Manage access-control roles

ONTAP 9

NetApp
July 13, 2022

Table of Contents

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`)
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` • `set`
	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	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, Snapshot copies, and files • Managing LUNs • Performing SnapLock operations, except privileged delete • Configuring protocols: NFS, SMB, iSCSI, and FC. including FCoE • 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, including volume moves • Managing quotas, qtrees, Snapshot copies, and files • Managing LUNs • Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE • 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, and FC, including FCoE • 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 Snapshot copies • Viewing volumes and network information
vsadmin-snaplock	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, Snapshot copies, 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