



Access control in SnapDrive for UNIX

Snapdrive for Unix

NetApp
June 10, 2021

This PDF was generated from https://docs.netapp.com/us-en/snapdrive-unix/aix/concept_what_access_control_settings_are.html on June 10, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Access control in SnapDrive for UNIX 1
 - What access control settings are 1
 - Available access control levels 2
 - Setting up access control permission 2
 - Viewing the access control permission 3

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} filename`

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.
```

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.