



Add an ONTAP RBAC role using security login commands

SnapCenter Software

Soumik Das, Archana
August 08, 2021

Table of Contents

Add an ONTAP RBAC role using security login commands. 1

Add an ONTAP RBAC role using security login commands

You can use the security login commands to add an ONTAP RBAC role when your storage systems are running clustered ONTAP.

What you will need

- Before you create an ONTAP RBAC role for storage systems running clustered ONTAP, you must identify the following:
 - The task (or tasks) that you want to perform
 - The privileges required to perform these tasks
- Configuring an RBAC role requires that you perform the following actions:
 - Grant privileges to commands and/or command directories.

There are two levels of access for each command/command directory: all-access and read-only.

You must always assign the all-access privileges first.

- Assign roles to users.
- Vary your configuration depending on whether your SnapCenter plug-ins are connected to the Cluster Administrator IP for the entire cluster or directly connected to a SVM within the cluster.

About this task

To simplify configuring these roles on storage systems, you can use the RBAC User Creator for Data ONTAP tool, which is posted on the NetApp Communities Forum.

This tool automatically handles setting up the ONTAP privileges correctly. For example, RBAC User Creator for Data ONTAP tool automatically adds the privileges in the correct order so that the all-access privileges appear first. If you add the read-only privileges first and then add the all-access privileges, ONTAP marks the all-access privileges as duplicates and ignores them.



If you later upgrade SnapCenter or ONTAP, you should re-run the RBAC User Creator for Data ONTAP tool to update the user roles you created previously. User roles created for an earlier version of SnapCenter or ONTAP do not work properly with upgraded versions. When you re-run the tool, it automatically handles the upgrade. You do not need to recreate the roles.

More information about setting up ONTAP RBAC roles, see the [ONTAP 9 Administrator Authentication and RBAC Power Guide](#).



For consistency, the SnapCenter documentation refers to the roles as using privileges. The OnCommand System Manager GUI uses the term “attribute” instead of “privilege.” When setting up ONTAP RBAC roles, both these terms mean the same thing.

Steps

1. On the storage system, create a new role by entering the following command:

```
security login role create <role_name> -cmddirname "command" -access all
```

```
-vserver <svm_name\>
```

- `svm_name` is the name of the SVM. If you leave this blank, it defaults to cluster administrator.
- `role_name` is the name you specify for the role.
- `command` is the ONTAP capability.



You must repeat this command for each permission. Remember that all-access commands must be listed before read-only commands.

For information about the list of permissions, see [ONTAP CLI commands for creating roles and assigning permissions](#).

2. Create a user name by entering the following command:

```
security login create -username <user_name\> -application ontapi -authmethod  
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment  
"user_description"
```

- `user_name` is the name of the user you are creating.
- `<password>` is your password. If you do not specify a password, the system will prompt you for one.
- `svm_name` is the name of the SVM.

3. Assign the role to the user by entering the following command:

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod <password\>
```

- `<user_name>` is the name of the user you created in Step 2. This command lets you modify the user to associate it with the role.
- `<svm_name>` is the name of the SVM.
- `<role_name>` is the name of the role you created in Step 1.
- `<password>` is your password. If you do not specify a password, the system will prompt you for one.

4. Verify that the user was created correctly by entering the following command:

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

`user_name` is the name of the user you created in Step 3.

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.