Control de acceso basado en funciones de SnapDrive para UNIX

Snapdrive for Unix

NetApp
August 08, 2024

Tabla de contenidos

Control de acceso basado en funciones de SnapDrive para UNIX

El control de acceso basado en roles (RBAC) se usa para el inicio de sesión de usuario y permisos de roles. Con RBAC, los administradores pueden gestionar grupos de usuarios al definir roles. Si necesita restringir el acceso a la base de datos a administradores específicos, debe configurar cuentas de administrador para ellos. Además, si desea restringir la información, estos administradores pueden ver y las operaciones que pueden realizar, debe aplicar roles a las cuentas de administrador que cree.

El control de acceso basado en roles se utiliza en SnapDrive para UNIX con la ayuda de la consola de Operations Manager. La consola de Operations Manager proporciona acceso granular a objetos de almacenamiento como LUN, qtrees, volúmenes, agregados y unidades vFiler.

Información relacionada

Comprobaciones obligatorias para SnapRestore basado en volúmenes

Restaurar copias de Snapshot en un sistema de almacenamiento de destino

Procedimiento de desconexión de presión

Lo que es el control de acceso basado en roles (RBAC) de SnapDrive para UNIX

RBAC permite que los administradores de SnapDrive restrinjan el acceso a un sistema de almacenamiento para diversas operaciones de SnapDrive. Este acceso limitado o completo para operaciones de almacenamiento depende del rol asignado al usuario.

SnapDrive 4.0 para UNIX y versiones posteriores requieren una comprobación de acceso RBAC para todas las operaciones de SnapDrive para UNIX. Este comportamiento permite que los administradores de almacenamiento limiten las operaciones que pueden realizar los usuarios de SnapDrive según los roles asignados. El control de acceso basado en roles se implementa mediante la infraestructura de Operations Manager. En las versiones anteriores a SnapDrive 4.0 para UNIX, había un control de acceso limitado y solo el usuario raíz podía ejecutar operaciones de SnapDrive para UNIX. SnapDrive 4.0 para UNIX y versiones posteriores ofrece compatibilidad para usuarios locales que no son raíz y usuarios de Network Information System (NIS) utilizando la infraestructura RBAC de la consola de Operations Manager. SnapDrive para UNIX no requiere la contraseña raíz del sistema de almacenamiento y se comunica con el sistema de almacenamiento mediante el usuario de sd-<hostname>.

De manera predeterminada, no se utiliza la funcionalidad RBAC de la consola de Operations Manager. Debe activar la funcionalidad RBAC configurando la variable *`rbac-method=dfm`* en la `snapdrive.conf` File y reinicie el daemon SnapDrive para UNIX.

Para poder utilizar esta función, se deben cumplir los siguientes requisitos:

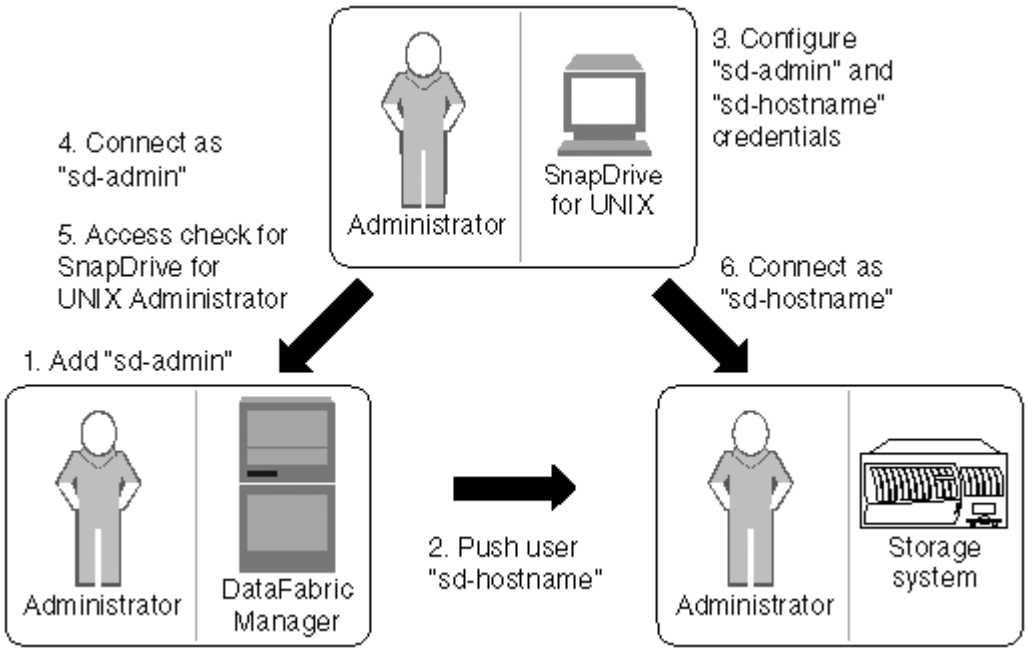
- Operations Manager Console 3.7 o posterior.
- El servidor de consola de Operations Manager debe estar presente y configurado en la red IP que contiene los hosts SnapDrive y los sistemas de almacenamiento.

- Los ajustes de comunicación de la consola de Operations Manager se deben configurar durante la instalación de SnapDrive.
- El daemon SnapDrive para UNIX debe estar en ejecución.

Interacción de la consola de SnapDrive para UNIX y Operations Manager

El uso del control de acceso basado en roles (RBAC) depende de la infraestructura de la consola de Operations Manager. El administrador de la consola de Operations Manager debe crear nombres de usuario para uso de SnapDrive para UNIX. Todas las solicitudes de operaciones de almacenamiento se envían primero a la consola de Operations Manager para obtener una comprobación de acceso. Una vez que la consola de Operations Manager verifica una operación de almacenamiento de un usuario de SnapDrive específico, la operación se completa.

El siguiente diagrama muestra todo el control de acceso basado en roles para operaciones de almacenamiento.



1. El administrador de la consola de Operations Manager agrega el usuario de sd-admin en la consola de Operations Manager.
2. El administrador de la consola de Operations Manager crea un usuario de host sd en el sistema de almacenamiento.
3. El administrador de la consola de Operations Manager envía credenciales de sd-admin y sd-hostname a SnapDrive para el administrador de UNIX.
4. El administrador de SnapDrive configura SnapDrive con las credenciales de usuario recibidas.
5. La consola de Operations Manager realiza la comprobación de acceso para el uso de SnapDrive para UNIX con las credenciales de usuario agregadas por el administrador de SnapDrive.
6. Una vez autenticado el usuario de SnapDrive, el usuario puede conectarse al sistema de almacenamiento.

Cuando un usuario de SnapDrive desea realizar alguna operación de almacenamiento, el usuario emite el comando correspondiente en la línea de comandos. La solicitud se envía a la consola de Operations Manager para realizar una comprobación de acceso. La consola del Gestor de operaciones comprueba si el usuario solicitado tiene los permisos adecuados para realizar la operación SnapDrive. El resultado de la comprobación de acceso se devuelve a SnapDrive. Según el resultado, al usuario se le permite o no realizar las operaciones de almacenamiento en el sistema de almacenamiento.

Si el usuario se verifica después de la comprobación de acceso, el usuario se conecta al sistema de almacenamiento como sd-hostname.

> sd-hostname y sd-admin son los nombres de usuario recomendados. Es posible configurar SnapDrive para UNIX con otros nombres de usuario.

La configuración del control de acceso basado en roles de SnapDrive para UNIX

Debe completar varias tareas para configurar el control de acceso basado en roles (RBAC) para SnapDrive para UNIX. Puede usar la consola de Operations Manager o la interfaz de línea de comandos para ejecutar las tareas.

Configuración de sd-admin en la consola de Operations Manager

El administrador de la consola de Operations Manager puede crear el usuario de sd-admin.

El administrador de la consola de Operations Manager crea un usuario llamado sd-admin, con la capacidad de realizar una comprobación de acceso principal en el grupo global (global `DFM.Core.AccessCheck`). Una vez que el administrador de la consola de Operations Manager configura el usuario de sd-admin, debe enviar manualmente la información de las credenciales al administrador de SnapDrive para UNIX. Para obtener más información acerca del uso de la consola de Operations Manager para configurar usuarios y funciones, consulte la *Guía de administración de la consola de Operations Manager* y la Ayuda en línea.

> Puede utilizar cualquier nombre en lugar de sd-admin; sin embargo, es mejor utilizar sd-admin.

Para crear una función en la consola de Operations Manager, seleccione **Configuración** > **roles**. En la página de configuración de sd-admin, debe asignar el administrador de la consola de Operations Manager `DFM.Database.Write` Capacidad del grupo global para el rol de sd-admin, de modo que SnapDrive para UNIX pueda actualizar entidades de almacenamiento en la consola de Operations Manager.

Configuración de sd-admin mediante la interfaz de línea de comandos

El administrador del sistema de almacenamiento puede configurar el usuario sd-admin mediante la interfaz de línea de comandos.

Pasos

1. Agregue un usuario llamado sd-admin.

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. Agregue un administrador llamado sd-admin.

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. Cree una función denominada sd-admin-role.

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. Añada una funcionalidad al rol creado en el paso 3.

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. También puede otorgar el administrador de Operations Manager `DFM.Database.Write` capacidad del grupo global para `<sd-admin>` Para permitir que SnapDrive para UNIX actualice las entidades de los sistemas de almacenamiento en Operations Manager.

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. Añada una función sd-admin al usuario sd-admin.

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

Incorporación de sd-hostname al sistema de almacenamiento

El administrador de la consola de Operations Manager puede crear el usuario de host sd en el sistema de almacenamiento usando la consola de Operations Manager. Una vez realizados los pasos, el administrador de la consola de Operations Manager debe enviar manualmente las credenciales al administrador de SnapDrive para UNIX. Puede utilizar cualquier nombre en lugar de sd-hostname; sin embargo, es mejor usar sd-hostname.

Pasos

1. Obtenga la contraseña raíz del sistema de almacenamiento y almacene la contraseña.

   Para agregar la contraseña para el sistema de almacenamiento, seleccione **Administración** > **sistema de almacenamiento**.

2. Cree un usuario de sd-hostname para cada sistema UNIX.
3. Asigne capacidades `api- y.. login-` a una función, como sd-role.
4. Incluya esta función (sd-role) en un nuevo grupo de usuarios, como sd-usergroup.
5. Asocie este grupo de usuarios (sd-usergroup) al usuario sd-hostname del sistema de almacenamiento.

Adición de un nombre de host de sd al sistema de almacenamiento mediante la CLI

El administrador del sistema de almacenamiento puede crear y configurar el usuario de sd-hostname mediante el comando useradmin.

Pasos

1. Añada almacenamiento.

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

2. Configure la contraseña del host.

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.xyz.netapp
.in
```

3. Crear un rol en el host.

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

4. Cree un grupo de usuarios.

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

5. Cree un usuario local.

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

Configurar las credenciales de usuario en SnapDrive para UNIX

El administrador de SnapDrive para UNIX recibe credenciales de usuario del administrador de la consola de Operations Manager. Estas credenciales de usuario deben configurarse en SnapDrive para UNIX con el fin de que las operaciones de almacenamiento sean correctas.

Pasos

1. Configurar sd-admin en el sistema de almacenamiento.

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

2. Configuración de sd-hostname en el sistema de almacenamiento.

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. Compruebe los pasos 1 y 2 utilizando `snapdrive config list` comando.

```
user name       appliance name          appliance type
-------------------------------------------------------
sd-admin        ops_mngr_server         DFM
sd-unix_host    storage_array1          StorageSystem
```

4. Configure SnapDrive para UNIX para utilizar el control de acceso basado en roles (RBAC) de Operations Manager Console configurando la variable de configuración `rbac-method="dfm"` en la `snapdrive.conf` archivo.

> Las credenciales de usuario se cifran y guardan en el existente `.sdupw` archivo. La ubicación predeterminada del archivo anterior es `/opt/NetApp/snapdrive/.sdupw`.

Formatos de nombres de usuario para realizar comprobaciones de acceso con la consola de Operations Manager

SnapDrive para UNIX utiliza los formatos de nombre de usuario para realizar comprobaciones de acceso con la consola de Operations Manager. Estos formatos dependen de si usted es un sistema de información de red (NIS) o un usuario local.

SnapDrive para UNIX utiliza los siguientes formatos para comprobar si un usuario está autorizado a realizar determinadas tareas:

- Si es un usuario NIS que ejecuta `snapdrive` SnapDrive para UNIX utiliza el formato `<nisdomain>\<username>` (por ejemplo: `netapp.com\marc`)
- Si es un usuario local de un host UNIX como lnx197-141, SnapDrive para UNIX utiliza el formato `<hostname>\<username>` formato (por ejemplo, `lnx197-141\john`)
- Si es administrador (raíz) de un host UNIX, SnapDrive para UNIX siempre trata al administrador como un usuario local y utiliza el formato `lnx197-141\root`.

Variables de configuración para el control de acceso basado en roles

Debe configurar las diversas variables de configuración relacionadas con el control de acceso basado en roles en la `snapdrive.conf` archivo.

Variable	Descripción
`contact-http-dfm-port = 8088`	Especifica el puerto HTTP que se utilizará para comunicarse con un servidor de consola de Operations Manager. El valor predeterminado es 8088.
`contact-ssl-dfm-port = 8488`	Especifica el puerto SSL que se debe utilizar para comunicarse con un servidor de consola de Operations Manager. El valor predeterminado es 8488.
`rbac-method=dfm`	Especifica los métodos de control de acceso. Los posibles valores son `native` y.. `dfm`. Si el valor es `native`, el archivo de control de acceso almacenado en `/vol/vol0/sdprbac/sdhost-name.prbac` se utiliza para comprobaciones de acceso. Si el valor se establece en `dfm`, La consola de Operations Manager es un requisito previo. En este caso, SnapDrive para UNIX envía comprobaciones de acceso a la consola de Operations Manager.

Variable	Descripción
rbac-cache=on	SnapDrive para UNIX mantiene una memoria caché de consultas de comprobación de acceso y los resultados correspondientes. SnapDrive para UNIX utiliza esta caché sólo cuando todos los servidores de consola de Operations Manager configurados están inactivos. Puede establecer este valor en cualquiera de los dos `on` para habilitar la caché, o a. `off` para deshabilitarla. El valor predeterminado es desactivado para que pueda configurar SnapDrive para UNIX con la consola de Operations Manager y establecer la `rbac-method` variable de configuración a. `dfm`.
rbac-cache-timeout	Especifica el periodo de tiempo de espera de la caché rbac y se aplica solo cuando el *rbac-cache* está habilitado. El valor predeterminado es `24` horas SnapDrive para UNIX utiliza esta caché sólo cuando todos los servidores de consola de Operations Manager configurados están inactivos.
use-https-to-dfm=on	Esta variable le permite configurar SnapDrive para UNIX para que utilice el cifrado SSL (HTTPS) cuando se comunica con la consola de Operations Manager. El valor predeterminado es `on`.

Comandos y funcionalidades de SnapDrive

En el control de acceso basado en roles (RBAC), se requiere una funcionalidad específica para que cada operación se complete correctamente. Un usuario debe tener asignado el conjunto correcto de capacidades para realizar operaciones de almacenamiento.

En la siguiente tabla, se enumeran los comandos y las capacidades correspondientes requeridas:

Comando	Capacidad
`storage show`	SD.Storage.Read on volume
`storage list`	SD.Storage.Read on volume

Comando	Capacidad
`storage create`	• Para LUN dentro de volúmenes: `SD.Storage.Write` En el volumen • Para las LUN dentro de qtrees: `SD.Storage.Write` en qtree
`storage resize`	`SD.Storage.Write` En la LUN
`storage delete`	`SD.Storage.Delete` En la LUN
`snap show`	`SD.SnapShot.Read` en el volumen
`snap list`	`SD.SnapShot.Read` en el volumen
`snap delete`	`SD.Storage.Delete` en el volumen
`snap rename`	`SD.Storage.Write` en el volumen
`snap connect`	• Para clones de LUN en el volumen: `SD.SnapShot.Clone` en el volumen • Para clones de LUN en qtree: `SD.SnapShot.Clone` en qtree • Para clones de volúmenes tradicionales: `SD.SnapShot.Clone` en el sistema de almacenamiento • Para volumen FlexClone: `SD.SnapShot.Clone` en el volumen principal • Para volúmenes FlexClone sin restricciones: `SD.SnapShot.UnrestrictedClone` en el volumen principal

Comando	Capacidad
`snap connect-split`	• Para clones de LUN (LUN clonada y dividida en volumen): `SD.SnapShot.Clone` en el volumen y. `SD.Storage.Write` en el volumen • Para clones de LUN (LUN clonada y dividida en qtree): `SD.SnapShot.Clone` en qtree y. `SD.Storage.Write` en qtree • Para clones de volúmenes tradicionales que están divididos: `SD.SnapShot.Clone` en el sistema de almacenamiento y. `SD.Storage.Write` en el sistema de almacenamiento • Para clones de volúmenes flexibles, que están divididos: `SD.SnapShot.Clone` en el volumen principal.
`clone split start`	• Para los clones de LUN en los que la LUN reside en el volumen o en el qtree: `SD.SnapShot.Clone` que contiene el volumen o el qtree • Para clones de volúmenes: `SD.SnapShot.Clone` en el volumen principal
`snap disconnect`	• Para los clones de LUN en los que la LUN reside en el volumen o en el qtree: `SD.SnapShot.Clone` que contiene el volumen o el qtree • Para clones de volúmenes: `SD.SnapShot.Clone` en el volumen principal • Para eliminar clones de volúmenes sin restricciones: `SD.SnapShot.DestroyUnrestrictedClone` en el volumen
`snap disconnect-split`	• Para los clones de LUN en los que la LUN reside en el volumen o en el qtree: `SD.SnapShot.Clone` en el volumen o el qtree que contiene • Para clones de volúmenes: `SD.Storage.Delete` en el volumen principal • Para eliminar clones de volúmenes sin restricciones: `SD.SnapShot.DestroyUnrestrictedClone` en el volumen

Comando	Capacidad
`snap restore`	• Para las LUN existentes en un volumen: `SD.SnapShot.Restore` en el volumen y. `SD.Storage.Write` En la LUN • Para las LUN que existen en un qtree: `SD.SnapShot.Restore` en qtree y. `SD.Storage.Write` En la LUN • Para las LUN que no están en los volúmenes: `SD.SnapShot.Restore` en el volumen y. `SD.Storage.Write` en el volumen • Para las LUN que no están en qtree: `SD.SnapShot.Restore` en qtree y. `SD.Storage.Write` en qtree • Para volúmenes: `SD.SnapShot.Restore` en el sistema de almacenamiento para los volúmenes tradicionales, o. `SD.SnapShot.Restore` en conjunto para volúmenes flexibles • Para restaurar snap de un único archivo en volúmenes: `SD.SnapShot.Restore` en el volumen • Para restaurar snap de un solo archivo en qtree: `SD.SnapShot.Restore` qtree • Para reemplazar copias Snapshot de referencia: `SD.SnapShot.DisruptBaseline` en el volumen
`host connect`, `host disconnect`	`SD.Config.Write` En la LUN
`config access`	`SD.Config.Read` en el sistema de almacenamiento
`config prepare`	`SD.Config.Write` en al menos un sistema de almacenamiento
`config check`	`SD.Config.Read` en al menos un sistema de almacenamiento
`config show`	`SD.Config.Read` en al menos un sistema de almacenamiento
`config set`	`SD.Config.Write` en el sistema de almacenamiento
`config set -dfm`, `config set -mgmtpath`,	`SD.Config.Write` en al menos un sistema de almacenamiento

Comando	Capacidad
`config delete`	`SD.Config.Delete` en el sistema de almacenamiento
`config delete dfm_appliance`, `config delete -mgmtpath`	`SD.Config.Delete` en al menos un sistema de almacenamiento
`config list`	`SD.Config.Read` en al menos un sistema de almacenamiento
`config migrate set`	`SD.Config.Write` en al menos un sistema de almacenamiento
`config migrate delete`	`SD.Config.Delete` en al menos un sistema de almacenamiento
`config migrate list`	`SD.Config.Read` en al menos un sistema de almacenamiento

SnapDrive para UNIX no comprueba ninguna capacidad del administrador (raíz).

Funciones preconfiguradas para facilitar la configuración de funciones de usuario

Las funciones preconfiguradas simplifican la tarea de asignar funciones a los usuarios.

En la siguiente tabla, se enumeran los roles predefinidos:

Nombre del rol	Descripción
GlobalSDStorage	Gestión del almacenamiento con SnapDrive para UNIX
GlobalSDConfig	Gestionar configuraciones con SnapDrive para UNIX
GlobalSDSnapshot	Gestión de copias Snapshot con SnapDrive para UNIX
GlobalSDFullControl	Uso completo de SnapDrive para UNIX

En la tabla anterior, Global se refiere a todos los sistemas de almacenamiento gestionados por una consola de Operations Manager.

Actualización automática del sistema de almacenamiento en la consola de Operations Manager

La consola del Gestor de operaciones detecta los sistemas de almacenamiento compatibles con la red. Supervisa periódicamente los datos que recopila de los sistemas de almacenamiento detectados. Los datos se actualizan en un intervalo establecido. El administrador de la consola de Operations Manager puede configurar el intervalo de actualización.

El intervalo de supervisión de LUN, el intervalo de supervisión de qtrees y el intervalo de supervisión de vFiler son campos importantes que deciden la frecuencia de actualizaciones de LUN, qtrees y vFiler. Por ejemplo, si se crea una nueva LUN en un sistema de almacenamiento, la nueva LUN no se actualiza inmediatamente en la consola de Operations Manager. Por este motivo y la comprobación de acceso emitida a la consola de Operations Manager correspondiente a ese LUN en la consola de Operations Manager falla. Para evitar esta situación, puede modificar el intervalo de supervisión de LUN para que se ajuste a sus requisitos.

1. Seleccione **Configuración** > **Opciones** en la consola de Operations Manager para cambiar el intervalo de monitorización.
2. El administrador de la consola de Operations Manager también puede actualizar de forma forzada la consola de Operations Manager mediante la ejecución `dfm host discovery filername` en la interfaz de línea de comandos.
3. También puede conceder el administrador de la consola de Operations Manager `DFM.Database.Write` Capacidad del grupo global para sd-admin para que SnapDrive para UNIX actualice las entidades del sistema de almacenamiento en la consola de Operations Manager.

   ```
   # dfm role add sd-admin-role DFM.Database.Write Global
   Added 1 capability to role sd-admin-role.
   ```

Varios servidores de consola de Operations Manager

SnapDrive para UNIX admite varios servidores de consola de Operations Manager. Esta función se requiere cuando más de un servidor de consola de Operations Manager gestiona un grupo de sistemas de almacenamiento. SnapDrive para UNIX contacta a los servidores de la consola de Operations Manager en el mismo orden en que los servidores de la consola de Operations Manager están configurados en SnapDrive para UNIX. Puede ejecutar el `snapdrive config list` para obtener el orden de configuración.

El siguiente ejemplo muestra el resultado de varios servidores de consola de Operations Manager:

```
# snapdrive config list
username    appliance name     appliance type
----------------------------------------------
root        storage_array1     StorageSystem
root        storage_array2     StorageSystem
sd-admin    ops_mngr_server1   DFM
sd-admin    ops_mngr_server2   DFM
```

En el ejemplo anterior, Storage_array1 es gestionado por OPS_mngr_server1 y Storage_array2 es gestionado por OPS_mngr_server2. En este ejemplo, SnapDrive para UNIX contacta primero con OPS_mngr_server1. Si OPS_mngr_server1 no puede determinar el acceso, SnapDrive para contactos UNIX OPS_mngr_server2.

SnapDrive para UNIX sólo se pone en contacto con la segunda consola de Operations Manager en las siguientes condiciones:

- Cuando la primera consola de Operations Manager no puede determinar el acceso. Esta situación puede ocurrir porque la primera consola de Operations Manager no gestiona el sistema de almacenamiento.
- Cuando la primera consola de Operations Manager está inactiva.

Consola del Gestor de operaciones no disponible

SnapDrive para UNIX necesita una consola de Operations Manager para comprobaciones de acceso. En ocasiones, es posible que el servidor de la consola de Operations Manager no esté disponible por varios motivos.

Cuando el método de RBAC *`rbac-method = dfm`* Is Set (establecer) y Operations Manager Console no está disponible, SnapDrive for UNIX muestra el siguiente mensaje de error:

```
[root]# snapdrive storage delete -lun storage_array1:/vol/vol2/qtree1/lun1
0002-333 Admin error: Unable to connect to the DFM ops_mngr_server
```

SnapDrive para UNIX también puede mantener una memoria caché de los resultados de la comprobación de acceso del usuario que devuelve la consola de Operations Manager. Esta caché es válida por 24 horas y no se puede configurar. Si la consola de Operations Manager no está disponible, SnapDrive para UNIX utiliza la caché para determinar el acceso. Esta caché se utiliza sólo cuando no responden todos los servidores de consola de Operations Manager configurados.

Para que SnapDrive para UNIX utilice la caché a fin de realizar una comprobación de acceso, debe activar la *`rbac-cache`* la variable de configuración debe estar activada para mantener la caché de los resultados de acceso. La *`rbac-cache`* la variable de configuración está desactivada de forma predeterminada.

Para utilizar SnapDrive para UNIX incluso cuando la consola de Operations Manager no está disponible, el administrador del servidor debe restablecer el método de control de acceso basado en roles (RBAC) a. *`rbac-method = native`* en la `snapdrive.conf` archivo. Después de cambiar la `snapdrive.conf` File, debe reiniciar el daemon de SnapDrive para UNIX. Cuando *`rbac-method = native`* Está establecido, sólo el usuario raíz puede utilizar SnapDrive para UNIX.

RBAC y ejemplos de operaciones de almacenamiento

El control de acceso basado en roles permite realizar operaciones de almacenamiento en función de las funcionalidades que tenga asignadas. Recibirá un mensaje de error si no dispone de las funcionalidades adecuadas para realizar la operación de almacenamiento.

Funcionamiento con un único filespec en un único objeto de almacenamiento

SnapDrive for UNIX muestra un mensaje de error cuando no se trata de un usuario autorizado para crear un filespec en un volumen especificado.

Filespec: Filespec puede ser un sistema de ficheros, volumen host, grupo de discos o LUN.

```
[john]$ snapdrive storage create -fs /mnt/testfs -filervol
storage_array1:/vol/vol1 -dgsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

En este ejemplo, Juan es un usuario no raíz y no está autorizado a crear un filespec en el volumen especificado. John debe pedir al administrador de la consola de Operations Manager que conceda `SD.Storage.Write` acceso en el volumen `storage_array1:/vol/vol1`.

Funcionamiento con un único filespec sobre múltiples objetos de almacenamiento

SnapDrive para UNIX muestra un mensaje de error cuando el administrador no tiene el permiso requerido en varios objetos de almacenamiento para realizar las operaciones de almacenamiento.

Filespec: Filespec puede ser cualquiera que sea un sistema de ficheros, volumen host, grupo de discos o LUN

```
[root]# snapdrive storage create -fs /mnt/testfs -lun
storage_array1:/vol/vol1/lun2 -lun storage_array1:/vol/vol2/lun2  -lunsize
100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
unix_host\root on Operations Manager server ops_mngr_server
```

En este ejemplo, el filespec abarca dos volúmenes de sistema de almacenamiento: Vol1 y vol2. El administrador (raíz) de unix_host no tiene `SD.Storage.Write` acceso en ambos volúmenes. Por lo tanto, SnapDrive para UNIX muestra un mensaje de error en cada volumen. Para continuar `storage create`, El administrador (root) debe pedir al administrador de la consola de Operations Manager que le conceda `SD.Storage.Write` acceso en los dos volúmenes.

Funcionamiento con múltiples filespec y objetos de almacenamiento

En el ejemplo siguiente se muestra el mensaje de error que se recibirá cuando no sea un usuario autorizado para realizar la operación específica.

```
[marc]$ snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array1:/vol/vol2/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user nis_domain\marc on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
nis_domain\marc on Operations Manager server ops_mngr_server
```

En este ejemplo, tres LUN residen en dos volúmenes del sistema de almacenamiento: Vol1 y vol2. El usuario Marc pertenece a nis_domain y no está autorizado a crear filespec en vol1 y vol2. SnapDrive para UNIX muestra los dos mensajes de error en el ejemplo anterior. Los mensajes de error muestran que el usuario debe tener `SD.Storage.Write` acceso en vol1 y vol2.

Operación con varios objetos de almacenamiento

En el ejemplo siguiente se muestra el mensaje de error que se recibirá cuando no sea un usuario autorizado para realizar la operación específica.

```
[john]$ snapdrive storage show -all

Connected LUNs and devices:

device filename   adapter  path  size  proto  state  clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----  -----  --------
---------------
/dev/sdao            -     -     200m  iscsi  online  No
storage_array1:/vol/vol2/passlun1           -
/dev/sda1            -     -     200m  fcp    online  No
storage_array1:/vol/vol2/passlun2           -

Host devices and file systems:

dg: testfs1_SdDg                dgtype lvm
hostvol: /dev/mapper/testfs1_SdDg-testfs1_SdHv  state: AVAIL
fs: /dev/mapper/testfs1_SdDg-testfs1_SdHv       mount point: /mnt/testfs1
(persistent) fstype jfs2

device filename   adapter  path  size  proto  state   clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----   -----  --------
---------
/dev/sdn             -      P    108m  iscsi  online   No
storage_array1:/vol/vol2/testfs1_SdLun         -
/dev/sdn1             -      P    108m  fcp  online   No
storage_array1:/vol/vol2/testfs1_SdLun1         -

0002-719 Warning: SD.Storage.Read access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

John está autorizado a enumerar entidades de almacenamiento en vol2 pero no en vol1. SnapDrive for UNIX muestra las entidades de vol1 y muestra un mensaje de advertencia para vol2.

> Para `storage list`, `storage show`, `snap list`, y. `snap show` Los comandos SnapDrive para UNIX muestran una advertencia en lugar de un error.

El funcionamiento con varios servidores de consola de Operations Manager gestiona los sistemas de almacenamiento

El siguiente resultado muestra el mensaje de error que recibiría cuando los sistemas de almacenamiento son gestionados por varias consola de Operations Manager.

```
[root]# snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array2:/vol/vol1/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server1
SD.Storage.Write access denied on volume storage_array2:/vol/vol1 for user
unix_host\root on Operations Manager server ops_mngr_server2
```

storage_array1 es gestionado por ops_mngr_server1 y storage_array2 es gestionado por ops_mngr_server2. El administrador de unix_host no está autorizado a crear filesppecs en Storage_array1 y Storage_array2. En el ejemplo anterior, SnapDrive para UNIX muestra la consola de Operations Manager utilizada para determinar el acceso.