



What access control settings are Snapdrive for Unix

Ivana Devine
January 21, 2021

Table of Contents

What access control settings are 1

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/vol10/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/vol10/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/vol10/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.

Setting up access control from a given host to a given Vserver unit is a manual operation. The access from a given host is controlled by a file residing in the root volume of the affected Vserver unit. This file has the name `/vol/<vserver root volume>/sdhost-name.prbac`, where *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 mount the Vserver root volume on the host system and create `*.prbac` files, execute the following command:

```
mount <vservename>:/ <mntpoint>
```

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.

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.