Security features in SnapDrive for UNIX

Snapdrive for Unix

NetApp
February 12, 2024

Table of Contents

Security features in SnapDrive for UNIX

Before you use SnapDrive for UNIX, you must understand its security features and learn how to access them.

What the Security features are

SnapDrive for UNIX provides certain features that allow you to work with it more securely. These features give you more control over which users can perform operations on a storage system and from which host.

The security features allow you to perform the following tasks:

- Set up access control permissions
- Specify login information for the storage systems
- Specify that SnapDrive for UNIX use HTTPS

The access control feature allows you to specify which operations a host running SnapDrive for UNIX can perform on a storage system. You set these permissions individually for each host. In addition, to allow SnapDrive for UNIX to access a storage system, you must supply the login name and password for that storage system.

The HTTPS feature lets you specify SSL encryption for all interactions with the storage system through the Manage ONTAP interface, including sending the passwords. This behavior is the default in SnapDrive 4.1 for UNIX and later releases for AIX hosts; however, you can disable SSL encryption by changing the value of the `use-https-to-filer` configuration variable to `off`.

Access control in SnapDrive for UNIX

SnapDrive for UNIX allows you to control the level of access that each host has to each storage system to which the host is connected.

The access level in SnapDrive for UNIX indicates which operations the host is allowed to perform when it targets a given storage system. Except for the show and list operations, the access control permissions can affect all Snapshot and storage operations.

What access control settings are

To determine user access, SnapDrive for UNIX checks one of two permissions files in the root volume of the storage system. You must check the rules set in those file to evaluate access control.

- `sdhost-name.prbac` file is in the directory `/vol/vol0/sdprbac` (SnapDrive permissions roles-based access control).

  The file name is `sdhost-name.prbac`, where *`host-name`* is the name of the host to which the permissions apply. You can have a permissions file for each host attached to the storage system. You can use the `snapdrive config access` command to display information about the permissions available for a host on a specific storage system.

If the `sdhost-name.prbac` does not exist, then use the `sdgeneric.prbac` file to check the access permissions.

- `sdgeneric.prbac` file is also in the directory `/vol/vol0/sdprbac`.

  The file name `sdgeneric.prbac` is used as the default access settings for multiple hosts that do not have access to `sdhost-name.prbac` file on the storage system.

If you have both `sdhost-name.prbac` and `sdgeneric.prbac` files available in the `/vol/vol0/sdprbac` path, then use the `sdhost-name.prbac` to check the access permissions, as this overwrites the values provided for `sdgeneric.prbac` file.

If you do not have both `sdhost-name.prbac` and `sdgeneric.prbac` files, then check the configuration variable *`all-access-if-rbac-unspecified`* that is defined in the `snapdrive.conf` file.

Setting up access control from a given host to a given vFiler unit is a manual operation. The access from a given host is controlled by a file residing in the root volume of the affected vFiler unit. The file contains `/vol/<vfiler root volume>/sdprbac/sdhost-name.prbac`, where the *`host-name`* is the name of the affected host, as returned by `gethostname(3)`. You should ensure that this file is readable, but not writable, from the host that can access it.

To determine the name of the host, run the `hostname` command.

If the file is empty, unreadable, or has an invalid format, SnapDrive for UNIX does not grant the host access to any of the operations.

If the file is missing, SnapDrive for UNIX checks the configuration variable *`all-access-if-rbac-unspecified`* in the `snapdrive.conf` file. If the variable is set to `on` (default value), it allows the hosts complete access to all these operations on that storage system. If the variable is set to `off`, SnapDrive for UNIX denies the host permission to perform any operations governed by access control on that storage system.

Available access control levels

SnapDrive for UNIX provides various access control levels to the users. These access levels are related to the Snapshot copies and storage system operations.

You can set the following access levels:

- NONE—The host has no access to the storage system.
- SNAP CREATE—The host can create Snapshot copies.
- SNAP USE—The host can delete and rename Snapshot copies.
- SNAP ALL—The host can create, restore, delete, and rename Snapshot copies.
- STORAGE CREATE DELETE—The host can create, resize, and delete storage.
- STORAGE USE—The host can connect and disconnect storage, and also perform clone split estimate and clone split start on storage.
- STORAGE ALL—The host can create, delete, connect, and disconnect storage, and also perform clone split estimate and clone split start on storage.

- ALL ACCESS—The host has access to all the preceding SnapDrive for UNIX operations.

Each level is distinct. If you specify permission for only certain operations, SnapDrive for UNIX can execute only those operations. For example, if you specify STORAGE USE, the host can use SnapDrive for UNIX to connect and disconnect storage, but it cannot perform any other operations governed by access control permissions.

Setting up access control permission

You can set up access control permission in SnapDrive for UNIX by creating a special directory and file in the root volume of the storage system.

Ensure that you are logged in as a root user.

Steps

1. Create the directory `sdprbac` in the root volume of the target storage system.

   One way to make the root volume accessible is to mount the volume using NFS.

2. Create the permissions file in the `sdprbac` directory. Ensure the following statements are true:
   - The file must be named `sdhost-name.prbac` where host-name is the name of the host for which you are specifying access permissions.
   - The file must be read-only to ensure that SnapDrive for UNIX can read it, but that it cannot be modified.

     To give a host named dev-sun1 access permission, you would create the following file on the storage system: `/vol/vol1/sdprbac/sddev-sun1.prbac`

3. Set the permissions in the file for that host.

   You must use the following format for the file:

   - You can specify only one level of permissions. To give the host full access to all operations, enter the string ALL ACCESS.
   - The permission string must be the first thing in the file. The file format is invalid if the permission string is not in the first line.
   - Permission strings are case-insensitive.
   - No white space can precede the permission string.
   - No comments are allowed.

     These valid permission strings allow the following access levels:

   - NONE—The host has no access to the storage system.
   - SNAP CREATE—The host can create Snapshot copies.
   - SNAP USE—The host can delete and rename Snapshot copies.
   - SNAP ALL—The host can create, restore, delete, and rename Snapshot copies.
   - STORAGE CREATE DELETE—The host can create, resize, and delete storage.
   - STORAGE USE—The host can connect and disconnect storage, and also perform clone split estimate and clone split start on storage.

- STORAGE ALL—The host can create, delete, connect, and disconnect storage, and also perform clone split estimate and clone split start on storage.
- ALL ACCESS—The host has access to all the preceding SnapDrive for UNIX operations. Each of these permission strings is discrete. If you specify SNAP USE, the host can delete or rename Snapshot copies, but it cannot create Snapshot copies or restore or perform any storage provisioning operations.

Regardless of the permissions you set, the host can perform show and list operations.

4. Verify the access permissions by entering the following command:

   `snapdrive config access show` *`filer_name`*

Viewing the access control permission

You can view the access control permissions by running the `snapdrive config access show` command.

Steps

1. Run the `snapdrive config access show` command.

   This command has the following format: `snapdrive config access {show | list} filername`

   You can use the same parameters regardless of whether you enter the `show` or `list` version of the command.

   This command line checks the storage system toaster to determine which permissions the host has. Based on the output, the permissions for the host on this storage system are 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
   #
   ```

   In this example, the permissions file is not on the storage system, so SnapDrive for UNIX checks the variable *`all-access-if-rbac-unspecified`* in the `snapdrive.conf` file to determine which permissions the host has. This variable is set to on, which is equivalent to creating a permissions file with the access level set to ALL ACCESS.

```
# 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
#
```

This example shows the kind of message you receive if no permissions file is on the storage system toaster, and the variable *all-access-if-rbac-unspecified* in the `snapdrive.conf` file is set to `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.
```

Login information for storage systems

A user name or password allows SnapDrive for UNIX to access each storage system. It also provides security because, in addition to being logged in as root, the person running SnapDrive for UNIX must supply the correct user name or password when prompted for it. If a login is compromised, you can delete it and set a new user login.

You created the user login for each storage system when you set it up. For SnapDrive for UNIX to work with the storage system, you must supply it with this login information. Depending on what you specified when you set up the storage systems, each storage system could use either the same login or a unique login.

SnapDrive for UNIX stores these logins and passwords in encrypted form on each host. You can specify that SnapDrive for UNIX encrypt this information when it communicates with the storage system by setting the *snapdrive.conf* configuration variable *use-https-to-filer=on*.

Specifying login information

You must specify the user login information for a storage system. Depending on what you specified when you set up the storage system, each storage system could use either the same user name or password or a unique user name or password. If all the storage systems use the same user name or password information, you must perform the following steps once. If the storage systems use unique user names or passwords, you must repeat the following steps for each storage system.

Ensure that you are logged in as a root user.

Steps

1. Enter the following command:

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

   user_name is the user name that was specified for that storage system when you first set it up.

   filername is the name of the storage system.

   [filername…] defines that you can enter multiple storage system names on one command line if they all have the same user login or password. You must enter the name of at least one storage system.

2. At the prompt, enter the password, if there is one.

   If no password was set, press Enter (the null value) when prompted for a password.

   This example sets up a user called `root` for a storage system called toaster:

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

   This example sets up one user called `root` for three storage systems:

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

3. If you have another storage system with a different user name or password, repeat these steps.

Verifying storage system user names associated with SnapDrive for UNIX

You can verify which user name SnapDrive for UNIX has associated with a storage system by executing the `snapdrive config list` command.

You must have logged in as root user.

Steps

1. Enter the following command:

   `snapdrive config list`

   This command displays the user name or storage system pairs for all systems that have users specified within SnapDrive for UNIX. It does not display the passwords for the storage systems.

   This example displays the users associated with the storage systems named rapunzel and medium storage system:

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

Deleting a user login for a storage system

You can delete a user login for one or more storage systems, by executing the `snapdrive config delete` command.

Ensure that you are logged in as a root user.

Steps

1. Enter the following command:

   `snapdrive config delete` ***`appliance_name [appliance_name]`***

   `appliance_name` is the name of the storage system for which you want to delete the user login information.

   SnapDrive for UNIX removes the user name or password login information for the storage systems you specify.

   > To enable SnapDrive for UNIX to access the storage system, you must specify a new user login.

Setting up HTTP

You can configure SnapDrive for UNIX to use HTTP for your host platform.

Ensure that you are logged in as a root user.

Steps

1. Make a backup of the `snapdrive.conf` file.
2. Open the `snapdrive.conf` file in a text editor.

3. Change the value of the *use-https-to-filer* variable to `off`.

   A good practice any time you modify the `snapdrive.conf` file is to perform the following steps:

   a. Comment out the line you want to modify.
   b. Copy the commented-out line.
   c. Un-comment the copied text by removing the pound (#) sign.
   d. Modify the value.
4. Save the file after you make your changes.

   SnapDrive for UNIX automatically checks this file each time it starts. You must restart the SnapDrive for UNIX daemon for the changes to take effect.

Copyright information

Trademark information