Funciones de seguridad de SnapDrive para UNIX

Snapdrive for Unix

NetApp
June 20, 2025

Tabla de contenidos

Funciones de seguridad de SnapDrive para UNIX

Antes de utilizar SnapDrive para UNIX, debe comprender sus características de seguridad y aprender a acceder a ellas.

Características de seguridad

SnapDrive para UNIX proporciona ciertas funciones que le permiten trabajar con él de forma más segura. Estas funciones le permiten controlar mejor los usuarios que pueden realizar operaciones en un sistema de almacenamiento y desde qué host.

Las funciones de seguridad permiten realizar las siguientes tareas:

- Configure los permisos de control de acceso
- Especifique la información de inicio de sesión para los sistemas de almacenamiento
- Especifique que SnapDrive para UNIX utilice HTTPS

La función de control de acceso permite especificar las operaciones que un host donde se ejecuta SnapDrive para UNIX puede ejecutar en un sistema de almacenamiento. Debe configurar estos permisos individualmente para cada host. Además, para permitir que SnapDrive para UNIX acceda a un sistema de almacenamiento, debe proporcionar el nombre de inicio de sesión y la contraseña para ese sistema de almacenamiento.

La función HTTPS permite especificar el cifrado SSL para todas las interacciones con el sistema de almacenamiento a través de la interfaz Manage ONTAP, incluido el envío de contraseñas. Este comportamiento es el predeterminado en SnapDrive 4.1 para UNIX y versiones posteriores para hosts AIX; sin embargo, puede deshabilitar el cifrado SSL cambiando el valor de `use-https-to-filer` variable de configuración a. `off`.

Control de accesos en SnapDrive para UNIX

SnapDrive para UNIX le permite controlar el nivel de acceso que tiene cada host a cada sistema de almacenamiento al que está conectado el host.

El nivel de acceso en SnapDrive para UNIX indica las operaciones que se permite que el host realice cuando se dirige a un sistema de almacenamiento determinado. Excepto para las operaciones de presentación y lista, los permisos de control de acceso pueden afectar a todas las operaciones de Snapshot y almacenamiento.

Qué configuración de control de acceso son

Para determinar el acceso de los usuarios, SnapDrive para UNIX comprueba uno de los dos archivos de permisos en el volumen raíz del sistema de almacenamiento. Debe comprobar las reglas establecidas en esos archivos para evaluar el control de acceso.

- `sdhost-name.prbac` el archivo está en el directorio `/vol/vol0/sdprbac` (Control de acceso basado en roles con permisos SnapDrive).

  El nombre de archivo es `sdhost-name.prbac`, donde *`host-name`* es el nombre del host al que se aplican los permisos. Es posible tener un archivo de permisos para cada host conectado al sistema de almacenamiento. Puede utilizar el `snapdrive config access` comando para mostrar información

sobre los permisos disponibles para un host en un sistema de almacenamiento específico.

Si la `sdhost-name.prbac` no existe y, a continuación, utiliza el `sdgeneric.prbac` archivo para comprobar los permisos de acceso.

- `sdgeneric.prbac` el archivo también se encuentra en el directorio `/vol/vol0/sdprbac`.

  El nombre del archivo `sdgeneric.prbac` se usa como configuración de acceso predeterminada para varios hosts al que no tiene acceso `sdhost-name.prbac` de ficheros en el sistema de almacenamiento.

Si usted tiene ambos `sdhost-name.prbac` y.. `sdgeneric.prbac` archivos disponibles en la `/vol/vol0/sdprbac` y, a continuación, utilice la `sdhost-name.prbac` para comprobar los permisos de acceso, ya que se sobrescriben los valores proporcionados `sdgeneric.prbac` archivo.

Si no tiene ambos `sdhost-name.prbac` y.. `sdgeneric.prbac` archivos y, a continuación, compruebe la variable de configuración *`all-access-if-rbac-unspecified`* que se define en la `snapdrive.conf` archivo.

La configuración del control de acceso desde un host determinado a una unidad vFiler determinada es una operación manual. El acceso desde un host determinado se controla mediante un archivo que reside en el volumen raíz de la unidad vFiler afectada. El archivo contiene `/vol/<vfiler root volume>/sdprbac/sdhost-name.prbac`, donde *`host-name`* es el nombre del host afectado, como devuelve `gethostname(3)`. Debe asegurarse de que este archivo sea legible, pero no editable, desde el host que puede acceder a él.

Para determinar el nombre del host, ejecute el `hostname` comando.

Si el archivo está vacío, no se puede leer o tiene un formato no válido, SnapDrive para UNIX no concede el acceso de host a ninguna de las operaciones.

Si falta el archivo, SnapDrive para UNIX comprueba la variable de configuración *`all-access-if-rbac-unspecified`* en la `snapdrive.conf` archivo. Si la variable está establecida en `on` (valor predeterminado), permite que los hosts tengan acceso completo a todas estas operaciones en ese sistema de almacenamiento. Si la variable está establecida en `off`, SnapDrive para UNIX deniega el permiso de host para realizar cualquier operación regida por el control de acceso en ese sistema de almacenamiento.

Niveles de control de acceso disponibles

SnapDrive para UNIX ofrece diversos niveles de control de acceso a los usuarios. Estos niveles de acceso se relacionan con las copias de Snapshot y las operaciones de los sistemas de almacenamiento.

Se pueden configurar los siguientes niveles de acceso:

- NONE: El host no tiene acceso al sistema de almacenamiento.
- SNAP CREATE: El host puede crear copias de Snapshot.
- USO SNAP—el host puede eliminar y cambiar el nombre de las copias Snapshot.
- SNAP ALL: El host puede crear, restaurar, eliminar y cambiar el nombre de las copias Snapshot.
- STORAGE CREATE DELETE: El host puede crear, redimensionar y eliminar almacenamiento.

- USO DE ALMACENAMIENTO: El host puede conectar y desconectar el almacenamiento, así como realizar estimación de división de clones y comenzar a usar el almacenamiento.
- TODO el ALMACENAMIENTO: El host puede crear, eliminar, conectar y desconectar el almacenamiento, y también realizar cálculos de división de clones y comenzar a dividir clones en el almacenamiento.
- TODOS LOS ACCESOS: El host tiene acceso a todas las operaciones anteriores de la SnapDrive para UNIX.

Cada nivel es distinto. Si especifica permisos solo para determinadas operaciones, SnapDrive para UNIX puede ejecutar únicamente esas operaciones. Por ejemplo, si especifica EL USO DE ALMACENAMIENTO, el host puede utilizar SnapDrive para UNIX para conectar y desconectar el almacenamiento, pero no puede realizar ninguna otra operación regulada por los permisos de control de acceso.

Configurar el permiso de control de acceso

Para configurar los permisos de control de acceso en SnapDrive para UNIX, se puede crear un directorio y un archivo especiales en el volumen raíz del sistema de almacenamiento.

Asegúrese de que ha iniciado sesión como usuario raíz.

Pasos

1. Cree el directorio `sdprbac` en el volumen raíz del sistema de almacenamiento de destino.

   Una manera de que el volumen raíz sea accesible es montar el volumen con NFS.

2. Cree el archivo de permisos en `sdprbac` directorio. Asegúrese de que las siguientes afirmaciones son verdaderas:
   - El archivo debe tener el nombre `sdhost-name.prbac` donde host-name es el nombre del host para el cual se especifican permisos de acceso.
   - El archivo debe ser de sólo lectura para garantizar que SnapDrive para UNIX pueda leerlo, pero que no se pueda modificar.

     Para otorgar a un host el permiso de acceso dev-sun1, debe crear el siguiente archivo en el sistema de almacenamiento: `/vol/vol1/sdprbac/sddev-sun1.prbac`

3. Configure los permisos del archivo para ese host.

   Debe utilizar el siguiente formato para el archivo:

   - Sólo puede especificar un nivel de permisos. Para otorgar al host acceso completo a todas las operaciones, introduzca la cadena DE ACCESO.
   - La cadena de permisos debe ser la primera cosa del archivo. El formato de archivo no es válido si la cadena de permisos no está en la primera línea.
   - Las cadenas de permisos no distinguen mayúsculas y minúsculas.
   - Ningún espacio en blanco puede preceder a la cadena de permisos.
   - No se permiten comentarios.

     Estas cadenas de permisos válidas permiten los siguientes niveles de acceso:

   - NONE: El host no tiene acceso al sistema de almacenamiento.

- SNAP CREATE: El host puede crear copias de Snapshot.
- USO SNAP—el host puede eliminar y cambiar el nombre de las copias Snapshot.
- SNAP ALL: El host puede crear, restaurar, eliminar y cambiar el nombre de las copias Snapshot.
- STORAGE CREATE DELETE: El host puede crear, redimensionar y eliminar almacenamiento.
- USO DE ALMACENAMIENTO: El host puede conectar y desconectar el almacenamiento, así como realizar estimación de división de clones y comenzar a usar el almacenamiento.
- TODO el ALMACENAMIENTO: El host puede crear, eliminar, conectar y desconectar el almacenamiento, y también realizar cálculos de división de clones y comenzar a dividir clones en el almacenamiento.
- TODOS LOS ACCESOS: El host tiene acceso a todas las operaciones anteriores de la SnapDrive para UNIX. Cada una de estas cadenas de permisos es discreta. Si especifica EL USO SNAP, el host puede eliminar o cambiar el nombre de las copias Snapshot, pero no puede crear copias Snapshot ni restaurar ni realizar ninguna operación de aprovisionamiento de almacenamiento.

Independientemente de los permisos establecidos, el host puede realizar operaciones de visualización y lista.

4. Verifique los permisos de acceso con el siguiente comando:

   snapdrive config access show *filer_name*

Ver el permiso de control de acceso

Puede ver los permisos de control de acceso ejecutando el `snapdrive config access show` comando.

Pasos

1. Ejecute el `snapdrive config access show` comando.

   Este comando tiene el formato siguiente: `snapdrive config access {show | list} filername`

   Puede usar los mismos parámetros independientemente de si introduce el `show` o. `list` la versión del comando.

   Esta línea de comandos comprueba la tostadora del sistema de almacenamiento para determinar qué permisos tiene el host. Según la salida, los permisos del host en este sistema de almacenamiento SON SNAP ALL.

```
# snapdrive config access show toaster
This host has the following access permission to filer, toaster:
SNAP ALL
Commands allowed:
snap create
snap restore
snap delete
snap rename
#
```

En este ejemplo, el archivo de permisos no está en el sistema de almacenamiento, por lo que SnapDrive para UNIX comprueba la variable *all-access-if-rbac-unspecified* en la `snapdrive.conf` archivo para determinar qué permisos tiene el host. Esta variable se establece en on, lo que equivale a crear un archivo de permisos con el nivel de acceso establecido en TODOS LOS ACCESOS.

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

Este ejemplo muestra el tipo de mensaje que recibe si no hay ningún archivo de permisos en el tostador del sistema de almacenamiento y la variable *all-access-if-rbac-unspecified* en la `snapdrive.conf` el archivo está definido como `off`.

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

Información de inicio de sesión para sistemas de almacenamiento

Gracias a un nombre de usuario o una contraseña, SnapDrive para UNIX puede acceder a cada sistema de almacenamiento. También proporciona seguridad porque, además de haber iniciado sesión como root, la persona que ejecuta SnapDrive para UNIX debe proporcionar el nombre de usuario o la contraseña correctos cuando se le solicite. Si un inicio de sesión está comprometido, puede eliminarlo y establecer un nuevo inicio de sesión de usuario.

Se creó el inicio de sesión de usuario para cada sistema de almacenamiento al configurarlo. Para que SnapDrive para UNIX funcione con el sistema de almacenamiento, debe suministrar esta información de inicio de sesión. Según lo que haya especificado al configurar los sistemas de almacenamiento, cada sistema de almacenamiento podría utilizar el mismo inicio de sesión o un inicio de sesión único.

SnapDrive para UNIX almacena estos inicios de sesión y contraseñas en formato cifrado en cada host. Puede especificar que SnapDrive para UNIX cifre esta información cuando se comunica con el sistema de almacenamiento mediante la configuración del *`snapdrive.conf`* variable de configuración *`use-https-to-filer=on`*.

Especificar información de inicio de sesión

Debe especificar la información de inicio de sesión de usuario para un sistema de almacenamiento de. Según lo especificado al configurar el sistema de almacenamiento, cada sistema de almacenamiento podría usar el mismo nombre de usuario o una misma contraseña, o bien un nombre de usuario o una contraseña únicos. Si todos los sistemas de almacenamiento utilizan la misma información de nombre de usuario o contraseña, se deben realizar una vez los pasos siguientes. Si los sistemas de almacenamiento utilizan nombres de usuario o contraseñas únicos, se deben repetir los siguientes pasos para cada sistema de almacenamiento.

Asegúrese de que ha iniciado sesión como usuario raíz.

Pasos

1. Introduzca el siguiente comando:

   `snapdrive config set` *`user_name filername`* `[`*`filername`*`…]`

   `user_name` es el nombre de usuario que se especificó para ese sistema de almacenamiento cuando se lo configuró por primera vez.

   `filername` es el nombre del sistema de almacenamiento.

   `[filername…]` define que puede introducir varios nombres de sistemas de almacenamiento en una línea de comandos si todos tienen el mismo inicio de sesión o contraseña de usuario. Debe introducir el nombre de al menos un sistema de almacenamiento.

2. En el aviso, introduzca la contraseña, si la hay.

   Si no se ha establecido ninguna contraseña, pulse Intro (el valor nulo) cuando se le solicite una contraseña.

   En este ejemplo se configura un usuario llamado `root` para un sistema de almacenamiento llamado tostadora:

   ```
   # snapdrive config set `root` toaster
   Password for root:
   Retype Password:
   ```

En este ejemplo se configura un usuario llamado `root` para tres sistemas de almacenamiento:

```
# snapdrive config set root toaster oven broiler
Password for root:
Retype Password:
```

3. Si tiene otro sistema de almacenamiento con un nombre de usuario o una contraseña diferentes, repita estos pasos.

Verificación de los nombres de usuario del sistema de almacenamiento asociados con SnapDrive para UNIX

Puede verificar qué nombre de usuario SnapDrive para UNIX ha asociado a un sistema de almacenamiento ejecutando el `snapdrive config list` comando.

Debe haber iniciado sesión como usuario raíz.

Pasos

1. Introduzca el siguiente comando:

   `snapdrive config list`

   Este comando muestra el nombre de usuario o las parejas del sistema de almacenamiento de todos los sistemas con usuarios especificados en SnapDrive para UNIX. No muestra las contraseñas de los sistemas de almacenamiento.

   Este ejemplo muestra los usuarios asociados a los sistemas de almacenamiento llamados rapunzel y sistema de almacenamiento de tamaño medio:

```
# snapdrive config list
user name           storage system name
----------------------------
rumplestiltskins    rapunzel
longuser            mediumstoragesystem
```

Eliminar un inicio de sesión de usuario en un sistema de almacenamiento

Puede eliminar un inicio de sesión de usuario para uno o más sistemas de almacenamiento ejecutando el `snapdrive config delete` comando.

Asegúrese de que ha iniciado sesión como usuario raíz.

Pasos

1. Introduzca el siguiente comando:

   `snapdrive config delete *appliance_name [appliance_name]*`

appliance_name es el nombre del sistema de almacenamiento para el que se desea eliminar la información de inicio de sesión de usuario.

SnapDrive para UNIX quita la información de inicio de sesión de nombre de usuario o contraseña de los sistemas de almacenamiento que especifique.

Para habilitar SnapDrive para UNIX con el fin de acceder al sistema de almacenamiento, debe especificar un nuevo inicio de sesión de usuario.

Configuración de HTTP

Puede configurar SnapDrive para UNIX para que utilice HTTP en la plataforma host.

Asegúrese de que ha iniciado sesión como usuario raíz.

Pasos

1. Haga una copia de seguridad del `snapdrive.conf` archivo.
2. Abra el `snapdrive.conf` archivo en un editor de texto.
3. Cambie el valor de *`use-https-to-filer`* variable a. `off`.

   Una buena práctica en cualquier momento que modifique el `snapdrive.conf` el archivo debe realizar los siguientes pasos:

   a. Comente la línea que desea modificar.
   b. Copie la línea comentada-Out.
   c. Descomente el texto copiado eliminando el signo de almohadilla (#).
   d. Modifique el valor.
4. Guarde el archivo después de realizar los cambios.

   SnapDrive para UNIX comprueba automáticamente este archivo cada vez que se inicia. Debe reiniciar el daemon SnapDrive para UNIX para que los cambios surtan efecto.

Información de copyright

Información de la marca comercial