ONTAP management interface basics

ONTAP 9

NetApp
March 24, 2022

Table of Contents

ONTAP management interface basics

Access the cluster by using the CLI (cluster administrators only)

Access the cluster by using the serial port

You can access the cluster directly from a console that is attached to a node's serial port.

Steps

1. At the console, press Enter.

   The system responds with the login prompt.

2. At the login prompt, do one of the following:

To access the cluster with…	Enter the following account name…
The default cluster account	**admin**
An alternative administrative user account	*username*

   The system responds with the password prompt.

3. Enter the password for the admin or administrative user account, and then press Enter.

Access the cluster by using SSH

You can issue SSH requests to the cluster to perform administrative tasks. SSH is enabled by default.

What you'll need

- You must have a user account that is configured to use `ssh` as an access method.

  The `-application` parameter of the `security login` commands specifies the access method for a user account. The `security login` man pages contain additional information.

- If you use an Active Directory (AD) domain user account to access the cluster, an authentication tunnel for the cluster must have been set up through a CIFS-enabled storage virtual machine (SVM), and your AD domain user account must also have been added to the cluster with `ssh` as an access method and `domain` as the authentication method.
- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

  The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

About this task

- You must use an OpenSSH 5.7 or later client.
- Only the SSH v2 protocol is supported; SSH v1 is not supported.
- ONTAP supports a maximum of 64 concurrent SSH sessions per node.

  If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

  If the rate of incoming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- ONTAP supports only the AES and 3DES encryption algorithms (also known as *ciphers*) for SSH.

  AES is supported with 128, 192, and 256 bits in key length. 3DES is 56 bits in key length as in the original DES, but it is repeated three times.

- When FIPS mode is on, SSH clients should negotiate with Elliptic Curve Digital Signature Algorithm (ECDSA) public key algorithms for the connection to be successful.
- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.
- If you use a Windows AD user name to log in to ONTAP, you should use the same uppercase or lowercase letters that were used when the AD user name and domain name were created in ONTAP.

  AD user names and domain names are not case-sensitive. However, ONTAP user names are case-sensitive. Case mismatch between the user name created in ONTAP and the user name created in AD results in a login failure.

- Beginning with ONTAP 9.3, you can enable SSH multifactor authentication for local administrator accounts.

  When SSH multifactor authentication is enabled, users are authenticated by using a public key and a password.

- Beginning with ONTAP 9.4, you can enable SSH multifactor authentication for LDAP and NIS remote users.

Steps

1. From an administration host, enter the `ssh` command in one of the following formats:
   - **ssh *username@hostname_or_IP* [*command*]**
   - **ssh -l *username hostname_or_IP* [*command*]**

If you are using an AD domain user account, you must specify *username* in the format of *domainname**AD_accountname* (with double backslashes after the domain name) or "*domainname**AD_accountname*" (enclosed in double quotation marks and with a single backslash after the domain name).

hostname_or_IP is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

command is not required for SSH-interactive sessions.

Examples of SSH requests

The following examples show how the user account named “joe” can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

The following examples show how the user account named “john” from the domain named “DOMAIN1” can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

The following example shows how the user account named “joe” can issue an SSH MFA request to access a cluster whose cluster management LIF is 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Related information

Administrator authentication and RBAC

SSH login security

Beginning with ONTAP 9.5, you can view information about previous logins, unsuccessful attempts to log in, and changes to your privileges since your last successful login.

Security-related information is displayed when you successfully log in as an SSH admin user. You are alerted about the following conditions:

- The last time your account name was logged in.
- The number of unsuccessful login attempts since the last successful login.
- Whether the role has changed since the last login (for example, if the admin account's role changed from "admin" to "backup.")
- Whether the add, modify, or delete capabilities of the role were modified since the last login.

If any of the information displayed is suspicious, you should immediately contact your security department.

To obtain this information when you login, the following prerequisites must be met:

- Your SSH user account must be provisioned in ONTAP.
- Your SSH security login must be created.
- Your login attempt must be successful.

Restrictions and other considerations for SSH login security

The following restrictions and considerations apply to SSH login security information:

- The information is available only for SSH-based logins.
- For group-based admin accounts, such as LDAP/NIS and AD accounts, users can view the SSH login information if the group of which they are a member is provisioned as an admin account in ONTAP.

  However, alerts about changes to the role of the user account cannot be displayed for these users. Also, users belonging to an AD group that has been provisioned as an admin account in ONTAP cannot view the count of unsuccessful login attempts that occurred since the last time they logged in.

- The information maintained for a user is deleted when the user account is deleted from ONTAP.
- The information is not displayed for connections to applications other than SSH.

Examples of SSH login security information

The following examples demonstrate the type of information displayed after you login.

- This message is displayed after each successful login:

```
Last Login : 7/19/2018 06:11:32
```

- These messages are displayed if there have been unsuccessful attempts to login since the last successful login:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- These messages are displayed if there have been unsuccessful attempts to login and your privileges were modified since the last successful login:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Enable Telnet or RSH access to the cluster

As a security best practice, Telnet and RSH are disabled in the predefined management firewall policy (`mgmt`). To enable the cluster to accept Telnet or RSH requests, you must create a new management firewall policy that has Telnet or RSH enabled, and then associate the new policy with the cluster management LIF.

About this task

ONTAP prevents you from changing predefined firewall policies, but you can create a new policy by cloning the predefined `mgmt` management firewall policy, and then enabling Telnet or RSH under the new policy. However, Telnet and RSH are not secure protocols, so you should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

Perform the following steps to enable Telnet or RSH access to the clusters:

Steps

1. Enter the advanced privilege mode:
   `set advanced`
2. Enable a security protocol (RSH or Telnet):
   `security protocol modify -application *security_protocol* -enabled true`

3. Create a new management firewall policy based on the `mgmt` management firewall policy:
   system services firewall policy clone -policy mgmt -destination-policy *policy-name*
4. Enable Telnet or RSH in the new management firewall policy:
   system services firewall policy create -policy *policy-name* -service *security_protocol* -action allow -ip-list *ip_address/netmask*
   To allow all IP addresses, you should specify `-ip-list 0.0.0.0/0`
5. Associate the new policy with the cluster management LIF:
   network interface modify -vserver *cluster_management_LIF* -lif cluster_mgmt -firewall-policy *policy-name*

Access the cluster by using Telnet

You can issue Telnet requests to the cluster to perform administrative tasks. Telnet is disabled by default.

What you'll need

The following conditions must be met before you can use Telnet to access the cluster:

- You must have a cluster local user account that is configured to use Telnet as an access method.

  The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- Telnet must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that Telnet requests can go through the firewall.

  By default, Telnet is disabled. The `system services firewall policy show` command with the `-service telnet` parameter displays whether Telnet has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

  The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

About this task

- Telnet is not a secure protocol.

  You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent Telnet sessions per node.

  If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

  If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as

PuTTY.

Steps

1. From an administration host, enter the following command:

   telnet *hostname_or_IP*

   hostname_or_IP is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

Example of a Telnet request

The following example shows how the user named “joe”, who has been set up with Telnet access, can issue a Telnet request to access a cluster whose cluster management LIF is 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

Access the cluster by using RSH

You can issue RSH requests to the cluster to perform administrative tasks. RSH is not a secure protocol and is disabled by default.

What you’ll need

The following conditions must be met before you can use RSH to access the cluster:

- You must have a cluster local user account that is configured to use RSH as an access method.

  The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- RSH must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that RSH requests can go through the firewall.

  By default, RSH is disabled. The `system services firewall policy show` command with the `-service rsh` parameter displays whether RSH has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

  The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

About this task

- RSH is not a secure protocol.

You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent RSH sessions per node.

  If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

  If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

Steps

1. From an administration host, enter the following command:

   rsh hostname_or_IP -l username:passwordcommand

   hostname_or_IP is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

   command is the command you want to execute over RSH.

Example of an RSH request

The following example shows how the user named “joe”, who has been set up with RSH access, can issue an RSH request to run the `cluster show` command:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

Use the ONTAP command-line interface

Using the ONTAP command-line interface

The ONTAP command-line interface (CLI) provides a command-based view of the management interface. You enter commands at the storage system prompt, and command results are displayed in text.

The CLI command prompt is represented as `cluster_name::>`.

If you set the privilege level (that is, the `-privilege` parameter of the `set` command) to `advanced`, the prompt includes an asterisk (*), for example:

`cluster_name::*>`

About the different shells for CLI commands (cluster administrators only)

About the different shells for CLI commands overview (cluster administrators only)

The cluster has three different shells for CLI commands, the *clustershell*, the *nodeshell*, and the *systemshell*. The shells are for different purposes, and they each have a different command set.

- The clustershell is the native shell that is started automatically when you log in to the cluster.

  It provides all the commands you need to configure and manage the cluster. The clustershell CLI help (triggered by `?` at the clustershell prompt) displays available clustershell commands. The `man` *`command_name`* command in the clustershell displays the man page for the specified clustershell command.

- The nodeshell is a special shell for commands that take effect only at the node level.

  The nodeshell is accessible through the `system node run` command.

  The nodeshell CLI help (triggered by `?` or `help` at the nodeshell prompt) displays available nodeshell commands. The `man` *`command_name`* command in the nodeshell displays the man page for the specified nodeshell command.

  Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

- The systemshell is a low-level shell that is used only for diagnostic and troubleshooting purposes.

  The systemshell and the associated “diag” account are intended for low-level diagnostic purposes. Their access requires the diagnostic privilege level and is reserved only for technical support to perform troubleshooting tasks.

Access of nodeshell commands and options in the clustershell

Nodeshell commands and options are accessible through the nodeshell:

`system node run –node` *`nodename`*

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

Nodeshell options that are supported in the clustershell can be accessed by using the `vserver options clustershell` command. To see these options, you can do one of the following:

- Query the clustershell CLI with `vserver options -vserver` *`nodename_or_clustername`* `-option-name?`
- Access the `vserver options` man page in the clustershell CLI with `man vserver options`

If you enter a nodeshell or legacy command or option in the clustershell, and the command or option has an equivalent clustershell command, ONTAP informs you of the clustershell command to use.

If you enter a nodeshell or legacy command or option that is not supported in the clustershell, ONTAP informs you of the “not supported” status for the command or option.

Display available nodeshell commands

You can obtain a list of available nodeshell commands by using the CLI help from the nodeshell.

Steps

1. To access the nodeshell, enter the following command at the clustershell’s system prompt:

   system node run -node {*nodename*|local}

   `local` is the node you used to access the cluster.

   > The `system node run` command has an alias command, `run`.

2. Enter the following command in the nodeshell to see the list of available nodeshell commands:

   [*commandname*] help

   `commandname` is the name of the command whose availability you want to display. If you do not include *`commandname`*, the CLI displays all available nodeshell commands.

   You enter `exit` or type Ctrl-d to return to the clustershell CLI.

Example of displaying available nodeshell commands

The following example accesses the nodeshell of a node named node2 and displays information for the nodeshell command `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

Methods of navigating CLI command directories

Commands in the CLI are organized into a hierarchy by command directories. You can run commands in the hierarchy either by entering the full command path or by navigating through the directory structure.

When using the CLI, you can access a command directory by typing the directory's name at the prompt and then pressing Enter. The directory name is then included in the prompt text to indicate that you are interacting with the appropriate command directory. To move deeper into the command hierarchy, you type the name of a command subdirectory followed by pressing Enter. The subdirectory name is then included in the prompt text and the context shifts to that subdirectory.

You can navigate through several command directories by entering the entire command. For example, you can display information about disk drives by entering the `storage disk show` command at the prompt. You can also run the command by navigating through one command directory at a time, as shown in the following example:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

You can abbreviate commands by entering only the minimum number of letters in a command that makes the command unique to the current directory. For example, to abbreviate the command in the previous example, you can enter `st d sh`. You can also use the Tab key to expand abbreviated commands and to display a command's parameters, including default parameter values.

You can use the `top` command to go to the top level of the command hierarchy, and the `up` command or `..` command to go up one level in the command hierarchy.

Commands and command options preceded by an asterisk (*) in the CLI can be executed only at the advanced privilege level or higher.

Rules for specifying values in the CLI

Most commands include one or more required or optional parameters. Many parameters require you to specify a value for them. A few rules exist for specifying values in the CLI.

- A value can be a number, a Boolean specifier, a selection from an enumerated list of predefined values, or a text string.

  Some parameters can accept a comma-separated list of two or more values. Comma-separated lists of values do not need to be in quotation marks (" "). Whenever you specify text, a space, or a query character (when not meant as a query or text starting with a less-than or greater-than symbol), you must enclose the entity in quotation marks.

- The CLI interprets a question mark ("?") as the command to display help information for a particular command.
- Some text that you enter in the CLI, such as command names, parameters, and certain values, is not case-sensitive.

  For example, when you enter parameter values for the `vserver cifs` commands, capitalization is ignored. However, most parameter values, such as the names of nodes, storage virtual machines (SVMs), aggregates, volumes, and logical interfaces, are case-sensitive.

- If you want to clear the value of a parameter that takes a string or a list, you specify an empty set of quotation marks ("") or a dash ("-").

- The hash sign (“#”), also known as the pound sign, indicates a comment for a command-line input; if used, it should appear after the last parameter in a command line.

  The CLI ignores the text between “#” and the end of the line.

In the following example, an SVM is created with a text comment. The SVM is then modified to delete the comment:

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

In the following example, a command-line comment that uses the “#” sign indicates what the command does.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

Methods of viewing command history and reissuing commands

Each CLI session keeps a history of all commands issued in it. You can view the command history of the session that you are currently in. You can also reissue commands.

To view the command history, you can use the `history` command.

To reissue a command, you can use the `redo` command with one of the following arguments:

- A string that matches part of a previous command

  For example, if the only `volume` command you have run is `volume show`, you can use the `redo volume` command to reexecute the command.

- The numeric ID of a previous command, as listed by the `history` command

  For example, you can use the `redo 4` command to reissue the fourth command in the history list.

- A negative offset from the end of the history list

  For example, you can use the `redo -2` command to reissue the command that you ran two commands ago.

For example, to redo the command that is third from the end of the command history, you would enter the following command:

```
cluster1::> redo -3
```

Keyboard shortcuts for editing CLI commands

The command at the current command prompt is the active command. Using keyboard shortcuts enables you to edit the active command quickly. These keyboard shortcuts are similar to those of the UNIX tcsh shell and the Emacs editor.

The following table lists the keyboard shortcuts for editing CLI commands. “Ctrl-” indicates that you press and hold the Ctrl key while typing the character specified after it. “Esc-” indicates that you press and release the Esc key and then type the character specified after it.

If you want to…	Use the following keyboard shortcut…
Move the cursor back by one character	Ctrl-B
	Back arrow
Move the cursor forward by one character	Ctrl-F
	Forward arrow
Move the cursor back by one word	Esc-B
Move the cursor forward by one word	Esc-F
Move the cursor to the beginning of the line	Ctrl-A
Move the cursor to the end of the line	Ctrl-E
Remove the content of the command line from the beginning of the line to the cursor, and save it in the cut buffer. The cut buffer acts like temporary memory, similar to what is called a *clipboard* in some programs.	Ctrl-U
Remove the content of the command line from the cursor to the end of the line, and save it in the cut buffer	Ctrl-K
Remove the content of the command line from the cursor to the end of the following word, and save it in the cut buffer	Esc-D
Remove the word before the cursor, and save it in the cut buffer	Ctrl-W

If you want to…	Use the following keyboard shortcut…
Yank the content of the cut buffer, and push it into the command line at the cursor	Ctrl-Y
Delete the character before the cursor	Ctrl-H
	Backspace
Delete the character where the cursor is	Ctrl-D
Clear the line	Ctrl-C
Clear the screen	Ctrl-L
Replace the current content of the command line with the previous entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the previous entry.	Ctrl-P
	Esc-P
	Up arrow
Replace the current content of the command line with the next entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the next entry.	Ctrl-N
	Esc-N
	Down arrow
Expand a partially entered command or list valid input from the current editing position	Tab
	Ctrl-I
Display context-sensitive help	?
Escape the special mapping for the question mark (“?”) character. For instance, to enter a question mark into a command’s argument, press Esc and then the “?” character.	Esc-?
Start TTY output	Ctrl-Q
Stop TTY output	Ctrl-S

Use of administrative privilege levels

ONTAP commands and parameters are defined at three privilege levels: *admin*, *advanced*, and *diagnostic*. The privilege levels reflect the skill levels required in

performing the tasks.

- **admin**

  Most commands and parameters are available at this level. They are used for common or routine tasks.

- **advanced**

  Commands and parameters at this level are used infrequently, require advanced knowledge, and can cause problems if used inappropriately.

  You use advanced commands or parameters only with the advice of support personnel.

- **diagnostic**

  Diagnostic commands and parameters are potentially disruptive. They are used only by support personnel to diagnose and fix problems.

Set the privilege level in the CLI

You can set the privilege level in the CLI by using the `set` command. Changes to privilege level settings apply only to the session you are in. They are not persistent across sessions.

Steps

1. To set the privilege level in the CLI, use the `set` command with the `-privilege` parameter.

Example of setting the privilege level

The following example sets the privilege level to advanced and then to admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

Set display preferences in the CLI

You can set display preferences for a CLI session by using the `set` command and `rows` command. The preferences you set apply only to the session you are in. They are not persistent across sessions.

About this task

You can set the following CLI display preferences:

- The privilege level of the command session
- Whether confirmations are issued for potentially disruptive commands
- Whether `show` commands display all fields

- The character or characters to use as the field separator
- The default unit when reporting data sizes
- The number of rows the screen displays in the current CLI session before the interface pauses output

  If the preferred number of rows is not specified, it is automatically adjusted based on the actual height of the terminal. If the actual height is undefined, the default number of rows is 24.

- The default storage virtual machine (SVM) or node
- Whether a continuing command should stop if it encounters an error

Steps

1. To set CLI display preferences, use the `set` command.

   To set the number of rows the screen displays in the current CLI session, you can also use the `rows` command.

   For more information, see the man pages for the `set` command and `rows` command.

Example of setting display preferences in the CLI

The following example sets a comma to be the field separator, sets `GB` as the default data-size unit, and sets the number of rows to 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

Methods of using query operators

The management interface supports queries and UNIX-style patterns and wildcards to enable you to match multiple values in command-parameter arguments.

The following table describes the supported query operators:

Operator	Description
*	Wildcard that matches all entries. For example, the command `volume show -volume *tmp*` displays a list of all volumes whose names include the string `tmp`.
!	NOT operator. Indicates a value that is not to be matched; for example, **`!vs0`** indicates not to match the value `vs0`.

Operator	Description
|	OR operator. Separates two values that are to be compared; for example, **`vs0 | vs2`** matches either vs0 or vs2. You can specify multiple OR statements; for example, `a | b* | *c*` matches the entry `a`, any entry that starts with `b`, and any entry that includes `c`.
..	Range operator. For example, **`5..10`** matches any value from `5` to `10`, inclusive.
<	Less-than operator. For example, **`<20`** matches any value that is less than `20`.
>	Greater-than operator. For example, **`>5`** matches any value that is greater than `5`.
<=	Less-than-or-equal-to operator. For example, **`⇐5`** matches any value that is less than or equal to `5`.
>=	Greater-than-or-equal-to operator. For example, **`>=5`** matches any value that is greater than or equal to `5`.
`{query}`	Extended query. An extended query must be specified as the first argument after the command name, before any other parameters. For example, the command `volume modify {-volume *tmp*} -state offline` sets offline all volumes whose names include the string `tmp`.

If you want to parse query characters as literals, you must enclose the characters in double quotes (for example, “^”, “.”, “*”, or “$”) for the correct results to be returned.

You can use multiple query operators in one command line. For example, the command `volume show -size >1GB -percent-used <50 -vserver !vs1` displays all volumes that are greater than 1 GB in size, less than 50% utilized, and not in the storage virtual machine (SVM) named “vs1”.

Methods of using extended queries

You can use extended queries to match and perform operations on objects that have specified values.

You specify extended queries by enclosing them within curly brackets ({}). An extended query must be specified as the first argument after the command name, before any other parameters. For example, to set

offline all volumes whose names include the string `tmp`, you run the command in the following example:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Extended queries are generally useful only with `modify` and `delete` commands. They have no meaning in `create` or `show` commands.

The combination of queries and modify operations is a useful tool. However, it can potentially cause confusion and errors if implemented incorrectly. For example, using the (advanced privilege) `system node image modify` command to set a node's default software image automatically sets the other software image not to be the default. The command in the following example is effectively a null operation:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

This command sets the current default image as the non-default image, then sets the new default image (the previous non-default image) to the non-default image, resulting in the original default settings being retained. To perform the operation correctly, you can use the command as given in the following example:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

Methods of customizing show command output by using fields

When you use the `-instance` parameter with a `show` command to display details, the output can be lengthy and include more information than you need. The `-fields` parameter of a `show` command enables you to display only the information you specify.

For example, running `volume show -instance` is likely to result in several screens of information. You can use `volume show -fields` *`fieldname[,fieldname…]`* to customize the output so that it includes only the specified field or fields (in addition to the default fields that are always displayed.) You can use `-fields ?` to display valid fields for a `show` command.

The following example shows the output difference between the `-instance` parameter and the `-fields` parameter:

```
cluster1::> volume show -instance

                                    Vserver Name: cluster1-1
                                     Volume Name: vol0
                                  Aggregate Name: aggr0
                                     Volume Size: 348.3GB
                              Volume Data Set ID: -
                       Volume Master Data Set ID: -
                                    Volume State: online
                                     Volume Type: RW
                                    Volume Style: flex
                                             ...
                           Space Guarantee Style: volume
                       Space Guarantee in Effect: true
                                             ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- ----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

About positional parameters

You can take advantage of the positional parameter functionality of the ONTAP CLI to increase efficiency in command input. You can query a command to identify parameters that are positional for the command.

What a positional parameter is

- A positional parameter is a parameter that does not require you to specify the parameter name before specifying the parameter value.
- A positional parameter can be interspersed with nonpositional parameters in the command input, as long

as it observes its relative sequence with other positional parameters in the same command, as indicated in the ***command_name ?*** output.

- A positional parameter can be a required or optional parameter for a command.
- A parameter can be positional for one command but nonpositional for another.

> Using the positional parameter functionality in scripts is not recommended, especially when the positional parameters are optional for the command or have optional parameters listed before them.

Identify a positional parameter

You can identify a positional parameter in the ***command_name ?*** command output. A positional parameter has square brackets surrounding its parameter name, in one of the following formats:

- [*-parameter_name*] *parameter_value* shows a required parameter that is positional.
- [[*-parameter_name*] *parameter_value*] shows an optional parameter that is positional.

For example, when displayed as the following in the ***command_name ?*** output, the parameter is positional for the command it appears in:

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

However, when displayed as the following, the parameter is nonpositional for the command it appears in:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

Examples of using positional parameters

In the following example, the ***volume create ?*** output shows that three parameters are positional for the command: `-volume`, `-aggregate`, and `-size`.

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
   [-aggregate] <aggregate name>          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
  [ -policy <text> ]                      Export Policy
  [ -user <user name> ]                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
  ...
```

In the following example, the `volume create` command is specified without taking advantage of the positional parameter functionality:

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

The following examples use the positional parameter functionality to increase the efficiency of the command input. The positional parameters are interspersed with nonpositional parameters in the `volume create` command, and the positional parameter values are specified without the parameter names. The positional parameters are specified in the same sequence indicated by the **`volume create ?`** output. That is, the value for `-volume` is specified before that of `-aggregate`, which is in turn specified before that of `-size`.

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

Methods of accessing ONTAP man pages

ONTAP manual (man) pages explain how to use ONTAP commands. They are available at the command line and on the NetApp Support Site.

The `man` *`command_name`* command displays the manual page of the specified command. If you do not specify a command name, the manual page index is displayed. You can use the `man man` command to view information about the `man` command itself. You can exit a man page by entering **`q`**.

The ONTAP 9 man pages contains command references for the admin-level and advanced-level ONTAP commands.

Manage CLI sessions (cluster administrators only)

Manage records of CLI sessions

Manage records of CLI sessions overview

You can record a CLI session into a file with a specified name and size limit, then upload the file to an FTP or HTTP destination. You can also display or delete files in which you previously recorded CLI sessions.

A record of a CLI session ends when you stop the recording or end the CLI session, or when the file reaches the specified size limit. The default file size limit is 1 MB. The maximum file size limit is 2 GB.

Recording a CLI session is useful, for example, if you are troubleshooting an issue and want to save detailed information or if you want to create a permanent record of space usage at a specific point in time.

Record a CLI session

You can use the `system script start` and `system script stop` commands to record a CLI session.

Steps

1. To start recording the current CLI session into a file, use the `system script start` command.

   For more information about using the `system script start` command, see the man page.

   ONTAP starts recording your CLI session into the specified file.

2. Proceed with your CLI session.
3. To stop recording the session, use the `system script stop` command.

   For more information about using the `system script stop` command, see the man page.

   ONTAP stops recording your CLI session.

Commands for managing records of CLI sessions

You use the `system script` commands to manage records of CLI sessions.

If you want to…	Use this command…
Start recording the current CLI session in to a specified file	`system script start`
Stop recording the current CLI session	`system script stop`
Display information about records of CLI sessions	`system script show`

If you want to…	Use this command…
Upload a record of a CLI session to an FTP or HTTP destination	`system script upload`
Delete a record of a CLI session	`system script delete`

Related information

ONTAP 9 commands

Commands for managing the automatic timeout period of CLI sessions

The timeout value specifies how long a CLI session remains idle before being automatically terminated. The CLI timeout value is cluster-wide. That is, every node in a cluster uses the same CLI timeout value.

By default, the automatic timeout period of CLI sessions is 30 minutes.

You use the `system timeout` commands to manage the automatic timeout period of CLI sessions.

If you want to…	Use this command…
Display the automatic timeout period for CLI sessions	`system timeout show`
Modify the automatic timeout period for CLI sessions	`system timeout modify`

Related information

ONTAP 9 commands

Cluster access with System Manager

Use System Manager to access a cluster

If you prefer to use a graphic interface instead of the command-line interface (CLI) for accessing and managing a cluster, you can do so by using System Manager, which is included with ONTAP as a web service, is enabled by default, and is accessible by using a browser.

What you'll need

- You must have a cluster user account that is configured with the `admin` role and the `http`, `ontapi`, and `console` application types.
- You must have enabled cookies and site data in the browser.

About this task

You can use a cluster management LIF or node management LIF to access System Manager. For uninterrupted access to System Manager, you should use a cluster management LIF.

Steps

1. Point the web browser to the IP address of the cluster management LIF:
   - If you are using IPv4: **`https://cluster-mgmt-LIF`**
   - If you are using IPv6: **`https://[cluster-mgmt-LIF]`**

     Only HTTPS is supported for browser access of System Manager.

   If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a Certificate Authority (CA) signed digital certificate on the cluster for server authentication.
2. **Optional:** If you have configured an access banner by using the CLI, then read the message that is displayed in the **Warning** dialog box, and choose the required option to proceed.

   This option is not supported on systems on which Security Assertion Markup Language (SAML) authentication is enabled.
   - If you do not want to continue, click **Cancel**, and close the browser.
   - If you want to continue, click **OK** to navigate to the System Manager login page.
3. Log in to System Manager by using your cluster administrator credentials.

Related information

Managing access to web services

Accessing a node's log, core dump, and MIB files by using a web browser

About System Manager

System Manager is a graphical management interface that enables you to manage storage systems and storage objects (such as disks, volumes, and aggregates) and perform common management tasks related to storage systems from a web browser. As a cluster administrator, you can use System Manager to administer the entire cluster and its resources.

System Manager is no longer available as an executable file and is now included with ONTAP software as a web service, enabled by default, and accessible by using a browser.

The name of System Manager has changed from previous versions. Versions 9.5 and earlier were named OnCommand System Manager. Versions 9.6 and later are now called System Manager.

System Manager enables you to perform many common tasks such as the following:

- Create a cluster, configure a network, and set up support details for the cluster.
- Configure and manage storage objects such as disks, aggregates, volumes, qtrees, and quotas.
- Configure protocols such as CIFS and NFS, and provision file sharing.
- Configure protocols such as FC, FCoE, NVMe, and iSCSI for block access.

- Create and configure network components such as subnets, broadcast domains, data and management interfaces, and interface groups.
- Set up and manage mirroring and vaulting relationships.
- Perform cluster management, storage node management, and storage virtual machine (SVM) management operations.
- Create and configure SVMs, manage storage objects associated with SVMs, and manage SVM services.
- Monitor and manage HA configurations in a cluster.
- Configure Service Processors to remotely log in, manage, monitor, and administer the node, regardless of the state of the node.

For more information about System Manager, see the NetApp Support Site.

Ways to manage access to System Manager

You can enable or disable a web browser's access to System Manager. You can also view the System Manager log.

You can control a web browser's access to System Manager by using `vserver services web modify -name sysmgr -vserver` *`cluster_name`* `-enabled` [`true`|`false`].

System Manager logging is recorded in the `/mroot/etc/log/mlog/sysmgr.log` files of the node that hosts the cluster management LIF at the time System Manager is accessed. You can view the log files by using a browser. The System Manager log is also included in AutoSupport messages.