Manage access-control roles

ONTAP 9

NetApp
January 08, 2026

Table of Contents

Manage access-control roles

Learn about managing ONTAP access-control roles

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 ONTAP 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.

Before you begin

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
   ```

   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
   ```

   Learn more about `security login modify` in the ONTAP command reference.

Define custom roles for ONTAP administrators

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.

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.

Before you begin

You must be a cluster administrator to perform this task.

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
   ```

   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
```

Learn more about `security login role create` in the ONTAP command reference.

Related information

- security login role create
- storage aggregate plex offline
- storage encryption

Predefined roles for ONTAP 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 with ONTAP 9.12.1)	Read/Write	• All command directories (`DEFAULT`) • `security login rest-role` • `security login role`
	Read only	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`
	None	`volume file show-disk-usage`
autosupport	all	• `set` • `system node autosupport`
	none	All other command directories (`DEFAULT`)

backup	all	`vserver services ndmp`
	readonly	`volume`
	none	All other command directories (`DEFAULT`)
readonly	all	• `security login password` For managing own user account local password and key information only • `set`
	• Beginning with ONTAP 9.8, readonly • Prior to ONTAP 9.8, none	`security`
	readonly	All other command directories (`DEFAULT`)
snaplock	all	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`
	none	• `volume move governor` • `volume move recommend`
	none	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.

Related information

- security login
- set
- volume
- vserver services ndmp

Predefined roles for ONTAP 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	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, snapshots, and files • Managing LUNs • Performing SnapLock operations, except privileged delete • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface • Monitoring the health of the SVM
vsadmin-volume	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, snapshots, and files • Managing LUNs • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Monitoring network interface • Monitoring the health of the SVM

vsadmin-protocol	• Managing own user account local password and key information • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Managing LUNs • Monitoring network interface • Monitoring the health of the SVM
vsadmin-backup	• Managing own user account local password and key information • Managing NDMP operations • Making a restored volume read/write • Managing SnapMirror relationships and snapshots • Viewing volumes and network information
vsadmin-snaplock	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, snapshots, and files • Performing SnapLock operations, including privileged delete • Configuring protocols: NFS and SMB • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface
vsadmin-readonly	• Managing own user account local password and key information • Monitoring the health of the SVM • Monitoring network interface • Viewing volumes and LUNs • Viewing services and protocols

Manage ONTAP administrator access with System Manager

The role assigned to an administrator determines which functions the administrator can perform with System Manager. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create

the administrator's account, or you can assign a different role later.

Depending on how you have enabled account access, you might need to perform any of the following:

- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

Assigning a role to an administrator

Assign a role to an administrator, as follows:

Steps

1. Select **Cluster > Settings**.
2. Select → next to **Users and Roles**.
3. Select + Add under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user.

Changing an administrator's role

Change the role for an administrator, as follows:

Steps

1. Click **Cluster > Settings**.
2. Select the name of user whose role you want to change, then click the ⋮ that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.

Access JIT privilege elevation in ONTAP

Beginning with ONTAP 9.17.1, cluster administrators can configure just-in-time (JIT) privilege elevation to allow ONTAP users to temporarily elevate their privileges to perform certain tasks. When JIT is configured for a user, they can temporarily elevate their privilege to a role that has the necessary permissions to perform a task. After the session expires, the user returns to their original access level.

Cluster administrators can configure the duration for which a user can access JIT elevation. For example, cluster administrators can configure user access to JIT elevation with a 30 minute per-session limit (the *session validity period*) for a 30-day period (the *JIT validity period*). During the 30-day period, the user can elevate their privilege as many times as needed, but each session is limited to 30 minutes.

About this task

- JIT privilege elevation is only available to users accessing ONTAP with SSH. Elevated privilege is only available within the current SSH session, but you can elevate privileges within as many concurrent SSH

sessions as needed.

- JIT privilege elevation is only supported for users using password, nsswitch, or domain authentication to log in. Multi-factor authentication (MFA) is not supported for JIT privilege elevation.
- A user's JIT session will be terminated if the configured session or JIT validity period expires, or if a cluster administrator revokes JIT access for the user.

Before you begin

- To access JIT privilege elevation, a cluster administrator must configure JIT access for your account. The cluster administrator determines the role to which you can elevate your privileges, and the duration for which you can access elevated privileges.

Steps

1. Temporarily elevate your privileges to the configured role:

   ```
   security jit-privilege elevate
   ```

   After entering this command, you are prompted to enter your login password. If JIT access is configured for your account, you will be granted elevated access for the configured session duration. After the session duration expires, you will return to your original access level. You can elevate your privileges as many times as needed within the configured JIT validity period.

2. View the remaining time in your JIT session:

   ```
   security jit-privilege show-remaining-time
   ```

   If you are currently in a JIT session, this command displays the remaining time.

3. If needed, end your JIT session early:

   ```
   security jit-privilege reset
   ```

   If you are currently in a JIT session, this command ends the JIT session and restores your original access level.

Configure JIT privilege elevation in ONTAP

Beginning with ONTAP 9.17.1, cluster administrators can configure just-in-time (JIT) privilege elevation to allow ONTAP users to temporarily elevate their privileges to perform certain tasks. When JIT is configured for a user, they can temporarily elevate their privilege to a role that has the necessary permissions to perform a task. After the session duration expires, the user returns to their original access level.

Cluster administrators can configure the duration for which a user can access JIT elevation. For example, you can configure user access to JIT elevation with a 30 minute per-session limit (the *session validity period*) for a 30-day period (the *JIT validity period*). During the 30-day period, the user can elevate their privilege as many times as needed, but each session is limited to 30 minutes.

JIT privilege elevation supports the principle of least privilege, allowing users to perform tasks that require elevated privileges without permanently granting them those privileges. This helps reduce the risk of unauthorized access or accidental changes to the system. The following examples describe some common use cases for JIT privilege elevation:

- Allow temporary access to the `security login create` and `security login delete` commands to enable onboarding and offboarding of users.
- Allow temporary access to `system node image update` and `system node upgrade-revert` during an update window. After the update is complete, command access is revoked.
- Allow temporary access to `cluster add-node`, `cluster remove-node`, and `cluster modify` to enable cluster expansion or reconfiguration. Once the cluster changes are complete, command access is revoked.
- Allow temporary access to `volume snapshot restore` to enable restore operations and backup target management. Once the restore or configuration is complete, command access is revoked.
- Allow temporary access to `security audit log show` to enable audit log review and export during a compliance check.

For a more expansive list of common JIT use cases, refer to Common JIT use cases.

Cluster administrators can set up JIT access for ONTAP users, and configure the default JIT validity periods either globally across the cluster or for specific SVMs.

About this task

- JIT privilege elevation is only available to users accessing ONTAP with SSH. Elevated privileges are only available within the user's current SSH session, but they can elevate privileges within as many concurrent SSH sessions as needed.
- JIT privilege elevation is only supported for users using password, nsswitch, or domain authentication to log in. Multi-factor authentication (MFA) is not supported for JIT privilege elevation.

Before you begin

- You must be an ONTAP cluster administrator at the `admin` privilege level to perform the following tasks.

Modify global JIT settings

You can modify the default JIT settings globally across the ONTAP cluster or for a specific SVM. These settings determine the default session validity period and the maximum JIT validity period for users who are configured for JIT access.

About this task

- The default `default-session-validity-period` value is one hour. This setting determines how long a user can access elevated privileges in a JIT session before needing to re-elevate.
- The default `max-jit-validity-period` value is 90 days. This setting determines the maximum period during which a user can access JIT elevation after the configured start date. You can configure the JIT validity period for individual users, but it cannot exceed the maximum JIT validity period.

Steps

1. Check the current JIT settings:

```
security jit-privilege show -vserver <svm_name>
```

`-vserver` is optional. If you don't specify a SVM, the command shows the global JIT settings.

2. Modify the JIT settings globally or for an SVM:

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

If you don't specify a SVM, the command modifies the global JIT settings. The following example will set the default JIT session duration to 45 minutes and the maximum JIT duration to 30-days for SVM `svm1`: `security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

In this example, users will be able to access JIT elevation for 45 minutes at a time and can initiate JIT sessions for a maximum of 30-days after their configured start date.

Configure JIT privilege elevation access for a user

You can assign JIT privilege elevation access to ONTAP users.

Steps

1. Check the current JIT access for a user:

```
security jit-privilege user show -username <username>
```

`-username` is optional. If you don't specify a username, the command shows the JIT access for all users.

2. Assign new JIT access for a user:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- If `-vserver` is not specified, JIT access is assigned at the cluster level.
- `-role` is the RBAC role that the user will be elevated to. If not specified, `-role` defaults to `admin`.
- `-session-validity-period` is the duration for which the user can access the elevated role before needing to start a new JIT session. If not specified, the global or SVM `default-session-validity-period` is used.
- `-jit-validity-period` is the maximum duration for which a user can initiate JIT sessions after the configured start date. If not specified, the `session-validity-period` is used. This parameter cannot exceed the global or SVM `max-jit-validity-period`.
- `-start-time` is the date and time after which the user can initiate JIT sessions. If not specified, the

current date and time is used.

The following example will allow `ontap_user` to access the `admin` role for 1 hour before needing to start a new JIT session. `ontap_user` will be able to initiate JIT sessions for a 60-day period starting at 1PM on July 1, 2025:
`security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. If needed, revoke a user's JIT access:

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

This command will revoke a user's JIT access, even if their access has not expired. If `-vserver` is not specified, the JIT access is revoked at the cluster level. If the user is in an active JIT session, the session will be terminated.

Common JIT use cases

The following table contains common use cases for JIT privilege elevation. For each use case, an RBAC role would need to be configured to provide access to the relevant commands. Each command links to the ONTAP command reference, with more information about the command and its parameters.

Use case	Commands	Details
User and role management	• `security login create` • `security login delete`	Temporarily elevate to add/remove users or change roles during onboarding or offboarding.
Certificate management	• `security certificate create` • `security certificate install`	Grant short-term access for certificate installation or renewal.
SSH/CLI access control	• `security login create -application ssh`	Temporarily grant SSH access for troubleshooting or vendor support.
License management	• `system license add` • `system license delete`	Grant rights to add or remove licenses during feature activation or deactivation.
System upgrades and patching	• `system node image update` • `system node upgrade-revert`	Elevate for the upgrade window, then revoke.

Use case	Commands	Details
Network security settings	• `security login role create` • `security login role modify`	Allow temporary changes to network-related security roles.
Cluster management	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Elevate for cluster expansion or reconfiguration.
SVM management	• `vserver create` • `vserver delete` • `vserver modify`	Temporarily grant an SVM admin rights for provisioning or decommissioning.
Volume management	• `volume create` • `volume delete` • `volume modify`	Elevate for volume provisioning, resizing, or removal.
Snapshot management	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Elevate for snapshot deletion or restore during recovery.
Network configuration	• `network interface create` • `network port vlan create`	Grant rights for network changes during maintenance windows.
Disk/aggregate management	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Elevate for adding or removing disks or managing aggregates.
Data protection	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Temporarily elevate for configuring or restoring SnapMirror relationships.

Use case	Commands	Details
Performance tuning	• `qos policy-group create` • `qos policy-group modify`	Elevate for performance troubleshooting or tuning.
Audit log access	• `security audit log show`	Temporarily elevate for audit log review or export during compliance checks.
Event and alert management	• `event notification create` • `event notification modify`	Elevate for configuring or testing event notifications or SNMP traps.
Compliance-driven data access	• `volume show` • `security audit log show`	Grant temporary read-only access for auditors to review sensitive data or logs.
Privileged access reviews	• `security login show` • `security login role show`	Temporarily elevate to review and report on privileged access. Grant read-only elevated access for a limited time.

Related information

- cluster
- event notification
- network
- qos policy-group
- security
- snapmirror
- storage
- system
- volume
- vserver

Copyright information

Trademark information