



# **Manage access-control roles**

ONTAP 9

NetApp

February 24, 2023

# Table of Contents

- Manage access-control roles . . . . . 1
  - Manage access-control roles overview . . . . . 1
  - Modify the role assigned to an administrator . . . . . 1
  - Define custom roles . . . . . 1
  - Predefined roles for cluster administrators . . . . . 3
  - Predefined roles for SVM administrators . . . . . 5

# Manage access-control roles

## Manage access-control roles overview

The role assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.

## Modify the role assigned to an administrator

You can use the `security login modify` command to change the role of a cluster or SVM administrator account. You can assign a predefined or custom role.

### What you'll need

You must be a cluster administrator to perform this task.

### Step

1. Change the role of a cluster or SVM administrator:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

For complete command syntax, see the [worksheet](#).

### Creating or modifying login accounts

The following command changes the role of the AD cluster administrator account `DOMAIN1\guest1` to the predefined `readonly` role.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

The following command changes the role of the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` to the custom `vol_role` role.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

## Define custom roles

You can use the `security login role create` command to define a custom role. You can execute the command as many times as necessary to achieve the exact combination of capabilities that you want to associate with the role.

## What you'll need

You must be a cluster administrator to perform this task.

### About this task

- A role, whether predefined or custom, grants or denies access to ONTAP commands or command directories.

A command directory (`volume`, for example) is a group of related commands and command subdirectories. Except as described in this procedure, granting or denying access to a command directory grants or denies access to each command in the directory and its subdirectories.

- Specific command access or subdirectory access overrides parent directory access.

If a role is defined with a command directory, and then is defined again with a different access level for a specific command or for a subdirectory of the parent directory, the access level that is specified for the command or subdirectory overrides that of the parent.



You cannot assign an SVM administrator a role that gives access to a command or command directory that is available only to the `admin` cluster administrator—for example, the `security` command directory.

### Step

1. Define a custom role:

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

For complete command syntax, see the [worksheet](#).

The following commands grant the `vol_role` role full access to the commands in the `volume` command directory and read-only access to the commands in the `volume snapshot` subdirectory.

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all  
  
cluster1::>security login role create -role vol_role -cmddirname "volume  
snapshot" -access readonly
```

The following commands grant the `SVM_storage` role read-only access to the commands in the `storage` command directory, no access to the commands in the `storage encryption` subdirectory, and full access to the `storage aggregate plex offline nonintrinsic` command.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

## Predefined roles for cluster administrators

The predefined roles for cluster administrators should meet most of your needs. You can create custom roles as necessary. By default, a cluster administrator is assigned the predefined `admin` role.

The following table lists the predefined roles for cluster administrators:

This role...	Has this level of access...	To the following commands or command directories
admin	all	All command directories (DEFAULT)

admin-no-fsa (available beginning in ONTAP 9.12.1)	Read/Write	<ul style="list-style-type: none"> <li>• All command directories (DEFAULT)</li> <li>• security login rest-role</li> <li>• security login role</li> </ul>
	Read only	<ul style="list-style-type: none"> <li>• security login rest-role create</li> <li>• security login rest-role delete</li> <li>• security login rest-role modify</li> <li>• security login rest-role show</li> <li>• security login role create</li> <li>• security login role create</li> <li>• security login role delete</li> <li>• security login role modify</li> <li>• security login role show</li> <li>• volume activity-tracking</li> <li>• volume analytics</li> </ul>
	None	volume file show-disk-usage
autosupport	all	<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>
	none	All other command directories (DEFAULT)

backup	all	vserver services ndmp
	readonly	volume
	none	All other command directories (DEFAULT)
readonly	all	<ul style="list-style-type: none"> <li>• security login password</li> </ul> <p>For managing own user account local password and key information only</p> <ul style="list-style-type: none"> <li>• set</li> </ul>
	none	security
	readonly	All other command directories (DEFAULT)
none	none	All command directories (DEFAULT)



The autosupport role is assigned to the predefined autosupport account, which is used by AutoSupport OnDemand. ONTAP prevents you from modifying or deleting the autosupport account. ONTAP also prevents you from assigning the autosupport role to other user accounts.

## Predefined roles for SVM administrators

The predefined roles for SVM administrators should meet most of your needs. You can create custom roles as necessary. By default, an SVM administrator is assigned the predefined `vsadmin` role.

The following table lists the predefined roles for SVM administrators:

Role name	Capabilities
-----------	--------------

vsadmin	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing volumes, except volume moves</li> <li>• Managing quotas, qtrees, Snapshot copies, and files</li> <li>• Managing LUNs</li> <li>• Performing SnapLock operations, except privileged delete</li> <li>• Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Monitoring jobs</li> <li>• Monitoring network connections and network interface</li> <li>• Monitoring the health of the SVM</li> </ul>
vsadmin-volume	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing volumes, including volume moves</li> <li>• Managing quotas, qtrees, Snapshot copies, and files</li> <li>• Managing LUNs</li> <li>• Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Monitoring network interface</li> <li>• Monitoring the health of the SVM</li> </ul>
vsadmin-protocol	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Managing LUNs</li> <li>• Monitoring network interface</li> <li>• Monitoring the health of the SVM</li> </ul>



vsadmin-backup	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing NDMP operations</li> <li>• Making a restored volume read/write</li> <li>• Managing SnapMirror relationships and Snapshot copies</li> <li>• Viewing volumes and network information</li> </ul>
vsadmin-snaplock	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing volumes, except volume moves</li> <li>• Managing quotas, qtrees, Snapshot copies, and files</li> <li>• Performing SnapLock operations, including privileged delete</li> <li>• Configuring protocols: NFS and SMB</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Monitoring jobs</li> <li>• Monitoring network connections and network interface</li> </ul>
vsadmin-readonly	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Monitoring the health of the SVM</li> <li>• Monitoring network interface</li> <li>• Viewing volumes and LUNs</li> <li>• Viewing services and protocols</li> </ul>

## Copyright information

Copyright © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.