al objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplo

En el siguiente ejemplo, se añaden los privilegios «ShebPrivilege» y «SeeTakeOwnershipPrivilege» al usuario «'CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Quitar privilegios de usuarios o grupos locales o de dominio

Puede administrar derechos de usuario para usuarios o grupos locales o de dominio

eliminando privilegios. Esto proporciona una seguridad mejorada al permitirle personalizar los privilegios máximos que tienen los usuarios y los grupos.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

Acerca de esta tarea

Al quitar privilegios de usuarios o grupos locales o de dominio, debe tener en cuenta lo siguiente:

- Puede eliminar uno o varios privilegios.
- Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

  Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Elimine uno o más privilegios de un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Compruebe que los privilegios deseados se han eliminado del objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

En el siguiente ejemplo se eliminan los privilegios «DeeTcbPrivilege» y «SeeTakeOwnershipPrivilege» del usuario «'CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Restablecer privilegios para usuarios y grupos locales o de dominio

Es posible restablecer privilegios para los grupos y usuarios locales o de dominio. Esto puede ser útil si ha realizado modificaciones a los privilegios de un usuario o grupo local

o de dominio y esas modificaciones ya no se desean ni se necesitan.

Acerca de esta tarea

Al restablecer los privilegios de un usuario o grupo local o de dominio, se quitan todas las entradas de privilegios de ese objeto.

Pasos

1. Restablecer los privilegios de un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Compruebe que los privilegios se restablecen en el objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplos

En el siguiente ejemplo, se restablecen los privilegios para el usuario «'CIFS_SERVER\sue'» en la máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver) vs1. De forma predeterminada, los usuarios normales no tienen privilegios asociados a sus cuentas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

En el ejemplo siguiente se restablecen los privilegios para el grupo "'BUILTIN\Administrators'", eliminando de forma efectiva la entrada de privilegios:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Muestra información acerca de anulaciones de privilegios

Puede mostrar información acerca de los privilegios personalizados asignados a cuentas o grupos de usuarios locales o de dominio. Esta información le ayuda a determinar si se aplican los derechos de usuario deseados.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca este comando…
Privilegios personalizados para todos los grupos y usuarios locales y de dominio en la máquina virtual de almacenamiento (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Privilegios personalizados para un dominio o un grupo y usuario local específicos de la SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Consulte la página del manual para obtener más información.

Ejemplo

El siguiente comando muestra todos los privilegios asociados explícitamente con los usuarios y grupos locales o de dominio para SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

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.