ONTAP® 9

Administrator Authentication and RBAC Power Guide

October 2016 | [215-11616_A0]
doccomments@netapp.com

Updated for ONTAP 9.1
Release Candidate Documentation - Contents Subject To Change

NetApp®

Contents

Deciding whether to use the Administrator Authentication and RBAC Power Guide

This guide describes how to enable login accounts for Data ONTAP cluster and Storage Virtual Machine (SVM) administrators, and how to use role-based access control (RBAC) to define the capabilities of administrators.

You should use this guide if you want to enable login accounts and RBAC in the following way:

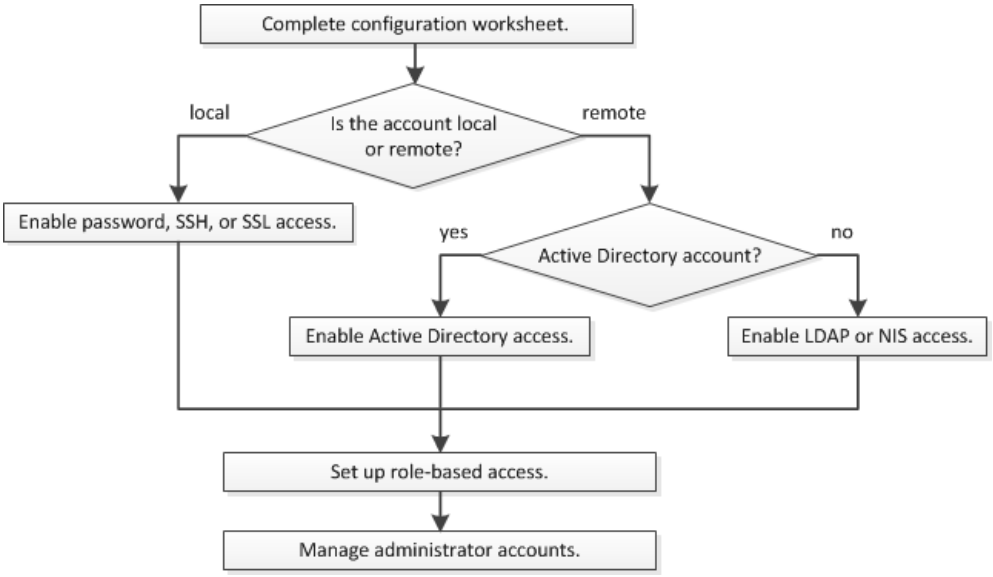
- You want to use the Data ONTAP command-line interface (CLI), not OnCommand System Manager or an automated scripting tool.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You are not using SNMP to collect information about the cluster.

If this guide is not suitable for your situation, you should see the following documentation instead:

- *ONTAP 9 Commands: Manual Page Reference*
- *ONTAP 9 Cluster Management Using OnCommand System Manager*
- *NetApp Documentation: OnCommand Workflow Automation (current releases)*
- *NetApp Technical Report 4220: SNMP Support in Data ONTAP 8.2.x and Data ONTAP 8.3.x*

Administrator authentication and RBAC workflow

You can enable local or remote administrator accounts. A local account is one in which the account information, public key, or security certificate resides on the storage system. A remote account is one in which the account information resides elsewhere. Each account can have a predefined or custom role.



Worksheets for administrator authentication and RBAC configuration

Before creating login accounts and setting up RBAC, you should gather information for each item in the configuration worksheets.

Creating or modifying login accounts

You supply these values with the `security login create` command when you enable login accounts to access an SVM. You supply the same values with the `security login modify` command when you modify how an account accesses an SVM.

Field	Description	Your value
`-vserver`	The name of the SVM the account accesses. The default is the name of the admin SVM for the cluster.	
`-user-or-group-name`	The user or group name of the account. Specifying a group name enables access to each user in the group. You can associate a user name or group name with multiple applications.	
`-application`	The application used to access the SVM: • **`http`** • **`ontapi`** • **`snmp`** • **`ssh`**	
`-authmethod`	The method used to authenticate the account: • **`cert`** for SSL certificate authentication • **`domain`** for Active Directory authentication • **`nsswitch`** for LDAP or NIS authentication • **`password`** for user password authentication • **`publickey`** for public key authentication • **`community`** for SNMP community strings • **`usm`** for SNMP user security model	

Field	Description	Your value
`-role`	The access control role assigned to the account. • For the cluster (the admin SVM), the default is **`admin`** • For a data SVM, the default is **`vsadmin`**	
`-comment`	Optional. Descriptive text for the account. Enclose the text in double quotation marks (“"”).	
`-is-ns-switch-group`	Whether the account is an LDAP or NIS group account, **`yes`** or **`no`**.	

Defining custom roles

You supply these values with the `security login role create` command when you define a custom role. For more information about the rules that govern role setup, see

Field	Description	Your value
`-vserver`	Optional. The name of the SVM associated with the role.	
`-role`	The name of the role.	
`-cmddirname`	The command or command directory to which the role gives access. Enclose command subdirectory names in double quotation marks (“"”). For example, “**`volume snapshot`**”. Enter **`DEFAULT`** to specify all command directories.	

Field	Description	Your value
`-access`	Optional. The access level for the role. For command directories: • **`none`** (the default for custom roles) denies access to commands in the command directory • **`readonly`** grants access to the `show` commands in the command directory and its subdirectories • **`all`** grants access to all commands in the command directory and its subdirectories For *nonintrinsic commands* (commands not ending in `create`, `modify`, `delete`, or `show`): • **`none`** (the default for custom roles) denies access to the command • **`readonly`** is N/A • **`all`** grants access to the command To grant or deny access to intrinsic commands, you must specify the command directory.	
`-query`	Optional. The query object used to filter the access level, in the form of a valid option for the command, or for a command in the command directory. Enclose the query object in double quotation marks (“”). For example, if the command directory is **`volume`**, the query object “**`-aggr aggr0`**” would enable access for the `aggr0` aggregate only.	

Associating a public key with a user account

You supply these values with the `security login publickey create` command when you associate an SSH public key with a user account.

Field	Description	Your value
`-vserver`	Optional. The name of the SVM the account accesses.	
`-username`	The user name of the account. The default, **`admin`**, is the default name of the cluster administrator.	

Field	Description	Your value
`-index`	The index number of the public key. The default is 0 if the key is the first key created for the account, otherwise one more than the highest existing index number for the account.	
`-publickey`	The OpenSSH public key. Enclose the key in double quotation marks (“"”).	
`-role`	The access control role assigned to the account.	
`-comment`	Optional. Descriptive text for the public key. Enclose the text in double quotation marks (“"”).	

Installing a CA-signed server digital certificate

You supply these values with the `security certificate generate-csr` command when you generate a digital certificate signing request (CSR) for use in authenticating an SVM as an SSL server.

Field	Description	Your value
`-common-name`	The name of the certificate, either a fully qualified domain name or a custom common name.	
`-size`	The number of bits in the private key. The higher the value, the more secure the key. The default is **`2048`**. Possible values are **`512`**, **`1024`**, **`1536`**, and **`2048`**.	
`-country`	The country of the SVM, in a two-letter code. The default is **`US`**. See the man page for a list of codes.	
`-state`	The state or province of the SVM.	
`-locality`	The locality of the SVM.	
`-organization`	The organization of the SVM.	
`-unit`	The unit in the organization of the SVM.	
`-email-addr`	The email address of the contact administrator for the SVM.	
`-hash-function`	The cryptographic hashing function for signing the certificate. The default is **`SHA256`**. Possible values are **`SHA1`**, **`SHA256`**, and **`MD5`**.	

You supply these values with the `security certificate install` command when you install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. Only options relevant to this guide are shown in the following table.

Field	Description	Your value
`-vserver`	The name of the SVM to install the certificate on.	
`-type`	The certificate type: • **`server`** for server certificates and intermediate certificates • **`client-ca`** for the public key certificate of the root CA of the SSL client • **`server-ca`** for the public key certificate of the root CA of the SSL server to which Data ONTAP is a client • **`client`** for a self-signed or CA-signed digital certificate and private key for Data ONTAP as an SSL client	

Configuring Active Directory domain controller access

You supply these values with the `security login domain-tunnel create` command when you have already configured a CIFS server for a data SVM and want to configure the SVM as a gateway, or *tunnel*, for AD domain controller access to the cluster.

Field	Description	Your value
`-vserver`	The name of the SVM for which the CIFS server has been configured.	

You supply these values with the `vserver active-directory create` command when you have not configured a CIFS server and want to create an SVM computer account on the AD domain.

Field	Description	Your value
`-vserver`	The name of the SVM for which you want to create an AD computer account.	
`-account-name`	The NetBIOS name of the computer account.	
`-domain`	The fully qualified domain name (FQDN).	
`-ou`	The organizational unit in the domain. The default is **`CN=Computers`**. Data ONTAP appends this value to the domain name to produce the AD distinguished name.	

Configuring LDAP or NIS server access

You supply these values with the `vserver services name-service ldap client create` command when you create an LDAP client configuration for the SVM. Only options relevant to this guide are shown in the following table.

Field	Description	Your value
`-vserver`	The name of the SVM for the client configuration.	
`-client-config`	The name of the client configuration.	
`-servers`	A comma-separated list of IP addresses for the LDAP servers the client connects to.	
`-schema`	The schema the client uses to make LDAP queries.	
`-use-start-tls`	Whether the client uses Start TLS to encrypt communication with the LDAP server, **`true`** or **`false`**.	

You supply these values with the `vserver services name-service ldap create` command when you associate an LDAP client configuration with the SVM.

Field	Description	Your value
`-vserver`	The name of the SVM to associate the client configuration with.	
`-client-config`	The name of the client configuration.	
`-client-enabled`	Whether the SVM can use the LDAP client configuration, **`true`** or **`false`**.	

You supply these values with the `vserver services name-service nis-domain create` command when you create a NIS domain configuration on an SVM.

Field	Description	Your value
`-vserver`	The name of the SVM to create the domain configuration on.	
`-domain`	The name of the domain.	
`-active`	Whether the domain is active, **`true`** or **`false`**.	
`-servers`	A comma-separated list of IP addresses for the NIS servers used by the domain configuration.	

You supply these values with the `vserver services name-service ns-switch create` command when you specify the look-up order for name service sources.

Field	Description	Your value
`-vserver`	The name of the SVM on which to configure the name service look-up order.	
`-database`	The name service database: • **`hosts`** for files and DNS name services • **`group`** for files, LDAP, and NIS name services • **`passwd`** for files, LDAP, and NIS name services • **`netgroup`** for files, LDAP, and NIS name services • **`namemap`** for files and LDAP name services	
`-sources`	The order in which to look up name service sources, in a comma-separated list: • **`files`** • **`dns`** • **`ldap`** • **`nis`**	

Creating login accounts

You can enable local or remote cluster and SVM administrator accounts. A local account is one in which the account information, public key, or security certificate resides on the storage system. AD account information is stored on a domain controller. LDAP and NIS accounts reside on LDAP and NIS servers.

Cluster and SVM administrators

A *cluster administrator* accesses the admin SVM for the cluster. The admin SVM and a cluster administrator with the reserved name **admin** are automatically created when the cluster is set up.

A cluster administrator with the default **admin** role can administer the entire cluster and its resources. The cluster administrator can create additional cluster administrators with different roles as needed.

An *SVM administrator* accesses a data SVM. The cluster administrator creates data SVMs and SVM administrators as needed.

SVM administrators are assigned the **vsadmin** role by default. The cluster administrator can assign different roles to SVM administrators as needed.

Merged roles

If you enable multiple remote accounts for the same user, the user is assigned the union of all roles specified for the accounts. That is, if an LDAP or NIS account is assigned the **vsadmin** role, and the AD group account for the same user is assigned the **vsadmin-volume** role, the AD user logs in with the more inclusive **vsadmin** capabilities. The roles are said to be *merged*.

Choices

- Enabling local account access on page 13
- Enabling Active Directory account access on page 16
- Enabling LDAP or NIS account access on page 17

Enabling local account access

A local account is one in which the account information, public key, or security certificate resides on the storage system. You can use the `security login create` command to enable local accounts to access an admin or data SVM.

Choices

- Enabling password account access on page 13
- Enabling SSH public key accounts on page 14
- Enabling SSL certificate accounts on page 15

Enabling password account access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with a password. You are prompted for the password after you enter the command.

Before you begin

You must be a cluster administrator to perform this task.

About this task

If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

Modifying the role assigned to an administrator on page 19

Step

1. Enable local administrator accounts to access an SVM using a password:

   `security login create -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 on page 6

Example

The following command enables the cluster administrator account **`admin1`** with the predefined **`backup`** role to access the admin SVM **`engCluster`** using a password. You are prompted for the password after you enter the command.

```
cluster1::>security login create -vserver engCluster -user-or-group-
name admin1 -application ssh -authmethod password -role backup
```

Related information

ONTAP 9 man page: security login create

Enabling SSH public key accounts

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSH public key.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- You must associate the public key with the account before the account can access the SVM.
  Associating a public key with a user account on page 24
  You can perform this task before or after you enable account access.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.
  Modifying the role assigned to an administrator on page 19

Step

1. Enable local administrator accounts to access an SVM using an SSH public key:

   `security login create -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 on page 6

Example

The following command enables the SVM administrator account **svmadmin1** with the predefined **vsadmin-volume** role to access the SVM **engData1** using an SSH public key:

```
cluster1::>security login create -vserver engData1 -user-or-group-
name svmadmin1 -application ssh -authmethod publickey -role vsadmin-
volume
```

After you finish

If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

Associating a public key with a user account on page 24

Related information

ONTAP 9 man page: security login create

Enabling SSL certificate accounts

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSL certificate.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- You must install a CA-signed server digital certificate before the account can access the SVM.
  Generating and installing a CA-signed server certificate on page 25
  You can perform this task before or after you enable account access.
- If you are unsure of the access control role you want to assign to the login account, you can add the role later with the `security login modify` command.
  Modifying the role assigned to an administrator on page 19

Note: For cluster administrator accounts, certificate authentication is supported only with the **http** and **ontapi** applications. For SVM administrator accounts, certificate authentication is supported only with the **ontapi** application.

Step

1. Enable local administrator accounts to access an SVM using an SSL certificate:

   security login create -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 on page 6

Example

The following command enables the SVM administrator account **svmadmin2** with the default **vsadmin** role to access the SVM **engData2** using an SSL digital certificate.

```
cluster1::>security login create -vserver engData2 -user-or-group-
name svmadmin2 -application ontapi -authmethod cert
```

After you finish

If you have not installed a CA-signed server digital certificate, you must do so before the account can access the SVM.

Generating and installing a CA-signed server certificate on page 25

Related information

ONTAP 9 man page: security login create

Enabling Active Directory account access

You can use the `security login create` command to enable Active Directory (AD) user or group accounts to access an admin or data SVM. Any user in the AD group can access the SVM with the role that is assigned to the group.

Before you begin

- The cluster time must be synchronized to within five minutes of the time on the AD domain controller.
- You must be a cluster administrator to perform this task.

About this task

- You must configure AD domain controller access to the cluster or SVM before the account can access the SVM.
  Configuring Active Directory domain controller access on page 27
  You can perform this task before or after you enable account access.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.
  Modifying the role assigned to an administrator on page 19

Note: AD group account access is supported only with the **SSH** and **ontapi** applications.

Step

1. Enable AD user or group administrator accounts to access an SVM:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod domain -role *role* -comment *comment*

   For complete command syntax, see the worksheet.

   Creating or modifying login accounts on page 6

Example

The following command enables the AD cluster administrator account **DOMAIN1\guest1** with the predefined **backup** role to access the admin SVM **engCluster**.

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

The following command enables the SVM administrator accounts in the AD group account **DOMAIN1\adgroup** with the predefined **vsadmin-volume** role to access the SVM **engData**.

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

After you finish

If you have not configured AD domain controller access to the cluster or SVM, you must do so before the account can access the SVM.

Configuring Active Directory domain controller access on page 27

Related information

ONTAP 9 man page: security login create

Enabling LDAP or NIS account access

You can use the `security login create` command to enable LDAP or NIS user or group accounts to access an admin or data SVM. Any user in the LDAP or NIS group can access the SVM with the role assigned to the group.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- You must configure LDAP or NIS server access to the SVM before the account can access the SVM.
  Configuring LDAP or NIS server access on page 29
  You can perform this task before or after you enable account access.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.
  Modifying the role assigned to an administrator on page 19

Step

1. Enable LDAP or NIS user or group accounts to access an SVM:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod nsswitch -role` *`role`* `-comment` *`comment`* `-is-ns-switch-group yes|no`

   For complete command syntax, see the worksheet.

   Creating or modifying login accounts on page 6

   #### Example

   The following command enables the LDAP or NIS cluster administrator account **`guest2`** with the predefined **`backup`** role to access the admin SVM **`engCluster`**.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-
   name guest2 -application ssh -authmethod nsswitch -role backup
   ```

   The following command enables the LDAP or NIS SVM group administrator account **`svmadmin2`** with the predefined **`vsadmin-volume`** role to access the SVM **`engData1`**.

```
cluster1::>security login create -vserver engData1 -user-or-group-
name svmadmin2 -application ssh -authmethod nsswitch -role vsadmin-
volume -is-ns-switch-group yes
```

After you finish

If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

Configuring LDAP or NIS server access on page 29

Related information

ONTAP 9 man page: security login create

Managing 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.

Related concepts

Predefined roles for cluster administrators on page 21
Predefined roles for SVM administrators on page 21

Related tasks

Modifying the role assigned to an administrator on page 19
Defining custom roles on page 20

Modifying 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.

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`*

   For complete command syntax, see the worksheet.

   Creating or modifying login accounts on page 6

   #### Example

   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
   ```

Related information

ONTAP 9 man page: security login modify

Defining 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.

Before you begin

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.

Note: 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.

   Defining custom roles on page 7

Example

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
```

Related information

ONTAP 9 man page: security login role create

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**)

Note: 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, CIFS, 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, CIFS, 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, CIFS, 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 CIFS • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface

Role name	Capabilities
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

Managing user accounts

Depending on how you have enabled account access, you may need to associate a public key with a local account, install a CA-signed server digital certificate, or configure AD, LDAP, or NIS access. You can perform all of these tasks before or after enabling account access.

Related tasks

Associating a public key with a user account on page 24
Generating and installing a CA-signed server certificate on page 25
Configuring Active Directory domain controller access on page 27
Configuring LDAP or NIS server access on page 29
Changing a user password on page 32
Locking and unlocking a user account on page 32

Associating a public key with a user account

For SSH public key authentication, you must associate the public key with a user account before the account can access the SVM. You can use the `security login publickey create` command to associate a key with a user account.

Before you begin

- You must have generated the SSH key.
- You must be a cluster or SVM administrator to perform this task.

About this task

If you authenticate an account over SSH with both a password and an SSH public key, the account is authenticated first with the public key.

Step

1. Associate a public key with an administrator account:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-comment` *`comment`*

   For complete command syntax, see the worksheet.

   Associating a public key with a user account on page 8

   ### Example

   The following command associates a public key with the SVM administrator account **`svmadmin1`** for the SVM **`engData1`**. The public key is assigned index number 5.

   ```
   cluster1::>security login publickey create -vserver engData1 -
   username svmadmin1 -index 5 -publickey
   "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J
   /vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIza
   FciDy7hgnmdj9eNGedGr/JNrftQbLD1hZybX+72DpQB0tYWBhe6eDJ1oPLob
   ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
   ```

Related information

ONTAP 9 man page: security login publickey create

Generating and installing a CA-signed server certificate

On production systems, it is a best practice to install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR), and the `security certificate install` command to install the certificate you receive back from the certificate authority.

Related tasks

Generating a certificate signing request on page 25
Installing a CA-signed server certificate on page 26

Generating a certificate signing request

You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Steps

1. Generate a CSR:

   security certificate generate-csr -common-name *FQDN_or_common_name* -size 512|1024|1536|2048 -country *country* -state *state* -locality *locality* -organization *organization* -unit *unit* -email-addr *email_of_contact* -hash-function SHA1|SHA256|MD5

   For complete command syntax, see the worksheet.

   Installing a CA-signed server digital certificate on page 9

Example

The following command creates a CSR with a **2048**-bit private key generated by the **SHA256** hashing function for use by the **Software** group in the **IT** department of a company whose custom common name is **server1.companyname.com**, located in **Sunnyvale**, **California**, **USA**. The email address of the SVM contact administrator is **web@example.com**. The system displays the CSR and the private key in the output.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

```
Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copy the certificate request from the CSR output, and send it in electronic form (such as email) to a trusted third-party CA for signing.

   After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

Related information

ONTAP 9 man page: security certificate generate-csr

Installing a CA-signed server certificate

You can use the `security certificate install` command to install a CA-signed server certificate on an SVM. ONTAP prompts you for the certificate authority (CA) root and intermediate certificates that form the certificate chain of the server certificate.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Step

1. Install a CA-signed server certificate:

   `security certificate install -vserver` *`SVM_name`* `-type` *`certificate_type`*

   For complete command syntax, see the worksheet.

   Installing a CA-signed server digital certificate on page 9

   Note: ONTAP prompts you for the CA root and intermediate certificates that form the certificate chain of the server certificate. The chain starts with the certificate of the CA that issued the server certificate, and can range up to the root certificate of the CA. Any missing intermediate certificates result in the failure of server certificate installation.

Example

The following command installs the CA-signed **`server`** certificate and intermediate certificates on the SVM **`engData2`**.

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
```

```
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Related information

ONTAP 9 man page: security certificate install

Configuring Active Directory domain controller access

You must configure AD domain controller access to the cluster or SVM before an AD account can access the SVM. If you have already configured a CIFS server for a data SVM, you can configure the SVM as a gateway, or *tunnel*, for AD access to the cluster. If you have not configured a CIFS server, you can create a computer account for the SVM on the AD domain.

Choices

- Configuring an authentication tunnel on page 28
- Creating an SVM computer account on the domain on page 28

Configuring an authentication tunnel

If you have already configured a CIFS server for a data SVM, you can use the `security login domain-tunnel create` command to configure the SVM as a gateway, or *tunnel*, for AD access to the cluster.

Before you begin

- You must have configured a CIFS server for a data SVM.
- You must have enabled an AD domain user account to access the admin SVM for the cluster.
- You must be a cluster administrator to perform this task.

Step

1. Configure a CIFS-enabled data SVM as an authentication tunnel for AD domain controller access to the cluster:

   `security login domain-tunnel create -vserver` *`SVM_name`*

   For complete command syntax, see the worksheet.

   Configuring Active Directory domain controller access on page 10

   Note: The SVM must be running for the user to be authenticated.

Example

The following command configures the CIFS-enabled data SVM **`engData`** as an authentication tunnel.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Related information

ONTAP 9 man page: security login domain-tunnel create

Creating an SVM computer account on the domain

If you have not configured a CIFS server for a data SVM, you can use the `vserver active-directory create` command to create a computer account for the SVM on the domain.

Before you begin

You must be a cluster or SVM administrator to perform this task.

About this task

After you enter the `vserver active-directory create` command, you are prompted to provide the credentials for an AD user account with sufficient privileges to add computers to the specified organizational unit in the domain. The password of the account cannot be empty.

Step

1. Create a computer account for an SVM on the AD domain:

   `vserver active-directory create -vserver` *`SVM_name`* `-account-name` *`NetBIOS_account_name`* `-domain` *`domain`* `-ou` *`organizational_unit`*

   For complete command syntax, see the worksheet.

   Configuring Active Directory domain controller access on page 10

Example

The following command creates a computer account named **ADSERVER1** on the domain **example.com** for the SVM **engData**. You are prompted to enter the AD user account credentials after you enter the command.

```
cluster1::>vserver active-directory create -vserver engData -account-
name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must
supply the name and password of a Windows account with sufficient
privileges to add computers to the "CN=Computers" container within
the "example.com" domain.

Enter the user name: Administrator

Enter the password:
```

Related information

ONTAP 9 man page: vserver active-directory create

Configuring LDAP or NIS server access

You must configure LDAP or NIS server access to an SVM before LDAP or NIS accounts can access the SVM. The switch feature lets you use LDAP or NIS as alternative name service sources.

Related tasks

Configuring LDAP server access on page 29
Configuring NIS server access on page 30
Creating a name service switch on page 31

Configuring LDAP server access

You must configure LDAP server access to an SVM before LDAP accounts can access the SVM. You can use the `vserver services name-service ldap client create` command to create an LDAP client configuration on the SVM. You can then use the `vserver services name-service ldap create` command to associate the LDAP client configuration with the SVM.

Before you begin

- You must have installed a CA-signed server digital certificate on the SVM.
  Generating and installing a CA-signed server certificate on page 25
- You must be a cluster or SVM administrator to perform this task.

About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX AD servers)

It is best to use the default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema and modifying the copy. For more information, see the *Data ONTAP 8.3.1 NFS Configuration Power Guide*.

ONTAP 9 NFS Configuration Power Guide

Steps

1. Create an LDAP client configuration on an SVM:

   vserver services name-service ldap client create -vserver *SVM_name* -client-config *client_configuration* -servers *LDAP_server_IPs* -schema *schema* -use-start-tls true|false

   For complete command syntax, see the worksheet.

   Configuring LDAP or NIS server access on page 11

   #### Example

   The following command creates an LDAP client configuration named **corp** on the SVM **engData**. The client makes anonymous binds to the LDAP servers with the IP addresses **172.160.0.100** and **172.16.0.101**. The client uses the **RFC-2307** schema to make LDAP queries. Communication between the client and server is encrypted using Start TLS.

   ```
   cluster1::>vserver services name-service ldap client create
   -vserver engData -client-config corp -servers
   172.16.0.100,172.16.0.101 -schema RFC-2307 -use-start-tls true
   ```

2. Associate the LDAP client configuration with the SVM:

   vserver services name-service ldap create -vserver *SVM_name* -client-config *client_configuration* -client-enabled true|false

   For complete command syntax, see the worksheet.

   Configuring LDAP or NIS server access on page 11

   #### Example

   The following command associates the LDAP client configuration **corp** with the SVM **engData**, and enables the LDAP client on the SVM.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

Related information

ONTAP 9 man page: vserver services name-service ldap client create
ONTAP 9 man page: vserver services name-service ldap create

Configuring NIS server access

You must configure NIS server access to an SVM before NIS accounts can access the SVM. You can use the `vserver services name-service nis-domain create` command to create an NIS domain configuration on an SVM.

Before you begin

- All configured servers must be available and accessible before you configure the NIS domain on the SVM.
- You must be a cluster or SVM administrator to perform this task.

About this task

You can create multiple NIS domains. Only one NIS domain can be set to **active** at a time.

Step

1. Create an NIS domain configuration on an SVM:

   vserver services name-service nis-domain create -vserver *SVM_name* -domain *client_configuration* -active true|false -servers *NIS_server_IPs*

   For complete command syntax, see the worksheet.

   Configuring LDAP or NIS server access on page 11

Example

The following command creates an NIS domain configuration on the SVM **engData**. The NIS domain **nisdomain** is active on creation and communicates with an NIS server with the IP address **192.0.2.180**.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -servers 192.0.2.180
```

Related information

ONTAP 9 man page: vserver services name-service nis-domain create

Creating a name service switch

The name service switch feature lets you use LDAP or NIS as alternative name service sources. You can use the `vserver services name-service ns-switch modify` command to specify the look-up order for name service sources.

Before you begin

- You must have configured LDAP and NIS server access.
- You must be a cluster administrator or SVM administrator to perform this task.

Step

1. Specify the lookup order for name service sources:

   vserver services name-service ns-switch modify -vserver *SVM_name* -database *name_service_switch_database* -sources *name_service_source_order*

   For complete command syntax, see the worksheet.

   Configuring LDAP or NIS server access on page 11

Example

The following command specifies the lookup order of the LDAP and NIS name service sources for the **passwd** database on the **engData** SVM.

```
cluster1::>vserver services name-service ns-switch
modify -vserver engData -database passwd -source files ldap,nis
```

Related information

ONTAP 9 man page: vserver services name-service ns-switch create

Changing a user password

You should change your initial password immediately after logging into the system for the first time. If you are an SVM administrator, you can use the `security login password` command to change your own password. If you are a cluster administrator, you can use the command to change any user's password.

Before you begin

- You must be a cluster or SVM administrator to change your own password.
- You must be a cluster administrator to change another user's password.

About this task

The new password must observe the following rules:

- It cannot contain the user name
- It must be at least eight characters long
- It must contain at least one letter and one number
- It cannot be the same as the last six passwords

Note: You can use the `security login role config modify` command to modify the password rules for accounts associated with a given role. For more information, see the man page.

`security login role config modify`

Step

1. Change a user password:

   `security login password -vserver` ***`SVM_name`*** **`-username`** ***`user_name`***

   #### Example

   The following command changes the password of the administrator **`admin1`** for the SVM **`vs1.example.com`**. You are prompted to enter the current password, then enter and reenter the new password.

   ```
   vs1.example.com::>security login password -vserver engData -username
   admin1
   Please enter your current password:
   Please enter a new password:
   Please enter it again:
   ```

Related information

ONTAP 9 man page: security login password

Locking and unlocking a user account

You can use the `security login lock` command to lock an account, and the `security login unlock` command to unlock the account.

Before you begin

You must be a cluster administrator to perform these tasks.

Steps

1. Lock an administrator account:

   security login lock -vserver *SVM_name* -username *user_name*

   Example

   The following command locks the administrator account **admin1** for the SVM **vs1.example.com**:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

2. Unlock an administrator account:

   security login unlock -vserver *SVM_name* -username *user_name*

   Example

   The following command unlocks the administrator account **admin1** for the SVM **vs1.example.com**:

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

Related information

ONTAP 9 man page: security login lock
ONTAP 9 man page: security login unlock

Managing failed login attempts

Repeated failed login attempts sometimes indicate that an intruder is attempting to access the storage system. You can take a number of steps to ensure that an intrusion does not take place.

How you will know that login attempts have failed

The Event Management System (EMS) notifies you about failed login attempts every hour. You can find a record of failed login attempts in the `audit.log` file.

What to do if repeated login attempts fail

In the short term, you can take a number of steps to prevent an intrusion:

- Require that passwords be composed of a minimum number of uppercase characters, lowercase characters, special characters, and/or digits
- Impose a delay after a failed login attempt
- Limit the number of allowed failed login attempts, and lock out users after the specified number of failed attempts
- Expire and lock out accounts that are inactive for a specified number of days

You can use the `security login role config modify` command to perform these tasks. For more information, see the man page.

`security login role config modify`

Over the long term, you can migrate existing MD5-algorithm accounts to the more secure SHA-512 algorithm by requiring users to change their passwords.

Enforcing SHA-2 on user account passwords on page 34

Enforcing SHA-2 on user account passwords

User accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

Steps

1. Migrate the MD5 user accounts to using the SHA-512 password hash function:
   a. Expire all MD5 user accounts:

      security login expire-password -vserver * -username * -hash-function md5

      Doing so forces MD5 account users to change their passwords upon next login.

   b. Ask users of MD5 accounts to log in through a console or SSH session.

      The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. Optional: For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:
   a. Lock accounts that still use the MD5 hash function (advanced privilege level):

      security login expire-password -vserver * -username * -hash-function md5 -lock-after *integer*

      After the number of days specified by `-lock-after`, users cannot access their MD5 accounts.

   b. Unlock the accounts when the users are ready to change their passwords:

      security login unlock -vserver *vserver_name* -username *user_name*

   c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

Where to find additional information

After you have enabled login accounts for Data ONTAP cluster and SVM administrators, you can perform more advanced tasks.

- *ONTAP 9 Commands: Manual Page Reference*
  Describes additional commands for enabling administrator account access and for using RBAC to define administrator capabilities.
- *ONTAP 9 Cluster Management Using OnCommand System Manager*
  Describes how to use OnCommand System Manager to perform tasks related to administrator authentication and RBAC.
- *NetApp Documentation: OnCommand Workflow Automation (current releases)*
  Describes how to use the OnCommand Workflow Automation scripting tool to perform tasks related to administrator authentication and RBAC.
- *ONTAP 9 System Administration Reference*
  Describes general system administration for storage systems running clustered Data ONTAP.
- *NetApp Technical Report 4220: SNMP Support in Data ONTAP 8.2.x and Data ONTAP 8.3.x*
  Describes how the SNMP agent on the storage system responds to queries and sends traps to network management stations.

Copyright information

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

C

D

T

U

W