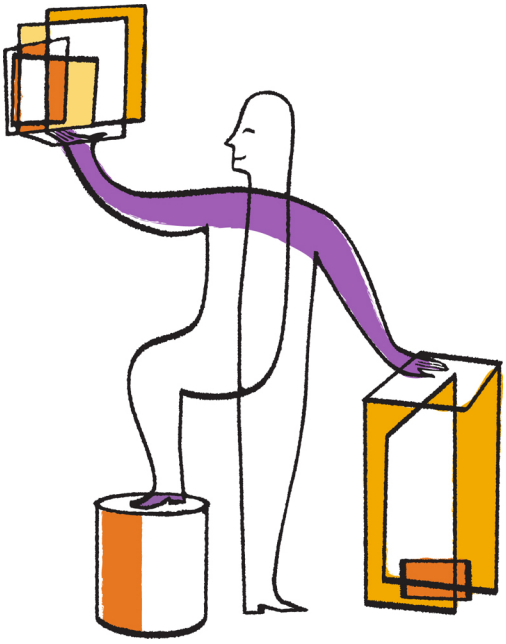
Clustered Data ONTAP® 8.2

System Administration Guide for Cluster Administrators



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
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-07956_A0
May 2013

Contents

Differences between cluster and Vserver administrators

Cluster administrators administer the entire cluster and the virtual storage servers (Vservers) it contains. Vserver administrators administer only their own data Vservers.

Cluster administrators can administer the entire cluster and its resources. They can also set up data Vservers and delegate Vserver administration to Vserver administrators. The specific capabilities that cluster administrators have depend on their access-control roles. By default, a cluster administrator with the “admin” account name or role name has all capabilities for managing the cluster and Vservers.

Vserver administrators can administer only their own data Vservers' storage and network resources, such as volumes, protocols, LIFs, and services. The specific capabilities that Vserver administrators have depend on the access-control roles that are assigned by cluster administrators. For more information about Vserver administrator capabilities, see the *Clustered Data ONTAP System Administration Guide for Vserver Administrators*.

Related concepts

Managing Vservers (cluster administrators only) on page 92
Predefined roles for cluster administrators on page 139
Predefined roles for Vserver administrators on page 140

Data ONTAP management interface basics

You can administer the cluster by using the Data ONTAP command-line interface (CLI) or the web interface. The CLI provides a command-based mechanism that is similar to the UNIX tcsh shell. The web interface enables you to use a web browser to manage the cluster.

Related concepts

What a cluster is on page 30
Understanding the different shells for CLI commands (cluster administrators only) on page 18

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

You can access the cluster by using the serial console, SSH, Telnet, or RSH. These protocols enable you to access the cluster to run CLI commands.

Accessing 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.

Accessing the cluster by using SSH

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

Before you begin

- 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. For more information, see the `security login` man pages.

- 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 Vserver, 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

- The Data ONTAP 8.2 release family supports OpenSSH client version 5.4p1 and OpenSSH server version 5.4p1.

  Only the SSH v2 protocol is supported; SSH v1 is not supported.
- Data 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 in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.
- Data ONTAP supports only the AES and 3DES encryption algorithms (also known as *ciphers*) for SSH.
- If you want to access the Data ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.

Step

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::> system services web show
External Web Services: true
               Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: true
        SSLv2 Enabled: false
cluster1::>
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
cluster1::> system services web show
External Web Services: true
               Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: true
        SSLv2 Enabled: false
$
```

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::> system services web show
External Web Services: true
               Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: true
        SSLv2 Enabled: false
cluster1::>
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 system services web show
Password:
cluster1::> system services web show
External Web Services: true
               Status: online
   HTTP Protocol Port: 80
```

```
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: true
        SSLv2 Enabled: false
$
```

Enabling Telnet or RSH access to the cluster

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

Data ONTAP prevents you from changing predefined firewall policies. However, you can create a new policy by cloning the predefined `mgmt` management firewall policy and then enabling Telnet or RSH under the new policy.

Steps

1. Use the `system services firewall policy clone` command to create a new management firewall policy based on the `mgmt` management firewall policy.

   Example

   ```
   cluster1::> system services firewall policy clone -policy mgmt
   -new-policy-name mgmt1
   ```

2. Use the `system services firewall policy create` command to enable Telnet or RSH in the new management firewall policy.

   Example

   ```
   cluster1::> system services firewall policy create -policy mgmt1
   -service telnet -action allow -ip-list 0.0.0.0/0
   ```

   ```
   cluster1::> system services firewall policy create -policy mgmt1
   -service rsh -action allow -ip-list 0.0.0.0/0
   ```

3. Use the `network interface modify` command to associate the new policy with the cluster management LIF.

Example

```
cluster1::> network interface modify -vserver cluster1
-lif cluster_mgmt -firewall-policy mgmt1
```

Accessing the cluster by using Telnet

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

Before you begin

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.
- Data 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 Data ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.

Step

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/amd64
login: joe
Password:
cluster1::>
```

Related concepts

Managing firewall service and policies on page 151
Access methods for user accounts on page 135

Accessing 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.

Before you begin

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.

- Data 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.

Step

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

   rsh *hostname_or_IP* -l *username*:*password command*

   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 system services web
show
External Web Services: true
              Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: true
        SSLv2 Enabled: false

admin_host$
```

Using the Data ONTAP command-line interface

The Data 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*`::*>`.

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

The cluster has three different shells for CLI commands, the *clustershell*, the *nodeshell*, and the *systemshell*. Depending on the task you perform, you might need to use different shells to execute different commands.

- 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.
- The systemshell is a low-level shell that is used only for diagnostic and troubleshooting purposes. The systemshell is not intended for general administrative purposes. You access the systemshell only with guidance from technical support.

Displaying 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.

   Note: 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]]
```

Uses of the systemshell and the diagnostic account

A diagnostic account, named “diag”, is provided with your storage system. You can use the diag account to perform troubleshooting tasks in the systemshell. The diag account and the systemshell are intended only for low-level diagnostic purposes and should be used only with guidance from technical support.

The diag account is the only account that can be used to access the systemshell, through the advanced command `system node systemshell`. The diag account is locked by default. Before accessing the systemshell for the first time, you must first unlock the diag account (`security login unlock`) and then set the diag account password (`security login password`). Neither the diag account nor the systemshell is intended for general administrative purposes.

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.

Note: 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, Vservers, aggregates, volumes, and logical interfaces, are case-sensitive.
- If you want to clear the value of a parameter that takes a text string, 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, a Vserver is created with a text comment. The Vserver is then modified to delete the comment:

```
cluster1::> vserver create -vserver vs0 -rootvolume root_vs0 -aggregate myaggr
-ns-switch nis -nm-switch file -language en_US -rootvolume-security-style unix
-comment "My Vserver"
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 -username 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 current active command. You can edit the command by using key combinations. These key combinations are similar to those of the UNIX tcsh shell and the Emacs editor.

The following table lists the keyboard shortcuts for editing CLI commands. A caret (^) indicates that you must press the Ctrl key with the specified key.

Edit Command	Action
^b	Move the cursor back one character.
^f	Move the cursor forward one character.
^a	Move the cursor to the beginning of the line.
^e	Move the cursor to the end of the line.
^k	Remove the contents of the edit buffer, from the cursor to the end of the line, and save it in the cut buffer.
^y	Yank the contents of the cut buffer, pushing it into the edit buffer at the cursor.
ESC b	Move the cursor back one word.

Edit Command	Action
ESC f	Move the cursor forward one word.
ESC d	Cut the contents of the edit buffer, beginning at the cursor and continuing to the end of the following word.
^w	Delete the word before the cursor.
^h	Delete the character before the cursor.
Backspace	Delete the character before the cursor.
^d	Delete the character after the cursor.
^p	Replace the current contents of the edit buffer with the previous entry on the history list. For each successive ^p action, the history cursor moves to the previous entry.
^n	Replace the current contents of the edit buffer with the next entry on the history buffer.
Down arrow	Down history.
Up arrow	Up history.
Back arrow	Go backward one character.
Forward arrow	Go forward one character.
^q	TTY start output.
^s	TTY stop output.
^u	Clear the current edit buffer.
^v	Escapes a special mapping for the following character. For instance, to enter a question mark into a command's arguments, press ^v, then press ?.
?	Display context-sensitive help.

Use of administrative privilege levels

Data 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.

Setting 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.

Step

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
```

Related references

Use of administrative privilege levels on page 22

Setting 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 you are connected to the system through a console connection, the default number of rows is 24. If you are connected to the system through an SSH connection, the number of default rows is determined by the terminal configuration.
- The default Vserver or node

- Whether a continuing command should stop if it encounters an error

Step

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`.
|	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.

Operator	Description
<	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, if you are using a query to identify antivirus policies that contain the characters `^.*$`, you must enclose these characters in double quotes (`"^.*$"`) 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 Vserver 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 `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 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::>
```

Methods of accessing Data ONTAP man pages

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

The `man` *`command_name`* command displays the man page of the specified command. If you do not specify a command name, the man 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 *Clustered Data ONTAP Commands: Manual Page Reference* is a compilation of man pages for the admin-level and advanced-level Data ONTAP commands. It is available on the NetApp Support Site.

Related information

NetApp Support Site: support.netapp.com

Managing CLI sessions (cluster administrators only)

You can create a log for a CLI session and upload it to a specified destination to keep as a record. In addition, you can specify the automatic timeout period of a CLI session to have the session automatically disconnected after the number of minutes specified by the timeout value has elapsed.

Managing records of CLI sessions

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.

Recording 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.

   Data 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.

   Data 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`
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`

For more information, see the man pages.

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 can manage the timeout value for CLI sessions by using the `system timeout` commands.

Commands for managing the automatic timeout period of CLI sessions

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`

For more information, see the man pages.

Understanding OnCommand 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.

You can use System Manager to manage storage systems running the following versions of Data ONTAP:

- Data ONTAP 8.1.2
- Data ONTAP 8.2

You can also use System Manager to manage V-Series systems.

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

- 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 and iSCSI for block access.
- Verify and configure network configuration settings in the storage systems.
- Set up and manage SnapMirror relationships and SnapVault relationships.
- Perform cluster management, storage node management, and Vserver management operations in a cluster environment.
- Create and configure Vservers, manage storage objects associated with a Vserver, and manage Vserver services.

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

Related information

NetApp Support Site: support.netapp.com

Cluster management basics (cluster administrators only)

After a cluster is created, the cluster administrator can display the cluster status and attributes, rename the cluster, or assign epsilon to another node in the cluster.

For information about setting up a cluster and joining nodes to a cluster, see the *Clustered Data ONTAP Software Setup Guide*.

Only the cluster administrator can perform cluster-level management tasks. The Vserver administrator cannot access the cluster or perform cluster-level tasks.

What a cluster is

You can group pairs of nodes together to form a scalable cluster. Creating a cluster enables the nodes to pool their resources and distribute work across the cluster, while presenting administrators with a single entity to manage. Clustering also enables continuous service to end users if individual nodes go offline.

A cluster can contain up to 24 nodes (unless the iSCSI or FC protocols are enabled, in which case the cluster can contain up to eight nodes). Each node in the cluster can view and manage the same volumes as any other node in the cluster. The total file-system namespace, which comprises all of the volumes and their resultant paths, spans the cluster.

When new nodes are added to a cluster, there is no need to update clients to point to the new nodes. The existence of the new nodes is transparent to the clients.

If you have a two-node cluster, you must configure cluster high availability (HA). For more information, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

You can create a cluster on a standalone node, called a single node cluster. This configuration does not require a cluster network, and enables you to use the cluster ports to serve data traffic.

The nodes in a cluster communicate over a dedicated, physically isolated and secure Ethernet network. The cluster logical interfaces (LIFs) on each node in the cluster must be on the same subnet. For information about network management for cluster and nodes, see the *Clustered Data ONTAP Network Management Guide*.

For information about setting up a cluster or joining a node to the cluster, see the *Clustered Data ONTAP Software Setup Guide*.

Related concepts

Understanding quorum and epsilon on page 32
What the cluster management server is on page 32

Related tasks

Reassigning epsilon to another node in the cluster on page 36

Considerations for single node clusters

A single node cluster is a special implementation of a cluster running on a standalone node. You can deploy a single node cluster if your workload only requires a single node, but does not need nondisruptive operations.

For example, you could deploy a single node cluster to provide data protection for a remote office. In this scenario, the single node cluster would use SnapMirror and SnapVault to replicate the site's data to the primary data center.

In a single node cluster, the HA mode is set to standalone, which enables the node to use all of the nonvolatile memory (NVRAM) on the NVRAM card. In addition, single node clusters do not use a cluster network, and you can use the cluster ports as data ports that can host data LIFs.

Single node clusters are typically configured when the cluster is set up, by using the Cluster Setup wizard. However, you can remove nodes from an existing cluster to create a single node cluster.

The following features and operations are not supported for single node clusters:

- Storage failover and cluster HA
  Single node clusters operate in a standalone HA mode. If the node goes offline, clients will not be able to access data stored in the cluster.
- Any operation that requires more than one node
  For example, you can not move volumes or perform most copy operations.
- Infinite Volumes
  Infinite Volumes must contain aggregates from at least two nodes.
- Storing cluster configuration backups in the cluster
  By default, the configuration backup schedule creates backups of the cluster configuration and stores them on different nodes throughout the cluster. However, if the cluster consists of a single node and you experience a disaster in which the node becomes inaccessible, you will not be able to recover the cluster unless the cluster configuration backup file is stored at a remote URL.

Related tasks

Adding nodes to the cluster on page 40
Removing nodes from the cluster on page 41

Related references

Commands for managing configuration backup schedules on page 186

What the cluster management server is

A cluster management server, also called an *admin Vserver*, is a specialized Vserver implementation that presents the cluster as a single manageable entity. In addition to serving as the highest-level administrative domain, the cluster management server owns resources that do not logically belong with a data Vserver.

The cluster management server is always available on the cluster. You can access the cluster management server through the console, remote LAN manager, or the cluster management LIF.

Upon failure of its home network port, the cluster management LIF automatically fails over to another node in the cluster. Depending on the connectivity characteristics of the management protocol you are using, you might or might not notice the failover. If you are using a connectionless protocol (for example, SNMP) or have a limited connection (for example, HTTP), you are not likely to notice the failover. However, if you are using a long-term connection (for example, SSH), then you will have to reconnect to the cluster management server after the failover.

When you create a cluster, you must specify all of the characteristics of the cluster management LIF, including its IP address, netmask, gateway, and port. For more information about creating a cluster, see the *Clustered Data ONTAP Software Setup Guide*.

Unlike a data Vserver or node Vserver, a cluster management server does not have a root volume or host user volumes (though it can host system volumes). Furthermore, a cluster management server can only have LIFs of the cluster management type.

If you run the `vserver show` command, the cluster management server appears in the output listing for that command.

Related concepts

Types of Vservers on page 94

Understanding quorum and epsilon

Quorum and epsilon are important measures of cluster health and function that together indicate how clusters address potential communications and connectivity challenges.

Quorum is a precondition for a fully-functioning cluster. When a cluster is in quorum, a simple majority of nodes are healthy and can communicate with each other. When quorum is lost, the cluster loses the ability to accomplish normal cluster operations. Only one collection of nodes can have quorum at any one time because all of the nodes collectively share a single view of the data. Therefore, if two non-communicating nodes are permitted to modify the data in divergent ways, it is no longer possible to reconcile the data into a single data view.

Each node in the cluster participates in a voting protocol that elects one node *master*; each remaining node is a *secondary*. The master node is responsible for synchronizing information across the cluster.

When quorum is formed, it is maintained by continual voting; if the master node goes offline, a new master is elected by the nodes that remain online.

Because there is the possibility of a tie in a cluster that has an even number of nodes, one node has an extra fractional voting weight called *epsilon*. When the connectivity between two equal portions of a large cluster fails, the group of nodes containing epsilon maintains quorum, assuming that all of the nodes are healthy. For example, if a single link is established between 12 nodes in one room and 12 nodes in another room to compose a 24-node cluster and the link fails, then the group of nodes that holds epsilon would maintain quorum and continue to serve data while the other 12 nodes would stop serving data. However, if the node holding epsilon was unhealthy or offline, then quorum would not be formed, and all of the nodes would stop serving data.

Epsilon is automatically assigned to the first node when the cluster is created. If the node that holds epsilon becomes unhealthy or is taken over by its high availability partner, epsilon does not move to another node but is rather no longer a factor in determining quorum.

In general, assuming reliable connectivity among the nodes of the cluster, a larger cluster is more stable than a smaller cluster. The quorum requirement of a simple majority of half the nodes plus epsilon is easier to maintain in a cluster of 24 nodes than in a cluster of two nodes.

A two-node cluster presents some unique challenges for maintaining quorum. In a two-node cluster, neither node holds epsilon; instead, both nodes are continuously polled to ensure that if one node fails, the other has full read-write access to data, as well as access to logical interfaces and management functions.

What a cluster replication ring is

A *replication ring* is a set of identical processes running on all nodes in the cluster.

The basis of clustering is the replicated database (RDB). An instance of the RDB is maintained on each node in a cluster. There are a number of processes that use the RDB to ensure consistent data across the cluster. These processes include the management application (`mgmt`), volume location database (`vldb`), virtual-interface manager (`vifmgr`), and SAN management daemon (`bcomd`).

For instance, the `vldb` replication ring for a given cluster consists of all instances of `vldb` running in the cluster.

RDB replication requires healthy cluster links among all nodes in the cluster. If the cluster network fails in whole or in part, file services can become unavailable. The `cluster ring show` displays the status of replication rings and can assist with troubleshooting efforts.

Displaying the nodes in a cluster

You can display information about the nodes in a cluster and their state.

Step

1. To display general information about the nodes in a cluster, use the `cluster show` command.

   The command displays the following information:

   - Node name
   - Whether the node is healthy
   - Whether the node is eligible to participate in the cluster
   - Whether the node holds epsilon (advanced privilege level or higher only)

Examples of displaying the nodes in a cluster

The following example displays information about all nodes in a four-node cluster:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
node2                 true    true
node3                 true    true
```

The following example displays detailed information about the node named node1 at the advanced privilege level:

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

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

Displaying cluster attributes

You can display a cluster's unique identifier (UUID), name, serial number, location, and contact information.

Step

1. To display a cluster's attributes, use the `cluster identity show` command.

Example of displaying cluster attributes

The following example displays the name, serial number, location, and contact information of a cluster.

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

Modifying cluster attributes

After a cluster has been created, you can modify its attributes such as the cluster name, location, and contact information.

About this task

You cannot change a cluster's UUID, which is set when the cluster is created.

Step

1. To modify cluster attributes, use the `cluster identity modify` command.

   The name of a cluster must begin with a letter and can include the following special characters: ".", "-", "_". Any name more than 44 characters in length is truncated.

Example of renaming a cluster

The following example renames the current cluster to cluster2:

```
cluster1::> cluster identity modify -newname cluster2
```

Reassigning epsilon to another node in the cluster

Only one node in the cluster can hold epsilon. Epsilon gives the holding node an extra fractional voting weight in the quorum.

About this task

You must follow the steps specifically; otherwise, you can leave the cluster vulnerable to failure or cause data outages.

Steps

1. If you are currently at the `admin` privilege level, set the privilege level to `advanced` by using the `set` command with the `-privilege` parameter.
2. Remove epsilon from the node that holds it currently by using the `cluster modify` command with the `-epsilon` parameter set to `false` for the node.

   You can use the `cluster show` command with the `-epsilon` parameter to identify the node that holds epsilon currently.
3. Assign epsilon to another node by using the `cluster modify` command with the `-epsilon` parameter set to `true` for the node.

Example of reassigning epsilon to another node

The following example removes epsilon from node1 and assigns it to node4:

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

cluster1::*> cluster show -epsilon *
Node         Health  Eligibility   Epsilon
------------ ------- ------------  ------------
node1        true    true          true
node2        true    true          false
node3        true    true          false
node4        true    true          false
4 entries were displayed.

cluster1::*> cluster modify -node node1 -epsilon false

cluster1::*> cluster modify -node node4 -epsilon true

cluster1::*> cluster show -epsilon *
Node         Health  Eligibility   Epsilon
------------ ------- ------------  ------------
node1        true    true          false
node2        true    true          false
node3        true    true          false
```

```
node4        true    true          true
4 entries were displayed.
```

Displaying the status of cluster replication rings

You can display the status of cluster replication rings to help you diagnose cluster-wide problems. If your cluster is experiencing problems, support personnel might ask you to perform this task to assist with troubleshooting efforts.

Step

1. To display the status of cluster replication rings, use the `cluster ring show` command at the advanced privilege level.

Example of displaying cluster ring-replication status

The following example displays the status of the VLDB replication ring on a node named node0:

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

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

Managing nodes (cluster administrators only)

A *node* is a controller in a cluster. You can display information about a node, set node attributes, rename a node, add or remove a node, or start or stop a node. You can also manage a node remotely by using a remote management device.

A node is connected to other nodes in the cluster over a cluster network. It is also connected to the disk shelves that provide physical storage for the Data ONTAP system or to third-party storage arrays that provide array LUNs for Data ONTAP use. Services and components that are controlled by the node, not by the cluster, can be managed by using the `system node` commands.

A *node Vserver* represents a node in the cluster. If you run the `vserver show` command, the output includes node Vservers in the list.

Displaying node attributes

You can display the attributes of one or more nodes in the cluster, for example, the name, owner, location, model number, serial number, how long the node has been running, health state, and eligibility to participate in a cluster.

Step

1. To display the attributes of a specified node or about all nodes in a cluster, use the `system node show` command.

Example of displaying information about a node

The following example displays detailed information about node1:

```
cluster1::> system node show -node node1
              Node: node1
             Owner: Eng IT
          Location: Lab 5
             Model: model_number
     Serial Number: 12345678
         Asset Tag: -
            Uptime: 23 days 04:42
   NVRAM System ID: 118051205
         System ID: 0118051205
         Vendor: NetApp
            Health: true
       Eligibility: true
```

Modifying node attributes

You can modify the attributes of a node as needed. The attributes you can modify include owner, location, asset tag, and the node's eligibility to participate in the cluster.

Step

1. To set attributes for a node, use the `system node modify` command.

   If you set the local node's eligibility to `false`, the node will no longer be active in the cluster and you will not be able to see any nodes from it. If you set another node's eligibility to `false`, it will no longer be visible from other nodes in the cluster.

Example of modifying node attributes

The following example modifies the attributes of a node named node1. The node's owner is set to Joe Smith and its asset tag to js1234.

```
cluster1::> system node  modify -node node1 -owner "Joe Smith"
-assettag js1234
```

Renaming a node

You can change a node's name as needed.

Step

1. To rename a node, use the `system node rename` command.

   The maximum length of a node's name is 47 characters.

Example

The following command renames node “node1” to “node1a”:

```
cluster1::> system node rename -node node1 -newname node1a
```

Adding nodes to the cluster

After a cluster is created, you can add nodes to it by using the Cluster Setup wizard. You add only one node at a time.

Before you begin

The following conditions must be met before you add nodes to the cluster:

- If you are adding nodes to a multiple-node cluster, more than half of the existing nodes in the cluster must be healthy (indicated by `cluster show`).
- If you are adding nodes to a two-node cluster, cluster HA must be disabled.
  The *Clustered Data ONTAP High-Availability Configuration Guide* contains information about cluster HA.
- If you are adding a second node to a single-node cluster, the second node must be installed, and the cluster network must be configured.
  The *Adding a second controller to create an HA pair in clustered Data ONTAP* flyer contains details.

About this task

Nodes must be in even numbers so that they can form HA pairs.

Steps

1. Power on the node that you want to add to the cluster.

   The node boots, and the Cluster Setup wizard starts on the console.

2. Use the Cluster Setup wizard to add the node to the cluster.

   For detailed information about the Cluster Setup wizard, see the *Clustered Data ONTAP Software Setup Guide*.

3. If IPv6 is enabled in the cluster, use the `network interface create` command to create the node's node management LIF with an IPv6 address.

   #### Example

   The following command creates node management LIF “mgmt1” with an IPv6 address on node2.

   ```
   cluster1::> network interface create -vserver node2 -lif mgmt1 -role
   node-mgmt -home-node node2 -home-port e1a -address 3d20:16fe::101 -
   netmask-length 64
   ```

4. Repeat the preceding steps for each additional node that you want to add.

After you finish

After adding nodes to the cluster, you should enable storage failover for each HA pair. You must also synchronize the time. For detailed information, see the *Clustered Data ONTAP Software Setup Guide*.

Removing nodes from the cluster

You can remove unwanted nodes from the cluster. You can remove only one node at a time. After you remove a node, you must also remove its failover partner.

Before you begin

Removing a node from a cluster requires that more than half of the nodes in the cluster be healthy (indicated by `cluster show`).

Steps

1. To remove a node from the cluster, use the advanced command `cluster unjoin` from another node in the cluster.

   The system informs you of the following:

   - You must also remove the node's failover partner from the cluster.
   - After the node is removed and before it can rejoin a cluster, you must use boot menu option `(4) Clean configuration and initialize all disks` to erase the node's configuration and initialize all disks.

   For information about how to use the `cluster unjoin` command, see the man page.

   A failure message is generated if you have conditions that you must address before removing the node. For example, the message might indicate that the node has shared resources that you must remove or that the node is in a cluster HA configuration or storage failover configuration that you must disable.

2. If a failure message indicates error conditions, address those conditions and rerun the `cluster unjoin` command.

   The node is automatically rebooted after it is successfully removed from the cluster.

3. If the node will rejoin the same cluster or join a new cluster, do the following after the node is rebooted:

   a) During the boot process, press Ctrl-C to display the boot menu when prompted to do so.
   b) Select boot menu option `(4) Clean configuration and initialize all disks` to erase the node's configuration and initialize all disks.

4. Repeat the preceding steps to remove the failover partner from the cluster.

After you finish

If you removed nodes in order to have a single node cluster, you can modify the cluster ports to serve data traffic by modifying the cluster ports to be data ports, and creating data LIFs on the data ports. For more information, see the *Clustered Data ONTAP Network Management Guide*.

Related tasks

Rebooting a node at the system prompt on page 45

Accessing a node's log files or core dump files by using a web browser

You can use a web browser to access a node's log files or core dump files through the cluster's management LIF. The files remain accessible even when the node is down, provided that the node is taken over by its partner.

Before you begin

The following conditions must be met:

- The cluster management LIF must be up.
  The `network interface show` command displays the status of all LIFs in the cluster.
- You must have set up the web protocol engine to support HTTP.
  If you want to use HTTPS for secure web access, you must have also enabled SSL and installed a digital certificate.
  The `system services web show` command displays the configuration of the web protocol engine at the cluster level.
- If a firewall is enabled, you must have added the HTTP or HTTPS protocol service to an existing firewall policy to allow web access requests to go through.
  The `system services firewall policy show` command displays information about firewall policies.
- You must have enabled the Service Processor infrastructure (`spi`) web service.
  The `vserver services web show` command shows whether a web service is enabled.
- Your cluster user account must already be set up with the `http` access method.
  The `security login show` command shows user accounts' access and login methods and their access-control roles.
- Your access-control role must already be granted access to the `spi` web service for the cluster.
  The `vserver services web access show` command shows what roles are granted access to which web services.

Steps

1. Do one of the following:

To access...	Point the web browser to...
A node's log files	(http:// or https://)*cluster-mgmt-ip*/spi/*node-name*/etc/log/
A node's core dump files	(http:// or https://)*cluster-mgmt-ip*/spi/*node-name*/etc/crash/

2. If prompted by the browser, enter your cluster user account name and password to access the files.

Related concepts

Managing the web protocol engine on page 164
Managing firewall service and policies on page 151
Managing web services on page 166
Managing access to web services on page 163
Access methods for user accounts on page 135
Managing SSL on page 168

Rules governing node root volumes and root aggregates

A node's root volume contains special directories and configuration files for that node. The root aggregate contains the root volume. A few rules govern a node's root volume and root aggregate.

A node's root volume is a FlexVol volume that is installed at the factory and reserved for system files, log files, and core files. The directory name is `/mroot`, which is accessible only through the systemshell and with guidance from technical support.

The following rules govern the node's root volume:

- Do not change the preconfigured size for the root volume or modify the content of the root directory, unless technical support instructs you to do so.

  The minimum size for a node's root volume depends on the platform model. For information about the minimum size for the root FlexVol volume, see the *Hardware Universe* (formerly the *System Configuration Guide*) at *support.netapp.com/knowledge/docs/hardware/NetApp/syscfg/index.shtml*.

  Editing configuration files directly in the root directory might result in an adverse impact on the health of the node and possibly the cluster. If you need to modify system configurations, you use Data ONTAP commands to do so.
- Do not store user data in the root volume.

  Storing user data in the root volume increases the storage giveback time between nodes in an HA pair.
- Do not set the root volume's fractional reserve to any value other than 100%.
- Contact technical support if you need to designate a different volume to be the new root volume or move the root volume to another aggregate.

The node's root aggregate contains the node's root volume. Starting with Data ONTAP 8.1, new systems are shipped with the root volume in a dedicated, 64-bit root aggregate that contains three disks. By default, a node is set up to use a hard disk drive (HDD) aggregate for the root aggregate. When no HDDs are available, the node is set up to use a solid-state drive (SSD) aggregate for the root aggregate.

The root aggregate must be dedicated to the root volume only. You must not include or create data volumes in the root aggregate.

Freeing up space on a node's root volume

A warning message appears when a node's root volume has become full or almost full. The node cannot operate properly when its root volume is full. You can free up space on a node's root volume by deleting core dump files, packet trace files, and root volume Snapshot copies.

Steps

1. Display the node's core dump files and their names by using the `system node coredump show` command.
2. Delete unwanted core dump files from the node by using the `system node coredump delete` command.
3. Access the nodeshell by entering the following command:

   `system node run -node` ***`nodename`***

   `nodename` is the name of the node whose root volume space you want to free up.
4. Switch to the nodeshell advanced privilege level by entering the following command in the nodeshell:

   `priv set advanced`
5. Display and delete the node's packet trace files through the nodeshell:
   a) Display all files in the node's root volume by entering the following command:

      `ls /etc/`
   b) If any packet trace files (`*.trc`) are in the node's root volume, delete them individually by entering the following command:

      `rm /etc/`*`file_name`*`.trc`
6. Identify and delete the node's root volume Snapshot copies through the nodeshell:
   a) Identify the root volume name by entering the following command:

      `vol status`

      The root volume is indicated by the word "root" in the "Options" column of the `vol status` command output.

Example

In the following example, the root volume is `vol0`.

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

b) Display root volume Snapshot copies by entering the following command:

snap list *root_vol_name*

c) Delete unwanted root volume Snapshot copies by entering the following command:

snap delete *root_vol_name snapshot_name*

7. Exit the nodeshell and return to the clustershell by entering the following command:

exit

Starting and stopping a node

You can start a node from the system prompt or boot environment prompt. You can also start a node by using the remote management device (which can be the SP or the RLM depending on the platform model). You can stop a node by halting it at the system prompt.

Rebooting a node at the system prompt

You can reboot a node in normal mode from the system prompt. A node is configured to boot from the boot device, such as a PC CompactFlash card.

Step

1. Reboot a node by using the `system node reboot` command.

   If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the reboot. If the LIF migration fails or times out, the rebooting process is aborted, and Data ONTAP displays an error to indicate the LIF migration failure.

   The node begins the reboot process. The Data ONTAP login prompt appears, indicating that the reboot process is complete.

Booting Data ONTAP at the boot environment prompt

You can boot the current release or the backup release of Data ONTAP when you are at the boot environment prompt of a node.

Steps

1. To access the boot environment prompt from the storage system prompt, use the `system node halt` command.

   The storage system console displays the boot environment prompt.

2. At the boot environment prompt, enter one of the following commands:

To boot...	Enter...
The current release of Data ONTAP	**boot_ontap**
The Data ONTAP primary image from the boot device	**boot_primary**
The Data ONTAP backup image from the boot device	**boot_backup**

Rebooting a node remotely

You can reboot a node remotely by using the remote management device.

Steps

1. From the administration host, log in to the remote management device of the node you want to reboot by entering the following command:

   ssh *username@IP_for_remote_management_device*

   One of the following remote management device CLI prompts appears, depending on the platform model:
   ```
   SP>
   RLM>
   ```

2. To power on the node, enter the following command at the CLI prompt for the remote management device:

   system power on

3. To access the system console, enter the following command at the CLI prompt for the remote management device:

   system console

4. If the node does not reboot automatically, enter one of the following commands at the boot environment prompt:

To use the...	Enter...
Current release of Data ONTAP	**boot_ontap**
Data ONTAP primary image from the boot device	**boot_primary**
Data ONTAP backup image from the boot device	**boot_backup**

Shutting down a node

You can shut down a node if it becomes unresponsive or if support personnel direct you to do so as part of troubleshooting efforts.

Step

1. To shut down a node, use the `system node halt` command.

   If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the shutdown. If the LIF migration fails or times out, the shutdown process is aborted, and Data ONTAP displays an error to indicate the LIF migration failure.

   You can manually trigger a core dump with the shutdown by using both the `-dump` and `-skip-lif-migration` parameters.

Example of shutting down a node

The following example shuts down the node named “node1” for hardware maintenance:

```
cluster1::> system node halt -node node1 -reason 'hardware
maintenance'
```

Managing a node by using the boot menu

You can use the boot menu to correct configuration problems of a node, reset the admin password, initialize disks, reset node configuration, and restore node configuration information back to the boot device.

Steps

1. Reboot the node to access the boot menu by using the `system node reboot` command at the system prompt.

   The node begins the reboot process.

2. During the reboot process, press Ctrl-C to display the boot menu when prompted to do so.

The node displays the following options for the boot menu:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
Selection (1-8)?
```

Note: Boot menu option **(2) Boot without /etc/rc** has no effect on systems operating in clustered Data ONTAP.

3. Select one of the following options by entering the corresponding number:

To...	Select...
Continue to boot the node in normal mode	**1) Normal Boot**
Change the password of the node, which is also the “admin” account password	**3) Change Password**
Initialize the node's disks and create a root volume for the node	**4) Clean configuration and initialize all disks** **Attention:** This menu option erases all data on the disks of the node and resets your node configuration to the factory default settings. You select this menu option after the node has unjoined the cluster and before it rejoins another cluster. This menu option reboots the node before initializing the disks. For a V-Series system that has a disk shelf, this menu option initializes only the disks on the disk shelf, not the array LUNs. For a V-Series system that does not have a disk shelf, this menu option initializes the root volume on the storage array.
Perform aggregate and disk maintenance operations and obtain detailed aggregate and disk information.	**5) Maintenance mode boot** You exit Maintenance mode by using the `halt` command.
Restore the configuration information from the node's root volume to the boot device, such as a PC CompactFlash card	**6) Update flash from backup config** Data ONTAP stores some node configuration information on the boot device. When the node reboots, the information on the boot device is automatically backed up onto the node's root volume. If the boot device becomes corrupted or needs to be replaced, you use this menu option to restore the configuration information from the node's root volume back to the boot device.

To...	Select...
Install new software on a V-Series system	**7) Install new software first** If the Data ONTAP software on the boot device does not include support for the storage array that you want to use for the root volume, you can use this menu option to obtain a version of the software that supports your storage array and install it on the node. This menu option is only for installing a newer version of Data ONTAP software on a V-Series system that has no root volume installed. Do *not* use this menu option to upgrade the Data ONTAP software on either a FAS system or a V-Series system.
Reboot the node	**8) Reboot node**

Recovering from a corrupted image of a node's boot device

You can recover from a corrupted image of the boot device (such as the CompactFlash card) for a node by using the remote management device.

Steps

1. Log in to the remote management device by entering the following command at the administration host:

   ssh *username@IP_for_remote_management_device*

   The CLI prompt for the remote management device appears. It can be one of the following, depending on the platform model:

   ```
   SP>
   ```

   ```
   RLM>
   ```

2. At the CLI prompt for the remote management device, perform one of the following steps:

   - To reboot the node by using the primary BIOS firmware image, enter the following command:

     system reset primary
   - To reboot the node by using the backup BIOS firmware image, enter the following command:

     system reset backup

   The console informs you that the command will cause a “dirty system shutdown” and asks you whether to continue.

3. Enter **y** to continue.

   The node shuts down immediately.

Managing a node remotely

You can manage a node remotely by using a remote management device, which can be the SP or the RLM, depending on the platform model. The device stays operational regardless of the operating state of the node. You can also download the RSA as an upgrade to the remote management device.

The RLM is included in the 31xx, 6040, and 6080 platforms.

The SP is included in all other platform models.

Additionally, you can download the Remote Support Agent (RSA), a firmware upgrade to the SP and the RLM, from the NetApp Support Site. The RSA enables technical personnel to use the SP or the RLM for remote support. When problem diagnostics are needed, the RSA automatically uploads core files and transfers diagnostics data such as log files to technical support, reducing your involvement in the troubleshooting process. The RSA is not bundled with Data ONTAP. For more information about the RSA, see the *Remote Support Agent Configuration Guide for Clustered Data ONTAP* and the NetApp Remote Support Diagnostics Tool page on the NetApp Support Site.

Related information

NetApp Remote Support Diagnostics Tool page: support.netapp.com/NOW/download/tools/rsa

Managing a node remotely by using the Service Processor

The Service Processor (SP) is a remote management device that enables you to access, monitor, and troubleshoot a node remotely.

The SP provides the following capabilities:

- The SP enables you to access a node remotely to diagnose, shut down, power-cycle, or reboot the node, regardless of the state of the node controller.
  The SP is powered by a standby voltage, which is available as long as the node has input power to at least one of its power supplies.
  You can log in to the SP by using a Secure Shell client application from an administration host. You can then use the SP CLI to monitor and troubleshoot the node remotely. In addition, you can use the SP to access the serial console and run Data ONTAP commands remotely.
  You can access the SP from the serial console or access the serial console from the SP. The SP allows you to open both an SP CLI session and a separate console session simultaneously.
  For instance, when a temperature sensor becomes critically high or low, Data ONTAP triggers the SP to shut down the motherboard gracefully. The serial console becomes unresponsive, but you can still press Ctrl-G on the console to access the SP CLI. You can then use the `system power on` or `system power cycle` command from the SP to power on or power-cycle the node.
- The SP monitors environmental sensors and logs events to help you take timely and effective service actions.
  The SP monitors the node temperatures, voltages, currents, and fan speeds. When an environmental sensor has reached an abnormal condition, the SP logs the abnormal readings, notifies Data ONTAP of the issue, and sends alerts and “down system” notifications as necessary

through an AutoSupport message, regardless of whether the node can send AutoSupport messages.

Other than generating these messages on behalf of a node that is down and attaching additional diagnostic information to AutoSupport messages, the SP has no effect on the AutoSupport functionality. The AutoSupport configuration settings and message content behavior are inherited from Data ONTAP.

Note: The SP does not rely on the `system node autosupport modify` command's `-transport` parameter setting to send notifications. The SP uses the Simple Mail Transport Protocol (SMTP).

If SNMP is enabled for the SP, the SP generates SNMP traps to configured trap hosts for all "down system" events.

The SP also logs events such as boot progress, Field Replaceable Unit (FRU) changes, Data ONTAP-generated events, and SP command history.

- The SP has a nonvolatile memory buffer that stores up to 4,000 events in a system event log (SEL) to help you diagnose issues.

  The SEL stores each audit log entry as an audit event. It is stored in onboard flash memory on the SP. The event list from the SEL is automatically sent by the SP to specified recipients through an AutoSupport message.

  The SEL contains the following data:

  - Hardware events detected by the SP—for example, sensor status about power supplies, voltage, or other components
  - Errors detected by the SP—for example, a communication error, a fan failure, or a memory or CPU error
  - Critical software events sent to the SP by the node—for example, a panic, a communication failure, a boot failure, or a user-triggered "down system" as a result of issuing the SP `system reset` or `system power cycle` command
- The SP monitors the serial console regardless of whether administrators are logged in or connected to the console.

  When messages are sent to the console, the SP stores them in the console log. The console log persists as long as the SP has power from either of the node power supplies. Because the SP operates with standby power, it remains available even when the node is power-cycled or turned off.
- Hardware-assisted takeover is available if the SP is configured.

  For more information about hardware-assisted takeover, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

Configuring the SP network

Before you can access the SP of a node, the SP network must be configured and enabled. You can configure the SP to use IPv4, IPv6, or both. The SP IPv4 configuration supports static and DHCP addressing, and the SP IPv6 configuration supports static addressing only.

Before you begin

To configure IPv6 connections for the SP, IPv6 must already be configured and enabled for Data ONTAP. The `network options ipv6` commands manage IPv6 settings for Data ONTAP. For more information about IPv6 configuration, see the *Clustered Data ONTAP Network Management Guide*.

Steps

1. Configure and enable the SP by using the `system node service-processor network modify` command.
   - The `-address-type` parameter specifies whether the IPv4 or IPv6 configuration of the SP is to be modified.
   - The `-enable` parameter enables the network interface of the specified IP address type.
   - The `-dhcp` parameter specifies whether to use the network configuration from the DHCP server or the network address that you provide.
     You can enable DHCP (by setting `-dhcp` to `v4`) only if you are using IPv4. You cannot enable DHCP for IPv6 configurations.
   - The `-ip-address` parameter specifies the public IP address for the SP.
   - The `-netmask` parameter specifies the netmask for the SP (if using IPv4.)
   - The `-prefix-length` parameter specifies the network prefix-length of the subnet mask for the SP (if using IPv6.)
   - The `-gateway` specifies the gateway IP address for the SP.

   For more information about the `system node service-processor network modify` command, see the man page.
2. Display the SP network configuration to verify the settings by using the `system node service-processor network show` command.

Example of configuring the SP network

The following example configures the SP of a node to use IPv4, enables the SP, and displays the SP network configuration to verify the settings.

```
cluster1::> system node service-processor network modify -node local
-address-type IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system node service-processor network show -instance -node local
```

```
                          Node: node1
                  Address Type: IPv4
             Interface Enabled: true
                Type of Device: SP
                        Status: online
                   Link Status: up
                   DHCP Status: none
                    IP Address: 192.168.123.98
                   MAC Address: ab:cd:ef:fe:ed:02
                       Netmask: 255.255.255.0
 Prefix Length of Subnet Mask: -
   Router Assigned IP Address: -
        Link Local IP Address: -
           Gateway IP Address: 192.168.123.1


                          Node: node1
                  Address Type: IPv6
             Interface Enabled: false
                Type of Device: SP
                        Status: online
                   Link Status: disabled
                   DHCP Status: none
                    IP Address: -
                   MAC Address: ab:cd:ef:fe:ed:02
                       Netmask: -
 Prefix Length of Subnet Mask: -
   Router Assigned IP Address: -
        Link Local IP Address: -
           Gateway IP Address: -
2 entries were displayed.

cluster1::>
```

Accounts that can access the SP

Cluster user accounts that are created with the `service-processor` application type have access to the SP CLI on any node of the cluster that supports the SP. SP user accounts are managed from Data ONTAP and authenticated by password.

User accounts for accessing the SP are managed from Data ONTAP instead of the SP CLI. A cluster user account of any role can access the SP if it is created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`. The SP supports only password authentication.

By default, the cluster user account named “admin” includes the `service-processor` application type and has access to the SP. Vserver user accounts cannot access the SP.

Note: Data ONTAP prevents you from creating user accounts with names that are reserved for the system (such as “root” and “naroot”). You cannot use a system-reserved name to access the cluster or the SP.

You can display current SP user accounts by using the `-application service-processor` parameter of the `security login show` command.

Accessing the SP from an administration host

You can log in to the SP of a node from an administration host to perform node management tasks remotely.

Before you begin

The following conditions must be met:

- The administration host you use to access the SP must support SSHv2.
- Your user account must already be set up for accessing the SP.
  To access the SP, your user account must have been created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`.

About this task

If you configured the SP to use an IPv4 or IPv6 address, and if five SSH login attempts from a host fail consecutively within 10 minutes, the SP rejects SSH login requests and suspends the communication with the IP address of the host for 15 minutes. The communication resumes after 15 minutes, and you can try to log in to the SP again.

Data ONTAP prevents you from creating or using system-reserved names (such as “root” and “naroot”) to access the cluster or the SP.

Steps

1. Enter the following command from the administration host to log in to the SP:

   ssh *username@SP_IP_address*

2. When you are prompted, enter the password for *username*.

   The SP prompt appears, indicating that you have access to the SP CLI.

Examples of SP access from an administration host

The following example shows how to log in to the SP with a user account, joe, which has been set up to access the SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

The following examples show how to use the IPv6 global address or IPv6 router-advertised address to log in to the SP on a node that has SSH set up for IPv6 and the SP configured for IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Accessing the SP from the serial console

You can access the SP from the serial console to perform monitoring or troubleshooting tasks.

Steps

1. To access the SP CLI from the serial console, press Ctrl-G at the prompt.
2. Log in to the SP CLI when you are prompted.

   The SP prompt appears, indicating that you have access to the SP CLI.
3. To exit the SP CLI and return to the serial console, press Ctrl-D and then press Enter.

Example of accessing the SP CLI from the serial console

The following example shows the result of pressing Ctrl-G from the serial console to access the SP CLI. The `help system power` command is entered at the SP prompt, followed by pressing Ctrl-D and then Enter to return to the serial console.

```
cluster1::>
```

(Press Ctrl-G to access the SP CLI.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Press Ctrl-D and then Enter to return to the serial console.)

```
cluster1::>
```

Accessing the serial console from the SP

The SP's `system console` command enables you to log in to the serial console from the SP.

Steps

1. Enter the following command at the SP prompt:

   `system console`

   The message `Type Ctrl-D to exit` appears.

2. Log in to the console when you are prompted.

   The storage system prompt appears.

3. To exit from the serial console and return to the SP CLI, press Ctrl-D.

Example of accessing the serial console from the SP

The following example shows the result of entering the `system console` command at the SP prompt. The `system node image show` command is entered at the console, followed by pressing Ctrl-D, which returns you to the SP prompt.

```
SP> system console
Type Ctrl-D to exit.
```

(Log in to the console when you are prompted.)

```
login:
Password:
****************************************************
* This is a SP/RLM console session. Output from the *
* serial console is also mirrored on this session.  *
****************************************************
cluster1::>
cluster1::> system node image show
```

(Command output is displayed.)

(Press Ctrl-D to exit the serial console and return to the SP CLI.)

```
SP>
```

Relations among the SP CLI, SP console, and serial console sessions

You can open an SP CLI session to manage a node remotely and a separate SP console session to run Data ONTAP commands remotely. The SP console session mirrors output displayed in a concurrent

serial console session. The SP and the serial console have independent shell environments with independent login authentication.

Understanding how the SP CLI, SP console, and serial console sessions are related helps you manage a node remotely. The following describes the relations among the sessions:

- Only one administrator can log in to the SP CLI session at a time; however, the SP enables you to open both an SP CLI session and a separate SP console session simultaneously.
  The SP CLI is indicated with the SP prompt (`SP>`). From an SP CLI session, you can use the SP `system console` command to initiate an SP console session. At the same time, you can start a separate SP CLI session through SSH. If you press Ctrl-D to exit from the SP console session, you automatically return to the SP CLI session. If an SP CLI session already exists, a message asks you whether to terminate the existing SP CLI session. If you enter “y”, the existing SP CLI session is terminated, enabling you to return from the SP console to the SP CLI. This action is recorded in the SP event log.
- For security reasons, the SP CLI session and the serial console session have independent login authentication.
  When you initiate an SP console session from the SP CLI (by using the SP `system console` command), you are prompted for the serial console credential. When you access the SP CLI from a serial console session (by pressing Ctrl-G), you are prompted for the SP CLI credential.
- The SP console session and the serial console session have independent shell environments.
  The SP console session mirrors output that is displayed in a concurrent serial console session. However, the concurrent serial console session does not mirror the SP console session.
  The SP console session does not mirror output of concurrent SSH sessions.

Using online help at the SP CLI

The SP online help displays the SP CLI commands and options when you enter the question mark (?) or `help` at the SP prompt.

Steps

1. To display help information for the SP commands, enter one of the following at the SP prompt:
   - `help`
   - `?`

Example

The following example shows the SP CLI online help:

```
SP node1> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
rsa - commands for Remote Support Agent
```

```
system - commands to control the system
version - print SP version
```

For more information about the RSA command, see the *Remote Support Agent Configuration Guide for Clustered Data ONTAP*.

2. To display help information for the option of an SP command, enter the following command at the SP prompt:

   help *SP_command*

   Example

   The following example shows the SP CLI online help for the SP `events` command:

```
SP node1> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

Commands for managing a node at the SP admin privilege level

The SP commands at the admin privilege level enable you to display events, logs, and status information for node power, batteries, sensors, field-replaceable units (FRUs), or the SP itself. The commands also enable you to reboot the node or the SP and create a core dump.

The following SP commands are available at the admin privilege level:

Note: Some commands are platform-specific and might not be available on your platform.

If you want to...	Use this command...
Display system date and time	`date`
Display events that are logged by the SP	`events` {`all` | `info` | `newest` *`number`* | `oldest` *`number`* | `search` *`keyword`*}
Exit the SP CLI	`exit`
Display a list of available commands or subcommands of a specified command	`help` [*`command`*]
Set the privilege level to access the specified mode for the SP CLI	`priv set` {`admin` | `advanced` | `diag`} **Attention:** You should use advanced or diag commands only under the guidance of technical support.

If you want to...	Use this command...
Display the current privilege level for the SP CLI	`priv show`
Manage the Remote Support Agent (RSA) if it is installed on the node	`rsa` **Note:** For information about the RSA, see the *Remote Support Agent Configuration Guide for Clustered Data ONTAP*.
Display the SP log archives or the files in an archive	`sp log history show [-archive {latest | all | archive-name}] [-dump {all | file-name}]`
Reboot the SP	`sp reboot`
Display SP status and network configuration information	`sp status [-v | -d]` **Note:** The `-v` option displays SP statistics in verbose form. The `-d` option adds the SP debug log to the display.
Update the SP firmware by using the image at the specified location	`sp update image_URL` **Note:** *image_URL* must not exceed 200 characters.
Display the current time, the length of time the system has been up, and the average number of jobs in the run queue over the last 1, 5, and 15 minutes	`sp uptime`
Display ACP information or the status for expander sensors	`system acp [show | sensors show]`
Display battery information	`system battery show`
Log in to the system console	`system console` **Note:** You use Ctrl-D to exit from the system console and return to the SP CLI.
Create a core dump and reset the node	`system core` **Note:** This command has the same effect as pressing the Non-maskable Interrupt (NMI) button on a node. The SP stays operational as long as the input power to the node is not interrupted.

If you want to...	Use this command...
Display the settings for collecting system forensics on a watchdog reset event, display system forensics information collected during a watchdog reset event, or clear the collected system forensics information.	`system forensics` [`show` | `log dump` | `log clear`]
List all system FRUs and their IDs	`system fru list`
Display product information for the specified FRU	`system fru show` *`fru_id`* **Note:** You can display FRU IDs by using the `system fru list` command.
Display console logs	`system log`
Turn the node on or off, or perform a power-cycle (turning the power off and then back on)	`system power` {`on` | `off` | `cycle`} **Note:** The standby power stays on to keep the SP running without interruption. During the power-cycle, a brief pause occurs before power is turned back on. **Attention:** Using the `system power` command to turn off or power-cycle the node might cause an improper shutdown of the node (also called a *dirty shutdown*) and is not a substitute for a graceful shutdown using the Data ONTAP `system node halt` command.
Display the status for the power supply	`system power status`
Reset the node by using the specified BIOS firmware image	`system reset` {`primary` | `backup` | `current`} **Note:** The SP stays operational as long as the input power to the node is not interrupted.
Display the status for the environmental sensors, including their states and current values	`system sensors` **Note:** This command has an equivalent command, `system sensors show`.

If you want to...	Use this command...
Display the status and details for the specified sensor	`system sensors get` *`sensor_name`* **Note:** You can obtain *`sensor_name`* by using the `system sensors` or the `system sensors show` command.
Display the SP hardware and firmware version information	`version`

Commands for managing a node at the SP advanced privilege level

You can use the SP advanced privilege level to display the SP command history, SP debug file, SP messages file, and data history for field-replaceable units (FRUs). You can also manage the battery firmware and automatic update.

The following SP commands are available only at the advanced privilege level:

If you want to...	Use this command...
Display the SP command history	`sp log audit`
Display the SP debug information	`sp log debug`
Display the SP messages file	`sp log messages`
Display the status of battery firmware automatic update, or enable or disable battery firmware automatic update upon next SP boot	`system battery auto_update` [`status` | `enable` | `disable`]
Update the battery firmware from the image at the specified location	`system battery flash` *`image_URL`* **Note:** You use this command if the automatic battery firmware upgrade process has failed for some reason.
Compare the current battery firmware image against a specified firmware image	`system battery verify` [*`image_URL`*] **Note:** If *`image_URL`* is not specified, the default battery firmware image is used for comparison.
Display the FRU data history log	`system fru log show`

How to determine the status of a threshold-based SP sensor

Threshold-based sensors take periodic readings of a verity of system components. The SP compares the reading of a threshold-based sensor against its preset threshold limits that define a component's

acceptable operating conditions. Based on the sensor reading, the SP displays the sensor state to help you monitor the condition of the component.

Examples of threshold-based sensors include sensors for the system temperatures, voltages, currents, and fan speeds. The specific list of threshold-based sensors depends on the platform.

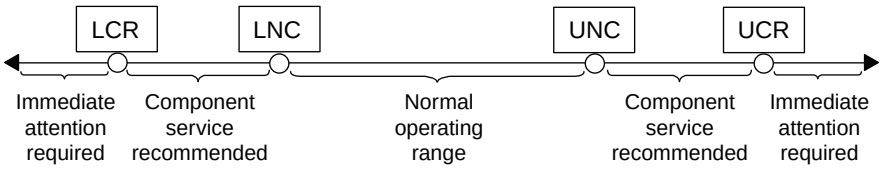
Threshold-based sensors have the following thresholds, displayed in the output of the SP command `system sensors`:

- lower critical (LCR)
- lower noncritical (LNC)
- upper noncritical (UNC)
- upper critical (UCR)

A sensor reading between LNC and LCR or between UNC and UCR means that the component is showing signs of problem and a system failure might occur as a result. Therefore, you should plan for component service soon.

A sensor reading below LCR or above UCR means that the component is malfunctioning and a system failure is about to occur. Therefore, the component requires immediate attention.

The following diagram illustrates the severity ranges that are specified by the thresholds:



You can find the reading of a threshold-based sensor under the Current column in the `system sensors` command output. As the reading of a threshold-based sensor crosses the noncritical and critical threshold ranges, the sensor reports a problem of increasing severity. When the reading exceeds a threshold limit, the sensor's status in the `system sensors` command output changes from `ok` to either `nc` (noncritical) or `cr` (critical), and an event message is logged in the SEL event log.

Some threshold-based sensors do not have all four threshold levels. For those sensors, the missing thresholds show `na` as their limits in the `system sensors` command output. `na` means that the particular sensor has no limit or severity concern for the given threshold, and the SP does not monitor the sensor for that threshold.

Example of the `system sensors` command output

The following example shows the information displayed by the `system sensors` command in the SP CLI:

```
SP node1> system sensors

Sensor Name      | Current    | Unit       | Status| LCR        | LNC        | UNC        | UCR
-----------------+------------+------------+-------+------------+------------+------------+-----------
CPU0_Temp_Margin | -55.000    | degrees C  | ok    | na         | na         | -5.000     | 0.000
CPU1_Temp_Margin | -56.000    | degrees C  | ok    | na         | na         | -5.000     | 0.000
```

```
In_Flow_Temp     | 32.000     | degrees C  | ok    | 0.000     | 10.000    | 42.000    | 52.000
Out_Flow_Temp    | 38.000     | degrees C  | ok    | 0.000     | 10.000    | 59.000    | 68.000
PCI_Slot_Temp    | 40.000     | degrees C  | ok    | 0.000     | 10.000    | 56.000    | 65.000
NVMEM_Bat_Temp   | 32.000     | degrees C  | ok    | 0.000     | 10.000    | 55.000    | 64.000
LM56_Temp        | 38.000     | degrees C  | ok    | na        | na        | 49.000    | 58.000
CPU0_Error       | 0x0        | discrete   | 0x0180| na        | na        | na        | na
CPU0_Therm_Trip  | 0x0        | discrete   | 0x0180| na        | na        | na        | na
CPU0_Hot         | 0x0        | discrete   | 0x0180| na        | na        | na        | na
CPU1_Error       | 0x0        | discrete   | 0x0180| na        | na        | na        | na
CPU1_Therm_Trip  | 0x0        | discrete   | 0x0180| na        | na        | na        | na
CPU1_Hot         | 0x0        | discrete   | 0x0180| na        | na        | na        | na
IO_Mid1_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000    | 55.000    | 64.000
IO_Mid2_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000    | 55.000    | 64.000
CPU_VTT          | 1.106      | Volts      | ok    | 1.028     | 1.048     | 1.154     | 1.174
CPU0_VCC         | 1.154      | Volts      | ok    | 0.834     | 0.844     | 1.348     | 1.368
CPU1_VCC         | 1.086      | Volts      | ok    | 0.834     | 0.844     | 1.348     | 1.368
1.0V             | 0.989      | Volts      | ok    | 0.941     | 0.951     | 1.057     | 1.067
1.05V            | 1.048      | Volts      | ok    | 0.980     | 0.999     | 1.106     | 1.125
1.1V             | 1.096      | Volts      | ok    | 1.028     | 1.038     | 1.154     | 1.174
1.2V             | 1.203      | Volts      | ok    | 1.125     | 1.135     | 1.261     | 1.280
1.5V             | 1.513      | Volts      | ok    | 1.436     | 1.455     | 1.571     | 1.591
1.8V             | 1.754      | Volts      | ok    | 1.664     | 1.703     | 1.896     | 1.935
2.5V             | 2.543      | Volts      | ok    | 2.309     | 2.356     | 2.621     | 2.699
3.3V             | 3.323      | Volts      | ok    | 3.053     | 3.116     | 3.466     | 3.546
5V               | 5.002      | Volts      | ok    | 4.368     | 4.465     | 5.490     | 5.636
STBY_1.8V        | 1.794      | Volts      | ok    | 1.678     | 1.707     | 1.892     | 1.911
…
```

Example of the `system sensors get` *`sensor_name`* command output for a threshold-based sensor

The following example shows the result of entering `system sensors get` *`sensor_name`* in the SP CLI for the threshold-based sensor 5V:

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID               : 5V (0x13)
 Entity ID              : 7.97
 Sensor Type (Analog)   : Voltage
 Sensor Reading         : 5.002 (+/- 0) Volts
 Status                 : ok
 Lower Non-Recoverable  : na
 Lower Critical         : 4.246
 Lower Non-Critical     : 4.490
 Upper Non-Critical     : 5.490
 Upper Critical         : 5.758
 Upper Non-Recoverable  : na
 Assertion Events       :
 Assertions Enabled     : lnc- lcr- ucr+
 Deassertions Enabled   : lnc- lcr- ucr+
```

Understanding the status of a discrete SP sensor

The Status column of the `system sensors` command output in the SL CLI shows the discrete sensors' conditions in hexadecimal values. To interpret the status values of most discrete sensors, you can use the `system sensors get` *`sensor_name`* command in the SL CLI.

Discrete sensors do not have thresholds. Their readings (displayed under the Current column in the `system sensors` command output) do not carry actual meanings and thus are ignored by the SP.

Examples of discrete sensors include sensors for the fan, power supply unit (PSU) fault, and system fault. The specific list of discrete sensors depends on the platform.

While the `system sensors get` *`sensor_name`* command displays the status information for most discrete sensors, it does not provide status information for the System_FW_Status, System_Watchdog, PSU1_Input_Type, and PSU2_Input_Type discrete sensors. However, you can use the following information to interpret these sensors' status values.

System_FW_Status

The System_FW_Status sensor's condition appears in the form of 0x*AABB*. You can combine the information of *AA* and *BB* to determine the condition of the sensor.

AA can have one of the following values:

01 System firmware error

02 System firmware hang

04 System firmware progress

BB can have one of the following values:

00 System software has properly shut down

01 Memory initialization in progress

02 NVMEM initialization in progress (when NVMEM is present)

04 Restoring memory controller hub (MCH) values (when NVMEM is present)

05 User has entered Setup

13 Booting the operating system or LOADER

1F BIOS is starting up

20 LOADER is running

21 LOADER is programming the primary BIOS firmware. You must not power down the system.

22 LOADER is programming the alternate BIOS firmware. You must not power down the system.

2F Data ONTAP is running

60 SP has powered off the system

61 SP has powered on the system

62 SP has reset the system

63 SP watchdog power cycle

64 SP watchdog cold reset

For instance, the System_FW_Status sensor status 0x042F means "system firmware progress (04), Data ONTAP is running (2F)."

System_Watchdog

The System_Watchdog sensor can have one of the following conditions:

0x0080	The state of this sensor has not changed
0x0081	Timer interrupt
0x0180	Timer expired
0x0280	Hard reset
0x0480	Power down
0x0880	Power cycle

For instance, the System_Watchdog sensor status 0x0880 means a watchdog timeout occurs and causes a system power cycle.

PSU1_Input_Type and PSU2_Input_Type

For direct current (DC) power supplies, the PSU1_Input_Type and PSU2_Input_Type sensors do not apply. For alternating current (AC) power supplies, the sensors' status can have one of the following values:

0x01*xx*	220V PSU type
0x02*xx*	110V PSU type

For instance, the PSU1_Input_Type sensor status 0x0280 means that the sensor reports that the PSU type is 110V.

Examples of the `system sensors get` *`sensor_name`* command output for discrete sensors

The following examples show the results of entering `system sensors get` *`sensor_name`* for the discrete sensors CPU0_Error and IO_Slot1_Present:

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID              : CPU0_Error (0x67)
 Entity ID             : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted       : Digital State
                         [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID              : IO_Slot1_Present (0x74)
 Entity ID             : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted       : Availability State
                        [Device Present]
```

Troubleshooting a node by using the SP

When you encounter a problem with a node, you can use the SP to display information about the problem, create a core dump, and reboot the node, even if the node's firmware is corrupted.

The following table describes the common SP commands that you can use at the SP prompt to troubleshoot a node:

If this condition occurs...	And you want to...	Enter this command at the SP CLI prompt...
An environmental sensor has reached an abnormal condition.	Display the status for all environmental sensors, their states, and the current values.	`system sensors show`
	Display the status and details for a specific sensor.	`system sensors get` *`sensor_name`*
The node is not responding properly.	Access the system console from the SP.	`system console`
	Create a core dump and reboot the node.	`system core`
	Power-cycle the node.	`system power cycle`

If this condition occurs...	And you want to...	Enter this command at the SP CLI prompt...
You receive an AutoSupport message indicating an event such as a panic or hardware component failure.	Display what has occurred at the system console.	`system log`
	Display all events.	`events all`
	Display a specific number of recent events.	`events newest` *number*
	Search for specific events regarding *keyword*.	`events search` *keyword*
The node firmware is corrupted.	Boot the node by using the backup image of the firmware.	`system reset backup`
A FRU is malfunctioning.	Display the FRU's product information.	`system fru list` to list all FRU IDs
		`system fru show` *fru_id* to display product information for a specific FRU

Managing the SP with Data ONTAP

You can use Data ONTAP to set up and display the SP configuration, display the SP status, reboot the SP, manage the SP firmware image, and manage access to the SP.

Methods of managing SP firmware updates

Starting with Data ONTAP 8.2, a baseline SP firmware image is packaged with the Data ONTAP image. By default, the SP automatic update functionality is enabled. You have the option to manually trigger an SP update.

Data ONTAP 8.2 and later releases include an SP firmware image that is called the *baseline image*. You do not need to download the baseline SP firmware image separately. If a new version of the SP firmware becomes subsequently available, you have the option to download it from the *System Firmware and Diagnostics Download* page on the NetApp Support Site and update the SP firmware to the downloaded version without upgrading the Data ONTAP version. For information about manually downloading and updating the SP firmware, see the SP Firmware Download and Installation Instructions on the NetApp Support Site.

Data ONTAP offers the following methods for managing SP firmware updates:

- The SP automatic update functionality is enabled by default, allowing the SP firmware to be automatically updated in the following scenarios:
  - When you upgrade to a new version of Data ONTAP

The Data ONTAP upgrade process automatically includes the SP firmware update, provided that the SP firmware version bundled with Data ONTAP is newer than the SP version running on the node.

Note: Data ONTAP detects a failed SP automatic update and triggers a corrective action to retry the SP automatic update up to three times. If all three retries have failed, you should contact technical support.

- When you download a version of the SP firmware from the NetApp Support Site and the downloaded version is newer than the one that the SP is currently running

You have the option to disable the SP automatic update functionality by using the `system node service-processor image modify` command. However, it is best to leave the functionality enabled. Disabling the functionality can result in suboptimal or nonqualified combinations between the Data ONTAP image and the SP firmware image.

- Data ONTAP enables you to trigger an SP update manually and specify how the update should take place by using the `system node service-processor image update` command.

  You can specify the following options:

  - The SP firmware package to use (`-package`)

    You can update the SP firmware to a downloaded package by specifying the package file name. The `system node image package show` command displays all package files (including the files for the SP firmware package) that are available on a node.
  - Whether to use the baseline SP firmware package for the SP update (`-baseline`)

    You can update the SP firmware to the baseline version that is bundled with the currently running version of Data ONTAP.
  - Whether to update the entire firmware image or only the changed portions (`-update-type`)
  - If updating the entire firmware image, whether to also reset log settings to the factory default and clear contents of all logs maintained by the SP, including the event logs, IPMI logs, and forensics logs (`-clear-logs`)

  For information about the `system node service-processor image update` command, see the man page.
- Data ONTAP enables you to display the status for the latest SP firmware update by using the `system node service-processor image update-progress show` command.

Any existing connection to the SP is terminated when the SP firmware is being updated. This is the case whether the SP firmware update is automatic or manually triggered.

Related information

NetApp Support Site: support.netapp.com

Restricting SP access to only the specified administration hosts

You can configure the SP to accept SSH requests from only the administration hosts that you specify.

Step

1. Enter the following command in the nodeshell to specify the administration host or hosts that you want to grant SP access:

   `options sp.ssh.access` ***`host_spec`***

   You can specify *`host_spec`* in the following forms:

   - `host[=|!=]`*`host_list`*
     `host_list` is a comma-separated list that includes host names, IP addresses, or IP addresses with a netmask.
   - `all` or `*`
     Allows all hosts to access the SP.
   - `none` or `-`
     Allows no hosts to access the SP.

   The default for *`host_spec`* is `*`.

   For more information and examples about using this option, see the na_spaccess(8) man page in the nodeshell.

Examples of restricting SP access to only the specified hosts

The following example grants SP SSH access to the administration host with the specified IP address:

```
node1> options sp.ssh.access host=192.168.123.98
```

The following example grants SP SSH access to two administration hosts, identified by their host names:

```
node1> options sp.ssh.access host=myhost1,myhost2
```

The following example grants SP SSH access to all hosts with their IP address prefix matching 3FFE:81D0:107:2082:

```
node1> options sp.ssh.access host=3FFE:81D0:107:2082::1/64
```

Configuring automatic logout of idle SSH connections to the SP

You can configure the automatic logout settings so that an SSH connection to the SP is automatically terminated after the connection has been idle for the number of minutes you specify.

About this task

Setting changes for automatic logout of idle SP SSH connections take effect only on SSH sessions that start after the changes.

Automatic logout does not take effect if you access the SP through the serial console.

Steps

1. Enter the following command in the nodeshell to enable SSH automatic logout for the SP:

   `options sp.autologout.enable on`

   Note: The default is `on`. Setting the option to `off` disables SSH automatic logout for the SP, causing the `sp.autologout.timeout` option to have no effect.

2. Enter the following command in the nodeshell to specify the number of minutes after which an idle SSH connection to the SP is automatically disconnected:

   `options sp.autologout.timeout` ***`minutes`***

   The default is 60 minutes.

Example of configuring automatic logout of idle SSH connections to the SP

The following example configures the SP to automatically disconnect SSH sessions that are idle for 30 minutes or more:

```
node1> options sp.autologout.enable on
node1> options sp.autologout.timeout 30
```

Data ONTAP commands for managing the SP

Data ONTAP provides commands for managing the SP, including setting up and displaying the SP network configuration, displaying the current SP status, rebooting the SP, managing the SP firmware image, and managing SSH access to the SP.

You can use the following Data ONTAP commands and nodeshell options to manage the SP:

If you want to...	Use this Data ONTAP command...
Set up or modify the SP network configuration of a node, including the following: • The IP address type (IPv4 or IPv6) • Whether the network interface of the specified IP address type should be enabled • If you are using IPv4, whether to use the network configuration from the DHCP server or the network address that you specify • The public IP address for the SP • The netmask for the SP (if using IPv4) • The network prefix-length of the subnet mask for the SP (if using IPv6) • The gateway IP address for the SP	`system node service-processor network modify`
Display the SP network configuration, including the following: • The configured address type (IPv4 or IPv6) and whether it is enabled • The remote management device type • The current SP status and link status • Network configuration, such as IP address, MAC address, netmask, prefix-length of subnet mask, router-assigned IP address, link local IP address, and gateway IP address	`system node service-processor network show` **Note:** Displaying complete SP network details requires the `-instance` parameter.
Display general SP information, including the following: • The remote management device type • The current SP status • Whether the SP network is configured • Network information, such as the public IP address and the MAC address • The SP firmware version and Intelligent Platform Management Interface (IPMI) version • Whether the SP firmware automatic update is enabled	`system node service-processor show` **Note:** Displaying complete SP information requires the `-instance` parameter.

If you want to...	Use this Data ONTAP command...
Reboot the SP on a node and optionally specify the SP firmware image (primary or backup) to use	`system node service-processor reboot-sp` **Attention:** You should avoid booting the SP from the backup image. Booting from the backup image is reserved for troubleshooting and recovery purposes only. It might require that the SP automatic firmware update be disabled, which is not a recommended setting. You should contact Technical Support before attempting to boot the SP from the backup image.
Display the details of the currently installed SP firmware image, including the following: • The remote management device type • The partition (primary or backup) that the SP is booted from, its status, and firmware version • Whether the firmware automatic update is enabled and the last update status	`system node service-processor image show` **Note:** The `-is-current` parameter indicates the partition (primary or backup) that the SP is currently booted from, not whether the installed firmware version is most current.
Enable or disable the SP automatic firmware update	`system node service-processor image modify` **Note:** By default, the SP firmware is automatically updated with the update of Data ONTAP or when a new version of the SP firmware is manually downloaded. Disabling the automatic update is not recommended because doing so can result in suboptimal or nonqualified combinations between the Data ONTAP image and the SP firmware image.
Manually download an SP firmware image on a node	`system node image get` **Note:** The SP firmware image is packaged with Data ONTAP. You do not need to download the SP firmware manually, unless you want to use an SP firmware version that is different from the one packaged with Data ONTAP.

If you want to...	Use this Data ONTAP command...
Manually update the SP firmware, by specifying the following: • The SP firmware package to use You can have the SP use a specific SP firmware package by specifying the package file name. The `system node image package show` command displays all package files (including the files for the SP firmware package) that are available on a node. • The installation baseline You can update the SP firmware to the baseline version that is bundled with the currently running version of Data ONTAP. • Whether to update the entire firmware image or only the changed portions • If updating the entire firmware image, whether to also reset log settings to the factory default and clear contents of all logs maintained by the SP, including the event logs, IPMI logs, and forensics logs	`system node service-processor image update`
Display the status for the latest SP firmware update, including the following information: • The start and end time for the latest SP firmware update • Whether an update is in progress and the percentage that is complete	`system node service-processor image update-progress show`
Enable or disable automatic logout of idle SSH connections to the SP	`options sp.autologout.enable` **Note:** This command is available through the nodeshell.
Specify the number of minutes after which an idle SSH connection to the SP is automatically disconnected	`options sp.autologout.timeout` **Note:** This command is available through the nodeshell. For this option to take effect, the `sp.autologout.enable` option must be set to `on`.

If you want to...	Use this Data ONTAP command...
Restrict SP access to only the specified administration hosts	`options sp.ssh.access` **Note:** This command is available through the nodeshell.

Disabling SNMP traps for only the SP

You can disable SNMP traps for only the SP and leave SNMP traps for Data ONTAP enabled.

Step

1. To disable SNMP traps for only the SP, enter the following command in the nodeshell:

   `options sp.snmp.traps off`

   The default is `on`.

   You cannot enable SNMP traps for only the SP when SNMP traps for Data ONTAP is disabled. If you disable SNMP traps for Data ONTAP, SNMP traps for the SP are also disabled.

Managing a node remotely by using the Remote LAN Module

The Remote LAN Module (RLM) is a remote management device that is provided on the 31xx, 6040, and 6080 platforms. The RLM provides remote node management capabilities, including remote access, monitoring, troubleshooting, logging, and alerting features.

The RLM stays operational regardless of the operating state of the node. It is powered by a standby voltage, which is available as long as the node has input power to at least one of its power supplies.

The RLM has a single temperature sensor to detect ambient temperature around the RLM board. Data generated by this sensor is not used for any node or RLM environmental policies. It is only used as a reference point that might help you troubleshoot node issues. For example, it might help a remote administrator determine if the node was shut down due to an extreme temperature change.

For instructions about how to cable a node to the RLM, see the *Installing or Replacing a Remote LAN Module* flyer.

- Without the RLM, you can access the node through the serial console or from an Ethernet connection using any supported network interface.
  You use the Data ONTAP CLI to administer the node.
- With the RLM, you can *remotely* access the node through the serial console.
  You use the Data ONTAP CLI to administer the node and the RLM.
- With the RLM, you can also access the node through an Ethernet connection using a secure shell client application.
  You use the RLM CLI to monitor and troubleshoot the node.

If you have a data center configuration where management traffic and data traffic are on separate networks, you can configure the RLM on the management network.

What the RLM does

The commands in the RLM CLI enable you to remotely access and administer the storage system and diagnose error conditions. Also, the RLM extends AutoSupport capabilities by sending alerts and notifications through an AutoSupport message.

Using the RLM CLI commands, you can perform the following tasks:

- Remotely administer the storage system by using the Data ONTAP CLI through the RLM's system console redirection feature
- Remotely access the storage system and diagnose error conditions, even if the storage system has failed, by performing the following tasks:
  - View the storage system console messages, captured in the RLM's console log
  - View storage system events, captured in the RLM's system event log
  - Initiate a storage system core dump
  - Power-cycle the storage system (or turn it on or off)
  - Reset the storage system
  - Reboot the storage system

The RLM extends AutoSupport capabilities by sending alerts and "down system" or "down filer" notifications through an AutoSupport message when the storage system goes down, regardless of whether the storage system can send AutoSupport messages. Other than generating these messages on behalf of a system that is down, and attaching additional diagnostic information to AutoSupport messages, the RLM has no effect on the storage system's AutoSupport functionality. The AutoSupport configuration settings and message content behavior of the RLM are inherited from Data ONTAP.

Note: The RLM does not rely on the `system node autosupport modify` command's `-transport` parameter setting to send notifications. The RLM uses the Simple Mail Transport Protocol (SMTP).

In addition to AutoSupport messages, the RLM generates SNMP traps to configured trap hosts for all "down system" or "down filer" events, if SNMP is enabled for the RLM.

The RLM has a nonvolatile memory buffer that stores up to 4,000 system events in a system event log (SEL) to help you diagnose system issues. The event list from the SEL is automatically sent by the RLM to specified recipients in an AutoSupport message. The records contain the following data:

- Hardware events detected by the RLM—for example, system sensor status about power supplies, voltage, or other components
- Errors (generated by the storage system or the RLM) detected by the RLM—for example, a communication error, a fan failure, a memory or CPU error, or a `boot image not found` message
- Critical software events sent to the RLM by the storage system—for example, a system panic, a communication failure, an unexpected boot environment prompt, a boot failure, or a user-

triggered “down system” as a result of issuing the `system reset` or `system power cycle` command.

The RLM monitors the storage system console regardless of whether administrators are logged in or connected to the console. When storage system messages are sent to the console, the RLM stores them in the console log. The console log persists as long as the RLM has power from either of the storage system’s power supplies. Because the RLM operates with standby power, it remains available even when the storage system is power-cycled or turned off.

Hardware-assisted takeover is available on systems that support the RLM and have the RLM modules set up. For more information about hardware-assisted takeover, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

The RLM supports the SSH protocol for CLI access from UNIX clients and PuTTY for CLI access from PC clients.

Prerequisites for configuring the RLM

Before you configure the RLM, you must gather information about your network and your AutoSupport settings.

The following is the information you need to gather:

- Network information

  You can configure the RLM using DHCP or static addressing. If you are using an IPv4 address for the RLM, you need the following information:

  - An available static IP address
  - The netmask of your network
  - The gateway of your network

  If you are using IPv6 for RLM static addressing, you need the following information:

  - The IPv6 global address
  - The subnet prefix for the RLM
  - The IPv6 gateway for the RLM
- AutoSupport information

  The RLM sends event notifications to the recipients and mail host specified in the `system node autosupport modify` command.

  It is best that you configure at least the AutoSupport recipients and mail host before configuring the RLM. Data ONTAP automatically sends AutoSupport configuration to the RLM, allowing the RLM to send alerts and notifications through an AutoSupport message to the system administrative recipients specified in AutoSupport. You are prompted to enter the name or the IP address of the AutoSupport mail host when you configure the RLM.

Configuring the RLM for a node

You can use the `rlm setup` command in the nodeshell to configure the RLM for a node. You can configure the RLM to use either a static or a DHCP address.

Before you begin

AutoSupport should be configured before you configure the RLM. Data ONTAP automatically sends the AutoSupport configuration to the RLM, allowing the RLM to send alerts and notifications through AutoSupport messages.

About this task

If you are running RLM firmware version 4.2 or later, and you have enabled IPv6 for Data ONTAP, you have the option to configure the RLM for only IPv4, for only IPv6, or for both IPv4 and IPv6. Disabling IPv6 on Data ONTAP also disables IPv6 on the RLM.

Attention: If you disable both IPv4 and IPv6, and if DHCP is also not configured, the RLM has no network connectivity.

Steps

1. From the nodeshell, enter the following command:

   `rlm setup`

2. When the RLM setup asks you whether to configure the RLM, enter **`y`**.
3. Do one of the following when the RLM setup asks you whether to enable DHCP on the RLM.
   - To use DHCP addressing, enter **`y`**.
   - To use static addressing, enter **`n`**.

   Note: DHCPv6 servers are not currently supported.

4. If you do not enable DHCP for the RLM, the RLM setup prompts you for static IP information. Provide the following information when prompted:
   - The IP address for the RLM

     Note: Entering **`0.0.0.0`** for the static IP address disables IPv4 for the RLM.

   - The netmask for the RLM
   - The IP address for the RLM gateway
   - The name or IP address of the mail host to use for AutoSupport
5. If you enabled IPv6 for Data ONTAP and your RLM firmware version is 4.2 or later, the RLM supports IPv6, and the RLM setup asks you whether to configure IPv6 connections for the RLM:
   - To configure IPv6 connections for the RLM, enter **`y`**.
   - To disable IPv6 connections for the RLM, enter **`n`**.

Note: You can use the `rlm status` command to find the RLM version information.

6. If you choose to configure IPv6 for the RLM, provide the following IPv6 information when prompted by the RLM setup:
   - The IPv6 global address
   - The subnet prefix for the RLM
   - The IPv6 gateway for the RLM

   Note: You cannot use the RLM setup to enable or disable the IPv6 router-advertised address for the RLM. However, when you enable or disable the IPv6 router-advertised address for Data ONTAP, the same configuration applies to the RLM.

   For information about enabling IPv6 for Data ONTAP, see the *Clustered Data ONTAP Network Management Guide*.
7. From the nodeshell, enter the following command to verify that the RLM network configuration is correct:

   `rlm status`
8. From the nodeshell, enter the following command to verify that the RLM AutoSupport function is working properly:

   `rlm test autosupport`

   Note: The RLM uses the same mail host information that Data ONTAP uses for AutoSupport.

Examples for configuring the RLM and displaying the configuration information

The following example shows that the RLM is configured for both IPv4 and IPv6 connections:

```
node1> rlm setup
      The Remote LAN Module (RLM) provides remote management capabilities
      including console redirection, logging and power control.
      It also extends autosupport by sending
      additional system event alerts. Your autosupport settings are used
      for sending these alerts via email over the RLM LAN interface.
Would you like to configure the RLM? y
Would you like to enable DHCP on the RLM LAN interface? n
Please enter the IP address for the RLM []:192.168.123.98
Please enter the netmask for the RLM []:255.255.255.0
Please enter the IP address for the RLM gateway []:192.168.123.1
Do you want to enable IPv6 on the RLM ? y
Do you want to assign IPv6 global address? y
Please enter the IPv6 address for the RLM []:fd22:8b1e:b255:204::1234
Please enter the subnet prefix for the RLM []: 64
Please enter the IPv6 Gateway for the RLM []:fd22:81be:b255:204::1
Verifying mailhost settings for RLM use...
```

The following example shows that the RLM is configured to use DHCP and IPv6:

```
node1> rlm setup
   The Remote LAN Module(RLM) provides remote management capabilities
   including console redirection, logging and power control.
```

```
   It also extends autosupport by sending
   additional system alerts. Your autosupport settings are used
   for sending these alerts via email over the RLM LAN interface.
Would you like to configure the RLM? y
Would you like to enable DHCP on the RLM LAN interface? y
Do you want to enable IPv6 on the RLM ? y
Do you want to assign IPv6 global address? y
Please enter the IPv6 address for the RLM [fd22:8b1e:b255:204::1234]:
Please enter the subnet prefix for the RLM [64]:
Please enter the IPv6 Gateway for the RLM [fd22:81be:b255:204::1]:
Verifying mailhost settings for RLM use...
```

The following example displays the RLM status and configuration information:

```
node1> rlm status
    Remote LAN Module    Status: Online
        Part Number:        110-00030
        Revision:           A0
        Serial Number:      123456
        Firmware Version:   4.2
        Mgmt MAC Address:   00:A0:98:01:7D:5B
        Ethernet Link:      up, 100Mb, full duplex, auto-neg complete
        Using DHCP:         no
    IPv4 configuration:
        IP Address:         192.168.123.98
        Netmask:            255.255.255.0
        Gateway:            192.168.123.1
    IPv6 configuration:
        Global IP:          fd22:8b1e:b255:204::1234
        Prefix Length:      64
        Gateway:            fd22:81be:b255:204::1
        Router Assigned IP: fd22:8b1e:b255:204:2a0:98ff:fe01:7d5b
        Prefix Length:      64
        Link Local IP:      fe80::2a0:98ff:fe00:7d1b
        Prefix Length:      64
```

Related concepts

Managing AutoSupport on page 203

Accounts that can access the RLM

Cluster user accounts that are created with the `service-processor` application type have access to the RLM CLI on any node of the cluster that supports the RLM. RLM user accounts are managed from Data ONTAP and authenticated by password.

User accounts for accessing the RLM are managed from Data ONTAP instead of the RLM CLI. A cluster user account of any role can access the RLM if it is created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`. The RLM supports only password authentication.

By default, the cluster user account named “admin” includes the `service-processor` application type and has access to the RLM. Vserver user accounts cannot access the RLM.

Note: Data ONTAP prevents you from creating user accounts with names that are reserved for the system (such as “root” and “naroot”). You cannot use a system-reserved name to access the cluster or the RLM.

Related concepts

Managing user accounts on page 134
Access methods for user accounts on page 135

Restricting RLM access to only the specified administration hosts

You can configure the RLM to accept SSH requests from only the administration hosts that you specify.

Before you begin

Your system must be running RLM firmware 4.1 or later for the RLM access control to be supported. For information about downloading and updating the RLM firmware, see the *Clustered Data ONTAP Upgrade and Revert/Downgrade Guide*.

Step

1. Enter the following command in the nodeshell to specify the administration host or hosts that you want to grant RLM access:

   `options rlm.ssh.access` ***`host_spec`***

   You can specify *`host_spec`* in the following forms:

   - `host[=|!=]`*`host_list`*
     `host_list` is a comma-separated list that includes host names, IP addresses, or IP addresses with a netmask.
   - `all` or `*`
     Allows all hosts to access the RLM.
   - `none` or `-`
     Allows no hosts to access the RLM.

   The default for *`host_spec`* is `*`.

   For more information and examples about using this option, see the na_rlmaccess(8) man page in the nodeshell.

Examples of restricting RLM access to only the specified hosts

The following example grants RLM SSH access to the administration host with the specified IP address:

```
node1> options rlm.ssh.access host=192.168.123.98
```

The following example grants RLM SSH access to two administration hosts, identified by their host names:

```
node1> options rlm.ssh.access host=myhost1,myhost2
```

The following example grants RLM SSH access to all hosts with their IP address prefix matching 3FFE:81D0:107:2082:

```
node1> options rlm.ssh.access host=3FFE:81D0:107:2082::1/64
```

Configuring automatic logout of idle SSH connections to the RLM

You can configure the automatic logout settings so that an SSH connection to the RLM is automatically terminated after the connection has been idle for the number of minutes you specify.

Before you begin

Your system must be running RLM firmware version 4.1 or later for the automatic logout configuration to be supported. For information about downloading and updating the RLM firmware, see the *Clustered Data ONTAP Upgrade and Revert/Downgrade Guide*.

About this task

Setting changes for automatic logout of idle RLM SSH connections take effect only on SSH sessions that start after the changes.

Automatic logout does not take effect if you access the RLM through the serial console.

Steps

1. Enter the following command in the nodeshell to enable SSH automatic logout for the RLM:

   `options rlm.autologout.enable on`

   Note: The default is `on`. Setting the option to `off` disables SSH automatic logout for the RLM, causing the `rlm.autologout.timeout` option to have no effect.

2. Enter the following command in the nodeshell to specify the number of minutes after which an idle SSH connection to the RLM is automatically disconnected:

   `options rlm.autologout.timeout` ***`minutes`***

   The default is 60 minutes.

Example of configuring automatic logout of idle SSH connections to the RLM

The following example configures the RLM to automatically disconnect SSH sessions that are idle for 30 minutes or more:

```
node1> options rlm.autologout.enable on
node1> options rlm.autologout.timeout 30
```

Logging in to the RLM from an administration host

You can log in to the RLM from an administration host to perform administrative tasks remotely, if the host has a Secure Shell client application that supports SSHv2 and your account name is configured with the `service-processor` application type.

About this task

If the RLM is running firmware version 4.0 or later and is configured to use an IPv4 address, the RLM rejects SSH login requests and suspends all communication with the IP address for 15 minutes if five SSH login attempts fail repeatedly within 10 minutes. The communication resumes after 15 minutes, and you can try to log in to the RLM again.

Steps

1. Enter the following command from the UNIX host:

   ssh ***username@RLM_IP_address***

2. When you are prompted, enter the password for *username*.

   The RLM prompt appears, indicating that you have access to the RLM CLI.

Examples of RLM access from an administration host

The following example shows how to log in to the RLM with a user account, joe, which has been set up on the storage system to access the RLM.

```
ssh joe@192.168.123.98
```

The following examples show how to use the IPv6 global address or IPv6 router-advertised address to log in to the RLM on a storage system that has SSH set up for IPv6 and the RLM configured for IPv6.

```
ssh joe@fd22:8b1e:b255:202::1234
```

```
ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
```

Accessing the serial console from the RLM

The RLM's `system console` command enables you to log in to the serial console from the RLM.

Steps

1. Enter the following command at the RLM prompt:

system console

The message `Type Ctrl-D to exit` appears.

2. Log in to the console when you are prompted.
3. To exit the serial console and return to the RLM CLI, press Ctrl-D.

Example of accessing the serial console from the RLM

The following example shows the result of entering the `system console` command at the RLM prompt. The `system node image show` command is entered at the console, followed by Ctrl-D, which returns you to the RLM prompt.

```
RLM> system console
Type Ctrl-D to exit.
```

(Log in to the console when you are prompted.)

```
login:
Password:
******************************************************
* This is a SP/RLM console session. Output from the *
* serial console is also mirrored on this session.  *
******************************************************
cluster1::>
cluster1::> system node image show
```

(Command output is displayed.)

(Press Ctrl-D to exit the storage serial console and return to the RLM CLI.)

```
RLM>
```

Relations among the RLM CLI, RLM console, and serial console sessions

You can open an RLM CLI session to manage a node remotely and a separate RLM console session to run Data ONTAP commands remotely. The RLM console session mirrors output displayed in a concurrent serial console session. The RLM and the serial console have independent shell environments with independent login authentication.

Understanding how the RLM CLI, RLM console, and serial console sessions are related helps you manage a node remotely. The following describes the relations among the sessions:

- Only one administrator can log in to the RLM CLI session at a time; however, the RLM enables you to open both an RLM CLI session and a separate RLM console session simultaneously. The RLM CLI is indicated with the RLM prompt (`RLM>`). From an RLM CLI session, you can use the RLM `system console` command to initiate an RLM console session. At the same time,

you can start a separate RLM CLI session through SSH. If you press Ctrl-D to exit from the RLM console session, you automatically return to the RLM CLI session. If an RLM CLI session already exists, a message asks you whether to terminate the existing RLM CLI session. If you enter “y”, the existing RLM CLI session is terminated, enabling you to return from the RLM console to the RLM CLI. This action is recorded in the RLM event log.

- For security reasons, the RLM CLI session and the serial console session have independent login authentication.

  When you initiate an RLM console session from the RLM CLI (by using the RLM `system console` command), you are prompted for the serial console credential.
- The RLM console session and the serial console session have independent shell environments.

  The RLM console session mirrors output that is displayed in a concurrent serial console session. However, the concurrent serial console session does not mirror the RLM console session.

  The RLM console session does not mirror output of concurrent SSH sessions.

Using online help at the RLM CLI

The RLM online help displays all RLM commands and options when you enter the question mark (?) or `help` at the RLM prompt.

Steps

1. To display help information for RLM commands, enter one of the following at the RLM prompt:
   - `help`
   - **?**

   #### Example

   The following example shows the RLM CLI online help:

   ```
   RLM node1> help
   date - print date and time
   exit - exit from the RLM command line interface
   events - print system events and event information
   help - print command help
   priv - show and set user mode
   rlm - commands to control the RLM
   rsa - commands for Remote Support Agent
   system - commands to control the system
   version - print RLM version
   ```

   For more information about the RSA command, see the *Remote Support Agent Configuration Guide for Clustered Data ONTAP*.

2. To display help information for the option of an RLM command, enter the following command at the RLM prompt:

   `help` ***`RLM_command`***

Example

The following example shows the RLM CLI online help for the RLM `events` command:

```
RLM node1> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

Commands for managing the RLM at the admin privilege level

You can perform most RLM tasks at the admin privilege level. For example, you can display system events and status information for environmental sensors, reboot the storage system or the RLM, and create a system core dump.

The following RLM commands are available at the admin privilege level:

If you want to...	Use this command...
Display system date and time	`date`
Display storage system events logged by the RLM	`events` {`all` | `info` | `newest` | `oldest` | *`search string`* }
Exit the RLM CLI	`exit`
Display a list of available commands or subcommands of a specified command	`help` [*`command`*]
Set the privilege level to access the specified mode	`priv set` {`admin` | `advanced` | `diag`}
Display the current privilege level	`priv show`
Reboot the RLM	`rlm reboot`
Display the RLM environmental sensor status	`rlm sensors` [`-c`] **Note:** The `-c` option, which takes a few seconds to display, shows current values rather than cached values.
Display RLM status	`rlm status [-v|-d]` **Note:** The `-v` option displays verbose statistics. The `-d` option displays RLM debug information.

If you want to...	Use this command...
Update the RLM firmware	`rlm update` *`http://path`* `[-f]` **Note:** The `-f` option issues a full image update.
Manage the RSA if it is installed on your storage system	`rsa` **Note:** For information about the RSA, see the *Remote Support Agent Configuration Guide for Clustered Data ONTAP*.
Log in to the Data ONTAP CLI	`system console` **Note:** Pressing Ctrl-d returns you to the RLM CLI.
Dump the system core and reset the system	`system core` **Note:** This command has the same effect as pressing the Non-maskable Interrupt (NMI) button on a storage system. The RLM stays operational as long as input power to the storage system is not interrupted.
Turn on or turn off the storage system, or perform a power-cycle (which turns off system power and then turns it back on)	`system power {on | off | cycle}` **Note:** Standby power stays on, even when the storage system is off. During power-cycling, a brief pause occurs before power is turned back on. **Attention:** Using the `system power` command to turn off or power-cycle the storage system might cause an improper shutdown of the system (also called a *dirty shutdown*) and is not a substitute for a graceful shutdown using the Data ONTAP `system node halt` command.
Display status for each power supply, such as presence, input power, and output power	`system power status`

If you want to...	Use this command...
Reset the storage system using the specified BIOS firmware image	`system reset {primary | backup | current}` **Note:** The RLM stays operational as long as input power to the storage system is not interrupted.
Display the RLM version information, including hardware and firmware information	`version`

Commands for managing the RLM at the advanced privilege level

In addition to using the RLM admin commands, you can use the RLM advanced privilege level to display RLM command history, RLM debug and message files, status of environmental sensors, and RLM statistics.

The following RLM commands are available only at the advanced privilege level:

If you want to display...	Use this command...
RLM command history or search for audit logs from the system event log (SEL)	`rlm log audit`
RLM debug file	`rlm log debug`
RLM message file	`rlm log messages`
List of environmental sensors, their states, and their current values	`system sensors`
RLM statistics	`rlm status -v`

Troubleshooting a node by using the RLM

When you encounter a problem with a node, you can use the RLM to display information about the problem, create a core dump, and reboot the node, even if the node's firmware is corrupted.

The following table describes the RLM commands that you can use to troubleshoot a node:

If this condition occurs...	And you want to...	Enter this command at the RLM CLI prompt...
You receive an AutoSupport message indicating an event such as a panic or hardware component failure.	Display what has occurred at the storage system console.	`system log`
	Display all events.	`events all`
	Display a specific number of recent events.	`events newest` *`number`*
	Search for specific events in the SEL.	`events search` *`string`*
The node is not responding properly.	Access the system console from the RLM.	`system console`
	Create a core dump and reboot the node.	`system core`
	Power-cycle the node.	`system power cycle`
The node firmware is corrupted.	Boot the node by using a backup copy of the node firmware.	`system reset backup`

Managing the RLM with Data ONTAP

You can manage the RLM from Data ONTAP by using the `rlm` commands in the nodeshell.

Data ONTAP commands for managing the RLM

Data ONTAP provides the `rlm` commands in the nodeshell for managing the RLM, including setting up the RLM, rebooting the RLM, displaying the status of the RLM, and updating the RLM firmware.

The following table describes the Data ONTAP commands and options for managing the RLM.

If you want to...	Use this Data ONTAP nodeshell command...
Initiate the interactive RLM setup script	`rlm setup`
Display whether the RLM has been configured	`options rlm.setup`
Display the list of available `rlm` commands	`rlm help`
Display the current status of the RLM, including the following: • Whether the RLM is online • The version that the RLM is running • Network and configuration information	`rlm status`

If you want to...	Use this Data ONTAP nodeshell command...
Reboot the RLM and trigger the RLM to perform a self-test	`rlm reboot` **Note:** Any console connection through the RLM is lost during the reboot.
Send a test email to all recipients specified in AutoSupport	`rlm test autosupport` **Note:** For this command to work, AutoSupport must be enabled and the recipients and mail host must be configured.
Perform an SNMP test on the RLM, forcing the RLM to send a test SNMP trap to all configured trap hosts	`rlm test snmp` **Note:** For information about SNMP traps, see the *Clustered Data ONTAP Network Management Guide*.
Update the RLM firmware	`rlm update` **Note:** Before using this command, you must use the `system node image get` command followed by the nodeshell command `software install` to download and install the new RLM firmware image. For information about downloading and updating the RLM firmware, see the *Clustered Data ONTAP Upgrade and Revert/Downgrade Guide*.
Display the RLM update status, including the following: • Whether an RLM update is currently in progress • Completion percentage • The start and end time for the update	`rlm update-status`
Enable or disable automatic logout of idle SSH connections to the RLM	`options rlm.autologout.enable`
Specify the number of minutes after which an idle SSH connection to the RLM is automatically disconnected	`options rlm.autologout.timeout` **Note:** For this option to take effect, the `rlm.autologout.enable` option must be set to `on`.

If you want to...	Use this Data ONTAP nodeshell command...
Restrict RLM access to only the specified administration hosts	`options rlm.ssh.access`

RLM and SNMP traps

If SNMP is enabled for the RLM, the RLM generates SNMP traps to configured trap hosts for all "down system" events.

You can enable SNMP traps for both Data ONTAP and the RLM. You can also disable the SNMP traps for only the RLM and leave the SNMP traps for Data ONTAP enabled.

For information about SNMP traps, see the *Clustered Data ONTAP Network Management Guide*.

Disabling SNMP traps for only the RLM

You can disable SNMP traps for only the RLM and leave SNMP traps for Data ONTAP enabled.

Step

1. To disable SNMP traps for only the RLM, enter the following command in the nodeshell:

   `options rlm.snmp.traps off`

   The default is `on`.

   You cannot enable SNMP traps for only the RLM when SNMP traps for Data ONTAP is disabled. If you disable SNMP traps for Data ONTAP, SNMP traps for the RLM are also disabled.

Troubleshooting RLM connection problems

If you are having difficulty connecting to the RLM, you should verify that you are using a secure shell client and that the IP configuration is correct.

Steps

1. Verify that you are using a secure shell client to connect to the RLM.
2. From the storage system, verify the RLM is online and the IP configuration is correct by entering the following command in the nodeshell:

   `rlm status`

3. From the administration host, test the network connection for the RLM by entering the following command:

   `ping` ***`rlm_IP_address`***

4. If the ping fails, do one of the following:
   - Verify that the RLM network port on the back of the storage system is cabled and active.

For more information, see the Installation and Setup Instructions for your storage system.

- Verify that the RLM has a valid IP address by entering the following command in the nodeshell:

  `rlm setup`

- Verify that the administration host has a route to the RLM.

5. Reboot the RLM by entering the following command in the nodeshell:

   `rlm reboot`

   Note: It takes approximately one minute for the RLM to reboot.

6. If the RLM does not reboot, repeat Steps 2 through 5. If the RLM still does not reboot, contact technical support for assistance.

Managing Vservers (cluster administrators only)

Cluster administrators can manage and administer the *virtual storage servers (Vservers)* within a cluster. A cluster must have at least one Vserver to serve data to the clients. Therefore, a cluster administrator must create and manage Vservers.

Cluster administrators can either choose to perform Vserver administration tasks in addition to the Vserver management tasks or delegate the administration of the Vservers to Vserver administrators.

To manage and administer Vservers, you must understand what a Vserver is, its benefits such as nondisruptive operation and scalability, and the associated management tasks.

A cluster administrator can perform the following Vserver management tasks:

- Creating Vservers
- Modifying Vservers
- Deleting Vservers
- Renaming Vservers
- Administering Vservers from the Vserver context
- Starting and stopping Vservers

Note: Both cluster administrators and Vserver administrators can view information about Vservers.

For more information about Vserver administrator capabilities, see the *Clustered Data ONTAP System Administration Guide for Vserver Administrators*.

What a Vserver is

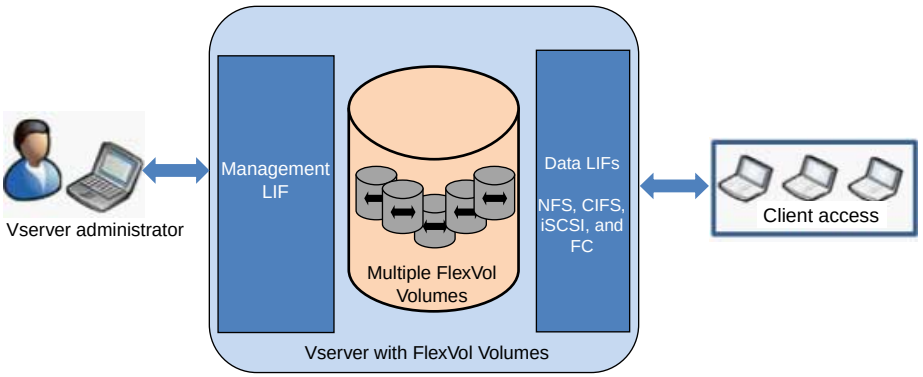
A *virtual storage server (Vserver)* contains data volumes and one or more LIFs through which it serves data to the clients. Starting with clustered Data ONTAP 8.1.1, a Vserver can either contain one or more FlexVol volumes, or a single Infinite Volume.

A Vserver securely isolates the shared virtualized data storage and network, and appears as a single dedicated server to its clients. Each Vserver has a separate administrator authentication domain and can be managed independently by a Vserver administrator.

In a cluster, Vserver facilitates data access. A cluster must have at least one Vserver to serve data. Vservers use the storage and network resources of the cluster. However, the volumes and LIFs are exclusive to the Vserver. Multiple Vservers can coexist in a single cluster without being bound to any node in a cluster. However, they are bound to the physical cluster on which they exist.

A cluster can have one or more Vservers with FlexVol volumes and Vservers with Infinite Volumes.

Vserver with FlexVol volumes

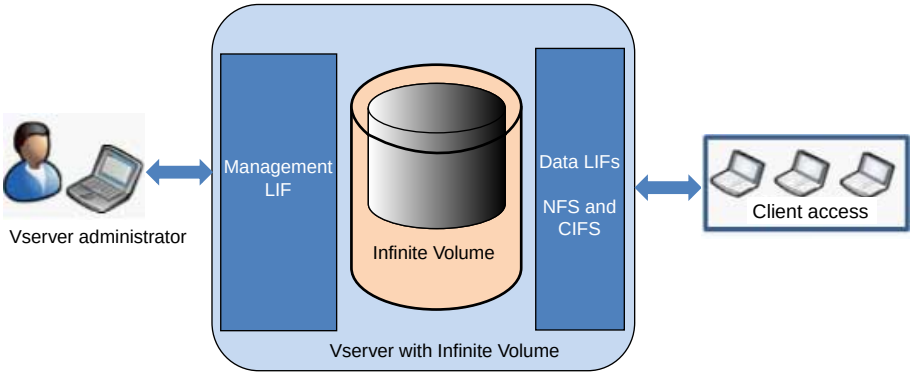


A Vserver with FlexVol volumes in a NAS environment presents a single directory hierarchical view and has a unique namespace. Namespace enables the NAS clients to access data without specifying the physical location of the data. Namespace also enables the cluster and Vserver administrators to manage distributed data storage as a single directory with multiple levels of hierarchy.

The volumes within each NAS Vserver are related to each other through junctions and are mounted on junction paths. These junctions present the file system in each volume. The root volume of a Vserver is a FlexVol volume that resides at the top level of the namespace hierarchy; additional volumes are mounted to the Vserver's root volume to extend the namespace. As volumes are created for the Vserver, the root volume of a Vserver contains junction paths.

A Vserver with FlexVol volumes can contain files and LUNs. It provides file-level data access by using NFS and CIFS protocols for the NAS clients, and block-level data access by using iSCSI, and Fibre Channel (FC) protocol (FCoE included) for SAN hosts.

Vserver with Infinite Volume



A Vserver with Infinite Volume can contain only one Infinite Volume to serve data. A Vserver with Infinite Volume includes only one junction path, which has a default value of `/NS`. The junction provides a single mount point for the large namespace provided by the Vserver with Infinite Volume. You cannot add more junctions to a Vserver with Infinite Volume. However, you can increase the size of the Infinite Volume.

A Vserver with Infinite Volume can contain only files. It provides file-level data access by using NFS and CIFS (SMB 1.0) protocols. A Vserver with Infinite Volume cannot contain LUNs and does not provide block-level data access.

About a Vserver's root volume

Every Vserver has a root volume that contains the paths where the data volumes are junctioned into the namespace. NAS clients' data access is dependent on the root volume namespace and SAN clients' data access is not dependent on the root volume namespace.

The root volume serves as the entry point to the namespace provided by that Vserver. The root volume of a Vserver is a FlexVol volume that resides at the top level of the namespace hierarchy and contains the directories that are used as mount points, the paths where data volumes are junctioned into the namespace.

In the unlikely event that the root volume of a Vserver namespace is unavailable, NAS clients cannot access the namespace hierarchy and therefore cannot access data in the namespace. For this reason, it is best to create a load-sharing mirror copy for the root volume on each node of the cluster so that the namespace directory information remains available in the event of a node outage or failover.

It is best not to store user data in the root volume of a Vserver. Root volume of a Vserver should be used for junction paths and user data should be stored in non-root volumes of a Vserver.

Types of Vservers

A cluster consists of three types of Vservers, which help in managing the cluster and its resources and the data access to the clients and applications.

A cluster contains the following types of Vservers:

- Admin Vserver
- Node Vserver
- Data Vserver

The cluster setup process automatically creates the admin Vserver for the cluster. A node Vserver is created when the node joins the cluster. The admin Vserver represents the cluster, and node Vserver represents the individual nodes of the cluster.

The data Vserver represents the data serving Vservers. After the cluster setup, a cluster administrator must create data Vservers and add volumes to these Vservers to facilitate data access from the cluster. A cluster must have at least one data Vserver to serve data to its clients.

Note: Unless otherwise specified, the term Vserver refers to data (data-serving) server, which applies to both Vserver with FlexVol volumes and Vserver with Infinite Volume.

Why you use Vservers

Vservers provide data access to clients without regard to physical storage or controller, similar to any storage system. When you use Vservers, they provide benefits such as nondisruptive operation, scalability, security and support unified storage.

A Vserver has the following benefits:

- Nondisruptive operation

  Vservers can operate continuously and nondisruptively for as long as they are needed. Vservers help clusters to operate continuously during software and hardware upgrades, addition and removal of nodes, and all administrative operations.
- Scalability

  Vservers meet on-demand data throughput and the other storage requirements.
- Security

  A Vserver appears as a single independent server, which enables multiple Vservers to coexist while ensuring no data flows among them.
- Unified Storage

  Vservers can serve data concurrently through multiple data access protocols. A Vserver provides file-level data access by using NAS protocols, such as CIFS and NFS, and block-level data access by using SAN protocols, such as iSCSI and FC (FCoE included). A Vserver can serve data to SAN and NAS clients independently at the same time.

  Note: A Vserver with Infinite Volume can serve data only through NFS and CIFS (SMB 1.0) protocols.
- Delegation of management

  A Vserver can have its own user and administration authentication. Vserver administrators can manage the Vservers that they are authorized to access. However, Vserver administrators have privileges assigned by the cluster administrators.
- Easy Management of large datasets

  With Vserver with Infinite Volume, management of large and unstructured data is easier as the Vserver administrator has to manage one data container instead of many.

Number of Vservers in a cluster

The number of Vservers that you can create in a cluster depends on the number of nodes and how the LIFs are configured and used in your cluster.

The following table lists the recommended number of Vservers in a cluster based on the number of LIFs configured:

Vservers with protocol type Nodes	Nodes per cluster						Vserver configuration
	1	2	4	6	8	10-24	
Vservers with NFS/CIFS protocol: one single LIF for data and management	125	250	500	750	1000	1000	Each Vserver with one active IP LIF for data and management, and one IP LIF reserved for failover.
Vservers with FC/FCoE protocol: one LIF for data and one LIF for management	125	250	250	250	250	NA	Each Vserver with two FC/FCoE LIFs on each node of the cluster and an IP LIF dedicated for management.
Vservers with iSCSI protocol: one LIF for data and one LIF for management	125	125	165	190	200	NA	Each Vserver with one iSCSI LIF on each node of the cluster and an IP LIF dedicated for management.

Note:

The numbers of Vservers in a cluster might not be same if the cluster has a combination of Vservers with different protocols.

The maximum number of nodes supported for Vservers in a NAS cluster is 24, and in a SAN cluster is 8. If any node in a cluster uses SAN protocols then the entire cluster is limited to 8 nodes.

Vservers with Infinite Volume do not exist in a SAN cluster. A Vserver with Infinite Volume cannot span more than 10 nodes of a NAS cluster.

Creating a Vserver

Cluster administrators can create Vservers with FlexVol volumes and Vservers with Infinite Volumes in a cluster to serve data to the clients.

You can use one of the following methods to create Vservers:

- The `vserver setup` command enables you to create fully configured Vservers with FlexVol volumes that can serve data immediately.

  Note: You cannot create fully configured Vservers with Infinite Volumes by using the `vserver setup` command.

  With the `vserver setup` command, you can quickly set up Vservers by following the prompts of the wizard.

- The `vserver create` command enables you to create Vservers with FlexVol Volumes or Vservers with Infinite Volume with the root volume and basic configuration, such as name service switch, name mapping switch, and root volume security style.

  You must run the various commands to fully configure the Vservers to serve data after creating a Vserver by using the `vserver create` command.

Before you create a Vserver, you must understand the various requirements and gather the required information such as language setting option for a Vserver.

Choices

- *List of language options* on page 97
- *Language configurations* on page 100
- *Completing the Vserver setup worksheet* on page 101
- *Creating a Vserver by using the CLI wizard* on page 106
- *Creating a Vserver by using the vserver create command* on page 113

List of language options

When you create a Vserver, the language is set for the Vserver. The language of the Vserver determines the default language setting for volumes in that Vserver. You can modify the language of a Vserver.

You can specify the language for a volume when creating a volume and it can be different from the Vserver's language. If you do not specify the language for a volume then it inherits the language setting of its Vserver. After the volume is created, you cannot modify the language of a volume. Therefore, you must be aware of the available language options.

The following table lists the various available language options that helps you choose and enter the correct value when creating a Vserver or volume:

Language values	Languages
c	POSIX
C.UTF-8	POSIX with UTF-8
ar	Arabic
ar.UTF-8	Arabic with UTF-8
cs	Czech
cs.UTF-8	Czech with UTF-8
da	Danish
da.UTF-8	Danish with UTF-8
de	German

Language values	**Languages**
de.UTF-8	German with UTF-8
en	English
en.UTF-8	English with UTF-8
en_us	English (US)
en_US.UTF-8	US English with UTF-8
es	Spanish
es.UTF-8	Spanish with UTF-8
fi	Finnish
fi.UTF-8	Finnish with UTF-8
fr	French
fr.UTF-8	French with UTF-8
he	Hebrew
he.UTF-8	Hebrew with UTF-8
hr	Croatian
hr.UTF-8	Croatian with UTF-8
hu	Hungarian
hu.UTF-8	Hungarian with UTF-8
it	Italian
it.UTF-8	Italian with UTF-8
ja_v1	Japanese euc-j
ja_v1.UTF-8	Japanese euc-j with UTF-8
ja_jp.pck_v2	Japanese PCK (sjis)
ja_JP.PCK_v2.UTF-8	Japanese PCK sjis with UTF-8
ko	Korean
ko.UTF-8	Korean with UTF-8
no	Norwegian
no.UTF-8	Norwegian with UTF-8

Language values	**Languages**
nl	Dutch
nl.UTF-8	Dutch with UTF-8
pl	Polish
pl.UTF-8	Polish with UTF-8
pt	Portuguese
pt.UTF-8	Portuguese with UTF-8
ro	Romanian
ro.UTF-8	Romanian with UTF-8
ru	Russian
ru.UTF-8	Russian with UTF-8
sk	Slovak
sk.UTF-8	Slovak with UTF-8
sl	Slovenian
sl.UTF-8	Slovenian with UTF-8
sv	Swedish
sv.UTF-8	Swedish with UTF-8
tr	Turkish
tr.UTF-8	Turkish with UTF-8
zh	Simplified Chinese
zh.UTF-8	Simplified Chinese with UTF-8
zh.GBK	Simplified Chinese (GBK)
zh.GBK.UTF-8	Simplified GBK Chinese with UTF-8
zh_TW	Traditional Chinese euc-tw
zh_TW.UTF-8	Traditional Chinese euc-tw with UTF-8
zh_TW.BIG5	Traditional Chinese Big 5
zh_TW.BIG5.UTF-8	Traditional Chinese Big 5 with UTF-8

Language configurations

The language configuration of a Vserver or a volume must match the client's language configuration for the file names to appear correctly. If there is a mismatch in the language configuration, then some file names might contain incorrect characters.

The following table helps you identify the language configuration for various clients depending on the client encoding types:

Clients protocol	Client encoding type	Language configuration
CIFS running on Win95/98/ME	ISO 8859-1	Match non-UTF-8 client locale. Do not append UTF-8 that is 'en_US'.
CIFS running on WinNT 3.1+	UCS-2	Unless other clients use non-UTF-8 locale, match UTF-8 client locale. Append UTF-8 that is 'en_US.UTF-8'. When other clients use non-UTF-8 locales, match non-UTF-8 client locale. Do not append UTF-8 that is 'en_US'.
NFSv2/3	Non-UTF-8 client locale	Match non-UTF-8 client locale. Do not append UTF-8 that is 'en_US'.
NFSv4	UTF-8	Unless other clients use non-UTF-8 locale, match UTF-8 client locale. Append UTF-8 that is 'en_US.UTF-8'. When other clients use non-UTF-8 locales, match non-UTF-8 client locale. Do not append UTF-8 that is 'en_US'.
FC or iSCSI		UTF-8 preferred, C/POSIX is acceptable.

Note: The default language setting for a Vserver is C.UTF-8.

Completing the Vserver setup worksheet

Before you start the Vserver Setup wizard to create and configure a Vserver, you must gather the required information to complete the wizard successfully.

Note: You can create and configure only Vservers with FlexVol volumes by using the Vserver Setup wizard.

The Vserver Setup wizard has the following subwizards, which you can run after you create a Vserver:

- Network setup
- Storage setup
- Services setup
- Data access protocol setup

Each subwizard has its specific requirements, depending on the types of services, protocols, and the protocol traffic.

You can use the following worksheet to record values for the setup process:

Vserver information

Types of information	Your values
Vserver name The name of a Vserver can contain alphanumeric characters and the following special characters: ".", "-", and "_". However, the name of a Vserver should not start with a number or the following special characters: "." and "-". The maximum number of characters allowed in a Vserver name is 47. **Note:** Vserver names must be unique. You must use the fully qualified domain name (FQDN) of the Vserver or another convention that ensures unique Vserver names.	
Data protocols Protocols that you want to configure or allow on that Vserver	
Client services Services that you want to configure on the Vserver	

Types of information	Your values
Aggregate name Aggregate on which you want to create the Vserver's root volume. The default aggregate name is used if you do not specify one.	
Language setting The default language 'C.UTF-8 ' is used if you do not specify one. The language is set for a Vserver. The language of the Vserver determines default language setting for volumes in that Vserver. **Note:** The language of a Vserver is inherited by its volumes if the language is not specified when creating the volumes. For all the available language options and Vserver language configurations, see *list of language options* on page 97 and *Vserver language configurations* on page 100.	
Vserver root volume's security style Determines the type of permissions that can be used to control data access to a volume For more information about the security styles, see the *Clustered Data ONTAP File Access and Protocols Management Guide*.	

Information for creating volumes on the Vserver

Types of information	Values
Volume name The default volume name is used if you do not specify one.	
Aggregate name Aggregate on which you want to create the volume. The default aggregate name is used if you do not specify one.	
Volume size	

Types of information	Values
Volume junction path The default junction path is used if you do not specify one.	

Information for creating an IP network interface on the Vserver

Types of information	Values
LIF name The default LIF name is used if you do not specify one.	
Protocols Protocols that can use the LIF **Note:** Protocols that can use the LIF cannot be modified after the LIF is created.	
Home node Home node is the node on which you want to create a LIF. The default home node is used if you do not specify one.	
Home port Home port is the port on which you want to create a LIF. The default home port is used if you do not specify one.	
IP address	
Network mask	
Default gateway IP address	

Information for creating an FC network interface on the Vserver

Types of information	Values
LIF name The default LIF name is used if you do not specify one.	

Types of information	Values
Protocols Protocols that can use the LIF **Note:** Protocols that can use the LIF cannot be modified after the LIF is created.	
Home node Home node is the node on which you want to create a LIF. The default home node is used if you do not specify one.	
Home port Home port is the port on which you want to create a LIF. The default home port is used if you do not specify one.	

Information for configuring LDAP

Types of information	Values
LDAP server IP address	
LDAP server port number The default LDAP server port number is used if you do not specify one.	
LDAP server minimum bind authentication level	
Bind domain name and *password*	
Base domain name	

Information for configuring NIS

Types of information	Values
NIS domain name	
IP addresses of the NIS servers	

Information for configuring DNS

Types of information	Values
DNS domain name	

Types of information	Values
IP addresses of the DNS servers	

Note: You do not need to enter any information to configure NFS on a Vserver. The NFS configuration is created when you specify the protocol value as `nfs`.

Information for configuring CIFS protocol

Types of information	Values
Domain name	
CIFS share name The default CIFS share name is used if you do not specify one. **Note:** You must not use space characters or Unicode characters in CIFS share names. You can use alphanumeric characters and any of the following special characters: ! @ # $ % & ( ) _ ' { } . ~ -.	
CIFS share path The default CIFS share path is used if you do not specify one.	
CIFS access control list The default CIFS access control list is used if you do not specify one.	

Information for configuring iSCSI protocol

Types of information	Values
igroup name The default igroup name is used if you do not specify one.	
Names of the initiators	
Operating system type of the initiator	
LUN name The default LUN name is used if you do not specify one.	

Types of information	Values
Volume for LUN Volume that is to be used for the LUN	
LUN size	

Information for configuring Fibre Channel (FC) protocol (FCoE included)

Types of information	Values
igroup name The default igroup name is used if you do not specify one.	
World wide port number (WWPN) of the initiators	
Operating system type of the initiator	
LUN name The default LUN name is used if you do not specify one.	
Volume for LUN Volume that is to be used for the LUN	
LUN size	

Creating a Vserver by using the CLI wizard

You can create and configure Vservers with FlexVol volumes fully to start serving data immediately or with minimal configuration to delegate administration to the Vserver administrator by using the `vserver setup` command.

Before you begin

You must have understood the *requirements and gathered the required information* on page 101 before you start the Vserver Setup wizard or any of the subwizards.

About this task

By using the `vserver setup` command, which launches a CLI wizard, you can perform the following tasks:

- Creating and configuring a Vserver fully
- Creating and configuring a Vserver with minimal network configuration

- Configuring existing Vservers
  - Setting up a network interface
  - Provisioning storage by creating volumes
  - Configuring services
  - Configuring protocols

    Note: When you select NDMP as one of the protocols for protocol configuration, NDMP is added to the allowed list of protocols of the Vserver. The Vserver setup wizard does not configure the NDMP protocol.

Steps

1. Depending on your requirements, enter the appropriate command:

If you want to...	Enter the following command...

Set up a Vserver by using the Vserver Setup wizard	**`vserver setup`**
	The `vserver setup` command prompts you to create and configure a Vserver in the following sequence:
	a. Create a Vserver
	b. Create data volumes
	c. Create logical interfaces
	d. Configure services
	e. Configure protocols
	The following example shows how to set up a Vserver by using the Vserver Setup wizard:
	`cluster1::>vserver setup`
	`Welcome to the Vserver Setup Wizard, which will lead you through`
	`the steps to create a virtual storage server that serves data to clients.`
	
	`You can enter the following commands at any time:`
	`"help" or "?" if you want to have a question clarified,`
	`"back" if you want to change your answers to previous questions, and`
	`"exit" if you want to quit the Vserver Setup Wizard. Any changes`
	`you made before typing "exit" will be applied.`
	
	`You can restart the Vserver Setup Wizard by typing "vserver setup". To accept a default`
	`or omit a question, do not enter a value.`
	
	`Vserver Setup wizard creates and configures only data Vservers.`
	`If you want to create a Vserver with Infinite Volume use the vserver create command.`
	
	`Step 1. Create a Vserver.`
	`You can type "back", "exit", or "help" at any question.`
	`.....`
	`Enter the Vserver name: vs2.example.com`
	`.....`

If you want to...	Enter the following command...

Set up a network interface for an existing Vserver	**vserver setup -vserver *vserver_name* -network true**
	vserver_name is the name of the Vserver.
	The following example shows how to set up a network interface by using the Vserver Setup wizard:
	`cluster1::> vserver setup -vserver vs2.example.com -network true`
	`Welcome to the Vserver Setup Wizard, which will lead you through the steps to create a virtual storage server that serves data to clients.`
	`.....`
	`Step 1. Create a Vserver.`
	`You can type "back", "exit", or "help" at any question.`
	`Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi, ndmp}`
	`[nfs,cifs,fcp,iscsi,ndmp]:`
	`Choose the Vserver client services to be configured {ldap, nis, dns}:`
	`Vserver vs2.example.com's allowed protocol list has been modified to nfs,cifs,fcp,iscsi,ndmp`
	`Step 2: Create a logical interface.`
	`You can type "back", "exit", or "help" at any question.`
	`Do you want to create a logical interface? {yes, no} [yes]:`
	`.....`

If you want to...	Enter the following command...

Provision storage by creating volumes on an existing Vserver	**`vserver setup -vserver` *`vserver_name`* `-storage true`**
	`vserver_name` is the name of the Vserver.
	The following example shows how to create volumes by using the Vserver Setup wizard:
	`cluster1::> vserver setup -vserver vs2.example.com -storage true`
	`Welcome to the Vserver Setup Wizard, which will lead you through`
	`the steps to create a virtual storage server that serves data to clients.`
	`.....`
	`Step 1. Create a Vserver.`
	`You can type "back", "exit", or "help" at any question.`
	`Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi, ndmp}`
	`[nfs,cifs,fcp,iscsi,ndmp]:`
	`Choose the Vserver client services to be configured {ldap, nis, dns}:`
	`Vserver vs2.example.com's allowed protocol list has been modified to nfs,cifs,fcp,iscsi,ndmp`
	`Step 2: Create a data volume`
	`You can type "back", "exit", or "help" at any question.`
	`Do you want to create a data volume? {yes, no} [yes]:`
	`.....`
	Note: You cannot set up IPv6 network interface by using the Vserver setup wizard.

If you want to...	Enter the following command...

Configure services for an existing Vserver	If you want to configure your Vserver to use `ldap` or `nis` as the name service (`-ns-switch`), you should also include `file` as a name service. Including `file` as a name service enables the Vserver user account authentication through the Vserver's local administrative repository.
	`vserver setup -vserver vserver_name -services ldap,nis,dns`
	`vserver_name` is the name of the Vserver.
	The following example shows how to configure services by using the Vserver Setup wizard:
	`cluster1::> vserver setup -vserver vs2.example.com -services ldap`
	
	`Welcome to the Vserver Setup Wizard, which will lead you through`
	`the steps to create a virtual storage server that serves data to clients.`
	
	`.....`
	
	`Step 1. Create a Vserver.`
	`You can type "back", "exit", or "help" at any question.`
	
	`Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi, ndmp}`
	`[nfs,cifs,fcp,iscsi,ndmp]:`
	`Choose the Vserver client services to be configured {ldap, nis, dns}:`
	
	`Vserver vs2.example.com's allowed protocol list has been modified to nfs,cifs,fcp,iscsi,ndmp`
	
	`Step 2: Configure LDAP (Lightweight Directory Access Protocol).`
	`You can type "back", "exit", or "help" at any question.`
	
	`Do you want to configure LDAP? {yes, no} [yes]:`
	`.....`

If you want to...	Enter the following command...

Configure protocols for an existing Vserver	You must have created LIFs for the protocols.
	`vserver setup -vserver vserver_name -protocols nfs,cifs,iscsi,fcp, ndmp`
	`vserver_name` is the name of the Vserver.
	Note: When you specify the protocols value as `fcp`, you can configure both FC and FCoE for a Vserver.
	The following example shows how to configure protocols by using the Vserver Setup wizard:
	`cluster1::> vserver setup -vserver vs2.example.com -protocols iscsi`
	`Welcome to the Vserver Setup Wizard, which will lead you through the steps to create a virtual storage server that serves data to clients.`
	`.....`
	`Step 1. Create a Vserver.`
	`You can type "back", "exit", or "help" at any question.`
	`Choose the Vserver client services to be configured {ldap, nis, dns}:`
	`Vserver vs2.example.com's allowed protocol list has been modified to nfs,cifs,fcp,iscsi,ndmp`
	`Step 2: Configure iSCSI.`
	`You can type "back", "exit", or "help" at any question.`
	`Do you want to configure iSCSI? {yes, no} [yes]:`
	`.....`

2. Follow the prompts to complete the Setup wizard:
   - To accept the default value for a prompt, press Enter.
   - To enter your own value for the prompt, enter the value and then press Enter.
3. Use the `vserver show` command to verify the newly created Vserver.

   You can view the attributes of the Vserver in detail by using the `vserver show -instance` command.

Example

The following example shows how to display information about all existing Vservers:

```
cluster1::>vserver show
                     Admin     Root                  Name    Name
Vserver          Type    State     Volume     Aggregate  Service Mapping
-----------      ------- --------- ---------- ---------- ------- -------
vs1.example.com   data   running   root_vol1   aggr1      file    file
cluster1          admin   -         -          -          -       -
cluster1-01       node    -         -          -          -       -
cluster1-02       node    -         -          -          -       -
```

```
vs2.example.com    data    running    root_vol2    aggr2       file     file
5 entries were displayed.
```

Result

When a Vserver is created, its root volume of 1 GB size is created. When you set up a Vserver, it is started automatically and is in running state. By default, the vsadmin user account is created and is in the locked state. The vsadmin role is assigned to the default vsadmin user account.

After you finish

To delegate the administration to a Vserver administrator, you must set up a password, unlock the vsadmin user account, and create a LIF for accessing and enable the firewall policy for managing the Vserver.

If you want to change the role of the default user vsadmin, you must set the password for vsadmin user before changing the role.

For Vservers with FlexVol volumes, it is best to create a load-sharing mirror copy for the root volume on each node of the cluster so that the namespace directory information remains available in the event of a node outage or failover. For more information about creating load-sharing mirror copy, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Related tasks

Delegating administration to a Vserver administrator on page 119
Displaying information about Vservers on page 122

Related references

Commands for managing user accounts on page 138

Creating a Vserver by using the vserver create command

You can either create a Vserver with FlexVol volumes or a Vserver with Infinite Volume to serve data to the clients by using the `vserver create` command. A cluster can have one or more Vservers with FlexVol volumes and Vservers with Infinite Volumes.

Before you begin

- The cluster must have at least one non-root aggregate created by using the `aggr create` command.
- You must have at least 1 GB of space on the aggregate for the Vserver root volume.
- You must have synchronized the time across the cluster by configuring and enabling NTP to prevent CIFS creation and authentication failures.

About this task

To name a Vserver, you can use alphanumeric characters and the following special characters: ".", "-", and "_". However, the name of a Vserver should not start with a number or the following special characters: "." and "-". The maximum number of characters allowed in a Vserver name is 47.

Note: Vserver names must be unique. When creating a Vserver, you must use the fully qualified domain name (FQDN) of the Vserver or another convention that ensures unique Vserver names.

When you create a Vserver, the language is set for the Vserver and is inherited by all its volumes if the volumes are created without any language setting. The language of the Vserver determines the default language setting for volumes in that Vserver.

`Language` is an optional parameter of the `vserver create` command. If you do not use this parameter, the default value `C.UTF-8` (or `POSIX.UTF-8`) is used. For more information about the available language options and Vserver language configurations, see *list of language options* on page 97 and *Vserver language configurations* on page 100.

If you want to configure your Vserver to use `ldap` or `nis` as the name service (`-ns-switch`), you should also include `file` as a name service. Including `file` as a name service enables the Vserver user account authentication through the Vserver's local administrative repository.

Step

1. Depending on the type of volume that a Vserver should contain, perform the appropriate action:

If you want to…	Then…

Create a Vserver with FlexVol volume	Use the `vserver create` command with the `is-repository` parameter set to `false`.
	Note: If you do not use the `is-repository` parameter, then the default value `false` is used.
	The following example illustrates how to create a Vserver vs0.example.com with FlexVol volume:
	`cluster1::>vserver create -vserver vs0.example.com -rootvolume root_vs0 -aggregate aggr1 -ns-switch nis -rootvolume-security-style unix -language C.UTF-8`
	`[Job 2059] Job succeeded: Vserver creation completed`

If you want to…	Then…

Create a Vserver with Infinite Volume	Use the `vserver create` command with the `is-repository` parameter set to `true`.
	The following example illustrates how to create a Vserver vs1 with Infinite Volume:
	`cluster1::>vserver create -vserver vs1.example.com -rootvolume root_vs0 -aggregate aggr1 -ns-switch nis -rootvolume-security-style unix -language C.UTF-8 -snapshot-policy default -is-repository true`
	`[Job 2061] Job succeeded: Vserver creation completed`

For more information about this command, see the man pages.

Note: Vserver create operation might fail due to any intermediate operation failures such as volume creation failure. As a result, the Vserver will be in initializing state. It is best to delete such Vservers because you cannot perform other Vserver operations on that Vserver. For example, you cannot create a Vserver peering relationship with Vservers in initializing state.

Result

When a Vserver is created, its root volume of size 1 GB is created.

The Vserver root volume does not contain any of the configuration information of the Vserver. Optionally, the Vserver root volume can also contain user data. However, it is best not to store user data in the root volume.

When you create a Vserver, it is started automatically and is in running state. By default, the vsadmin user account is created and is in the locked state. The vsadmin role is assigned to the default vsadmin user account.

After you finish

- You must specify the aggregates for a Vserver for all the volume related operations that require aggregate name.
- To delegate the Vserver administration to a Vserver administrator, you must set up a password and unlock the vsadmin user account.
- If you want to change the role of the default user vsadmin, you must set the password for vsadmin user before changing the role.
- After you create a Vserver with FlexVol volume, you can either use the `vserver setup` command or the relevant protocols and services commands to configure the Vserver.
- For Vservers with FlexVol volumes, it is best to create a load-sharing mirror copy for the root volume on each node of the cluster so that the namespace directory information remains available

in the event of a node outage or failover. For more information about creating load-sharing mirror copy, see the *Clustered Data ONTAP Logical Storage Management Guide*.

- After you create a Vserver with Infinite Volume, you can use the relevant protocols and services commands to configure the Vserver. You must create an Infinite Volume for the Vserver with Infinite Volume. For more information about creating an Infinite Volume, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Related concepts

Managing the cluster time (cluster administrators only) on page 175

Related tasks

Delegating administration to a Vserver administrator on page 119
Creating a Vserver by using the CLI wizard on page 106
Displaying information about Vservers on page 122
Modifying a Vserver on page 118

Related references

Commands for managing user accounts on page 138

Considerations for modifying a Vserver

When modifying a Vserver, a cluster administrator must understand the significance of the Vserver attributes such as aggregate list and maximum number of volumes on the Vserver. If the attributes such as aggregate list is not set for a Vserver, a Vserver administrator cannot perform volume operations that require aggregate name on that Vserver.

Vservers with FlexVol volumes

You must be aware of the following attributes and their effects when modifying a Vserver with FlexVol volumes:

- Name Service Switch
- Name Mapping Switch
- Snapshot policy
- Quota policy
- Admin state
  You can set the admin state of the Vserver at the advanced privilege level if the operations such as starting or stopping a Vserver fails.
- QoS policy group
- Maximum number of volumes that can be created on the Vserver
  When the value is set to `unlimited`, which is the default value, any number of volumes can be created on that Vserver. If you specify the value as 0, then volumes cannot be created on that

Vserver. Therefore, you must specify a value so that the Vserver administrator can create volumes.

Note: This parameter is effective only when you specify the list of aggregates for a Vserver.

- Language
  A Vserver's language is set when it is created. `C.UTF-8` is the default language option. When you modify the Vserver's language, the language setting of the existing volumes does not change. When a new volume is created without specifying the language, it inherits the Vserver's language.
- List of the aggregates available to create volumes
  You must specify the aggregate names for a Vserver which allows a Vserver administrator to view the list of available aggregates to perform any provisioning operations that require an aggregate name, for example, creating a volume or a FlexClone. When you specify the aggregate names for a Vserver, you can perform the limited provisioning operations same as the Vserver administrator. However, you can move the volumes and copy the volumes across aggregates.
  If you do not specify the aggregate names for a Vserver, the Vserver administrator cannot perform any provisioning operations that require an aggregate name. As a cluster administrator, you can perform all the operations that require an aggregate name.
- Allowed protocols list
  When you specify the list of allowed protocols, the remaining protocols are added to the disallowed protocols list automatically. Only the allowed protocols can be configured to serve data from a Vserver.

  Note: Only the protocols that have been licensed on the cluster can be part of the allowed protocols.
- Disallowed protocols list
  The disallowed protocols are not available for configuration and cannot serve data. When you disallow the protocol, you cannot modify the state of the protocol.
  If you add NDMP to the disallowed protocols list, you cannot establish NDMP sessions.

For the detailed description of all the parameters, see the man pages.

Vserver with Infinite Volume

You must be aware of the following attributes and their effects when modifying a Vserver with Infinite Volume:

- Name Service Switch
- Name Mapping Switch
- Snapshot policy
- List of the aggregates available to create an Infinite Volume
  You must specify the aggregate names for the Vserver with Infinite Volume because the aggregates list determines the aggregates that are used by the Infinite Volume when created.
  If you do not specify any aggregates for a Vserver with Infinite Volume, then the Infinite Volume spans across all the aggregates in the cluster if created by the cluster administrator. However, a Vserver administrator sees the empty aggregate list and will not have enough aggregates to create the Infinite Volume.

- Admin state
  You can set the admin state of the Vserver at the advanced privilege level if the operations such as starting or stopping a Vserver fails.
- Allowed protocols list
  Only NFS and CIFS are allowed in the protocol list.
- Disallowed protocols list
- If NFS and CIFS are a part of the disallowed protocols list, then the Vserver with Infinite Volume cannot serve data.

Note: You cannot modify the language, quota policy, and maximum number of volumes of a Vserver with Infinite Volume.

Modifying a Vserver

You can modify a Vserver and its attributes such as maximum number of volumes, aggregate list, and allowed protocols by using the `vserver modify` command.

Before you begin

You must have understood the *various attributes* on page 116 that can be modified for Vserver with FlexVol volumes and Vserver with Infinite Volume and the significance of these attributes.

Steps

1. Use the `vserver modify` command to modify the attributes of a Vserver.

   #### Example

   The following example shows how to modify a Snapshot policy named daily, add the comment "Sales team access," modify the quota policy to pol1, and modify allowed protocols to nfs, cifs, and ndmp for a Vserver named vs8.example.com:

   ```
   cluster1::>vserver modify -vserver vs8.example.com -allowed-protocols
   nfs,cifs,ndmp -snapshot-policy daily
   -comment "Sales team access" -quota-policy pol1
   ```

   For more information about this command, see the man pages.
2. Use the `vserver show` command to verify the modified attributes of the Vserver.

   #### Example

   The following example shows how to display the detailed information of the Vserver vs8.example.com:

   ```
   cluster1::> vserver show -instance -vserver vs8.example.com
   ```

```
                                    Vserver: vs8.example.com
                                Vserver Type: data
                                Vserver UUID: 6f181736-33a5-11e2-
bbb6-123478563412
                                 Root Volume: root_vs0
                                                          .
                                             .
                             Snapshot Policy: daily
                                     Comment: Sales team access
                                Quota Policy: pol1
                                             .
                                             .
                           Allowed Protocols: nfs, cifs, ndmp
                        Disallowed Protocols: fcp, iscsi
              Is Vserver with Infinite Volume: false
                            QoS Policy Group: -
```

Related tasks

Displaying information about Vservers on page 122

Delegating administration to a Vserver administrator

After setting up a functional Vserver or a Vserver with basic network configuration, you can optionally delegate the administration of the Vserver to a Vserver administrator. You can delegate Vserver administration by creating and assigning user accounts either with predefined roles or customized roles.

Before you begin

If you want to delegate the Vserver administration with any customized roles, you must have created customized roles by using the `security login role create` command.

Steps

1. Optional: Use the `vserver show -fields aggr-list` command to verify if the Vserver has any aggregates assigned.

   Note: If no aggregates are assigned to the Vserver, the Vserver administrator cannot create volumes.

2. Optional: If the Vserver does not have any assigned aggregates, use the `vserver modify` command to specify aggregates in the aggregates list of a Vserver.

   Example

   The following example shows how to specify the aggregates aggr1 and aggr2 for Vserver vs1.example.com:

   `vserver modify -vserver vs1.example.com -aggr-list aggr1,aggr2`

3. Optional: Only for a Vserver with FlexVol volume, use the `vserver modify` command with the `max-volumes` option to specify the maximum number of volumes that a Vserver administrator can create on that Vserver.

   Example

   The following example shows how to specify the maximum number of volumes for a Vserver vs1.example.com:

   ```
   vserver modify -vserver vs1.example.com -max-volumes 10
   ```

4. Use the `vserver modify` command to allow or disallow protocols for a Vserver.

   Example

   The following example shows how to disallow protocols for a Vserver vs1.example.com:

   ```
   vserver modify -vserver vs1.example.com -disallowed-protocols ndmp
   ```

   Only the allowed protocols are available for configuration and data access.

5. Depending on the type of protocols, enter the appropriate command to create a management LIF for a Vserver:

If you want to...	Then...
Create a new LIF for Vserver management	Use the `network interface create` command. **Note:** A dedicated Vserver management LIF is required for SAN protocols, where data and management protocols cannot share the same LIF. A Vserver management LIF can be created only on data ports. You can use the `network port show` command to determine the data ports. The following example shows how to create a data LIF lif3 for Vserver vs1.example.com to support vserver management: `network interface create -vserver vs1.example.com -lif lif3 -data-protocol none -role data -home-node node1-01 -home-port e0c -address 192.0.2.129 -netmask 255.255.255.128`
Use a LIF for NFS, CIFS, and Vserver management	Change the firewall policy to `mgmt` by using the `network interface modify` command. The following example shows how to modify a data LIF lif1 for Vserver vs1.example.com to support Vserver management: `network interface modify -vserver vs1.example.com -lif lif1 -firewall-policy mgmt`

6. Depending on the type of Vserver administrator roles, perform the appropriate action:

If you want to use...	Then...

vsadmin, a predefined role that is created and is in the locked state when a Vserver is created.	You must set up a password and unlock the user account to delegate the Vserver administration.
	a. Use the `security login password` command to set up a password
	a. Enter a password for the user account.
	b. Reenter the password to confirm.
	The following example shows how to set up a password for the user account vsadmin on Vserver vs1.example.com:
	`cluster1::>security login password -username vsadmin -vserver vs1.example.com`
	`Please enter a password for user 'vsadmin':`
	`Please enter it again:`
	`cluster1::>`
	b. Use the `security login unlock` command to unlock the user account.
	The following example shows how to unlock the user account vsadmin for Vserver vs1.example.com:
	`security login unlock -username vsadmin -vserver vs1.example.com`

Any customized role or other predefined roles, such as vsadmin-volume, vsadmin-protocol, or vsadmin-readonly	**a.** Use the `security login create` command to create a user account with a role.
	a. Enter a password for the user account.
	b. Reenter the password to confirm.
	The following example shows how to create user account vsadmin-monitor with vsadmin-readonly role for Vserver vs1.example.com:
	`cluster1::> security login create -username user1 -application ssh -authmethod password -vserver vs1.example.com -role vsadmin-readonly`
	`Please enter a password for user 'vsadmin-monitor':`
	`Please enter it again:`
	`cluster1::>`

For more information about these commands, see the man pages.

Result

After you assign a Vserver to a Vserver administrator, the Vserver administrator can log in to the Vserver by using the user name, password, and the management IP address.

Displaying information about Vservers

A cluster administrator can view the configuration information about one or more Vservers by using the `vserver show` command.

Step

1. Enter the appropriate command to view Vservers information:

If you want to...	Enter the following command...
View basic information about all the Vservers	**`vserver show`**
View detailed information about all the Vservers	**`vserver show -instance`**
View information about a Vserver	**`vserver show -vserver`** ***`Vserver_name`*** ***`Vserver_name`*** is the name of the Vserver.

For more information about this command, see the man pages.

The following example displays detailed information about all Vservers:

```
cluster1::>vserver show

                          Admin     Root                  Name    Name
Vserver          Type     State     Volume     Aggregate  Service Mapping
-----------     ------- --------- ---------- ---------- ------- -------
vs1.example.com  data     running   root_vol1   aggr1      file    file
cluster1         admin    -         -           -          -       -
cluster1-01      node     -         -           -          -       -
cluster1-02      node     -         -           -          -       -
vs2.example.com  data     running   root_vol2   aggr2      file    file
5 entries were displayed.

cluster1::> vserver show -instance

                  Vserver: vs1.example.com
                  Vserver Type: data
                  Vserver UUID: 49294a39-e762-11df-8768-123478563412
                  Root Volume: root_vol1
                  Aggregate: aggr1
                  .
                  .
                  Allowed Protocols: nfs
                  Disallowed Protocols: cifs, fcp, iscsi, ndmp

                  Vserver: cluster1
                  Vserver Type: admin
                  Vserver UUID: 00000000-0000-0000-0000-000000000000
                  Root Volume: -
                  Aggregate: -
                  .
                  .
                  Allowed Protocols: -
```

```
                  Disallowed Protocols: -


cluster1::> vserver show -vserver vs2.example.com

                  Vserver: vs1
                  Vserver Type: data
                  Vserver UUID: ca34e6b2-ddec-11df-b066-123478563412
                  Root Volume: root_vol2
                  .
                  .
                  Allowed Protocols: iscsi
                  Disallowed Protocols: nfs, cifs, fcp,
ndmp
```

Deleting a Vserver

You can delete Vservers that are no longer needed from the cluster by using the `vserver delete` command.

Before you begin

1. You must have deleted the Vserver peer relationship associated with the Vserver.
2. You must have disabled Snapshot copies, and DP and LS mirrors for all volumes.
3. If you are using LUNs, you must have unmapped the LUNs, taken them offline, and deleted them.
4. You must have deleted all the igroups that belong to the Vserver manually.
5. You must have unmounted all volumes on the Vserver, taken them offline, and deleted them including the root volume of the Vserver.
6. You must have deleted CIFS server.
7. You must have deleted any customized user accounts and roles associated with the Vserver.
8. You must have stopped the Vserver.

About this task

When you delete a Vserver, the following objects associated with the Vserver are also deleted automatically:

- LIFs, LIF failover groups, and LIF routing groups
- Export policies
- Sis policies

You cannot recover any Vserver related information after deleting a Vserver.

If you delete a Vserver that is configured to use Kerberos, or modify a Vserver to use a different service principal name (SPN), Vserver's original service principal name is not automatically deleted

or disabled from Kerberos realm. You must manually delete or disable the principal. You must have the Kerberos realm administrator's user name and password to delete or disable the principal.

If you need to move data from a first Vserver to a second Vserver before you delete the first Vserver, you can use SnapMirror commands. For more information about SnapMirror, see the *Clustered Data ONTAP Data Protection Guide*.

Step

1. Use the `vserver delete` command to delete a Vserver.

Example

The following example shows how to delete a Vserver named vs1.example.com:

```
cluster1::> vserver delete -vserver vs1.example.com
```

For more information about this command, see the man pages.

Note: Vserver delete operation might fail due to any intermediate operation failures. As a result, the Vserver will be in deleting state. It is best to delete such Vservers because you cannot perform other Vserver operations on that Vserver. For example, you cannot create a Vserver peering relationship with Vservers in deleting state.

Renaming a Vserver

You can rename a Vserver by using the `vserver rename` command. For example, you can rename a Vserver when you want the Vserver to have a unique name. You cannot rename a node or admin Vserver by using the `vserver rename` command.

Before you begin

The Vserver being renamed must not be in a Vserver peer relationship.

Steps

1. Use the `vserver rename` command to rename a Vserver.

Example

The following example shows how to rename a Vserver named vs1.example.com as vs2.example.com:

```
Cluster1::> vserver rename -vserver vs1.example.com -newname
vs2.example.com
```

For more information about this command, see the man pages.

2. Use the `vserver show` command to view the changes in the Vserver's name.

Administering a Vserver from the Vserver context

You can administer a Vserver and its resources from the context of a Vserver by using the `vserver context` command.

About this task

After you switch to the Vserver context, your capabilities will be same as that of the Vserver administrator. If you do not specify the user name while executing the `vserver context` command, then you will have capabilities same as that of the default Vserver administrator (vsadmin). If you specify the user name, then you will have capabilities same as that of the role of the user name.

If you want to switch from one Vserver to another, you must exit from the first Vserver.

Steps

1. Use the `vserver context` command to enter into the Vserver context.

Example

The following example shows how to switch the context from cluster to Vserver vs1.example.com:

```
cluster1::> vserver context -vserver vs1.example.com -username
vsadmin-volume

Info: Use 'exit' command to return.

vs1.example.com::>
```

For more information about `vserver context` command, see the man pages.

You can use a role of another Vserver administrator by specifying the `-username` option.

You are in the context of Vserver vs1. Your capabilities will be same as that of the vsadmin-volume role.

2. Enter the command you want to run from the Vserver context.

Example

The following example shows how to view the volumes that belong to the Vserver vs1.example.com from the Vserver vs1.example.com context:

```
vs1.example.com::> vol show
  (volume show)
Vserver          Volume     Aggregate    State      Type  Size  Available Used%
---------        ---------- ------------ ---------- ---- ----- ---------- -----
vs1.example.com   root_vol1  aggr3        online     RW   1GB    972.5MB    5%
vs1.example.com   vol1       aggr1        online     RW   20MB   18.88MB    5%
```

3. Type **`exit`** at the Vserver prompt to exit from the Vserver context.

Starting a Vserver

You can provide data access from a Vserver by starting the Vserver. You can start a Vserver by using the `vserver start` command.

About this task

When you start a Vserver, the protocols that were stopped either when the Vserver was stopped or stopped independently by issuing commands such as `vserver fcp stop`, will start serving data.

Step

1. Use the `vserver start` command to start a Vserver.

Example

The following example shows how to start the Vserver vs1.example.com:

```
cluster1::> vserver start -vserver vs1.example.com
[Job 71] Job succeeded: DONE

cluster1::> vserver show
                     Admin     Root                  Name    Name
Vserver           Type    State     Volume     Aggregate  Service Mapping
-----------       ------- --------- ---------- ---------- ------- -------
vs1.example.com   data    running   root_vol1   aggr1      file    file
cluster1          admin    -         -          -          -       -
cluster1-01       node     -         -          -          -       -
cluster1-02       node     -         -          -          -       -
```

For more information about `vserver start` command, see the man pages.

Result

Vserver is in `running` state and starts serving data to clients. When you start a Vserver with Infinite Volume, its data policy is automatically re-imported and its JSON format is checked. For more information about data policies and JSON requirements for data policies, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Related tasks

Displaying information about Vservers on page 122

Stopping a Vserver

You can stop a Vserver if you need to troubleshoot or delete the Vserver, or stop the data access from the Vserver by using the `vserver stop` command.

Before you begin

All clients connected to the Vserver must be disconnected.

Attention: If any clients are connected to a Vserver when you stop it, data loss might occur.

About this task

You cannot stop a Vserver during a storage failover (SFO) if the resources of that Vserver are part of the HA pair.

When you stop a Vserver, other operations such as SnapMirror data transfers continue to run as per the schedule.

Step

1. Use the `vserver stop` command to stop a Vserver.

Example

The following example shows how to stop the Vserver vs1.example.com:

```
cluster1::> vserver stop -vserver vs1.example.com

[Job 72] Job succeeded: DONE

cluster1::> vserver show
                               Admin     Root                  Name    Name
Vserver            Type        State     Volume     Aggregate  Service Mapping
-----------       ------- --------- ---------- ---------- ------- -------
vs1.example.com    data    stopped   root_vol1   aggr1      file    file
cluster1           admin    -         -          -          -       -
cluster1-01        node     -         -          -          -       -
cluster1-02        node     -         -          -          -       -
```

For more information about `vserver stop` command, see the man pages.

Result

Vserver is in `stopped` state and stops serving data to clients. A Vserver administrator cannot log in to the Vserver.

Related tasks

Displaying information about Vservers on page 122

Restoring a Vserver's root volume

If a Vserver's root volume becomes unavailable, clients cannot mount the root of the namespace. In such cases, you must restore the root volume by promoting another volume to facilitate data access to the clients.

About this task

When the Vserver root volumes becomes unavailable, you can restore the root volume by promoting another volume, which does not have other volumes junctioned to it.

For Vservers with FlexVol volumes, you can promote one of the following volumes as the root volume:

- Load-sharing mirror copy
- Data-protection mirror copy
- A new FlexVol volume

Note: If you want to restore the root volume of a Vserver with Infinite Volume, you must contact technical support.

Starting from clustered Data ONTAP 8.2, Vserver root volume is created with 1 GB size to prevent any failures when mounting any volume in the Vserver root volume due to lack of space or inodes. Therefore, if you are promoting a new FlexVol volume, it should be at least 1 GB in size.

Steps

1. Depending on the type of volume you select for promoting a root volume, perform the appropriate action:

If you want to promote...	Then...

A load-sharing mirror as the root volume of a Vserver	**a.** Use the `set -privilege advanced` command to set the privilege level to advanced.
	b. Use the `snapmirror promote` command to promote the load-sharing mirror copy as the root volume.
	c. Use the `vol show` command to verify the new root volume of the Vserver.
	The following example shows how to promote a load-sharing mirror copy vol_dstls as the root volume of the Vserver vs1.example.com:
	`cluster1::> set -privilege advanced`
	`Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support.`
	`Do you want to continue? {y|n}: y`
	`cluster1::*> snapmirror promote -destination-path vs1.example.com:vol_dstls`
	`Warning: Promote will delete the read-write volume cluster1://vs1.example.com/vol1 and replace it with cluster1://vs1.example.com/vol_dstls.`
	`Do you want to continue? {y|n}: y`
	`[Job 489] Job succeeded: SnapMirror: done`
	`cluster1::*> volume show -volume vol_dstls -instance`
	`Vserver Name: vs1.example.com`
	`Volume Name: vol_dstls`
	`.`
	`.`
	`Junction Path: /`
	`.`
	`Vserver Root Volume: true`
	`.`
	`.`
	You can use the `vol rename` command to rename the volume that was promoted as the root volume.

If you want to promote...	Then...

A data-protection mirror as the root volume of a Vserver	**a.** Use the `snapmirror break` command to break the SnapMirror relationship.
	b. Use the `set -privilege advanced` command to set the privilege level to advanced.
	c. Use the `volume make-vsroot` command to promote the data-protection mirror copy as the root volume.
	d. Use the `vol show` command to verify the new root volume of the Vserver.
	The following example shows how to promote a data-protection mirror copy vol_dstdp as the root volume of the Vserver vs1.example.com:
	`cluster1::`
	`> snapmirror break -destination-path vs1.example.com:vol_dstdp`
	`[Job 521] Job succeeded: SnapMirror Break Succeeded`
	`cluster1::> set -privilege advanced`
	`Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support.`
	`Do you want to continue? {y|n}: y`
	`cluster1::*> volume make-vsroot -volume vol_dstdp -vserver vs1.example.com`
	`[Job 522] Job succeeded: DONE`
	`cluster1::*> volume show -volume vol_dstdp -instance`
	`Vserver Name: vs1.example.com`
	`Volume Name: vol_dstdp`
	`.`
	`.`
	`Junction Path: /`
	`.`
	`Vserver Root Volume: true`
	`.`
	`.`
	You can use the `vol rename` command to rename the volume that was promoted as the root volume.

If you want to promote...	Then...

A new FlexVol volume	**a.** Use the `set -privilege advanced` command to set the privilege level to advanced.
	b. Use the `vol create` command to create a new FlexVol volume of 1 GB size.
	c. Use the `volume make-vsroot` command to promote the FlexVol volume as the root volume.
	d. Use the `vol show` command to verify the new root volume of the Vserver.
	The following example shows how to promote a FlexVol volume new_rootvol as the root volume of the Vserver vs1.example.com:
	`cluster1::> set -privilege advanced`
	`Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support.`
	`Do you want to continue? {y|n}:`
	`cluster1::*> vol create -vserver vs3 -volume new_rootvol -aggregate aggr0 -size 1GB`
	`(volume create)`
	`cluster1::*> volume make-vsroot -vserver vs1.example.com -volume new_rootvol`
	`cluster1::*> volume show -volume new_rootvol -instance`
	`Vserver Name: vs1.example.com`
	`Volume Name: new_rootvol`
	`.`
	`.`
	`Junction Path: /`
	`.`
	`Vserver Root Volume: true`
	`.`
	`.`

2. Use the `volume mount` command to remount the new root volume.

   For more information about these commands, see the man pages.

Result

When the new volume is promoted as the Vserver root volume, the other data volumes get associated with the new Vserver root volume.

Controlling and monitoring I/O performance to Vservers by using Storage QoS

You can control input/output (I/O) performance to Vservers with FlexVol volumes by assigning Vservers to Storage QoS policy groups. You might control I/O performance to ensure that workloads

achieve specific performance objectives or to throttle a workload that negatively impacts other workloads.

About this task

Policy groups enforce a maximum throughput limit (for example, 100 MB/s). You can create a policy group without specifying a maximum throughput, which enables you to monitor performance before you control the workload.

You can also assign FlexVol volumes, LUNs, and files to policy groups.

Note the following requirements about assigning a Vserver to a policy group:

- The Vserver must be the Vserver to which the policy group belongs.
  You specify the Vserver when you create the policy group.
- If you assign a Vserver to a policy group, you cannot also assign any storage objects contained by that Vserver to a policy group.

Note: Storage QoS is supported on clusters that have up to eight nodes.

Steps

1. Use the `qos policy-group create` command to create a policy group.

   #### Example

   The following command creates policy group pg-vs1 with a maximum throughput of 5,000 IOPS.

   ```
   cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
   throughput 5000iops
   ```

2. Use the `vserver modify` command with the `-qos-policy-group` parameter to assign a Vserver to a policy group.

   #### Example

   The following command assigns the Vserver vs1 to policy group pg-vs1.

   ```
   cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
   ```

3. Use the `qos statistics` commands to view performance data.

   #### Example

   The following command shows the performance of policy groups.

   ```
   cluster1::> qos statistics performance show
   Policy Group          IOPS      Throughput   Latency
   -------------------- -------- --------------- ----------
   ```

```
-total-                  12316       47.76MB/s  1264.00us
pg_app2                   7216       28.19MB/s   420.00us
pg_vs1                    5008       19.56MB/s     2.45ms
_System-Best-Effort         62       13.36KB/s     4.13ms
_System-Background          30           0KB/s        0ms
```

4. If necessary, use the `qos policy-group modify` command to adjust the policy group's maximum throughput limit.

Example

The following command modifies the maximum throughput for policy group pg-vs1 to 4,500 IOPS.

```
cluster1::> qos policy-group modify pg-vs1 -max-throughput 4500iops
```

Related concepts

Example: Proactively setting a limit on workloads in a shared storage infrastructure on page 255
Managing workload performance by using Storage QoS on page 244

Managing access to the cluster (cluster administrators only)

You can control access to the cluster and enhance security by managing user accounts, access-control roles and their password rules, firewall service and policies, public keys, digital certificates, web services, and audit settings.

Managing user accounts

You can create, modify, lock, unlock, or delete a cluster or Vserver user account, reset a user's password, or display information for all user accounts.

You can manage cluster or Vserver user accounts in the following ways:

- Creating a login method for a user by specifying the user's account name, associated Vserver, the access method, and the authentication method

  You can optionally specify the access-control role the user is assigned and add a comment about the user account.

  The maximum number of cluster user accounts you can create is 100. This limit includes the Active Directory domain user accounts that are added to the cluster. There is no limit to the number of Vserver user accounts you can create for a Vserver.
- Displaying users' login information, such as the account name, allowed access method, authentication method, access-control role, account comment, and account status
- Displaying information about SNMP users, including the account name, the associated Vserver, authentication method, hexadecimal engine ID, authentication protocol, privacy protocol, and security group
- Modifying the access-control role that is associated with a user’s login method

  It is best to use a single role for all access and authentication methods of a user account.
- Deleting a user's login method, such as the access method or the authentication method
- Changing the password for a user account
- Locking a user account to prevent the user from accessing the system
- Unlocking a previously locked user account to enable the user to access the system again

You use the `security login` commands to manage user accounts. You use the `security snmpusers` command to display information about SNMP users. For more information about these commands, see the appropriate man pages.

Note: The system prevents you from creating or using accounts with names that are reserved for the system (such as “root” and “naroot”.) You cannot use a system-reserved name to access the cluster, a Vserver, the SP, or the RLM.

Related concepts

Managing rule settings for user names and passwords in an access-control role on page 147

Related tasks

Customizing an access-control role to restrict user access to specific commands on page 145

Access methods for user accounts

Data ONTAP provides several methods that you can use to specify how a user account can access the storage system.

You use the `-application` parameter of the `security login` commands to specify the method that a user can use to access the storage system. The supported access methods include the following:

- System console (`console`)
- HTTP or HTTPS (`http`)
- Data ONTAP API (`ontapi`)
- RSH (`rsh`)
  RSH is disabled by default.
- The SP or RLM (`service-processor`)
- SNMP (`snmp`)
- SSH (`ssh`)
- Telnet (`telnet`)
  Telnet is disabled by default.

Vserver user accounts cannot use `console`, `rsh`, `service-processor`, or `telnet` as an access method.

If a firewall is enabled, the access method you use must also be added in the firewall policy to allow the access requests to go through the firewall. The `system services firewall policy show` command displays firewall policies. For more information, see the `system services firewall policy` man pages.

Related concepts

Accessing the cluster by using the CLI (cluster administrators only) on page 11

Related references

Commands for managing user accounts on page 138

Authentication methods for user accounts

Data ONTAP provides several methods that you can use to specify how a user account is authenticated.

The `-authmethod` parameter of the `security login` commands specifies how a user account is authenticated. The following authentication methods are supported:

- SSL certificate authentication (`cert`)
- SNMP community strings (`community`)
- Windows Active Directory authentication (`domain`)

  For Windows Active Directory authentication, a CIFS server must be created for the Vserver, and Windows domain users must be mapped to access-control roles by using the `security login create` command with the `-authmethod` parameter set to `domain`.

  In addition, to authenticate Windows Active Directory domain users for cluster access, a tunnel must be set up through a CIFS-enabled Vserver.
- LDAP or NIS authentication (`nsswitch`)

  To use LDAP or NIS authentication, Vserver users must be mapped to Vserver access-control roles by using the `security login create` command with the `-authmethod` parameter set to `nsswitch`. Data ONTAP supports only the RFC 2307 schema for LDAP authentication of Vserver accounts. It does not support any other schemas, such as Active Directory Identity Management for UNIX (AD-IDMU) and Active Directory Services for UNIX (AD-SFU).

  Cluster user accounts cannot use `nsswitch` as an authentication method.
- User password (`password`)
- SSH public key authentication (`publickey`)
- SNMP user-based security model (`usm`)

For more information about the `security login` commands, see the appropriate man pages.

Related references

Commands for managing user accounts on page 138

Authentication behavior when methods include both public key and password

When a user uses SSH to access the cluster or Vserver and the user account is configured with both the `publickey` and `password` authentication methods (the `-authmethod` parameter of the `security login` commands), the user is authenticated first with the public key.

If the public key authentication fails, the following occurs:

- Data ONTAP prompts the user to enter a password for authentication.
- If the password expiration functionality (the `-passwd-expiry-time` parameter of the `security login role config modify` command) is enabled and the user password has expired, Data ONTAP prompts the user to change the password before allowing the user to access the account.

Enabling Active Directory domain users to access the cluster

To enable Active Directory domain users to access the cluster, you must set up an authentication tunnel through a CIFS-enabled Vserver. You must also create cluster user accounts for the domain users. This functionality requires that CIFS is licensed on the cluster.

Steps

1. If a tunnel for authenticating Active Directory domain users' cluster access does not exist, complete the following steps:

   Note: The `security login domain-tunnel show` command displays the authentication tunnel if it has been set up.

   a) Create a CIFS server for a Vserver that you will use as an authentication tunnel by using the `vserver cifs create` command.

      You can use any data Vserver that has a CIFS server created as an authentication tunnel.

      For information about CIFS servers, see the *Clustered Data ONTAP File Access and Protocols Management Guide*.

   b) Specify the authentication tunnel by using the `security login domain-tunnel create` command.

      You can specify only one authentication tunnel.

2. Create a cluster user account to enable an Active Directory domain user to access the cluster by using the `security login create` command with the `–authmethod` parameter set to `domain`.

   Domain authentication supports only `ssh`, `ontapi`, and `http` for the `-application` parameter.

   The value of `-username` must be specified in the format of *`domainname`*`\`*`username`*, where *`domainname`* is the name of the CIFS domain server.

   If you delete the authentication tunnel, subsequent login sessions cannot be authenticated, and Active Directory domain users cannot access the cluster. Open sessions that were authenticated prior to the deletion of the authentication tunnel remain unaffected.

Example of enabling an Active Directory domain user to access the cluster

The following commands create a CIFS server for the vs0 Vserver, specify vs0 as the tunnel for Active Directory domain authentication, and create a cluster user account to enable the Administrator user of the DOMAIN1 domain to access the cluster through SSH:

```
cluster1::> vserver cifs create -vserver vs0 -cifs-server vs0cifs
-domain companyname.example.com
cluster1::> security login domain-tunnel create -vserver vs0
```

```
cluster1::> security login create -vserver cluster1 -username
DOMAIN1\Administrator -application ssh -authmethod domain
```

Commands for managing user accounts

You use the `security login` and `security snmpusers` commands to manage user accounts.

If you want to...	Use this command...
Create a login method for a user	`security login create`
Display information about user accounts	`security login show`
Display information about SNMP users	`security snmpusers`
Modify the access-control role of a user's login method	`security login modify` **Note:** It is best to use a single role for all access and authentication methods of a user account.
Delete a user's login method	`security login delete`
Change a user password	`security login password`
Lock a user account	`security login lock` **Note:** Data ONTAP requires that at least one cluster user account with the "admin" role capability and the `console` application type remain unlocked.
Unlock a user account	`security login unlock`
Specify a CIFS-enabled Vserver that you want to use as the tunnel for authenticating Active Directory domain users' cluster access	`security login domain-tunnel create`
Modify the tunnel that is used for Active Directory domain user authentication	`security login domain-tunnel modify`
Display the tunnel that is used for Active Directory domain user authentication	`security login domain-tunnel show`
Delete the tunnel that is used for Active Directory domain user authentication	`security login domain-tunnel delete`

For more information, see the man pages.

Managing access-control roles

You can use an access-control role to control the level of access a user has to the system. In addition to using the predefined roles, you can create new access-control roles, modify them, delete them, or specify account restrictions for users of a role.

You can manage access-control roles in the following ways:

- Creating an access-control role and specifying the command or command directory that the role's users can access
- Controlling the level of access the role has for the command or command directory and specifying a query that applies to the command or command directory
- Modifying an access-control role's access to a command or command directory
- Displaying information about access-control roles, such as the role name, the command or command directory that a role can access, the access level, and the query
- Deleting an access-control role
- Restricting a user's access to only a specified set of commands
- Modifying an access-control role's account restrictions and settings for user names and passwords
- Displaying the current settings for the restrictions on an access-control role or user account
- Displaying Data ONTAP APIs and their corresponding CLI commands

You use the `security login role` and `security login role config` commands to manage access-control roles. For information about these commands, see the appropriate man pages.

Predefined roles for cluster administrators

Data ONTAP provides several predefined roles for cluster user accounts. You can also create additional roles.

The following table describes the Data ONTAP predefined roles and their levels of access to command directories:

This role...	**Has this level of access...**	**To the following command directory or directories...**
`admin`	`all`	All command directories (`DEFAULT`)
`autosupport`	`all`	• `set` • `system node autosupport`
	`none`	All other command directories (`DEFAULT`)

This role...	Has this level of access...	To the following command directory or directories...
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)

You can create additional roles by using the `security login role create` command.

Predefined roles for Vserver administrators

The five predefined roles for a Vserver administrator are: vsadmin, vsadmin-volume, vsadmin-protocol, vsadmin-backup, and vsadmin-readonly. In addition to these predefined roles, you can create customized Vserver administrator roles by assigning a set of capabilities.

A Vserver can have its own user and administration authentication domain. You can delegate the administration of a Vserver to a Vserver administrator after creating a Vserver and user accounts.

Note: A Vserver with Infinite Volume does not support quotas, qtrees, and LUNs. Therefore, a Vserver administrator cannot perform the tasks related to quotas, qtrees, and LUNs on a Vserver with Infinite Volume.

The following table lists the predefined roles for a Vserver administrator along with the respective capabilities:

Vserver Administrator Role Name	**Description**
vsadmin	This role is the super user role for a Vserver and is assigned by default. A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Managing volumes, quotas, qtrees, Snapshot copies, FlexCache volumes, and files • Managing LUNs • Configuring protocols: NFS, CIFS, iSCSI, and FC (FCoE included) • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface • Monitoring the health of a Vserver vsadmin role is assigned by default.
vsadmin-volume	A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Managing volumes, quotas, qtrees, Snapshot copies, FlexCache volumes, and files • Managing LUNs • Configuring protocols: NFS, CIFS, iSCSI, and FC (FCoE included) • Configuring services: DNS, LDAP, and NIS • Monitoring network interface • Monitoring the health of a Vserver

Vserver Administrator Role Name	Description
vsadmin-protocol	A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Configuring protocols: NFS, CIFS, iSCSI, and FC (FCoE included) • Configuring services: DNS, LDAP, and NIS • Managing LUNs • Monitoring network interface • Monitoring the health of a Vserver
vsadmin-backup	A Vserver administrator with this role has the following capabilities: • Managing NDMP operations • Making a restored volume as read-write • Viewing volumes and LUNs **Note:** A Vserver administrator with vsadmin-backup role cannot manage own user account local password and key information.
vsadmin-readonly	A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Monitoring the health of a Vserver • Monitoring network interface • Viewing volumes and LUNs • Viewing services and protocols

Considerations for customizing an access-control role

Data ONTAP provides predefined access-control roles for cluster and Vserver administrators. You can create additional access-control roles for the cluster or a Vserver and customize their access to certain commands or command directories. Several considerations apply when you customize a role for specific access needs.

Syntax considerations

- An access-control role must include one or more rules (specified by the `security login role create` command) that include the following elements:

  - Vserver name (`-vserver`)

    This is the name of the admin Vserver (the cluster) or data Vserver that the role belongs to.
  - Role name (`-role`)
  - Capability (`-cmddirname`)

    The capability is a command (*intrinsic* or *nonintrinsic*) or command directory for which you want to specify an access level for the role.

    In the context of customizing a role, an *intrinsic command* is any command that ends with `create`, `modify`, `delete`, or `show`. All other commands are called *nonintrinsic commands*.
  - Access level (`-access`)

    The access level can be `all`, `readonly`, or `none`.

    How you specify the access level depends on whether the granted capability is a command or a command directory, and if it is a command, whether the command is intrinsic or nonintrinsic.
- When you specify a role's access for a command directory, the access by default applies to all the subdirectories and all the commands in the directory and subdirectories:

If the capability you grant to a role is…	**And the access level you specify is…**	**Then the effect is…**
A command directory	`all`	The role can access the specified directory and its subdirectories (if any), and the role can execute all commands in the directory or subdirectories.
	`readonly`	The role has read-only access to the specified directory and its subdirectories (if any). This combination results in the role's access to only the `show` command in the specified directory and subdirectories. All other commands in the directory are not accessible to the role.
	`none`	The role has no access to the specified directory, its subdirectories, or commands.

  For example, the following command grants the "vol_role" role of the "vs1" Vserver `all` access to the `volume` directory, all its subdirectories, and the commands in the directory and subdirectories:

```
security login role create -vserver vs1 -role vol_role -cmddirname "volume" -
access all
```

- Subdirectory access, if specified, overrides parent directory access.

  If a parent directory has an access level and its subdirectory is specified with a different access level, the access level specified for the subdirectory overrides that of the parent directory.

For example, the following commands grant the “vol_role” role of the “vs1” Vserver `all` access to the commands in the `volume` directory and subdirectories, except for the `volume snapshot` subdirectory, to which the role is restricted to `readonly` access:

```
security login role create -vserver vs1 -role vol_role -cmddirname "volume" -
access all

security login role create -vserver vs1 -role vol_role -cmddirname "volume
snapshot" -access readonly
```

- The access level you can specify for a command depends on whether the command is intrinsic or nonintrinsic:

If the capability you grant to a role is…	**And the access level you specify is…**	**Then the effect is…**
An intrinsic command (a command ending with `create`, `modify`, `delete`, or `show`)	`all`	An invalid combination. You cannot specify an access level on an intrinsic command; you must specify the access level on the *directory* of an intrinsic command.
	`readonly`	
	`none`	
A nonintrinsic command	`all`	The role can execute the specified command.
	`readonly`	An invalid combination. You cannot grant `readonly` access at the command level; you must specify it at the *directory* level.
	`none`	The role has no access to the specified command.

For example, the following command enables the “ssl_role” role of the “vs1” Vserver to access the `security ssl show` command but no other commands in the `security ssl` directory:

```
security login role create -vserver vs1 -role ssl_role -cmddirname "security
ssl" -access readonly
```

In the following example, the first four commands use command directories to restrict the access of the “login_role” role of the “cluster1” cluster to the `security login show` intrinsic command, and the last two commands grant the role additional access to the `security login password` and `security login role show-ontapi` nonintrinsic commands. The role has no access to other commands in the `security login` directory:

```
security login role create -vserver cluster1 -role login_role -cmddirname
"security login" -access readonly

security login role create -vserver cluster1 -role login_role -cmddirname
"security login domain-tunnel" -access none

security login role create -vserver cluster1 -role login_role -cmddirname
```

```
"security login publickey" -access none

security login role create -vserver cluster1 -role login_role -cmddirname
"security login role" -access none

security login role create -vserver cluster1 -role login_role -cmddirname
"security login password" -access all

security login role create -vserver cluster1 -role login_role -cmddirname
"security login role show-ontapi" -access all
```

- For a customized role, the commands and command directories for which you do not specify an access level have the default level of `none`, and the role has no access to unspecified commands or command directories.

General considerations

- It is recommended that you grant a customized role `all` access to the `security login password` command to enable users of the role to modify their passwords.
  For example, the following command grants the “guest_role” role of the “vs1” Vserver the capability to modify account passwords:

```
security login role create -vserver vs1 -role guest_role -cmddirname "security
login password" -access all
```

- You cannot grant a Vserver role any access to a command or command directory that is available to only the cluster administrator.
  For example, you cannot grant a Vserver role the access to the `system license` directory or its commands, because the capability for managing licenses is available to only the cluster administrator. For information about whether the Vserver administrator has access to a specific command, see the man pages.

Related tasks

Customizing an access-control role to restrict user access to specific commands on page 145

Customizing an access-control role to restrict user access to specific commands

The cluster administrator can restrict a user's access to only specific commands by customizing an access-control role with specified commands and mapping the user account to the role.

Steps

1. Create a customized access-control role that is restricted to only the specified command or commands by using the `security login role create` command with the `-cmddirname` parameter.

   The `security login role show` command displays the commands that a role can access.
2. Create a login method for a user account and map it to the customized role by using the `security login create` command with the `-role` parameter.

Examples of customizing an access-control role to restrict user account access

The following example creates an access-control role named “vol_snapshot”, which has access to only the `volume snapshot` commands, and a vs1 Vserver user account named “snapshot_admin”, which is assigned the “vol_snapshot” role. The user has full access to the `volume snapshot` commands, as defined by the role. The user can use SSH to access the Vserver and a password for authentication.

```
cluster1::> security login role create -vserver vs1 -role vol_snapshot
-cmddirname "volume snapshot"

cluster1::> security login role show -vserver vs1 -role vol_snapshot
           Role          Command/                              Access
Vserver    Name          Directory                    Query Level
---------- ------------- --------- --------------------------- --------
vs1        vol_snapshot  DEFAULT                               none
vs1        vol_snapshot  volume snapshot                       all
2 entries were displayed.

cluster1::> security login create -vserver vs1 -username snapshot_admin
-application ssh -authmethod password -role vol_snapshot

Please enter a password for user 'snapshot_admin':
Please enter it again:

cluster1::>
```

The following example creates an access-control role name “sec_login_readonly”. The role is customized to have read-only access to the `security login` directory but no access to the `security login domain-tunnel`, `security login publickey`, or `security login role` subdirectories. As a result, the role can access only the `security login show` command. A cluster user account named “new_admin” is then created and assigned the “sec_login_readonly” role. The user can use the console to access the cluster and a password for authentication.

```
cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login" -access readonly

cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login domain-tunnel" -access none

cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login publickey" -access none

cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login role" -access none

cluster1::> security login role show -vserver cluster1 -role sec_login_readonly
  (security login role show)
           Role                Command/                        Access
Vserver    Name                Directory                 Query Level
---------- ------------------- --------- --------------------- --------
cluster1   sec_login_readonly  DEFAULT                         none
cluster1   sec_login_readonly  security login                  readonly
cluster1   sec_login_readonly  security login domain-tunnel    none
cluster1   sec_login_readonly  security login publickey        none
cluster1   sec_login_readonly  security login role             none
5 entries were displayed.

cluster1::> security login create -vserver cluster1 -username new_admin
-application console -authmethod password -role sec_login_readonly
```

```
Please enter a password for user 'new_admin':
Please enter it again:

cluster1::>
```

Related concepts

Managing user accounts on page 134
Considerations for customizing an access-control role on page 142

Related references

Commands for managing user accounts on page 138
Commands for managing access-control roles on page 149

Managing rule settings for user names and passwords in an access-control role

The default rules for user names and passwords apply to users of all access-control roles. You can modify the rule settings of user names and passwords for a specific role to enhance user account security.

Following are the default rules for user names:

- A user name must be at least three characters long.
- A user name can contain only letters, only numbers, or a combination of letters and numbers.

Following are the default rules for passwords:

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

To enhance user account security, you can use parameters of the `security login role config modify` command to modify the following settings of an access-control role:

- Rule settings for user names:
  - The required minimum length of a user name (`-username-minlength`)
  - Whether a mix of alphabetic and numeric characters is required in a user name (`-username-alphanum`)
- Rule settings for passwords:
  - The required minimum length of a password (`-passwd-minlength`)
  - Whether a mix of alphabetic and numeric characters is required in a password (`-passwd-alphanum`)
  - The required number of special characters in a password (`-passwd-min-special-chars`)

  - Whether users must change their passwords when logging in to their accounts for the first time (`-require-initial-passwd-update`)
    Users can make initial password changes only through SSH or serial-console connections.
  - The number of previous passwords that cannot be reused (`-disallowed-reuse`)
  - The minimum number of days that must pass between password changes (`-change-delay`)
  - The number of days after which a password expires (`-passwd-expiry-time`)
- Rule settings about invalid login attempts:
  - The number of invalid login attempts that triggers the account to be locked automatically (`-max-failed-login-attempts`)
    When the number of a user's invalid login attempts reaches the value specified by this parameter, the user's account is locked automatically.
    The `security login unlock` command unlocks a user account.
  - The number of days for which an account is locked if invalid login attempts reach the allowed maximum (`-lockout-duration`)

You can display the current settings for the rules by using the `security login role config show` command. For information about the `security login role config` commands and the default settings, see the man pages.

Related references

Commands for managing access-control roles on page 149

Considerations for password rule settings

Some password rule settings require that users of a role change their passwords. To enable users to change passwords, the user accounts must have a proper access method, and their role must have the privilege to run the password reset command.

Users of a role are required to change their passwords in either of the following situations:

- The role's password settings require that users change their passwords when logging into their accounts for the first time.
  This setting is defined by the `-require-initial-passwd-update` parameter of the `security login role config modify` command.
- The role is set up to have user passwords expire by a certain time.
  This setting is defined by the `-passwd-expiry-time` parameter of the `security login role config modify` command.

To enable users to change their passwords, the following conditions must be met:

- Users must be granted SSH or console access.
  Passwords can be changed by their account users only through SSH or console connections.
  The `-application` parameter of the `security login modify` command grants a user the specified access method.

  Note: Console access is not supported for Vserver user accounts.

- Users' role must have the privilege to run the command for changing password (the `security login password` command).

  The `-cmddirname` parameter of the `security login role modify` command grants a role the privilege to run a command or command directory.

Regardless of the settings of the `-require-initial-passwd-update` and `-passwd-expiry-time` parameters of the `security login role config modify` command, when the "diag" user enters the systemshell from the clustershell, the systemshell does not require or prompt the "diag" user to change the password.

Related concepts

Access methods for user accounts on page 135

Related tasks

Customizing an access-control role to restrict user access to specific commands on page 145

Commands for managing access-control roles

You use the `security login role` commands to control the level of access users in a role have to the system. You use the `security login role config` commands to manage rule settings of user names and passwords for a role to enhance user account security.

If you want to...	Use this command...
Create an access-control role and specify the command or command directory that the role can access	`security login role create`
Modify the command or command directory that an access-control role can access	`security login role modify`
Display information about access-control roles	`security login role show`
Display Data ONTAP APIs and their corresponding CLI commands	`security login role show-ontapi`
Delete an access-control role	`security login role delete`

If you want to...	Use this command...
Modify the following account restrictions and rule settings for an access-control role: • The required minimum length of a user name • Whether a mix of alphabetic and numeric characters is required in a user name • The required minimum length of a password • Whether a mix of alphabetic and numeric characters is required in a password • The required number of special characters in a password • Whether users must change their passwords when logging in to their accounts for the first time • The number of previous passwords that cannot be reused • The minimum number of days that must pass between password changes • The number of days after which a password expires • The number of invalid login attempts that triggers the account to be locked automatically • The number of days for which an account is locked if invalid login attempts reach the allowed maximum	`security login role config modify`
Display user account restrictions and rule settings	`security login role config show`

If you want to...	Use this command...
Reset the following settings to the system default, which is disabled: • The required number of special characters in a password • Whether users must change their passwords when logging in to their accounts for the first time • The number of days after which a password expires • The number of invalid login attempts that triggers the account to be locked automatically • The number of days for which an account is locked if invalid login attempts reach the allowed maximum	`security login role config reset`

For more information, see the man pages for the `security login role` and `security login role config` commands.

Managing firewall service and policies

Setting up a firewall enhances the security of the storage system and helps you prevent unauthorized access to the system. You can enable, configure, and display information about firewall service and policies.

Firewall policies can be used to control access to only management service protocols such as SSH, HTTP, HTTPS, Telnet, NTP, NDMP, or SNMP, and not data protocols such as NFS or CIFS.

You can manage firewall service and policies in the following ways:

- Enabling or disabling firewall service
  By default, firewall service is enabled.
- Displaying the current configuration about firewall service
- Creating a firewall policy with the specified policy name and network service and putting it into effect for a logical interface
- Creating a new firewall policy that is an exact copy of an existing policy but with a new policy name
- Displaying information about firewall policies
- Modifying the IP addresses and netmasks that are used by a firewall policy
- Changing a LIF's firewall policy
- Deleting a firewall policy that is not being used by a LIF

Starting from Data ONTAP 8.2, you can create firewall policies with IPv6 addresses. For more information about IPv6 addresses, see the *Clustered Data ONTAP Network Management Guide*.

You can use the `system services firewall`, `system services firewall policy`, and `network interface modify` commands to manage firewall. For information about these commands, see the appropriate man pages.

Creating a firewall policy and assigning it to a LIF

You can create a firewall policy by specifying a policy name, a network service, and one or more IP addresses with their corresponding netmasks. After the policy is created, you can assign the firewall policy to a LIF.

About this task

- You cannot create a firewall policy with a `policy` value that is either `cluster`, `data`, `intercluster`, or `mgmt`.
  These values are defined for the system-defined firewall policies.
- If you want to change the service associated with a firewall policy, you must delete the existing firewall policy.
  After deleting the firewall policy, create a new firewall policy.
- If IPv6 is enabled on the cluster, you can create firewall policies with IPv6 addresses.
  Once IPv6 is enabled, `data` and `mgmt` firewall policies show ::/0 address (by default).

Steps

1. Use the `system-defined firewall policy show` command to view the information about firewall policies.

Example

The following example shows the system-defined firewall policies with both IPv4 and IPv6 addresses.

```
cluster1::> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
```

```
                    https      deny   0.0.0.0/0, ::/0
                    ndmp       allow  0.0.0.0/0, ::/0
                    ntp        deny   0.0.0.0/0, ::/0
                    rsh        deny   0.0.0.0/0, ::/0
                    snmp       deny   0.0.0.0/0, ::/0
                    ssh        deny   0.0.0.0/0, ::/0
                    telnet     deny   0.0.0.0/0, ::/0
intercluster
                    dns        deny   0.0.0.0/0
                    http       deny   0.0.0.0/0
                    https      deny   0.0.0.0/0
                    ndmp       allow  0.0.0.0/0
                    ntp        deny   0.0.0.0/0
                    rsh        deny   0.0.0.0/0
                    snmp       deny   0.0.0.0/0
                    ssh        deny   0.0.0.0/0
                    telnet     deny   0.0.0.0/0
mgmt
                    dns        allow  0.0.0.0/0, ::/0
                    http       allow  0.0.0.0/0, ::/0
                    https      allow  0.0.0.0/0, ::/0
                    ndmp       allow  0.0.0.0/0, ::/0
                    ntp        allow  0.0.0.0/0, ::/0
                    rsh        deny   0.0.0.0/0, ::/0
                    snmp       allow  0.0.0.0/0, ::/0
                    ssh        allow  0.0.0.0/0, ::/0
                    telnet     deny   0.0.0.0/0, ::/0
4 entries were displayed.
```

2. Use the `system services firewall policy create` command to create a firewall policy.

   Example

   The following example creates a policy named data_https that uses the HTTPS protocol and enables access from IP addresses on the 10.10 subnet:

   ```
   cluster1::> system services firewall policy create -policy data_https
   -service https -action allow -ip-list 10.10.0.0/16
   ```

3. Optional: Use the `system services firewall policy clone` command to create a firewall policy that is an exact copy of an existing policy, but has a new name.

   Example

   The following example demonstrates how you can create a new firewall policy named mgmt1 from an existing firewall policy named mgmt.

   ```
   cluster1::> firewall policy clone -policy mgmt -new-policy-name mgmt1
     (system services firewall policy clone)
   ```

4. Use the `network interface modify` command with the `-firewall-policy` parameter to assign the policy to a LIF.

Example

```
cluster1::> network interface modify -vserver vs1 -lif data1 -
firewall-policy data_https
```

For more information, see the `network interface modify` man page.

Commands for managing firewall service and policies

You can use the `system services firewall` commands to manage firewall service, the `system services firewall policy` commands to manage firewall policies, and the `network interface modify` command to manage firewall for a LIF.

If you want to...	Use this command...
Enable and configure firewall service	`system services firewall modify`
Display the current configuration for firewall service	`system services firewall show`
Create a firewall policy or add a service to an existing firewall policy	`system services firewall policy create`
Put a firewall policy into effect for a LIF	`network interface modify` **Note:** You use the `-firewall-policy` parameter to modify the firewall policy of a LIF.
Modify the IP addresses and netmasks used by a firewall policy	`system services firewall policy modify` **Note:** You cannot modify the default system-defined firewall policies
Display information about firewall policies	`system services firewall policy show`
Create a new firewall policy that is an exact copy of an existing policy	`system services firewall policy clone`
Delete a firewall policy that is not used by a logical interface	`system services firewall policy delete`

For more information, see the man pages for the `system services firewall`, `system services firewall policy`, and `network interface modify` commands.

Managing public keys

You can associate, modify, or delete a public key to manage a user's authentication.

You can manage public keys in the following ways:

- Adding a public key by associating an existing public key in a valid OpenSSH format with a user account

  Multiple public keys are allowed for a user account.
- Loading a public key from a universal resource identifier (URI), such as FTP or HTTP, and associating it with a user account

  You can also overwrite an existing public key with the one you are loading.
- Displaying information about public keys
- Modifying a public key that is associated with a specific user
- Deleting a public key that is associated with a specific user

To create or modify a public key or load a public key from a URI, your user account must be configured with the `publickey` login method (created by using the `security login create` command with the `-authmethod` parameter set to `publickey`).

You use the `security login publickey` commands to manage public keys. For information about these commands, see the appropriate man pages.

Commands for managing public keys

You use the `security login publickey` commands to manage public keys.

If you want to...	Use this command...
Associate an existing public key with a user account	`security login publickey create`
Load a public key from a URI and associate it with a user	`security login publickey load-from-uri`
Display information about public keys	`security login publickey show`
Modify a public key for a specific user	`security login publickey modify`
Delete a public key for a specific user	`security login publickey delete`

For more information, see the man pages for the `security login publickey` commands.

Managing digital certificates for server or client authentication

A digital certificate ensures that web communications are transmitted in encrypted form. It also ensures that information is sent privately and unaltered to only the specified server or from the authenticated client. Data ONTAP enables you to generate, install, and manage a self-signed or Certificate Authority (CA) signed digital certificate for server or client authentication.

The following facts apply to digital certificates (sometimes called public key certificates):

- A digital certificate is an electronic document that verifies the owner of a public key.
- A digital certificate can be either self signed (by owner) or CA signed.
  Which way to have a digital certificate signed depends on your security requirements and budget. You can obtain a self-signed digital certificate for free, but a digital certificate signed by a trusted CA can incur a considerable expense. A self-signed digital certificate is not as secure as a digital certificate signed by a CA. Therefore, it is not recommended in a production environment. A CA-signed digital certificate helps prevent man-in-the-middle attacks and provides better security protection than a self-signed digital certificate.
- By default, Data ONTAP uses the SHA256 cryptographic hashing function for signing a CSR or digital certificate, and the SHA1 and MD5 cryptographic hashing functions are also supported. Private keys generated by Data ONTAP are 2048-bit by default. Data ONTAP also enables you to generate a 512-bit, 1024-bit, or 1536-bit private key. However, the higher the value, the more secure the key is.

You can manage digital certificates in the following ways:

- Creating a self-signed or CA-signed digital certificate
  To obtain a self-signed digital certificate, you simply create one on the cluster or a Vserver. Data ONTAP automatically creates a self-signed digital certificate for server authentication of a Vserver when you create that Vserver.
  To obtain a CA-signed digital certificate, you generate a digital certificate signing request (CSR), which contains a private key and information that identifies you as the applicant. You then send the CSR to a CA electronically to apply for a digital certificate. After the CA sends you the signed digital certificate, you install it with the associated private key on the cluster or Vserver.
- Create a self-signed root CA digital certificate and self-signed digital certificates for clients to mutually authenticate the server and clients
- Display information about the installed digital certificates
- Revoke a compromised CA-issued digital certificate
- Delete self-signed or CA-signed digital certificates
  Before reverting to a release earlier than Data ONTAP 8.2, all digital certificates except for the server type (`security certificate show –type server`) must be deleted. Otherwise, the revert procedure fails.

You use the `security certificate` commands to manage digital certificates. For information about these commands, see the man pages.

Related tasks

Configuring access to web services on page 169

Generating and installing a CA-signed digital certificate for server authentication

You can generate and install a CA-signed digital certificate for server authentication. A CA-signed digital certificate helps prevent man-in-the-middle attacks and provides better security protection than a self-signed digital certificate.

Steps

1. If you do not already have a certificate signed by a CA, complete the following steps to obtain a CA-signed digital certificate:
   a) Generate a digital certificate signing request (CSR) by using the `security certificate generate-csr` command.

      The system displays the CSR output on the console. The output includes a certificate request and a private key.
   b) Copy the certificate request from the CSR output and send it in an electronic form (such as email) to a trusted 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 for future reference.

   For more information, see the `security certificate generate-csr` man page.
2. Install the CA-signed digital certificate by using the `security certificate install` command with the `-type server` parameter.

   For more information, see the `security certificate install` man page.
3. Enter the private key when the system prompts you to.

Examples of generating and installing a CA-signed digital certificate

The following command creates a CSR with a 2048-bit private key for use by the Software group in the IT department of a company whose custom common name is lab.companyname.com, located in Sunnyvale, California, USA. The email address of the contact administrator who manages the Vserver is web@companyname.com. The system displays the CSR and the private key on the console.

```
cluster1::> security certificate generate-csr -common-name
lab.companyname.com -size 2048 -country US -state CA
-locality Sunnyvale -organization IT -unit Software -email-addr
web@companyname.com

Certificate Signing Request:
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIICrjCCAZYCAQMwaTEQMA4GA1UEAxMHcnRwLmNvbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5DMQwwCgYDVQQHEwNSVFAxDTALBgNVBAoTBGNvcmUxDTALBgNVBAsT
BGNvcmUxDzANBgkqhkiG9w0BCQEWADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAK3azmz6UniwYDKVjA4iD3ImclAJ0sst3jPH2VqFwKbR9+srrC7l7yt8
1s3JMDBFZVXxv+GmBYWfOuzvMzajR2G7fg6/U2Z9XviXQo0m+FsqYt5H3ZEzhhK6
G8rIEqKPL9yY3RFxfVCwoRn7k/Q9IvKwj1vxywjKVYijN9o7l9Gl59jBvmAkKyH0
SXz6iIwGzC8so8jiUm6OQdU5viDNBxeo+tkHy12gKDEjy5TGnuOcVVQ56Cx0zYwG
cqg32elgMo3MFUFV+TtAVoPkBibC9AuZfrXfMBJW/IR4mDs+fQL0Q5becWzETCwu
9mY4kPt0YvyJiPXujMwG144giQMi6cUCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IB
kYz7hzkFpuMibAaCkp54Qrho
-----END CERTIFICATE REQUEST-----


Private Key:
-----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-----

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

The following command installs a CA-signed digital certificate for a Vserver named vs1:

```
cluster1::> security certificate install -vserver vs1 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
...
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
...
-----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
...
-----END CERTIFICATE-----


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

```
Note: You should keep a copy of your certificate and private key for future
reference.
If you revert to an earlier release, the certificate and private key are
deleted.
```

Installing a server intermediate certificate

You must install the intermediate certificate on the server if a certificate chain that begins at the trusted root CA, and ends with the SSL certificate issued to you, is missing the intermediate certificates.

About this task

An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, goes through the intermediate, and ends with the SSL certificate issued to you.

Step

1. Install the intermediate certificate by using the `security certificate install` command.

Providing mutual authentication

You can configure the server (which can be the cluster or a Vserver) to provide mutual authentication for greater security between the server and a group of clients.

About this task

When using mutual authentication, also called *two-way authentication*, both the server and the client present their certificates to each other and validate their respective identities to each other. To configure mutual authentication using a self-signed root CA certificate, you must create a self-signed root CA certificate, enable client authentication, generate and sign a certificate signing request (CSR) for each user, and install the client certificate on the client side. You must also set up user accounts for them to be authenticated by digital certificates.

You can also provide client authentication using a CSR signed by a third-party CA that is installed on the client and installing intermediate certificates of the CA that signed the certificate.

Steps

1. Create a self-signed root CA certificate for the server by using the `security certificate create` command.

Example

The following command creates a root CA certificate for Vserver vs1 for a software group in the IT department of a company whose custom common name is lab.companyname.com:

```
cluster1::> security certificate create -vserver vs1 -common-name
lab.companyname.com -type root-ca
```

2. Enable client authentication on the server by using the `security ssl modify` command and the `-client-enabled true` parameter.
3. Generate a CSR for a client by using the `security certificate generate-csr` command.

   You do this for every client that you need to authenticate.

Example

The following command generates a CSR whose custom common name is vs1admin:

```
cluster1::> security certificate generate-csr -common-name vs1admin

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIICojCCAYoCAQAwXTERMA8GA1UEAxMIdnMxYWRtaW4xCzAJBgNVBAYTAlVTMQkw
BwYDVQQIEwAxCTAHBgNVBAcTADEJMAcGA1UEChMAMQkwBwYDVQQLEwAxDzANBgkq
hkiG9w0BCQEWADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL6ohdT5
mMtVbZpH+iPPpkVzsv5vt5vztbBI1CC26Kc05U7vdooKhMw2OFuquyqEZHEmtsf2
Z+iEZasSq0G71ACbwFA4XFe25/TQM7/SRNY/+vtEWCFUeh6+kJwkUrI5Sw8QZ1d7
mbvFjYIaWyC/fED+KMcBbuxtB0LDpXjtxzGszhcr1l7/M++229YGsmglJ7GhuMAt
MUZcUTiYeqesoIQi4YCgMahJGr0oQZKr8uOtBs8LiNM8YHFP2xMXCH/BnV5WYSTD
Q0W4ettmBRIR+cmBesbNyL+AkQi+683+8d4mYmNjmFmEZLIpLHUV4heB8FaLO7cB
jpTcOADxeqagY5sCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQAnmw5U4llG20fz
ljcElizO2ET4HZxTnUU3YAcKpsmF6P6gB2nn28U1PWH8pHJamZGwoK4ZimNZGldY
AGmOHCbktamyPC2IzhqEmXC37DhV7XaDGp3dPSeTPnZiz8bFlypKLzcOX84y7J6g
Byvqhzl54eba7+DGMsk3429XviCVw6oE+Aq60VrV5Ij1YP+XMgjlQA7ZRdVKh3EG
iRrnDCXZILlUnj4u6d7XeahTSkxbyVW28HT9aYXjyESIrXYvbJGK19DT0VD2lG4K
/RLwcV5jihJ/AirrnfZ4lhcswx8n6YH0Ew6hwAef7raeOUhCU8GDq4dX3Umw/F28
mgFfsO2o
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvqiF1PmYy1Vtmkf6I8+mRXOy/m+3m/O1sEjUILbopzTlTu92
igqEzDY4W6q7KoRkcSa2x/Zn6IRlqxKrQbvUAJvAUDhcV7bn9NAzv9JE1j/6+0RY
IVR6Hr6QnCRSsjlLDxBnV3uZu8WNghpbIL98QP4oxwFu7G0HQsOleO3HMazOFyvW
Xv8z77bb1gayaCUnsaG4wC0xRlxROJh6p6yghCLhgKAxqEkavShBkqvy460GzwuI
0zxgcU/bExcIf8GdXlZhJMNDRbh622YFEhH5yYF6xs3Iv4CRCL7rzf7x3iZiY2OY
WYRksiksdRXiF4HwVos7twGOlNw4APF6pqBjmwIDAQABAoIBAQCt4NGVR0DDCBka
IFSPflv8cSUoCMjh8KSdrf3QDCAoBgSvNZLdF/S+rSA+8XkasH1N+Gmv+hgPpVd3
amJHY75YA7OjNZN553Sp/4uCgIiJAParW0wosXtiOJd332SP59J9XY9x6GZvKh8B
LXo4ZooyV9jmjXcVJeX+TKHHpMsKkCGWuDgNTU0rx5UMyrbMuvhnzl54jrb6CCte
3ZHqWH3FdtJmDaqyur30h4UpSlJZE4JrxcjIltQebBZZdYIN0O8oOLI6ZeuAi8ss
2tLEu/HmdbPiM9b/Mv5Q6ptwftS4SPveINvg8ziXXXySyX2TTbap2xZjMohlvApw
q0DJvBqJAoGBAPo6L/bP548TyU8xXXz/ko/4DQpTd/bWmhVq+Jj/8o2LfQwy2VFE
PvX9CvMuy+yPPSSk7vFfesVZ0gEolmS6xgNr3ZahxRVUR7ZcMnA6vKuYqqwY6Udc
AkFAOlRZGFvEcNXJN8I5ajZiGR1iYxfwg0ZlHy4tOsHQYk1jkWhKzCTNAoGBAMMO
hymam7aNbntQ9Myt2opiQ+vWPEyzdkLzn/1Ovy70Db9aaXHe6+fj0Rw0iAL91iVe
zERmcQypsj+BgXxPx1AMl1YsFBRleWdSlXdMPkN8RX7YjdSiy1ITPOlWWiLr61G/
NF9rJIs4cNdi9LbmgZ8arsvYoCM2mnWKSVxHCOoHAoGAMrRXw8udQIDh6go2x32C
```

```
VWoOOmlvhbU2w+BJP7edjtEVJcOoBa+ukmoULfLtn6Hm4eYKBR8z4Ymx5Eo1L3Qp
a8gPvtZI+Wl6nplQHy3HzX3CF910Z+FdE5vQNgdXyECmHKwJgHHh8+Ms86dcLR2v
fDRBfTntDhkL0mK6tEdz1oECgYAFhiPNydMfGGJIm8JTCZlm0eGajDao9Wwj+UJO
qiw/6Cl7gdP6pZWIu6rwYYx4iTfHVyfxx/TrpuKlacWA/8FlQvYGOrlW2ojVpEEX
X9Fjl+Ff9kIOA44+hMz0zr0+v++qIQAas64VQ0Pu1Z6Yj26cUuUgYMIoPSOisIfj
VR+rgQKBgCeScBiGK8p5Q/+x/5zEZxiT9fwPO3RC4OK07aOrYf+Y3p4JdL2nZLfP
QsTf/H02X5BI2kvSHbndyrbsHvu+V0X5n+8paAR+IJkm+QTUE1SCxuMYRk27r277
iUU3p8z4K6JWWGH1tKHR/NQ/gqLCKbUeetcoqf/RKo7LxsyNESLr
-----END RSA PRIVATE KEY-----

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

4. If you self-sign the certificate, complete the following steps:

a) Copy the certificate request and private key to a file for reference when you sign the CSR.

You do this for every client that you need to authenticate.

b) View the root CA certificate you created by using the `security certificate show` command.

You need the following information before you can sign the CSR:

- Certificate authority (CA)
- Serial number of the certificate
- Server name

You do this for every client that you need to authenticate.

Example

```
cluster1::> security certificate show -instance -vserver vs1
                              Vserver: vs1
            FQDN or Custom Common Name: lab.companyname.com
          Serial Number of Certificate: 50F84392
                 Certificate Authority: lab.companyname.com
                   Type of Certificate: root-ca
 Size of Requested Certificate(bits): 2048
               Certificate Start Date: Thu Jan 17 18:31:47 2013
           Certificate Expiration Date: Fri Jan 17 18:31:47 2014
               Public Key Certificate: -----BEGIN CERTIFICATE-----
                                       MIID
+zCCAuOgAwIBAgIEUPhDkjANBgkqhkiG9w0BAQsFADBbMQ8wDQYDVQQDEwZt
                                         .
                                         .
                                         .
```

c) Sign the CSR with the root CA generated previously by using the `security certificate sign` command.

You do this for every user client that you need to authenticate.

Example

```
cluster1::> security certificate sign -vserver vs1 -ca
lab.companyname.com -ca-serial 50F84392
```

5. If you have a third-party CA sign the CSR, complete the following steps:
   a) Have the third-party CA sign the CSR by following the steps listed in *Generating and installing a CA-signed digital certificate for server authentication* on page 157.
   b) Install the root certificate and each intermediate certificate of the CA that signed the certificate by using the `security certificate install` command with the `-type client-ca` parameter.

      You do this for each certificate.
6. If users are not set up to be authenticated by digital certificates, add users individually by using the `security login create` command with the `–authmethod` parameter set to `cert`.

   For cluster user accounts, digital certificate authentication is supported only with the `http` and `ontapi` access methods (`–application`). For Vserver user accounts, digital certificate authentication is supported only with the `ontapi` access method.

   The `security login show` command displays user login methods.
7. Install the certificate that you generated and signed on the user's client.

Commands for managing digital certificates

You use the `security certificate` commands to generate and install self-signed certificates, generate certificate signing requests for certificate authorities (CA) to sign, install CA-signed certificates, create your own CA-signed certificates, and view installed certificates.

If you want to...	Use this command...
Display CA-issued digital certificates	`security certificate ca-issued show`
Revoke a compromised CA-issued digital certificate	`security certificate ca-issued revoke`
Create and install a self-signed digital certificate	`security certificate create`
Delete a self-signed or CA-signed digital certificate	`security certificate delete`
Generate a digital certificate signing request that you will send to a CA for signing	`security certificate generate-csr`
Install a CA-signed digital certificate	`security certificate install`
Display information about installed digital certificates	`security certificate show`

If you want to...	Use this command...
Sign a digital certificate using a self-signed root CA	`security certificate sign`

For more information, see the man pages for the `security certificate` commands.

Managing access to web services

A web service is an application that users can access by using HTTP or HTTPS. The cluster administrator can set up the web protocol engine, configure SSL, enable a web service on the cluster or a Vserver, and enable users of a role to access a web service.

Data ONTAP supports the following web services:

- Service Processor infrastructure support (`spi`)

  You can enable this service for the nodes or the cluster. Enabling this service makes a node's log and core files available for HTTP or HTTPS access through the cluster's management LIF or any node's management LIF. Upon a request to access a node's log files or core files, the `spi` web service automatically creates a mount point from a node to another node's root volume where the files reside. You do not need to manually create the mount point.

  The `spi` web service also provides support for the Remote Support Agent (RSA), which is available on the NetApp Support Site for download as a firmware upgrade for the SP or the RLM. Using RSA requires that you enable the `spi` web service. For information about setting up and configuring RSA, see the *Remote Support Agent Configuration Guide for Clustered Data ONTAP*.
- Data ONTAP classic (`compat`)

  You can enable this service for the nodes only. This service provides an alternative interface to the `spi` web service for compatibility with earlier RSA versions. When both the `spi` and `compat` web services are enabled, a node's log and core files are available for HTTP or HTTPS access through the node's management LIF.
- Data ONTAP APIs (`ontapi`)

  This service enables you to run Data ONTAP APIs to execute administrative functions with a remote program.

  This service might be required for some external management tools. For example, if you use OnCommand System Manager, you should leave this service enabled.
- Support diagnostics (`supdiag`)

  This service controls access to a privileged environment on the system to assist problem analysis and resolution. You should enable this service only when directed by technical support. This service is not supported on Vservers.

Related concepts

Understanding OnCommand System Manager on page 29

Related information

NetApp Remote Support Diagnostics Tool page: support.netapp.com/NOW/download/tools/rsa

Managing the web protocol engine

You can configure the web protocol engine on the cluster to control whether web access is allowed and what SSL versions can be used. You can also display the configuration settings for the web protocol engine.

You can manage the web protocol engine at the cluster level in the following ways:

- Configuring the web protocol engine to control whether remote clients can use HTTP or HTTPS to access web service content
- Specifying whether SSLv3 or SSLv2 should be used for secure web access
  Data ONTAP supports SSLv3 and SSLv2. By default, SSLv3 is enabled and SSLv2 is disabled. If SSL is configured, Transport Layer Security 1.0 (TLSv1.0) is also enabled and cannot be disabled.
- Displaying the configuration and status of web services

You use the `system services web` commands to manage the web protocol engine at the cluster level.

If a firewall is enabled, the firewall policy for the logical interface (LIF) to be used for web services must be set up to allow HTTP or HTTPS access.

If you use HTTPS for web service access, SSL for the cluster or Vserver that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or Vserver.

Related concepts

Managing SSL on page 168
Managing web services on page 166

Related tasks

Creating a firewall policy and assigning it to a LIF on page 152
Configuring access to web services on page 169
Creating a firewall policy and assigning it to a LIF on page 152

Commands for managing the web protocol engine

You use the `system services web` commands to manage the web protocol engine. You use the `system services firewall policy create` and `network interface modify` commands to allow web access requests to go through the firewall.

If you want to...	Use this command...
Configure the web protocol engine at the cluster level: • Enabe or disable the web protocol engine for the cluster • Enable or disable SSLv2 or SSLv3 for the cluster	`system services web modify`
Display the configuration of the web protocol engine at the cluster level and determine whether the web protocols are functional throughout the cluster	`system services web show`
Display the configuration of the web protocol engine at the node level and the activity of web service handling for the nodes in the cluster	`system services web node show`
Create a firewall policy or add HTTP or HTTPS protocol service to an existing firewall policy to allow web access requests to go through firewall	`system services firewall policy create` Setting the `-service` parameter to `http` or `https` enables web access requests to go through firewall.
Associate a firewall policy with an LIF	`network interface modify` You can use the `-firewall-policy` parameter to modify the firewall policy of an LIF.

For more information, see the man pages.

Related references

Commands for managing SSL on page 168
Commands for managing firewall service and policies on page 154
Commands for managing digital certificates on page 162

Managing web services

You can enable or disable a web service for the cluster or a Vserver, display the settings for web services, and control whether users of a role can access a web service.

You can manage web services for the cluster or a Vserver in the following ways:

- Enabling or disabling a specific web service
- Specifying whether access to a web service is restricted to only encrypted HTTP (SSL)
- Displaying the availability of web services
- Allowing or disallowing users of a role to access a web service
- Displaying the roles that are permitted to access a web service

For a user to access a web service, all of the following conditions must be met:

- The user must be authenticated.
  For instance, a web service might prompt for a user name and password. The user's response must match a valid account.
- The user must be set up with the correct access method.
  Authentication only succeeds for users with the correct access method for the given web service. For the Data ONTAP API web service (`ontapi`), users must have the `ontapi` access method. For all other web services, users must have the `http` access method.

  Note: You use the `security login` commands to manage users' access methods and authentication methods.
- The web service must be configured to allow the user's access-control role.

  Note: You use the `vserver services web access` commands to control a role's access to a web service.

If a firewall is enabled, the firewall policy for the LIF to be used for web services must be set up to allow HTTP or HTTPS.

If you use HTTPS for web service access, SSL for the cluster or Vserver that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or Vserver.

Related concepts

Managing the web protocol engine on page 164
Managing user accounts on page 134
Access methods for user accounts on page 135
Managing SSL on page 168

Related tasks

Configuring access to web services on page 169

Commands for managing web services

You use the `vserver services web` commands to manage the availability of web services for the cluster or a Vserver. You use the `vserver services web access` commands to control a role's access to a web service.

If you want to...	Use this command...
Configure a web service for the cluster or a Vserver: • Enable or disable a web service • Specify whether only HTTPS can be used for accessing a web service	`vserver services web modify`
Display the configuration and availability of web services for the cluster or a Vserver	`vserver services web show`
Authorize a role to access a web service on the cluster or a Vserver	`vserver services web access create`
Display the roles that are authorized to access web services on the cluster or a Vserver	`vserver services web access show`
Prevent a role from accessing a web service on the cluster or a Vserver	`vserver services web access delete`

For more information, see the man pages.

Commands for managing mount points on the nodes

The `spi` web service automatically creates a mount point from one node to another node’s root volume upon a request to access the node’s log files or core files. Although you do not need to manually manage mount points, you can do so by using the `system node root-mount` commands.

If you want to...	Use this command...
Manually create a mount point from one node to another node's root volume	`system node root-mount create` **Note:** Only a single mount point can exist from a node to another.
Display existing mount points on the nodes in the cluster, including the time a mount point was created and its current state	`system node root-mount show`

If you want to...	Use this command...
Delete a mount point from one node to another node's root volume and force connections to the mount point to close	`system node root-mount delete`

For more information, see the man pages.

Managing SSL

The SSL protocol improves the security of web access by using a digital certificate to establish an encrypted connection between a web server and a browser.

You can manage SSL for the cluster or a Vserver in the following ways:

- Enabling SSL
- Generating and installing a digital certificate and associating it with the cluster or a Vserver
- Displaying the SSL configuration to see whether SSL has been enabled, and, if available, the SSL certificate name
- Setting up firewall policies for the cluster or a Vserver, so that web access requests can go through
- Defining which SSL versions (SSLv2 or SSLv3) can be used
- Restricting access to only HTTPS requests for a web service

Related concepts

Managing the web protocol engine on page 164
Managing web services on page 166
Managing digital certificates for server or client authentication on page 156

Related tasks

Configuring access to web services on page 169
Creating a firewall policy and assigning it to a LIF on page 152

Commands for managing SSL

You use the `security ssl` commands to manage the SSL protocol for the cluster or a Vserver.

If you want to...	Use this command...
Enable SSL for the cluster or a Vserver, and associate a digital certificate with it	`security ssl modify`
Display the SSL configuration and certificate name for the cluster or a Vserver	`security ssl show`

For more information, see the man pages.

Related references

Commands for managing web services on page 167
Commands for managing the web protocol engine on page 165
Commands for managing firewall service and policies on page 154
Commands for managing digital certificates on page 162

Configuring access to web services

Configuring access to web services allows authorized users to use HTTP or HTTPS to access the service content on the cluster or a Vserver.

Steps

1. If a firewall is enabled, ensure that HTTP or HTTPS access is set up in the firewall policy for the LIF that will be used for web services:

   Note: You can check whether a firewall is enabled by using the `system services firewall show` command.

   a) To verify that HTTP or HTTPS is set up in the firewall policy, use the `system services firewall policy show` command.

      You set the `-service` parameter of the `system services firewall policy create` command to `http` or `https` to enable the policy to support web access.

   b) To verify that the firewall policy supporting HTTP or HTTPS is associated with the LIF that provides web services, use the `network interface show` command with the `-firewall-policy` parameter.

      You use the `network interface modify` command with the `-firewall-policy` parameter to put the firewall policy into effect for a LIF.

2. To configure the cluster-level web protocol engine and make web service content accessible, use the `system services web modify` command.
3. If you plan to use secure web services (HTTPS), enable SSL and provide digital certificate information for the cluster or Vserver by using the `security ssl modify` command.
4. To enable a web service for the cluster or Vserver, use the `vserver services web modify` command.

   You must repeat this step for each service that you want to enable for the cluster or Vserver.

5. To authorize a role to access web services on the cluster or Vserver, use the `vserver services web access create` command.

   The role that you grant access must already exist. You can display existing roles by using the `security login role show` command or create new roles by using the `security login role create` command.

6. For a role that has been authorized to access a web service, ensure that its users are also configured with the correct access method by checking the output of the `security login show` command.

   To access the Data ONTAP API web service (`ontapi`), a user must be configured with the `ontapi` access method. To access all other web services, a user must be configured with the `http` access method.

   Note: You use the `security login create` command to add an access method for a user.

Related concepts

Managing SSL on page 168
Managing digital certificates for server or client authentication on page 156
Managing the web protocol engine on page 164
Managing web services on page 166
Managing access-control roles on page 139
Access methods for user accounts on page 135

Related tasks

Creating a firewall policy and assigning it to a LIF on page 152

Troubleshooting web service access problems

Configuration errors cause web service access problems to occur. You can address the errors by ensuring that the LIF, firewall policy, web protocol engine, web services, digital certificates, and user access authorization are all configured correctly.

The following table helps you identify and address web service configuration errors:

This access problem…	Occurs because of this configuration error...	To address the error...
Your web browser returns an `unable to connect` or `failure to establish a connection` error when you try to access a web service.	Your LIF might be configured incorrectly.	Ensure that you can ping the LIF that provides the web service. **Note:** You use the `network ping` command to ping a LIF. For information about network configuration, see the *Clustered Data ONTAP Network Management Guide*.
	Your firewall might be configured incorrectly.	Ensure that a firewall policy is set up to support HTTP or HTTPS and that the policy is assigned to the LIF that provides the web service. **Note:** You use the `system services firewall policy` commands to manage firewall policies. You use the `network interface modify` command with the `-firewall-policy` parameter to associate a policy with a LIF.
	Your web protocol engine might be disabled.	Ensure that the web protocol engine is enabled so that web services are accessible. **Note:** You use the `system services web` commands to manage the web protocol engine for the cluster.
Your web browser returns a `not found` error when you try to access a web service.	The web service might be disabled.	Ensure that each web service that you want to allow access to is enabled individually. **Note:** You use the `vserver services web modify` command to enable a web service for access.

This access problem…	Occurs because of this configuration error...	To address the error...
The web browser fails to log in to a web service with a user's account name and password.	The user cannot be authenticated, the access method is not correct, or the user is not authorized to access the web service.	Ensure that the user account exists and is configured with the correct access method and authentication method. Also, ensure that the user's role is authorized to access the web service. **Note:** You use the `security login` commands to manage user accounts and their access methods and authentication methods. Accessing the Data ONTAP API web service requires the `ontapi` access method. Accessing all other web services requires the `http` access method. You use the `vserver services web access` commands to manage a role's access to a web service.
You connect to your web service with HTTPS, and your web browser indicates that your connection is interrupted.	You might not have SSL enabled on the cluster or Vserver that provides the web service.	Ensure that the cluster or Vserver has SSL enabled and that the digital certificate is valid. **Note:** You use the `security ssl` commands to manage SSL configuration for HTTP servers and the `security certificate show` command to display digital certificate information.
You connect to your web service with HTTPS, and your web browser indicates that the connection is untrusted.	You might be using a self-signed digital certificate.	Ensure that the digital certificate associated with the cluster or Vserver is signed by a trusted CA. **Note:** You use the `security certificate generate-csr` command to generate a digital certificate signing request and the `security certificate install` command to install a CA-signed digital certificate. You use the `security ssl` commands to manage the SSL configuration for the cluster or Vserver that provides the web service.

Related concepts

Managing firewall service and policies on page 151

Managing the web protocol engine on page 164
Managing digital certificates for server or client authentication on page 156
Managing web services on page 166
Managing user accounts on page 134
Managing access-control roles on page 139
Managing SSL on page 168

Related tasks

Creating a firewall policy and assigning it to a LIF on page 152
Generating and installing a CA-signed digital certificate for server authentication on page 157

Managing audit settings

Audit logging creates a chronological record of management activities. You can specify what types of activities in the management interface are audited.

Data ONTAP enables you to audit two types of requests—set requests and get requests. A set request typically applies to non-display commands, such as creating, modifying, or deleting an object. A get request occurs when information is retrieved and displayed to a management interface. This is the type of request that is issued when you run a `show` command, for instance.

You use the `security audit` commands to manage audit settings. Regardless of the settings for the `security audit` commands, set requests are *always* recorded in the `command-history.log` file of the `/etc/log/mlog/` directory, and the file is sent by AutoSupport to the specified recipients.

You can also use the `security audit modify` command to specify whether the following requests are also recorded in the `mgwd.log` file of the `/etc/log/mlog/` directory for technical support and diagnostic purposes:

- Set requests for the CLI
- Set requests for the ONTAP API
- Get requests for the CLI
- Get requests for the ONTAP API

By default, auditing of set requests is enabled (that is, recorded in the `mgwd.log` file), and auditing of get requests is disabled.

The `command-history.log` and `mgwd.log` files are rotated when they reach 100 MB in size, and their previous 34 copies are preserved (with a maximum total of 35 files, respectively).

You can display the content of the `/etc/log` directory by using a web browser if your cluster user account and the required web services have been configured for the access.

Related tasks

Accessing a node's log files or core dump files by using a web browser on page 42

Commands for managing audit settings

You use the `security audit` commands to manage audit settings.

If you want to...	Use this command...
Set preferences for audit logging	`security audit modify`
Display the current audit settings	`security audit show`

For more information, see the man pages for the `security audit` commands.

Managing the cluster time (cluster administrators only)

Problems can occur when the cluster time is inaccurate. You can manually set the time zone, date, and time on the cluster. However, it is best to keep your cluster time synchronized automatically by using the Network Time Protocol (NTP) servers.

Data ONTAP enables you to manage the cluster time in the following ways:

- Configuring the NTP servers

  On a cluster running Data ONTAP 8.2 and later releases, NTP is always enabled on the cluster. To disable NTP (not recommended), you must contact technical support.

  Although NTP is always enabled, for the cluster to synchronize with an external time source, you must configure the NTP servers. The `system services ntp server` commands enable you to manage the NTP servers in the following ways:

  - Associating a node with an NTP server

    You can get a list of public NTP time servers from the NTP Public Services page.
  - Specifying the preferred NTP server and version for a node

    Data ONTAP 8.0 and 8.0.1 use NTP v4 by default. To address situations where certain time servers support only NTP v3, starting with Data ONTAP 8.0.2, the NTP version to be used for communicating with a newly configured NTP server defaults to v3 instead of v4. The NTP Daemon continues to use the highest supported version (v4 in this case) to communicate with the time servers that were configured prior to Data ONTAP 8.0.2.
  - Displaying information about NTP servers that are associated with a node or the cluster
  - Dissociating a node from an NTP server

  For more information about the `system services ntp server` commands, see the man pages.
- Manually setting the cluster time

  Data ONTAP enables you to manually manage the cluster time. The time you set takes effect across all nodes in the cluster. This capability is helpful for the following purposes:

  - Ensuring the intra-cluster time consistency

    If no external time server is used, setting the cluster time manually ensures a time setting that is consistent across all nodes in the cluster.
  - Manually correcting erroneous cluster time

    Even if an external time server is used, it is possible for the times on the nodes to become significantly incorrect (for example, a node's time has become incorrect after a reboot). In that case, you can manually specify an approximate time for the cluster until NTP can synchronize with an external time server.

  The `cluster date` commands enable you to manually manage the cluster time in the following ways:

- Setting or modifying the time zone, date, and time on the cluster
- Displaying the current time zone, date, and time settings of the cluster

For more information about the `cluster date` commands, see the man pages.

Related information

NTP Public Services: support.ntp.org

Commands for managing the cluster time

You use the `system services ntp server` commands to manage the NTP servers for the cluster. You use the `cluster date` commands to manage the cluster time manually.

The following commands enable you to manage the NTP servers on the cluster:

If you want to...	Use this command...
Associate a node with an NTP server and optionally specify the following options: • The preferred NTP server (advanced privilege level) • The version of NTP that is running on the specified NTP server	`system services ntp server create`
Modify NTP server options: • The preferred NTP server (advanced privilege level) • The NTP version to be used for communicating with a specific time server	`system services ntp server modify`
Display information about NTP servers associated with a node or the cluster	`system services ntp server show`
Dissociate a node from an NTP server	`system services ntp server delete`

The following commands enable you to manage the cluster time manually:

If you want to...	Use this command...
Set or modify the time zone, date, and time	`cluster date modify`
Display the time zone, date, and time settings for the cluster	`cluster date show`

For more information, see the man pages.

Managing licenses (cluster administrators only)

A license is a record of one or more software entitlements. Installing license keys, also known as *license codes*, enables you to use certain features or services on your cluster.

When you set up a cluster, the setup wizard prompts you to enter the cluster base license key. Some features require additional licenses. Data ONTAP feature licenses are issued as *packages*, each of which contains multiple features or a single feature. A package requires a license key, and installing the key enables you to access all features in the package. For information about the license packages, see the knowledgebase article *Data ONTAP 8.2 Licensing Overview and References* on the NetApp Support Site.

Starting with Data ONTAP 8.2, all license keys are 28 characters in length. Licenses installed prior to Data ONTAP 8.2 continue to work in Data ONTAP 8.2 and later releases. However, if you need to reinstall a license (for example, you deleted a previously installed license and want to reinstall it in Data ONTAP 8.2 or later, or you perform a controller replacement procedure for a node in a cluster running Data ONTAP 8.2 or later), Data ONTAP requires that you enter the license key in the 28-character format.

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support > Software Licenses**. For instance, you can search with the serial number of a node to find all license keys associated with the node. Your search results will include license information for all nodes in the cluster. You can also search by cluster serial number or sales order number. If you cannot locate your license keys from the Software Licenses page, you should contact your sales or support representative.

Data ONTAP enables you to manage licenses in the following ways:

- Add one or more license keys (`system license add`)
- Display information about installed licenses (`system license show`)
- Display the packages that require licenses and their current license status on the cluster (`system license status show`)
- Delete a license from the cluster or a node whose serial number you specify (`system license delete`)

  The cluster base license is required for the cluster to operate. Data ONTAP does not enable you to delete it.
- Display or remove expired or unused licenses (`system license clean-up`)

Related information

NetApp Support Site: support.netapp.com

License types and licensed method

Understanding license types and the licensed method helps you manage the licenses in a cluster.

License types

A package can have one or more of the following types of license installed in the cluster. The `system license show` command displays the installed license type or types for a package.

- Standard license (`license`)
  A standard license is a node-locked license. It is issued for a node with a specific system serial number (also known as a *controller serial number*). A standard license is valid only for the node that has the matching serial number.

  Note: The `sysconfig` command in the nodeshell displays the system serial number of a node.

  Installing a standard, node-locked license entitles a node to the licensed functionality. For the cluster to use licensed functionality, at least one node must be licensed for the functionality. It might be out of compliance to use licensed functionality on a node that does not have an entitlement for the functionality.
  Data ONTAP 8.2 and later releases treat a license installed prior to Data ONTAP 8.2 as a standard license. Therefore, in Data ONTAP 8.2 and later releases, all nodes in the cluster automatically have the standard license for the package that the previously licensed functionality is part of. The `system license show` command with the `-legacy yes` parameter indicates such licenses.
- Site license (`site`)
  A site license is not tied to a specific system serial number. When you install a site license, all nodes in the cluster are entitled to the licensed functionality. The `system license show` command displays site licenses under the cluster serial number.
  If your cluster has a site license and you remove a node from the cluster, the node does not carry the site license with it, and it is no longer entitled to the licensed functionality. If you add a node to a cluster that has a site license, the node is automatically entitled to the functionality granted by the site license.
- Evaluation license (`demo`)
  An evaluation license is a temporary license that expires after a certain period of time (indicated by the `system license show` command). It enables you to try certain software functionality without purchasing an entitlement. It is a cluster-wide license, and it is not tied to a specific serial number of a node.
  If your cluster has an evaluation license for a package and you remove a node from the cluster, the node does not carry the evaluation license with it.

Licensed method

It is possible to install both a cluster-wide license (the `site` or `demo` type) and a node-locked license (the `license` type) for a package. Therefore, an installed package can have multiple license types in

the cluster. However, to the cluster, there is only one *licensed method* for a package. The `licensed method` field of the `system license status show` command displays the entitlement that is being used for a package. The command determines the licensed method as follows:

- If a package has only one license type installed in the cluster, the installed license type is the licensed method.
- If a package does not have any licenses installed in the cluster, the licensed method is `none`.
- If a package has multiple license types installed in the cluster, the licensed method is determined in the following priority order of the license type—`site`, `license`, and `demo`.

  For example:

  - If you have a site license, a standard license, and an evaluation license for a package, the licensed method for the package in the cluster is `site`.
  - If you have a standard license and an evaluation license for a package, the licensed method for the package in the cluster is `license`.
  - If you have only an evaluation license for a package, the licensed method for the package in the cluster is `demo`.

Commands for managing licenses

You use the `system license` commands to manage licenses for the cluster.

If you want to...	Use this command...
Add one or more licenses	`system license add`
Display information about installed licenses, for example: • License package name and description • License type (`site`, `license`, or `demo`) • Expiration date, if applicable • The cluster or nodes that a package is licensed for • Whether the license was installed prior to Data ONTAP 8.2 (`legacy`) • Customer ID	`system license show` **Note:** Some information is displayed only when you use the `-instance` parameter.
Display all packages that require licenses and their current license status, including the following: • The package name • The licensed method • The expiration date, if applicable	`system license status show`

If you want to...	Use this command...
Delete the license of a package from the cluster or a node whose serial number you specify	`system license delete`
Display or remove expired or unused licenses	`system license clean-up`

For more information, see the man pages for the `system license` commands.

Managing jobs and schedules

A *job* is any asynchronous task. Jobs are typically long-running volume operations such as copy, move, and mirror. You can monitor, pause, stop, and restart jobs, and configure them to run on specified schedules.

Job categories

There are three categories of jobs that you can manage: server-affiliated, cluster-affiliated, and private.

A job can be in any of the following categories:

Server-Affiliated jobs These jobs are queued by the management framework to a specific node to be run.

Cluster-Affiliated jobs These jobs are queued by the management framework to any node in the cluster to be run.

Private jobs These jobs are specific to a node and do not use the replicated database (RDB) or any other cluster mechanism. The commands that manage private jobs require the advanced privilege level or higher.

Commands for managing jobs

Jobs are placed into a job queue and run when resources are available. If a job is consuming too many system resources, you can stop it or pause it until there is less demand on the system. You can also monitor and restart jobs.

If you want to...	Use this command...
Display information about all jobs	`job show`
Display information about jobs on a per-node basis	`job show-bynode`
Display information about cluster-affiliated jobs	`job show-cluster`
Display information about completed jobs	`job show-completed`

If you want to...	Use this command...
Display information about job history	`job history show` Up to 25,000 job records are stored for each node in the cluster. Consequently, attempting to display the full job history could take a long time. To avoid potentially long wait times, you should display jobs by node, Vserver, or record ID.
Display the list of private jobs	`job private show` **Note:** This command is only available at the advanced privilege level.
Display information about completed private jobs	`job private show-completed` **Note:** This command is only available at the advanced privilege level.
Display information about the initialization state for job managers	`job initstate show` **Note:** This command is only available at the advanced privilege level.
Monitor a job's progress	`job watch-progress`
Monitor a private job's progress	`job private watch-progress` **Note:** This command is only available at the advanced privilege level.
Pause a job	`job pause`
Pause a private job	`job private pause` **Note:** This command is only available at the advanced privilege level.
Resume a paused job	`job resume`
Resume a paused private job	`job private resume` **Note:** This command is only available at the advanced privilege level.
Stop a job	`job stop`
Stop a private job	`job private stop` **Note:** This command is only available at the advanced privilege level.

If you want to...	Use this command...
Delete a job	`job delete`
Delete a private job	`job private delete` **Note:** This command is only available at the advanced privilege level.
Disassociate a cluster-affiliated job with an unavailable node that owns it, so that another node can take ownership of the job	`job unclaim` **Note:** This command is only available at the advanced privilege level.

Note: You can use the `event log show` command to determine the outcome of a completed job.

For more information, see the man pages.

Commands for managing job schedules

Many tasks—for instance, volume snapshots—can be configured to run on specified schedules. Schedules that run at specific times are called *cron* schedules (similar to UNIX `cron` schedules). Schedules that run at intervals are called *interval* schedules. You use the `job schedule` commands to manage job schedules.

If you want to...	Use this command...
Display information about all schedules	`job schedule show`
Display the list of jobs by schedule	`job schedule show-jobs`
Display information about cron schedules	`job schedule cron show`
Display information about interval schedules	`job schedule interval show`
Create a cron schedule	`job schedule cron create`
Create an interval schedule	`job schedule interval create` You must specify at least one of the following parameters: `-days`, `-hours`, `-minutes`, or `-seconds`.
Modify a cron schedule	`job schedule cron modify`
Modify an interval schedule	`job schedule interval modify`
Delete a schedule	`job schedule delete`
Delete a cron schedule	`job schedule cron delete`

If you want to...	Use this command...
Delete an interval schedule	`job schedule interval delete`

For more information, see the man pages.

Backing up and restoring cluster configurations (cluster administrators only)

Backing up the cluster configuration enables you to restore the configuration of any node or the cluster in the event of a disaster or emergency.

What configuration backup files are

Configuration backup files are archive files (.7z) that contain information for all configurable options that are necessary for the cluster, and the nodes within it, to operate properly.

These files store the local configuration of each node, plus the cluster-wide replicated configuration. You use configuration backup files to back up and restore the configuration of your cluster.

There are two types of configuration backup files:

Node configuration backup file	Each healthy node in the cluster includes a node configuration backup file, which contains all of the configuration information and metadata necessary for the node to operate healthy in the cluster.
Cluster configuration backup file	These files include an archive of all of the node configuration backup files in the cluster, plus the replicated cluster configuration information (the replicated database, or RDB file). Cluster configuration backup files enable you to restore the configuration of the entire cluster, or of any node in the cluster. The cluster configuration backup schedules create these files automatically and store them on several nodes in the cluster.

Note: Configuration backup files contain configuration information only. They do not include any user data. For information about restoring user data, see the *Clustered Data ONTAP Data Protection Guide*.

Managing configuration backups

The configuration backup schedules automatically create configuration backup files for each node in the cluster, and for the cluster itself. You can change some of the settings for these schedules, and you can create configuration backup files manually.

How the node and cluster configurations are backed up automatically

Three separate schedules automatically create cluster and node configuration backup files and replicate them among the nodes in the cluster.

The configuration backup files are automatically created according to the following schedules:

- Every 8 hours
- Daily
- Weekly

At each of these times, a node configuration backup file is created on each healthy node in the cluster. All of these node configuration backup files are then collected in a single cluster configuration backup file along with the replicated cluster configuration and saved on one or more nodes in the cluster.

If you have a single node cluster, you should configure the configuration backup schedule to store the cluster configuration backups at a remote URL. This ensures that you can recover the cluster's configuration even if the node becomes inaccessible. For more information about setting up the configuration backup schedule for single node clusters, see the *Clustered Data ONTAP Software Setup Guide*.

Commands for managing configuration backup schedules

You use the `system configuration backup settings` commands to manage configuration backup schedules.

These commands are available at the advanced privilege level.

If you want to...	Use this command...
Change the settings for a configuration backup schedule, including: • Specifying a remote URL (either HTTP or FTP) where the configuration backup files will be uploaded in addition to the default locations in the cluster • Specifying a user name to be used to log in to the remote URL • Setting the number of backups to keep for each configuration backup schedule	`system configuration backup settings modify`
Set the password to be used to log in to the remote URL	`system configuration backup settings set-password`
View the settings for the configuration backup schedule	`system configuration backup settings show` **Note:** You set the `-instance` parameter to view the user name and the number of backups to keep for each schedule.

For more information, see the man pages.

Commands for managing configuration backup files

You use the `system configuration backup` commands to manage cluster and node configuration backup files.

These commands are available at the advanced privilege level.

If you want to...	Use this command...
Create a new node or cluster configuration backup file	`system configuration backup create`
Copy a configuration backup file from a node to another node in the cluster	`system configuration backup copy`
Upload a configuration backup file from a node in the cluster to a remote URL (either HTTP or FTP)	`system configuration backup upload` **Note:** The Web server to which you are uploading the configuration backup file must have PUT operations enabled. For more information, see your web server's documentation.
Download a configuration backup file from a remote URL to a node in the cluster	`system configuration backup download`
Rename a configuration backup file on a node in the cluster	`system configuration backup rename`
View the node and cluster configuration backup files for one or more nodes in the cluster	`system configuration backup show`
Delete a configuration backup file on a node	`system configuration backup delete` **Note:** This command deletes the configuration backup file on the specified node only. If the configuration backup file also exists on other nodes in the cluster, it remains on those nodes.

For more information, see the man pages.

Recovering a node configuration

You recover a node's configuration using a configuration backup file if the node, its root volume, or any of its configuration information is lost or corrupted.

Steps

1. *Finding a configuration backup file to use for recovering a node* on page 188
2. *Restoring the node configuration using a configuration backup file* on page 189

Finding a configuration backup file to use for recovering a node

You use a configuration backup file located at a remote URL or on a node in the cluster to recover a node configuration.

About this task

You can use either a cluster or node configuration backup file to restore a node configuration.

Step

1. Make the configuration backup file available to the node for which you need to restore the configuration.

If the configuration backup file is located...	Then...
At a remote URL	Use the `system configuration backup download` command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	**a.** Use the `system configuration backup show` command at the advanced privilege level to view the list of configuration backup files available in the cluster that contains the recovering node's configuration. **b.** If the configuration backup file you identify does not exist on the recovering node, then use the `system configuration backup copy` command to copy it to the recovering node.

If you previously re-created the cluster, you should choose a configuration backup file that was created after the cluster recreation. If you must use a configuration backup file that was created prior to the cluster recreation, then after recovering the node, you must re-create the cluster again.

Restoring the node configuration using a configuration backup file

You restore the node configuration using the configuration backup file that you identified and made available to the recovering node.

About this task

You should only perform this task to recover from a disaster that resulted in the loss of the node's local configuration files.

Steps

1. If the node is healthy, then from a different node, use the `cluster modify` command with the `-node` and `-eligibility` parameters to mark it ineligible and isolate it from the cluster.

   If the node is not healthy, then you should skip this step.

   #### Example

   This example modifies node2 to be ineligible to participate in the cluster so that its configuration can be restored.

   ```
   cluster1::> cluster modify -node node2 -eligibility false
   ```

2. Use the `system configuration recovery node restore` command at the advanced privilege level to restore the node's configuration from a configuration backup file.

   If the node lost its identity, including its name, then you should use the `-nodename-in-backup` parameter to specify the node name in the configuration backup file.

   #### Example

   This example restores the node's configuration using one of the configuration backup files stored on the node.

   ```
   cluster1::*> system configuration recovery node restore -backup
   cluster1.8hour.2011-02-22.18_15_00.7z

   Warning: This command overwrites local configuration files with
            files contained in the specified backup file. Use this
            command only to recover from a disaster that resulted
            in the loss of the local configuration files.
            The node will reboot after restoring the local configuration.
   Do you want to continue? {y|n}: y
   ```

   The configuration is restored, and the node reboots.

3. If you marked the node ineligible, then use the `system configuration recovery cluster sync` command to mark the node as eligible and synchronize it with the cluster.

After you finish

If you previously re-created the cluster, and if you are restoring the node configuration by using a configuration backup file that was created prior to that cluster recreation, then you must re-create the cluster again.

Related tasks

Synchronizing a node with the cluster on page 192

Recovering a cluster configuration

If cluster-wide quorum does not exist, then you recover the cluster configuration by finding a configuration to use for recovery, re-creating the cluster, and then rejoining each node to it.

Steps

1. *Finding a configuration to use for recovering a cluster* on page 190
2. *Restoring a cluster configuration from an existing configuration* on page 191

Finding a configuration to use for recovering a cluster

You use the configuration from either a node in the cluster or a cluster configuration backup file to recover a cluster.

Steps

1. Choose a type of configuration to recover the cluster.
   - A node in the cluster
     If the cluster consists of more than one node, and one of the nodes has a cluster configuration from when the cluster was in the desired configuration, then you can recover the cluster using the configuration stored on that node.
     In most cases, the node containing the replication ring with the most recent transaction ID is the best node to use for restoring the cluster configuration. Use the `cluster ring show` command at the advanced privilege level to view a list of the replicated rings available on each node in the cluster.
   - A cluster configuration backup file
     If you cannot identify a node with the correct cluster configuration, or if the cluster consists of a single node, then you can use a cluster configuration backup file to recover the cluster.
2. If you chose to use a cluster configuration backup file, then make the file available to the node you plan to use to recover the cluster.

If the configuration backup file is located...	Then...
At a remote URL	Use the `system configuration backup download` command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	**a.** Use the `system configuration backup show` command at the advanced privilege level to find a cluster configuration backup file that was created when the cluster was in the desired configuration. **b.** If the cluster configuration backup file is not located on the node you plan to use to recover the cluster, then use the `system configuration backup copy` command to copy it to the recovering node.

Restoring a cluster configuration from an existing configuration

You re-create the cluster using the cluster configuration that you chose and made available to the recovering node, and then rejoin each additional node to the new cluster.

About this task

You should only perform this task to recover from a disaster that resulted in the loss of the cluster's configuration.

Steps

1. On the recovering node, use the `system configuration recovery cluster recreate` command at the advanced privilege level to re-create the cluster.

   #### Example

   This example re-creates the cluster using the configuration information stored on the recovering node.

   ```
   cluster1::*>system configuration recovery cluster recreate -from node

   Warning: This command will destroy your existing cluster. It will
            rebuild a new single-node cluster consisting of this node
            and its current configuration. This feature should only be
            used to recover from a disaster. Do not perform any other
            recovery operations while this operation is in progress.
   Do you want to continue? {y|n}: y
   ```

   A new cluster is created, with a new UUID, on the recovering node.

2. Use the `cluster identity show` command to verify that the recovering node has a different UUID than the other nodes.

3. For each node that needs to be joined to the re-created cluster, do the following:

a) From a healthy node on the re-created cluster, use the `system configuration recovery cluster rejoin` command at the advanced privilege level to rejoin the target node to the cluster.

Example

This example rejoins the target node (*node2*) to the re-created cluster.

```
cluster1::*> system configuration recovery cluster rejoin -node
node2

Warning: This command will rejoin node "node2" into the local
         cluster, potentially overwriting critical cluster
         configuration files. This command should only be used
         to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
         This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

The target node reboots and then joins the cluster.

b) Use the `cluster show` command with the `-eligibility` parameter to verify that the target node is healthy and has formed quorum with the rest of the nodes in the cluster.

The target node must rejoin the re-created cluster before you can rejoin another node.

After you finish

If the cluster has SnapMirror peer relationships, then you need to re-create the relationships. For more information, see the *Clustered Data ONTAP Data Protection Guide*.

Synchronizing a node with the cluster

If cluster-wide quorum exists, but one or more nodes are out of synch with the cluster, then you synchronize the node to restore the replicated database (RDB) on the node and bring it into quorum.

Step

1. Use the `system configuration recovery cluster sync` command at the advanced privilege level to synchronize the node with the cluster configuration.

Example

This example synchronizes a node (*node2*) with the rest of the cluster.

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
```

```
          used to recover from a disaster. Do not perform any other
          recovery operations while this operation is in progress. This
          command will cause all the cluster applications on node
          "node2" to restart, interrupting administrative CLI and Web
          interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify
that the cluster applications go online.
```

Result

The RDB is replicated to the node, and the node becomes eligible to participate in the cluster.

Managing core dumps (cluster administrators only)

When a node panics, a core dump occurs and the system creates a core dump file that technical support can use to troubleshoot the problem. You can configure or display core dump attributes. You can also save, display, segment, upload, or delete a core dump file.

You can manage core dumps in the following ways:

- Configuring core dumps and displaying the configuration settings
- Displaying the status and attributes of core dumps
- Saving the core dump content and uploading the saved file to a specified location or to technical support
- Deleting core dump files that are no longer needed

A core dump file can be very large and time-consuming to upload. You must not further compress a core dump file. However, you can segment the file in the following ways:

- Configure the automatic segmenting of core dump files
- Manually segment a core dump file and manage the core segments

Only the cluster administrator can manage core dumps. The Vserver administrator cannot access or manage core dumps.

Related tasks

Accessing a node's log files or core dump files by using a web browser on page 42

Methods of segmenting core dump files

A core dump file can be very large, making it time consuming to upload to technical support when you need to. Segmenting the core dump file enables you to upload only the needed portion instead of the entire file.

You can segment a saved core dump file into a maximum of three core segments:

This core segment…	Contains system information from the memory of…
Primary core segment	Data ONTAP and the systemshell
Caching module core segment	Flash Cache family of modules
NVRAM core segment	NVRAM

Segmenting the core dump file enables you to upload a portion of the file as you need to. For instance, instead of uploading the entire core dump file to technical support for a core dump analysis, you can upload only the primary core segment of the file, and if necessary, upload the caching module core segment or NVRAM core segment later.

By using the `system node coredump segment config` commands, you can configure the automatic segmenting of the core dump file in the following ways:

- Specify whether to automatically segment a core dump file after it is saved
  The default setting for automatic segmenting is system dependent.
- Specify whether to automatically delete the original core dump file after it is segmented
  By default, automatic deletion of the original core dump file is disabled.
- Display the current configuration of the automatic segmenting of core dump files

By using the `system node coredump segment` commands, you can manually manage the segmenting of a core dump file in the following ways:

- Manually schedule a core segmenting job to segment a specified core dump file on a node into core segments and specify whether the original core dump file is to be deleted after the core segmenting is complete
- Display information about core segments
- Delete a specified core segment or all segments from a node
- Display the status of a core segmenting job
- Cancel a core segmenting job as specified by its job ID

Commands for managing core dumps

You use the `system node coredump config` commands to manage the configuration of core dumps, the `system node coredump` commands to manage the core dump files, and the `system node coredump reports` commands to manage application core reports.

If you want to...	**Use this command...**
Configure core dumps	`system node coredump config modify`
Display the configuration settings for core dumps	`system node coredump config show`
Display basic information about core dumps	`system node coredump show`
Manually trigger a core dump when you reboot a node	`system node reboot` with both the `-dump` and `-skip-lif-migration` parameters
Manually trigger a core dump when you shut down a node	`system node halt` with both the `-dump` and `-skip-lif-migration` parameters
Save a specified core dump	`system node coredump save`

If you want to...	Use this command...
Save all unsaved core dumps that are on a specified node	`system node coredump save-all`
Upload a saved core dump file to a specified location	`system node coredump upload`
Display status information about core dumps	`system node coredump status`
Delete a specified core dump	`system node coredump delete`
Delete all unsaved core dumps or all saved core files on a node	`system node coredump delete-all`
Display application core dump reports	`system node coredump reports show`
Upload an application core dump report to a specified location	`system node coredump reports upload`
Delete an application core dump report	`system node coredump reports delete`

For more information, see the man pages.

Commands for managing core segmenting

You use the `system node coredump segment config` commands to manage the automatic segmenting of core dump files. You use the `system node coredump segment` commands to manage core segments.

If you want to...	Use this command...
Configure the automatic segmenting of core dump files for a node, including: • Whether to automatically segment a core dump file after it is saved • Whether to automatically delete the original core dump file after it is segmented	`system node coredump segment config modify`
Show the current configuration of automatic core segmenting	`system node coredump segment config show`
Manually start segmenting a specified core dump file on a node into core segments and specify whether the original core dump file is to be deleted after the core segmenting is complete	`system node coredump segment start`

If you want to...	Use this command...
Display information about the core segments on a node, for example: • The core segment name • Total number of core segments for the full core • The time when the panic occurred that generated the core dump file	`system node coredump segment show`
Delete a specified core segment from a node	`system node coredump segment delete`
Delete all core segments from a node	`system node coredump segment delete-all`
Displays the status of a core segmenting job, including the following: • Job ID • Name of the core dump file that is being segmented • Job status • Percent completed	`system node coredump segment status`
Cancel a core segmenting job as specified by its job ID	`system node coredump segment stop`

For more information, see the man pages.

Monitoring the storage system

You can use event messages, the AutoSupport feature, dashboards, statistics, and environmental component sensors to monitor the storage system.

The cluster administrator can perform all system monitoring tasks. The Vserver administrator can perform only the following monitoring tasks:

- Display the Vserver health dashboard (by using the `dashboard health vserver show` commands)
- Manage and obtain performance data (by using the `statistics` commands)

Managing event messages

The Event Management System (EMS) collects and displays information about events that occur on your storage system. You can manage the event destination, event route, mail history records, and SNMP trap history records. You can also configure event notification and logging.

Event messages for high-severity events appear on your system console or LCD, if your system has one, and are written to the system's event log. An event message consists of the following elements:

- Message name
- Severity level
  Possible values include the following, listed in decreasing order of urgency:
  - EMERGENCY (the system is unusable)
  - ALERT (action must be taken immediately to prevent system failure)
  - CRITICAL
  - ERROR
  - WARNING
  - NOTICE (a normal but significant condition has occurred)
  - INFORMATIONAL
  - DEBUG
- Description
- Corrective action, if applicable

You can manage the following event capabilities:

- Event destination
  Specifies the destination to which events are sent. Destinations can be email addresses, SNMP trap hosts, or syslog servers.
- Event route

Specifies which events generate notifications. An event route is a mapping between events and their destinations. An event route includes information about severity, destinations, and notification thresholds.

- Event notification and logging
  Specifies the email “from” address, the email “to” address, whether to send events to the console, and the maximum size of the log file.
- Mail history records
  A list of emailed event notifications.
- SNMP trap history records
  A list of event notifications that have been sent to SNMP traps. For information about SNMP traps, see the *Clustered Data ONTAP Network Management Guide*.

Setting up the Event Management System

You can configure EMS to reduce the number of event messages that you receive, and to set up the event destinations and the event routes for a particular event severity.

Steps

1. To see what is currently configured for the mail locations, enter the following command:

   `event config show`

   #### Example

   The following command shows the configured mail locations:

   ```
   cluster1::> event config show

     Mail From: admin@localhost
   Mail Server: localhost
   ```

2. If you need to change the mail locations, enter the following command:

   `event config modify -mailserver` ***`name`*** **`-mailfrom`** ***`email address`***

   #### Example

   The following example shows how to change the mail locations and display the results:

   ```
   cluster1::> event config modify -mailserver mailhost.example.com
   -mailfrom admin@node1-example.com

   cluster1::> event config show

     Mail From: admin@node1-example.com
   Mail Server: mailhost.example.com
   ```

3. To create the destination for events, enter the following command and specify the name and email address:

   event destination create -name *destination* -mail *email address*

   You can send events to email addresses, SNMP trap hosts, and syslog servers.

   Example

   The following command creates an email destination and sends all important events to the specified email address:

   ```
   cluster1::> event destination create -name test_dest -mail
   me@example.com
   ```

4. Use the `event route add-destinations` command to define the severity level of messages to receive.

   The recommended practice is to set up event routes for critical and above events.

   Example

   The following example sends all critical, alert, and emergency events to the test_dest event destination, and displays the results:

   ```
   cluster1::> event route add-destinations {-severity <=CRITICAL}
   -destinations test_dest

   cluster1::> event dest show

                                                          Hide
   Name      Mail Dest.      SNMP Dest.  Syslog Dest.  Params
   --------  --------------- ----------- ------------- ------
   allevents -               -           -             false
   asup      -               -           -             false
   criticals -               -           -             false
   pager     -               -           -             false
   test_dest me@example.com  -           -             false
   traphost  -               -           -             false
   ```

5. To display all critical and above events, enter the following command:

   event route show -severity <=CRITICAL

   Example

   The following example shows the events with critical and above severity levels:

   ```
   cluster1::> event route show -severity -CRITICAL
   ```

```
                                                          Freq        Time
Message                  Severity    Destinations     Threshd
Threshd
-------------------------------------------------------------------------
--
adminapi.time.zoneDiff   ALERT       test_dest        0           3600
api.engine.killed        CRITICAL    test_dest        0           0
app.log.alert            ALERT       test_dest        0           0
app.log.crit             CRITICAL    test_dest        0           0
app.log.emerg            EMERGENCY   test_dest        0           0
```

6. If you are still getting too many event messages, use the `-timethreshold` option to specify how often events are sent to the destination.

Example

For example, the following event is displayed once per hour:

```
cluster1::> event route modify -messagename adminapi.time.zoneDiff
-timethreshold 3600
```

Result

When you have completed these steps, all critical events are automatically sent to the destination specified in the event route.

Finding corrective actions for events

You can use the `event route show` command to display information about event routes and to find corrective actions for events so that you can resolve system problems.

About this task

To find the corrective action for a single event, use the `-messagename` parameter. To find the corrective action for multiple events, use the `-instance` parameter.

Steps

1. Use the `event log show` command to display the events that have occurred.

Example

For example, you can display all the events that occur at a specific time interval:

```
cluster1::> event log show -time
"11/9/2010 13:45:00".."2/16/2012 09:58:00"

Time               Node     Severity   Event
-------------------------------------------
```

```
2/16/2012 09:56:31 cluster1 NOTICE     raid.rg.media_scrub.start:
owner="", rg="/aggr0/plex0/rg0"
. . .
```

2. Enter the following command to see the corrective action for an event:

   event route show -messagename *event name* -instance

   Example

   The following example displays the corrective action and other details for an event:

```
cluster1::> event route show -messagename adminapi.time.zoneDiff
-instance

Message Name: adminapi.time.zoneDiff
Severity: ALERT
Action: Change the name of the timezone value in the /etc/rc
file to the new timezone value.

Description: This message occurs when the timezone value being set
conflicts with a line already in the /etc/rc file.

Supports SNMP trap: false
Destinations: test_dest
Number of Drops Between Transmissions: 0
Dropping Interval (Seconds) Between Transmissions: 3600
```

Commands for managing events

You can use specific Data ONTAP commands in the `event` family for managing events on your storage system.

The following table lists commands for managing events:

If you want to...	Use this command...
Create an event destination	`event destination create`
Display information about event destinations	`event destination show`
Modify an event destination	`event destination modify`
Delete an event destination	`event destination delete`
Modify an event route or the frequency of event notifications	`event route modify`
Add an existing destination or destinations to an event route	`event route add-destinations`

If you want to...	Use this command...
Specify the severity level for an event route	`event route add-destinations` with the `-messagename` parameter
Remove a destination or destinations from an event route	`event route remove-destinations`
Display information about event routes	`event route show`
Display the corrective action for an event	`event route show` with the `-messagename` or `-instance` parameter
Display the event log	`event log show`
Display the configuration for event notification and logging	`event config show`
Modify the configuration for event notification and logging	`event config modify`
Display information about event occurrences	`event status show`
Display mail-history records	`event mailhistory show`
Delete mail-history records	`event mailhistory delete`
Display a list of event notifications that have been sent to SNMP traps	`event snmphistory show`
Delete an SNMP trap-history record	`event snmphistory delete`

For more information, see the man pages.

Managing AutoSupport

AutoSupport is a mechanism that proactively monitors the health of your system and automatically sends messages to NetApp technical support, your internal support organization, and a support partner. Although AutoSupport messages to technical support are enabled by default, you must set the correct options and have a valid mail host to have messages sent to your internal support organization.

Only the cluster administrator can perform AutoSupport management. The Vserver administrator has no access to AutoSupport.

AutoSupport is enabled by default when you configure your storage system for the first time. AutoSupport begins sending messages to technical support 24 hours after AutoSupport is enabled. You can shorten the 24-hour period by upgrading or reverting the system, modifying the AutoSupport configuration, or changing the system time to be something other than a 24-hour period.

Note: You can disable AutoSupport at any time, but you should leave it enabled. Enabling AutoSupport can significantly help speed problem determination and resolution should a problem occur on your storage system. By default, the system collects AutoSupport information and stores it locally even if you disable AutoSupport.

For more information about AutoSupport, see the NetApp Support Site.

Related information

The NetApp Support Site: support.netapp.com

When and where AutoSupport messages are sent

AutoSupport sends messages to different recipients, depending on the type of message. Learning when and where AutoSupport sends messages can help you understand messages that you receive through email or view on the My AutoSupport web site.

Note: Unless specified otherwise, settings in the following tables are parameters of the `system node autosupport modify` command.

Event-triggered messages

When events occur on the storage system that require corrective action, AutoSupport automatically sends an event-triggered message.

When the message is sent	Where the message is sent
AutoSupport responds to a trigger event in the EMS	Addresses specified in `-to` and `-noteto`. (Only critical, service-affecting events are sent.) Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

Scheduled messages

AutoSupport automatically sends several messages on a regular schedule.

When the message is sent	Where the message is sent
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a log message)	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a performance message), if the `-perf` parameter is set to `true`	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

When the message is sent	Where the message is sent
Weekly (by default, sent Sunday between 12:00 a.m. and 1:00 a.m.)	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

Manually triggered messages

You can manually initiate or resend an AutoSupport message.

When the message is sent	Where the message is sent
You manually initiate a message using the `system node autosupport invoke` command	If a URI is specified using the `-uri` parameter in the `system node autosupport invoke` command, the message is sent to that URI. If `-uri`is omitted, the message is sent to the addresses specified in `-to` and `-partner-address`. The message is also sent to technical support, if `-support` is set to `enable`.
You manually resend a past message using the `system node autosupport history retransmit` command	Only to the URI that you specify in the `-uri` parameter of the `system node autosupport history retransmit` command

Messages triggered by technical support

Technical support can request messages from AutoSupport using the AutoSupport On Demand feature.

When the message is sent	Where the message is sent
When AutoSupport obtains delivery instructions to generate new AutoSupport messages	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable` and the transport protocol is HTTPS
When AutoSupport obtains delivery instructions to resend past AutoSupport messages	Technical support, if `-support` is set to `enable` and the transport protocol is HTTPS

Related concepts

How AutoSupport On Demand obtains delivery instructions from technical support on page 206

How event-triggered AutoSupport messages work

AutoSupport creates event-triggered AutoSupport messages when the EMS processes a trigger event. An event-triggered AutoSupport message alerts recipients of problems that require corrective action,

and messages contain only information that is relevant to the problem. You can customize what content to include and who receives the messages.

AutoSupport uses the following process to create and send event-triggered AutoSupport messages:

1. When the EMS processes a trigger event, EMS sends AutoSupport a request.

   Note: A trigger event is an EMS event with an AutoSupport destination and a name that begins with a `callhome.` prefix.

2. AutoSupport creates an event-triggered AutoSupport message.
   AutoSupport collects basic and troubleshooting information from subsystems that are associated with the trigger to create a message that only includes information that is relevant to the trigger event.
   A default set of subsystems are associated with each trigger. However, you can choose to associate additional subsystems with a trigger by using the `system node autosupport trigger modify` command.

3. AutoSupport sends the event-triggered AutoSupport message to the recipients defined by the `system node autosupport modify` command with the `-to`, `-noteto`, `-partner-address`, and `-support` parameters.
   You can enable and disable delivery of AutoSupport messages for specific triggers by using the `system node autosupport trigger modify` command with the `-to` and `-noteto` parameters.

Example of data sent for a specific event

The `storage shelf PSU failed` EMS event triggers a message that contains basic data from the Mandatory, Log Files, Storage, RAID, HA, Platform, and Networking subsystems and troubleshooting data from the Mandatory, Log Files, and Storage subsystems.

You decide that you want to include data about NFS in any AutoSupport messages sent in response to a future `storage shelf PSU failed` event. You enter the following command to enable troubleshooting-level data for NFS for the `callhome.shlf.ps.fault` event:

```
cluster1::> system node autosupport trigger modify -node node1 -
autosupport-message shlf.ps.fault -troubleshooting-additional nfs
```

Note: The `callhome.` prefix is omitted from the `storage shelf PSU failed` event when you use the `system node autosupport trigger` commands.

How AutoSupport On Demand obtains delivery instructions from technical support

AutoSupport On Demand periodically communicates with technical support to obtain delivery instructions for sending, resending, and declining AutoSupport messages. AutoSupport On Demand

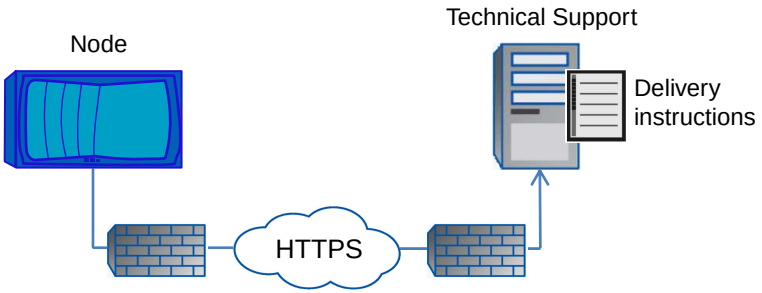
is enabled by default. It automatically communicates with technical support if AutoSupport is configured to send messages to technical support and the transport protocol is HTTPS.

The AutoSupport On Demand client, which runs on each node, periodically polls the AutoSupport On Demand service to obtain delivery instructions. The AutoSupport On Demand service resides in technical support. The client sends HTTPS requests to the same technical support location that AutoSupport messages are sent.

The AutoSupport On Demand client does not accept incoming connections.

Note: AutoSupport On Demand uses the "autosupport" user account to communicate with technical support. You should not delete this account.

The following illustration shows how AutoSupport On Demand sends HTTPS requests to technical support to obtain delivery instructions.



The delivery instructions can include requests for AutoSupport to do the following:

- Generate new AutoSupport messages.
  Technical support might request new AutoSupport messages to help triage issues.
- Retransmit previously generated AutoSupport messages.
  This request automatically happens if a message was not received due to a delivery failure.
- Disable delivery of AutoSupport messages for specific trigger events.
  Technical support might disable delivery of data that is not used.

What data AutoSupport messages contain

AutoSupport messages contain information from subsystems. Learning what AutoSupport messages contain can help you interpret or respond to messages that you receive via email or view on the My AutoSupport web site.

Type of message	What type of data the message contains
Event-triggered	Files containing context-sensitive data about the specific subsystem where the event occurred
Daily	Log files
Performance	Performance data sampled during the previous 24 hours

Type of message	What type of data the message contains
Weekly	Configuration and status data
Triggered by the `system node autosupport invoke` command	Depends on the value specified in the `-type` parameter : • `test` sends a short message that triggers an automated response from the NetApp mail handler so that you can confirm that AutoSupport messages are being received. • `performance` sends performance data. • `all` sends a set of data similar to the weekly message and includes troubleshooting data from each subsystem.
Triggered by AutoSupport On Demand	AutoSupport On Demand can request new messages or past messages. The type of data included in those messages is as follows: **New messages** Depends on the type of AutoSupport collection, which can be `test`, `all`, or `performance`. **Past messages** Depends on the type of message that is resent.

AutoSupport subsystems

Each subsystem provides basic and troubleshooting information that AutoSupport uses for its messages. Each subsystem is also associated with trigger events that allow AutoSupport to only collect information from subsystems that is relevant to the trigger event.

You can view information about subsystems and trigger events by using the `system node autosupport trigger show` command.

AutoSupport size and time budgets

AutoSupport collects information, organized by subsystem, and enforces a size and time budget on content for each subsystem.

Default budgets

AutoSupport stops collecting information and truncates the AutoSupport content if the subsystem content exceeds its size or time budget. If the content cannot be truncated easily (for example, binary files), AutoSupport omits that file. When troubleshooting missing data from AutoSupport messages, you should review the manifest.xml file using an XML viewer, or the My AutoSupport web site.

You should modify the default size and time budgets only with guidance from technical support. The CLI for AutoSupport size and time budgets is a diagnostic privilege command set.

Subsystem	Size budget (bytes)	Time budget (seconds)
asup_ems	2097152	60

Subsystem	Size budget (bytes)	Time budget (seconds)
cifs	2097152	60
dedupe	3670016	120
ha	2097152	60
kernel	2097152	60
log_files	5242880	120
mandatory	unlimited	unlimited
mhost	3670016	120
mot	2097152	60
multistore	2097152	60
networking	2097152	60
nfs	2097152	60
nht	2097152	60
performance	3670016	120
performance_asup	3670016	120
platform	2097152	60
raid	2097152	60
repository	2097152	60
san	2097152	60
secd	2097152	60
snapmirror	2097152	60
snapvault	2097152	60
storage	10485760	180
wafl	10485760	300

Files sent in event-triggered AutoSupport messages

Event-triggered AutoSupport messages only contain basic and troubleshooting information from subsystems that are associated with the event that caused AutoSupport to generate the message. The specific data helps you troubleshoot the problem.

AutoSupport uses the following criteria to control content in event-triggered AutoSupport messages:

- Which subsystems are included
  Data is grouped into subsystems, including common subsystems, such as Log Files, and specific subsystems, such as RAID. Each event triggers a message that contains only the data from specific subsystems.
- The detail level of each included subsystem
  Data for each included subsystem is provided at a basic or troubleshooting level.

You can view all possible events and determine which subsystems are included in messages about each event using the `system node autosupport trigger show` command with the `-instance` parameter.

In addition to the subsystems that are included by default for each event, you can add additional subsystems at either a basic or a troubleshooting level using the `system node autosupport trigger modify` command.

Log files sent in AutoSupport messages

AutoSupport messages can contain several key log files that enable technical support staff and your internal support organization to review recent system activity.

All types of AutoSupport messages include the following log files when the Log Files subsystem is enabled:

Log file	Amount of data included from the file
• Log files from the `/mroot/etc/log/mlog/` directory • The MESSAGES log file	Only new lines added to the logs since the last AutoSupport message up to a specified maximum. This ensures that AutoSupport messages have unique, relevant—not overlapping—data. (Log files from partners are the exception; for partners, the maximum allowed data is included.)
• Log files from the `/mroot/etc/log/shelflog/` directory • Log files from the `/mroot/etc/log/acp/` directory • Event Management System (EMS) log data	The most recent lines of data up to a specified maximum.

Files sent in weekly AutoSupport messages

Weekly AutoSupport messages contain additional configuration and status data that is useful to track changes in your system over time.

The following information is sent in weekly AutoSupport messages:

- Basic information about every subsystem
- Contents of selected `/mroot/etc` directory files

- Log files
- Output of commands that provide system information
- Additional information, including replicated database (RDB) information, service statistics, and more

Structure of AutoSupport messages sent via email

When an AutoSupport message is sent via email, the message has a standard subject, a brief body, and a large attachment in 7z file format that contains the data.

Note: If AutoSupport is configured to hide private data, certain information, such as the hostname, is omitted or masked in the header, subject, body, and attachments.

Subject

The subject line of messages sent by the AutoSupport mechanism contains a text string that identifies the reason for the notification. The format of the subject line is as follows:

HA Group Notification from *System_Name* (*Message*) *Severity*

- *System_Name* is either the hostname or the system ID, depending on the AutoSupport configuration

Body

The body of the AutoSupport message contains the following information:

- Date and timestamp of the message
- Version of Data ONTAP on the node that generated the message
- System ID, serial number, and hostname of the node that generated the message
- AutoSupport sequence number
- SNMP contact name and location, if specified
- System ID and hostname of the HA partner node
- Whether Data ONTAP was booted in Cluster-Mode

Attached files

The key information in an AutoSupport message is contained in files that are compressed together into a 7z file called `body.7z` and attached to the message.

The files contained in the attachment are specific to the type of AutoSupport message.

AutoSupport severity types

AutoSupport messages have severity types that help you understand the purpose of each message—for example, to draw immediate attention to a critical problem, or only to provide information.

Messages have one of the following severities:

- Critical: critical conditions
- Error: error conditions
- Warning: warning conditions
- Notice: normal but significant condition
- Info: informational message
- Debug: debug-level messages

If your internal support organization receives AutoSupport messages via email, the severity appears in the subject line of the email message.

AutoSupport transport protocols

AutoSupport supports HTTPS, HTTP, and SMTP as the transport protocols for delivering AutoSupport messages to NetApp technical support. All of these protocols run on IPv4 or IPv6 based on the address family to which the name resolves. If you enable AutoSupport messages to your internal support organization, those messages are sent by SMTP.

Protocol availability varies with the destination of the AutoSupport messages:

- If you enable AutoSupport to send messages to NetApp technical support, you can use any of the following transport protocols:

Protocol and port	Description
HTTPS on port 443	This is the default protocol. You should use this whenever possible. The certificate from the remote server is validated against the root certificate, unless you disable validation. The delivery uses an HTTP PUT request. With PUT, if the request fails during transmission, the request restarts where it left off. If the server receiving the request does not support PUT, the delivery uses an HTTP POST request.
HTTP on port 80	This protocol is preferred over SMTP. The delivery uses an HTTP PUT request. With PUT, if the request fails during transmission, the request restarts where it left off. If the server receiving the request does not support PUT, the delivery uses an HTTP POST request.
SMTP on port 25	You should use this protocol only if the network connection does not allow HTTPS or HTTP, because SMTP can introduce limitations on message length and line length.

- If you configure AutoSupport with specific email addresses for your internal support organization, those messages are always sent by SMTP.

For example, if you use the recommended protocol to send messages to NetApp technical support and you also want to send messages to your internal support organization, your messages would be transported using both HTTPS and SMTP, respectively.

AutoSupport limits the maximum file size for each protocol. The default setting for HTTP and HTTPS transfers is 10 MB. The default setting for SMTP transfers is 5 MB. If the size of the AutoSupport message exceeds the configured limit, AutoSupport delivers as much of the message as possible. You can edit the maximum size by modifying AutoSupport configuration. See the `system node autosupport modify` man page for more information.

The protocols require the following additional configuration:

- If you use HTTP or HTTPS to send AutoSupport messages to NetApp technical support and you have a proxy, you must identify the URL for that proxy.

  If the proxy uses a port other than the default port, which is 3128, you can specify the port for that proxy. You can also specify a username and password for proxy authentication.
- If you use SMTP to send AutoSupport messages either to your internal support organization or to NetApp technical support, you must have an external mail server.

  The storage system does not function as a mail server—it requires an external mail server at your site to send mail. The mail server must be a host that listens on the SMTP port (25), and it must be configured to send and receive 8-bit Multipurpose Internet Mail Extensions (MIME) encoding. Example mail hosts include a UNIX host running an SMTP server such as the sendmail program and a Windows NT server running the Microsoft Exchange server. You can have one or more mail hosts.

No matter what transport protocol you use, you can use IPv4 or IPv6 addresses based on the address family to which the name resolves.

Setting up AutoSupport

You can control whether and how AutoSupport information is sent to NetApp technical support and your internal support organization, and then test that the configuration is correct.

About this task

Perform this procedure on each node in your system where you want to configure AutoSupport.

For more information about the following commands, see the man pages.

Steps

1. Ensure AutoSupport is enabled by setting the `-state` parameter of the `system node autosupport modify` command to `enable`.
2. If you want technical support to receive AutoSupport messages, set the following parameters of the `system node autosupport modify` command:
   a) Set `-support` to `enable`.
   b) Select a transport protocol for messages to NetApp technical support by setting `-transport` to `smtp`, `http`, or `https`.
   c) If you chose HTTP or HTTPS as the transport protocol and you use a proxy, set `-proxy-url` to the URL of your proxy.

3. If you want your internal support organization or a support partner to receive AutoSupport messages, perform the following actions:

   a) Identify the recipients in your organization by setting the following parameters of the `system node autosupport modify` command:

Set this parameter	To this
`-to`	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive key AutoSupport messages
`-noteto`	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive a shortened version of key AutoSupport messages designed for cell phones and other mobile devices
`-partner-address`	Up to five comma-separated individual email addresses or distribution lists in your support partner organization that will receive all AutoSupport messages

   b) Check that addresses are correctly configured by listing the destinations using the `system node autosupport destinations show` command.

4. If you are sending messages to your internal support organization or you chose SMTP transport for messages to technical support, configure SMTP by setting the following parameters of the `system node autosupport modify` command:

   - Set `-mail-hosts` to one or more mail hosts, separated by commas. You can set a maximum of five.
   - Set `-from` to the email address that sends the AutoSupport message.
   - Set `-max-smtp-size` to the email size limit of your SMTP server.

5. If you want AutoSupport to specify a fully qualified domain name when it sends connection requests to your SMTP mail server, configure DNS.

   For information about configuring DNS, see the *Clustered Data ONTAP Network Management Guide*.

6. Optional: Change the following settings:

If you want to do this...	Set the following parameters of the `system node autosupport modify` command...
Hide private data by removing, masking, or encoding sensitive data in the messages	Set `-remove-private-data` to `true`. **Note:** If you change from `false` to `true`, all AutoSupport history and all associated files are deleted.
Stop sending performance data in periodic AutoSupport messages	Set `-perf` to `false`.

7. Check the overall configuration using the `system node autosupport show` commandwith the `-node` parameter.
8. Test that AutoSupport messages are being sent and received:
   a) Use the `system node autosupport invoke` command with the `-type` parameter set to `test`.

      Example

      ```
      cluster1::> system node autosupport invoke -type test -node node1
      ```

   b) Confirm that NetApp is receiving your AutoSupport messages by checking the email address that technical support has on file for the system owner, who should have received an automated response from the NetApp mail handler.
   c) Optional: Confirm that the AutoSupport message is being sent to your internal support organization or to your support partner by checking the email of any address that you configured for the `-to` , `-noteto` , or `-partner-address` parameters of the `system node autosupport modify` command.

Related tasks

Troubleshooting AutoSupport when messages are not received on page 218

Getting AutoSupport message descriptions

The descriptions of the AutoSupport messages that you receive are available through the online AutoSupport Message Matrices page.

Steps

1. Go to the AutoSupport Message Matrices page: *support.netapp.com/NOW/knowledge/docs/olio/autosupport/matrices/*
2. On the AutoSupport Message Matrices page under Select a Release, select your version of Data ONTAP and click **View Matrix**.

The Syslog Translator page appears with all AutoSupport message descriptions listed alphabetically by subject line.

Commands for managing AutoSupport

You use the `system node autosupport` commands to change or view AutoSupport configuration, display information about past AutoSupport messages, and send or resend an AutoSupport message.

Configure AutoSupport

If you want to...	Use this command...
Control whether any AutoSupport messages are sent	`system node autosupport modify` with the `-state` parameter
Control whether AutoSupport messages are sent to technical support	`system node autosupport modify` with the `-support` parameter
Set up AutoSupport or modify the configuration of AutoSupport	`system node autosupport modify`
Enable and disable AutoSupport messages to your internal support organization for individual trigger events, and specify additional subsystem reports to include in messages sent in response to individual trigger events	`system node autosupport trigger modify`

Display information about the configuration of AutoSupport

If you want to...	Use this command...
Display the AutoSupport configuration	`system node autosupport show` with the `-node` parameter
View a summary of all addresses and URLs that receive AutoSupport messages	`system node autosupport destinations show`
Display which AutoSupport messages are sent to your internal support organization for individual trigger events	`system node autosupport trigger show`

Display information about past AutoSupport messages

If you want to...	Use this command...
Display information about one or more of the 50 most recent AutoSupport messages	`system node autosupport history show`

If you want to...	Use this command...
View the information in the AutoSupport messages including the name and size of each file collected for the message along with any errors	`system node autosupport manifest show`

Send or resend AutoSupport messages

If you want to...	Use this command...
Retransmit a locally stored AutoSupport message, identified by its AutoSupport sequence number **Note:** If you retransmit an AutoSupport message, and if support already received that message, the support system will not create a duplicate case. If, on the other hand, support did not receive that message, then the AutoSupport system will analyze the message and create a case, if necessary.	`system node autosupport history retransmit`
Generate and send an AutoSupport message—for example, for testing purposes	`system node autosupport invoke` **Note:** Use the `-force` parameter to send a message even if AutoSupport is disabled. Use the `-uri` parameter to send the message to the destination you specify instead of the configured destination.

For more information, see the man pages.

Information included in the AutoSupport manifest

The AutoSupport manifest provides a detailed view of the files collected for each event-triggered AutoSupport message. The AutoSupport manifest also includes information about collection errors when AutoSupport cannot collect the files it needs.

The AutoSupport manifest includes the following information:

- Sequence number of the event-triggered AutoSupport message
- Which files AutoSupport included in the event-triggered AutoSupport message
- Size of each file, in bytes
- Status of the AutoSupport manifest collection
- Error description, if AutoSupport failed to collect one or more files

You can view the AutoSupport manifest by using the `system node autosupport manifest show` command.

This AutoSupport manifest is included with every AutoSupport message and presented in XML format, which means you can use a generic XML viewer to read AutoSupport messages.

What My AutoSupport is

My AutoSupport is a web-based application, working in conjunction with AutoSupport, that presents information enabling you to easily analyze data to model and optimize your storage infrastructure.

My AutoSupport is a web-based application hosted on the NetApp Support Site at *support.netapp.com* that you can access using a browser. Your system must have AutoSupport enabled and configured so that it sends data back to NetApp.

My AutoSupport provides a dashboard from which you can perform the following actions:

- Generate reports and export them to PDF or CSV files
- View information about configurations, performance, system health, installed software, and storage efficiency
- Access system and AutoSupport tools

You can access My AutoSupport by going to *http://support.netapp.com/NOW/asuphome/*.

Troubleshooting AutoSupport

If you do not receive AutoSupport messages, you can check a number of settings to resolve the problem.

Troubleshooting AutoSupport when messages are not received

If the system does not send the AutoSupport message, you can determine whether that is because AutoSupport cannot generate the message or cannot deliver the message.

Steps

1. Check delivery status of the messages by using the `system node autosupport history show` command.
2. Read the status.

This status	Means
initializing	The collection process is starting. If this state is temporary, all is well. However, if this state persists, there is an issue.
collection-failed	AutoSupport cannot create the AutoSupport content in the spool directory. You can view what AutoSupport is trying to collect by entering the `system node autosupport history show -detail` command.

This status	Means
collection-in-progress	AutoSupport is collecting AutoSupport content. You can view what AutoSupport is collecting by entering the `system node autosupport manifest show` command.
queued	AutoSupport messages are queued for delivery, but not yet delivered.
transmitting	AutoSupport is currently delivering messages.
sent-successful	AutoSupport successfully delivered the message. You can find out where AutoSupport delivered the message by entering the `system node autosupport history show -delivery` command.
ignore	AutoSupport has no destinations for the message. You can view the delivery details by entering the `system node autosupport history show -delivery` command.
re-queued	AutoSupport tried to deliver messages, but the attempt failed. As a result, AutoSupport placed the messages back in the delivery queue for another attempt. You can view the error by entering the `system node autosupport history show` command.
transmission-failed	AutoSupport failed to deliver the message the specified number of times and stopped trying to deliver the message. You can view the error by entering the `system node autosupport history show` command.
ondemand-ignore	The AutoSupport message was processed successfully, but the AutoSupport On Demand service chose to ignore it.

3. Perform one of the following actions:

For this status	Do this
initializing or collection-failed	Contact technical support because AutoSupport cannot generate the message.
ignore, re-queued, or transmission failed	Check that destinations are correctly configured for SMTP, HTTP, or HTTPS because AutoSupport cannot deliver the message.

Related tasks

Troubleshooting AutoSupport over SMTP on page 220
Troubleshooting AutoSupport over HTTP or HTTPS on page 220

Troubleshooting AutoSupport over HTTP or HTTPS

If the system does not send the expected AutoSupport message and you are using HTTP or HTTPS, you can check a number of settings to resolve the problem.

Before you begin

You determined that AutoSupport can generate the message, but not deliver the message over HTTP or HTTPS.

Steps

1. At the storage system's CLI, ensure that DNS is enabled and configured correctly by entering the following command:

   `vserver services dns`

2. Read the error for the AutoSupport message by using the `system node autosupport history show` command with the `-seq-num` and `-destination` parameters.
3. At the storage system's CLI, ensure that the system is routing out to the Internet successfully by entering the following command:

   `network traceroute`

4. Use the `system node run` command to run the nodeshell CLI on a specific node, and use the `rdfile` command to read the `/etc/log/mlog/notifyd.log` file.

Related tasks

Troubleshooting AutoSupport when messages are not received on page 218

Troubleshooting AutoSupport over SMTP

If the system does not send the AutoSupport message and you are using SMTP, you can check a number of settings to resolve the problem.

Before you begin

You determined that AutoSupport can generate the message, but not deliver the message over SMTP.

Steps

1. At the storage system's CLI, ensure that DNS for the cluster is enabled and configured correctly by entering the following command:

   `vserver services dns`

2. At the storage system's CLI, check that the mail host specified in the configuration is a host that the storage system can talk to by entering the following command:

   `network ping -node` *`node_name`* `-destination` *`mailhost`*

mailhost is the name or IP address of your mail host.

3. Log on to the host designated as the mail host, and make sure that it can serve SMTP requests by entering the following command (25 is the listener SMTP port number):

   netstat -aAn|grep 25

   A message will appear, similar to the following text:

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

4. At the storage system's CLI, ensure that the system is reaching the mail host successfully by entering the following command:

   network traceroute

5. From some other host, telnet to the SMTP port by entering the following command:

   telnet mailhost 25

   A message similar to the following text is displayed:

   ```
   Trying 192.9.200.16 ...
   Connected to filer.
   Escape character is '^]'.
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 95
   10:49:04 PST
   ```

6. Use the `system node run` command to run the nodeshell CLI on a specific node, and use the `rdfile` command to read the `/etc/log/mlog/notifyd.log` file.

Related tasks

Troubleshooting AutoSupport when messages are not received on page 218

Troubleshooting EMS events about rejected or failed SMTP attempts

If the system attempted to send an AutoSupport email, but the attempt resulted in an EMS event about a rejected or failed SMTP or an unknown user, you can check the relaying configuration for the mail host to determine whether relaying is denied or incorrectly configured.

About this task

The EMS identifiers for this event are `asup.smtp.fail` and `asup.smtp.reject`. You can use the EMS identifiers to view a description of the messages in the Syslog Translator on the NetApp Support Site.

Steps

1. From a Windows, UNIX, or Linux host, telnet to port 25 of the mail host by entering the following command:

```
telnet mailhost 25
```

2. Test whether relaying is denied on the mail host.
   a) Enter the following commands:

      ```
      HELO DOMAIN NAME
      MAIL FROM: your_email_address
      RCPT TO: autosupport@netapp.com
      ```

   b) If you receive a message similar to `relaying denied`, contact the mail host vendor because relaying is denied. Otherwise, continue to the next step.
3. Test whether relaying is incorrectly configured on the mail host.
   a) Enter the following commands:

      ```
      DATA
      SUBJECT: TESTING
      THIS IS A TEST
      .
      ```

      Note: Ensure that you enter the last period (.) on a line by itself. The period indicates to the mail host that the message is complete.

   b) If you receive a message similar to `unknown user` or `unknown mailbox`, contact the mail host vendor because relaying is incorrectly configured.

Monitoring the health of your system

Health monitors proactively monitor certain critical conditions in your cluster and raise alerts if they detect a fault or risk. If there are active alerts, the system health status reports a degraded status for the cluster. The alerts include the information that you need to respond to degraded system health.

If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions. After you resolve the problem, the system health status automatically returns to OK.

The system health status reflects multiple separate health monitors. A degraded status in an individual health monitor causes a degraded status for the overall system health.

How health monitoring works

Individual health monitors have a set of health policies that trigger alerts when certain conditions or state changes occur. Understanding how health monitoring works can help you respond to problems and control future alerts.

Health monitoring consists of the following components:

- Individual health monitors for specific subsystems, each of which has its own health status
  For example, the Storage subsystem has a node connectivity health monitor.

- An overall system health monitor that consolidates the health status of the individual health monitors

  A degraded status in any single subsystem results in a degraded status for the entire system. If no subsystems have alerts, the overall system status is OK.

Each health monitor is made up of the following key elements:

- Alerts that the health monitor can potentially raise

  Each alert has a definition, which includes details such as the severity of the alert and its probable cause.
- Health policies that identify when each alert is triggered

  Each health policy has a rule expression, which is the exact condition or change that triggers the alert.

A health monitor continuously monitors and validates the resources in its subsystem for condition or state changes. When a condition or state change matches a rule expression in a health policy, the health monitor raises an alert. An alert causes the subsystem's health status and the overall system health status to become degraded.

How you can respond to system health alerts

When a system health alert occurs, you can acknowledge it, learn more about it, repair the underlying condition, and prevent it from occurring again.

When a health monitor raises an alert, you can respond in any of the following ways:

- Get information about the alert, which includes the affected resource, alert severity, probable cause, possible effect, and corrective actions.
- Get detailed information about the alert, such as the time when the alert was raised and whether anyone else has acknowledged the alert already.
- Get health-related information about the state of the affected resource or subsystem, such as a specific shelf or disk.
- Acknowledge the alert to indicate that someone is working on the problem, and identify yourself as the "Acknowledger."
- Resolve the problem by taking the corrective actions provided in the alert, such as fixing cabling to resolve a connectivity problem.
- Delete the alert, if the system did not automatically clear it.
- Suppress an alert to prevent it from affecting the health status of a subsystem.

  Suppressing is useful when you understand a problem. After you suppress an alert, it can still occur, but the subsystem health displays as "ok-with-suppressed" when the suppressed alert occurs.

How you can control when system health alerts occur

You can control which alerts a health monitor generates by enabling and disabling the system health policies that define when alerts are triggered. This enables you to customize the health monitoring system for your particular context.

You can learn the name of a policy either by displaying detailed information about a generated alert or by displaying policy definitions for a specific health monitor, node, or alert ID.

Disabling health policies is different from suppressing alerts. When you suppress an alert, it doesn't affect the subsystem's health status, but the alert can still occur.

If you disable a policy, the condition or state that is defined in its policy rule expression no longer triggers an alert.

Example of an alert that you want to disable

For example, suppose an alert occurs that is not useful to you. You use the `system health alert show –instance` command to obtain the Policy ID for the alert. You use the policy ID in the `system health policy definition show` command to view information about the policy. After reviewing the rule expression and other information about the policy, you decide to disable the policy. You use the `system health policy definition modify` command to disable the policy.

How health alerts trigger AutoSupport messages and events

System health alerts trigger AutoSupport messages and events in the Event Management System (EMS), making it possible to monitor the health of the system using AutoSupport messages and the EMS in addition to using the health monitoring system directly.

Your system sends an AutoSupport message within five minutes of an alert. The AutoSupport message includes all alerts generated since the last AutoSupport message, except for alerts that duplicate an alert for the same resource and probable cause within the last week.

Some alerts do not trigger AutoSupport messages. An alert does not trigger an AutoSupport message if its health policy disables the sending of AutoSupport messages. For example, a health policy might disable AutoSupport messages by default because AutoSupport already generates a message when the problem occurs. You can configure policies to not trigger AutoSupport messages by using the `system health policy definition modify` command.

You can view a list of all of the alert-triggered AutoSupport messages sent in the last week using the `system health autosupport trigger history show` command.

Alerts also trigger the generation of events to the EMS. An event is generated each time an alert is created and each time an alert is cleared.

What health monitors are available

There are several health monitors that monitor different parts of a cluster.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
Cluster switch (cluster-switch)	Switch (Switch-Health)	Monitors cluster network switches and management network switches for temperature, utilization, interface configuration, redundancy (cluster network switches only), and fan and power supply operation. The cluster switch health monitor communicates with switches through SNMP. SNMPv2c is the default setting.
Node connectivity (node-connect)	CIFS non-disruptive operations (CIFS-NDO)	Monitors SMB connections to ensure non-disruptive operations to Hyper-V applications.
	Storage (SAS-connect)	Monitors shelves, disks, and adapters at the node level to ensure that they have appropriate paths and connections.
System	n/a	Aggregates information from other health monitors.
System connectivity (system-connect)	Storage (SAS-connect)	Monitors shelves at the cluster level to ensure that all shelves always have appropriate paths to two HA clustered nodes.

Getting notified of system health alerts

You can view system health alerts by using the `system health alert show` command. However, you should subscribe to specific Event Management System (EMS) messages to receive notifications when a health monitor generates an alert.

About this task

The following procedure shows you how to set up notifications for all hm.alert.raised messages and all hm.alert.cleared messages.

Steps

1. Use the `event destination create` command to define the destination to which you want to send the EMS messages.

Example

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Use the `event route add-destinations` command to route the hm.alert.raised message and the hm.alert.cleared message to a destination.

Example

```
cluster1::> event route add-destinations -messagename hm.alert* -
destinations health_alerts
```

Related concepts

Managing event messages on page 198

Responding to degraded system health

When your system's health status is degraded, you can show alerts, read about the probable cause and corrective actions, show information about the degraded subsystem, and resolve the problem.

About this task

You can discover that an alert was generated by viewing an AutoSupport message, an EMS event, or by using the `system health` commands.

Steps

1. Use the `system health alert show` command to view the alerts that are compromising the system's health.
2. Read the alert's probable cause, possible effect, and corrective actions to determine if you can resolve the problem or if you need more information.
3. If you need more information, take any of the following actions:
   - Use the `system health alert show -instance` command to view additional information available for the alert.
   - Use the specific commands in the `system health` command directory for the affected subsystem to investigate the problem.

Example

For example, if a disk has a problem, use the `system health node-connectivity disk` command to get more information about the disk.

4. Optional: Use the `system health alert modify` command with the `-acknowledge` parameter to indicate that you are working on a specific alert.

5. Take corrective action to resolve the problem as described by the Corrective Actions field in the alert.

   The Corrective Actions might include rebooting the system.

   When the problem is resolved, the alert is automatically cleared. If the subsystem has no other alerts, the health of the subsystem changes to OK. If the health of all subsystems is OK, the overall system health status changes to OK.

6. Use the `system health status show` command to confirm that the system health status is OK.

   If the system health status is not OK, repeat this procedure.

Example of responding to degraded system health

By reviewing a specific example of degraded system health caused by a shelf that lacks two paths to a node, you can see what the CLI displays when you respond to an alert.

After starting Data ONTAP, you check the system health and you discover that the status is degraded.

```
cluster1::>system health status show
        Status
        ---------------
        degraded
```

You show alerts to find out where the problem is, and see that shelf 2 does not have two paths to node1.

```
cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two paths following the
rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

You display details about the alert to get more information, including the alert ID.

```
cluster1::>system health alert show -monitor node-connect -alert-id DualPathToDiskShelf_Alert
-
instance
                 Node: node1
              Monitor: node-connect
             Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
            Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller node1.
    Corrective Actions: 1. Halt controller node1 and all controllers attached to disk shelf 2.
```

```
                        2. Connect disk shelf 2 to controller node1 via two paths following
the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
              Suppress: false
                Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

You acknowledge the alert to indicate that you are working on it.

```
cluster1::>system health alert modify -node node1 -alert-id DualPathToDiskShelf_Alert -
acknowledge true
```

You fix the cabling between shelf 2 and node1, and reboot the system. Then you check system health again, and see that the status is OK.

```
cluster1::>system health status show
        Status
        ---------------
        OK
```

Configuring discovery of cluster and management network switches

The cluster switch health monitor automatically attempts to discover your cluster and management network switches using the Cisco Discovery Protocol (CDP). You need to configure the health monitor if it cannot automatically discover a switch or if you do not want to use CDP for automatic discovery.

About this task

The `system health cluster-switch show` command lists the switches that the health monitor discovered. If you do not see a switch in that list, then the health monitor cannot automatically discover it.

Steps

1. If you want to use CDP for automatic discovery, do the following, otherwise, go to step 2:
   a) Ensure that the Cisco Discovery Protocol (CDP) is enabled on your switches.

      Refer to your switch documentation for instructions.
   b) Run the following command on each node in the cluster to verify whether CDP is enabled or disabled:

      run -node *node_name* -command options cdpd.enable

If CDP is enabled, go to step d. If CDP is disabled, go to step c.

c) Run the following command to enable CDP:

run -node *node_name* -command options cdpd.enable on

Wait five minutes before you go to the next step.

d) Use the `system health cluster-switch show` command to verify whether Data ONTAP can now automatically discover the switches.

2. If the health monitor cannot automatically discover a switch, use the `system health cluster-switch create` command to configure discovery of the switch.

Example

```
cluster1::> system health cluster-switch create -device switch1 -
address 192.0.2.250 -snmp-version SNMPv2c -community cshm1! -
discovered false -model NX5020 -type cluster-network
```

Wait five minutes before you go to the next step.

3. Use the `system health cluster-switch show` command to verify whether Data ONTAP can discover the switch for which you added information.

After you finish

Verify that the health monitor can monitor your switches.

Verifying the monitoring of cluster and management network switches

The cluster switch health monitor automatically attempts to monitor the switches that it discovers; however, monitoring might not happen automatically if the switches are not configured correctly. You should verify that the health monitor can monitor your switches.

Steps

1. Use the `system health cluster-switch show` command to identify the switches that the cluster switch health monitor discovered.

   If the `Model` column displays the value `OTHER`, then Data ONTAP cannot monitor the switch. Data ONTAP sets the value to `OTHER` if a switch that it automatically discovers is not supported for health monitoring.

   Note: If a switch does not display in the command output, then you need to configure discovery of the switch.

2. Upgrade to the latest supported switch software and reference configuration file (RCF) from the *Cisco Ethernet Switch page*.

   The community string in the switch's RCF must match the community string that the health monitor is configured to use. By default, the health monitor uses the community string `cshm1!`

If necessary, you can modify the community string that the health monitor uses by using the `system health cluster-switch modify` command.

3. Verify that the switch's management port is connected to the management network.

   This connection is required to perform SNMP queries.

Related tasks

Configuring discovery of cluster and management network switches on page 228

Commands for monitoring the health of your system

You can use the `system health` commands to display information about the health of system resources, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

Displaying health status

If you want to...	Use this command...
Display the health status of the system, which reflects the overall status of individual health monitors	`system health status show`
Display the health status of subsystems for which health monitoring is available	`system health subsystem show`

Displaying the status of cluster connectivity

If you want to...	Use this command...
Display the status of shelves from the cluster-level view, including the shelf's UUID and ID, its connected nodes, and the number of paths to the shelf	`system health system-connectivity shelf show` **Note:** Use the `-instance` parameter to display detailed information about each shelf.

Displaying the status of node connectivity

If you want to...	Use this command...
Display the status of shelves from the node-level view, along with other information, such as the owner node, shelf name, and how many disks and paths the shelf has	`system health node-connectivity shelf show` **Note:** Use the `-instance` parameter to display detailed information about each shelf.

If you want to...	Use this command...
Display the status of disks, along with other information, such as the owner node, disk name and bay number, and the number of paths to the disk	`system health node-connectivity disk show` **Note:** Use the `-instance` parameter to display detailed information about each disk.
Display the status of adapters, along with other information, such as the owner node, whether they are used and enabled, and the number of shelves attached	`system health node-connectivity adapter show` **Note:** Use the `-instance` parameter to display detailed information about each adapter.

Displaying the status of cluster and management network switches

If you want to...	Use this command...
Display the status and configuration of network interfaces	`system health cluster-switch interface show`
Display the status of fans	`system health cluster-switch fan show`
Display temperature status	`system health cluster-switch temperature show`
Display the status of power supplies	`system health cluster-switch power show`
Display CPU and memory utilization	`system health cluster-switch utilization show`

Managing the discovery of cluster and management network switches

If you want to...	Use this command...
Display the switches that the cluster monitors	`system health cluster-switch show`
Configure discovery of an undiscovered switch	`system health cluster-switch create`
Modify information about a switch that the cluster monitors (for example, device name, IP address, SNMP version, and community string)	`system health cluster-switch modify` **Note:** This command is available at the advanced privilege level.
Display the interval in which the health monitor polls switches to gather information	`system health cluster-switch polling-interval show`

If you want to...	Use this command...
Modify the interval in which the health monitor polls switches to gather information	`system health cluster-switch polling-interval modify`
Disable discovery and monitoring of a switch	`system health cluster-switch delete` **Note:** This command is available at the advanced privilege level.

Responding to generated alerts

If you want to...	Use this command...
Display information about generated alerts, such as the resource and node where the alert was triggered, and the alert's severity and probable cause.	`system health alert show` **Note:** Use the `-instance` parameter to display detailed information about each generated alert. Use other parameters to filter the list of alerts—for example, by node, resource, severity, and so on.
Indicate that someone is working on an alert	`system health alert modify` with the `-acknowledge` parameter
Suppress a subsequent alert so that it does not affect the health status of a subsystem	`system health alert modify` with the `-suppress` parameter
Delete an alert that was not automatically cleared	`system health alert delete`
Display information about the AutoSupport messages that alerts triggered within the last week—for example, to determine if an alert triggered an AutoSupport message	`system health autosupport trigger history show`

Configuring future alerts

If you want to...	Use this command...
Enable or disable the policy that controls whether a specific resource state raises a specific alert	`system health policy definition modify`

Displaying information about how health monitoring is configured

If you want to...	Use this command...
Display information about health monitors, such as their nodes, names, subsystems, and status	`system health config show` **Note:** Use the `-instance` parameter to display detailed information about each health monitor.
Display information about the alerts that a health monitor can potentially generate	`system health alert definition show` **Note:** Use the `-instance` parameter to display detailed information about each alert definition.
Display information about health monitor policies, which determine when alerts are raised	`system health policy definition show` **Note:** Use the `-instance` parameter to display detailed information about each policy. Use other parameters to filter the list of alerts—for example, by policy status (enabled or not), health monitor, alert, and so on.

For more information, see the man pages for the commands.

Using dashboards to display critical system information

Dashboards provide visibility into critical aspects of your cluster, including Vserver health, system and cluster performance, and storage space utilization. You can also configure alarm thresholds and view information about alarms.

You can configure alarm thresholds for the following:

- Aggregate utilization (aggregate-used)
- Average client latency of NFS and CIFS operations (op-latency)
- CPU utilization (cpu-busy)
- Packet error ratio (port-problems)
- Port utilization (port-util)

For example, you can modify the warning and critical alarm thresholds for space used on aggregates. You might set the warning threshold to 50% and the critical threshold to 60%. The cluster generates an "over threshold" alarm when the value exceeds the configured threshold. In addition, the Event Management System (EMS) generates a message when an alarm is generated or cleared, if you configured it to do so.

Getting notified of dashboard alarms

You can view dashboard alarms by using the `dashboard alarm show` command. You can also subscribe to specific Event Management System (EMS) messages to receive notifications of dashboard alarms.

Before you begin

You must have used the `dashboard alarm thresholds modify` command to specify that the EMS sends a message when an alarm is generated.

About this task

The EMS generates messages for dashboard alarms when the threshold value is equal or greater than the critical threshold (rising) and when the threshold value is less than the warning value (falling). You need to route EMS messages for the object type for which you want alarm notifications:

aggregate-used	The following EMS messages are related to this object type: • mgmtgwd.aggregate.used.rising • mgmtgwd.aggregate.used.falling
cpu-busy	The following EMS messages are related to this object type: • mgmtgwd.cpu.busy.rising • mgmtgwd.cpu.busy.falling
op-latency	The following EMS messages are related to this object type: • mgmtgwd.op.latency.rising • mgmtgwd.op.latency.falling
port-problems	The following EMS messages are related to this object type: • mgmtgwd.port.problems.rising • mgmtgwd.port.problems.falling
port-util	The following EMS messages are related to this object type: • mgmtgwd.port.util.rising • mgmtgwd.port.util.falling

Steps

1. Use the `event destination create` command to define the destination to which you want to send the EMS messages.

Example

```
cluster1::> event destination create -name dashboard_alarms -mail
admin@example.com
```

2. Use the `event route add-destinations` command to route EMS messages to a destination.

Example

The following example specifies that aggregate utilization messages go to the destination named dashboard_alarms.

```
cluster1::> event route add-destinations -messagename
mgmtgwd.aggregate.used* -destinations dashboard_alarms
```

Example

The following example specifies that all dashboard alarm messages go to the destination named dashboard_alarms.

```
cluster1::> event route add-destinations -messagename
mgmtgwd.aggregate.used*,mgmtgwd.port.problems*,mgmtgwd.op.latency*,
mgmtgwd.port.util*,mgmtgwd.cpu.busy* -destinations dashboard_alarms
```

Commands for managing dashboards

You use the `dashboard` commands to configure dashboards, display dashboard information, and display health status for Vservers.

Note: The `dashboard health vserver` commands support the NFS and CIFS protocols. They do not support the FC and iSCSI protocols.

If you want to...	Use this command...
Configure the following cluster-wide alarm settings: • The threshold value that generates a warning or critical alarm for an event • Whether an EMS message is sent when an alarm is generated • The interval at which objects are monitored by the alarm dashboard	`dashboard alarm thresholds modify`
Display settings about alarm thresholds	`dashboard alarm thresholds show`

If you want to...	Use this command...
Display information about alarms whose values exceed the configured threshold value	`dashboard alarm show`
Display information about system and cluster performance	`dashboard performance show`
Display information about storage space utilization and trend	`dashboard storage show`
Display information about general Vserver health, including the current operational status, issues, critical alerts, warnings, and informational messages	`dashboard health vserver show`
Display the health status of aggregates, LIFs, ports, protocols, and volumes in Vservers	`dashboard health vserver show-combined`
Display the health status of aggregates in Vservers	`dashboard health vserver show-aggregate`
Display the health status of volumes in Vservers	`dashboard health vserver show-volume`
Display the health status of LIFs in Vservers	`dashboard health vserver show-lif`
Display the health status of Vserver network ports	`dashboard health vserver show-port`
Display the health status of protocols in Vservers	`dashboard health vserver show-protocol`

For more information, see the man pages.

Monitoring cluster performance

You can view data about your cluster to monitor cluster performance. For example, you can monitor the performance of volumes by viewing statistics that show throughput and latency.

What objects, instances, and counters are

You can view performance data for specific objects in your cluster. Objects are comprised of instances and counters. Counters provide data about the instances of an object.

An object is any of the following:

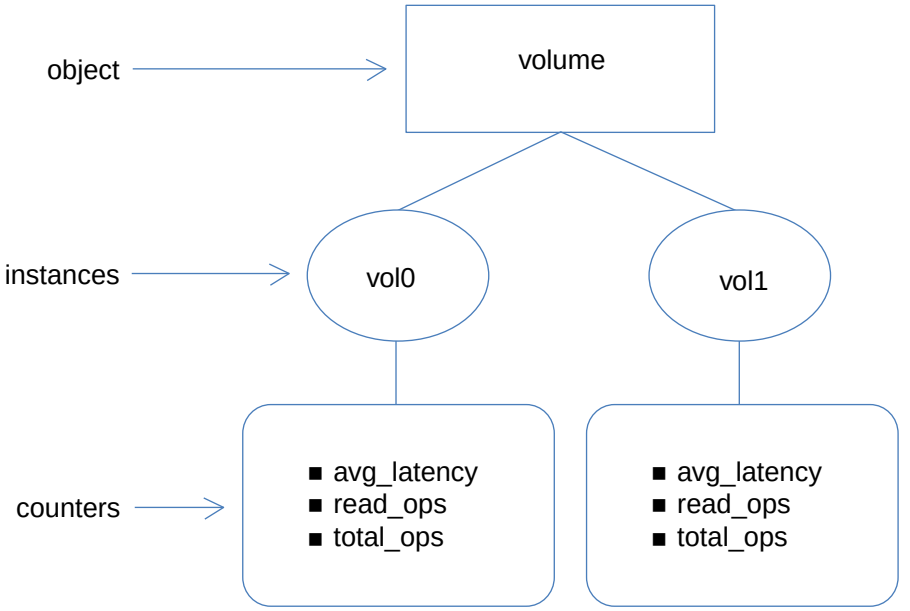
- Physical entities such as disks, processors, and ports
- Logical entities such as LUNs, volumes, and workloads
- Protocols such as CIFS, NFS, iSCSI, and FC

Each object has zero or more instances. For example, the LUN object has an instance for each LUN in your cluster.

A counter is a predefined performance metric that provides data about an object. Examples of data that counters provide include the following:

- Disk capacity
- The average latency for a volume
- The number of established SMB and SMB2 sessions

The following illustration shows the relationship between an object and its instances and counters. In this illustration, the volume object has two instances: vol0 and vol1. The object's counters provide data about each of these instances. The illustration shows three of the object's counters: avg_latency, read_ops, and total_ops.



Decisions to make before you view performance data

You can view performance data in several ways. You should make a few decisions before you view the data.

You should decide the following before you view performance data:

Decision	Considerations
How do you want to retrieve and display the data?	You have two choices: • You can collect and view a set of data for a specific time period. If you choose this option, you can view data for several objects and instances at a time. • You can view continuously updated data. If you choose this option, you can view data for only one object and one instance at a time.
For which objects do you want to view data?	You need to specify at least one object for which you want to view data.
Do you want data from all counters or from specific counters?	The default setting shows data for all counters in an object; however, you can specify specific counters to get the exact data that you need.
Do you want data for all instances of an object or for specific instances?	• If you collect data for a time period, the default setting shows data for all instances; however, you can specify one or more instances. • If you view continuously updated data and specify any object other than `cluster`, you must specify an instance.
Do you want data for the entire cluster or do you want to scope the data?	The default setting shows data for the entire cluster; however, you can scope the data to a specific Vserver or a specific node.

Viewing performance data for a time period

You can monitor cluster performance by collecting and viewing data for a specific time period (a sample). You can view data for several objects and instances at a time.

About this task

You can collect more than one data sample at a time. You can collect more than one sample from the same object at the same time.

Note: You cannot collect and view data for an object that has more than 5,000 instances. If an object has more than 5,000 instances, you need to specify the specific instances for which you want data.

For more information about the `statistics` commands, see the man pages.

Steps

1. Use the `statistics start` command to start collecting data.

   If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

2. Optional: Use the `statistics stop` command to stop collecting data for the sample.

   You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify performance trends.

3. Use the `statistics show` command to view the sample data.

Example: Monitoring NFSv3 performance

The following example shows performance data for the NFSv3 protocol.

The following command starts data collection for a new sample:

```
cluster1::> statistics start -object nfsv3 -sample-id nfs_sample
```

The following command shows data from the sample by specifying counters that show the number of successful read and write requests versus the total number of read and write requests:

```
cluster1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ---------------------------
    read_success                                40042
    read_total                                  40042
    write_success                             1492052
    write_total                               1492052
```

Viewing continuously updated performance data

You can monitor cluster performance by viewing data that continuously updates with the latest status. You can view data for only one object and one instance at a time.

About this task

For more information about the `statistics show-periodic` command, see the man page.

Step

1. Use the `statistics show-periodic` command to view continuously updated performance data.

   If you do not specify the `-object` parameter, the command returns summary data for the cluster.

Example: Monitoring volume performance

This example shows how you can monitor volume performance. For example, you might want to monitor volume performance if critical applications run on those volumes. Viewing the performance data can help you answer questions such as:

- What is the average response time for a volume?
- How many operations are completing per second?

The following command shows performance data for a volume by specifying counters that show the number of operations per second and latency:

```
cluster1::> statistics show-periodic -object volume -instance vol0
-counter write_ops|read_ops|total_ops|read_latency|write_latency|
avg_latency
cluster1: volume.vol0: 1/7/2013 20:15:51
      avg     read             total    write    write
  latency  latency read_ops      ops  latency      ops
 -------- -------- -------- -------- -------- --------
    202us    218us        0       22    303us        7
     97us     43us       31       71    149us       34
     39us      0us        0        3      0us        0
    152us      0us        0       16    152us       16
    162us      0us        0      342    144us      289
    734us      0us        0       15      0us        0
     49us      0us        0        1      0us        0
cluster: volume.vol0: 1/7/2013 20:16:07
      avg     read             total    write    write
  latency  latency read_ops      ops  latency      ops
 -------- -------- -------- -------- -------- --------
Minimums:
     39us      0us        0        1      0us        0
Averages for 7 samples:
    205us     37us        4       67    106us       49
```

```
Maximums:
    734us    218us       31      342    303us      289
```

Commands for monitoring cluster performance

Use the `statistics` commands to display performance data and specify the settings for displaying the data. For more information about these commands, see the man pages.

Collecting data for a time period

Use the following commands to collect data samples and to manage the samples that you collect. You need to collect a data sample before you can use the `statistics show` command.

If you want to...	Use this command...
Start data collection for a sample	`statistics start`
Stop data collection for a sample	`statistics stop`
View all samples	`statistics samples show`
Delete a sample	`statistics samples delete`

Viewing performance data

Use the following commands to view performance data. You need to collect a data sample before you can use the `statistics show` command.

If you want to...	Use this command...
View performance data for a time period (a sample)	`statistics show` **Note:** You should limit the scope of this command to only a few objects at a time to avoid a potentially significant impact on system performance.
View continuously updated performance data	`statistics show-periodic`

Viewing all objects, instances, and counters

Use the `statistics catalog` commands to view information about objects, instances, and counters.

If you want to...	Use this command...
View descriptions of objects	`statistics catalog object show`

If you want to...	Use this command...
View all instances of an object	`statistics catalog instance show`
View descriptions of counters in an object	`statistics catalog counter show`

Managing settings for the statistics commands

Use the `statistics settings` commands to modify settings for the `statistics` commands.

If you want to...	Use this command...
View the settings for the statistics commands	`statistics settings show`
Modify whether the commands display rate statistics in rates per second.	`statistics settings modify`

Viewing advanced performance data

Use the following commands to view advanced performance data about your cluster.

Note: The following commands are deprecated and will be removed in a future major release.

If you want to...	Use this command...
View information about SecD RPC usage statistics for the nodes in the cluster	`statistics secd show` **Note:** This command is available at the advanced privilege level. Use this command only as directed by support personnel to help analyze performance and diagnose problems.
View information about the contents of the Open Network Computing Remote Procedure Call (ONC RPC) replay caches for the nodes in the cluster	`statistics oncrpc show-replay-cache`
View information about the ONC RPC calls performed by the nodes in the cluster	`statistics oncrpc show-rpc-calls`

Displaying environmental information

Sensors help you monitor the environmental components of your system. The information you can display about environmental sensors include their type, name, state, value, and threshold warnings.

Step

1. To display information about environmental sensors, use the `system node environment sensors show` command.

Managing system performance (cluster administrators only)

You can use several features to improve system performance. Only the cluster administrator can manage system performance. The Vserver administrator cannot perform these tasks.

Managing workload performance by using Storage QoS

Storage QoS (Quality of Service) can help you manage risks around meeting your performance objectives. You use Storage QoS to limit the throughput to workloads and to monitor workload performance. You can reactively limit workloads to address performance problems and you can proactively limit workloads to prevent performance problems.

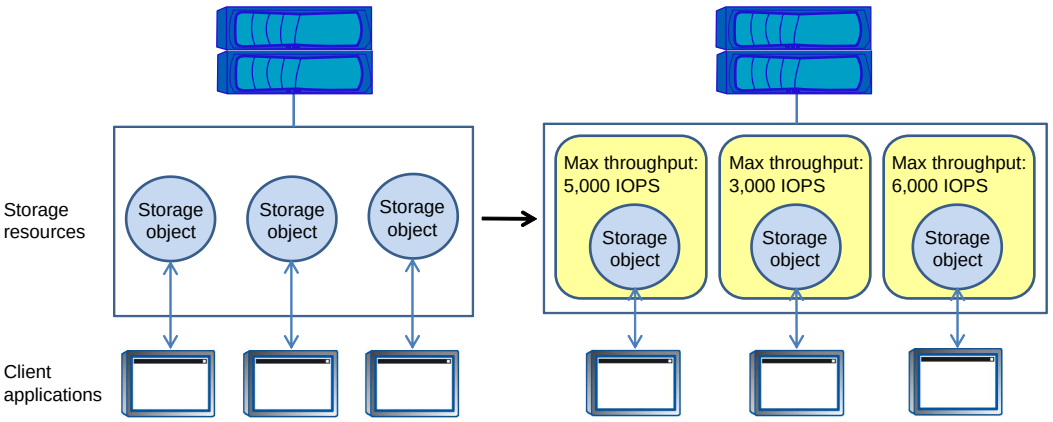
Storage QoS is supported on clusters that have up to eight nodes.

A workload represents the input/output (I/O) operations to one of the following storage objects:

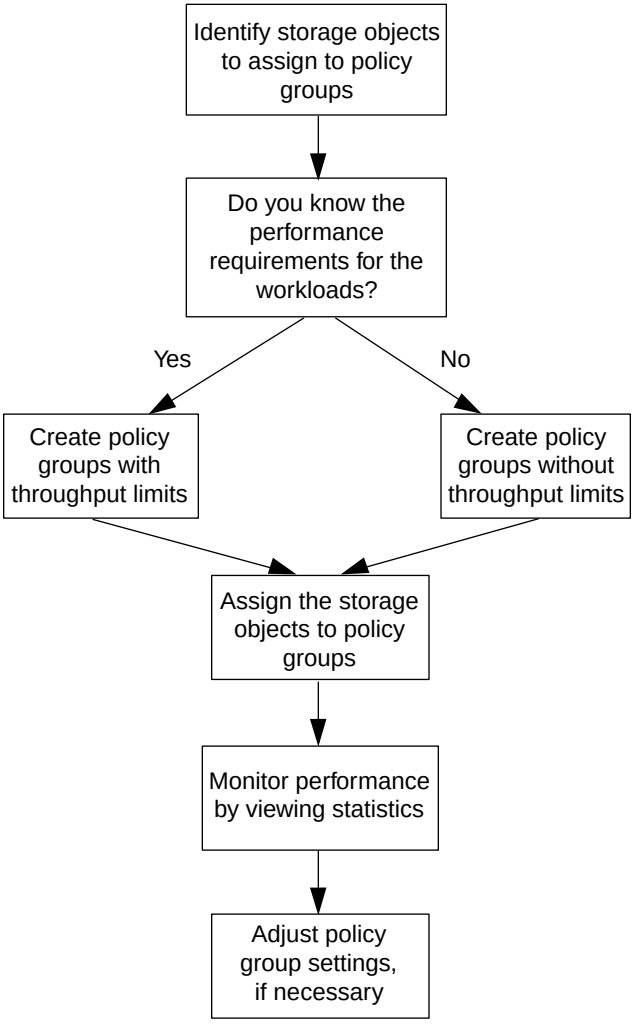
- A Vserver with FlexVol volumes
- A FlexVol volume
- A LUN
- A file (typically represents a virtual machine)

You assign a storage object to a policy group to control and monitor a workload. You can monitor workloads without controlling them.

The following illustration shows an example environment before and after using Storage QoS. On the left, workloads compete for cluster resources to transmit I/O. These workloads get "best effort" performance, which means you have less performance predictability (for example, a workload might get such good performance that it negatively impacts other workloads). On the right are the same workloads assigned to policy groups. The policy groups enforce a maximum throughput limit.



The following workflow shows how you use Storage QoS to control and monitor workloads:



Related tasks

Controlling and monitoring workload performance on page 251

How Storage QoS works

Storage QoS controls workloads that are assigned to policy groups by throttling and prioritizing client operations (SAN and NAS data requests) and system operations.

What policy groups are

A policy group is comprised of one or more workloads and a performance limit that applies collectively to all workloads in the policy group. There are two types of policy groups:

User-defined policy group	Enforces a maximum throughput limit on the storage objects that belong to the policy group by throttling input/output (I/O) requests.
System-defined policy group	Manages internal work that the cluster performs.

You can view performance data for both types of policy groups. The names of system-defined policy groups start with an underscore.

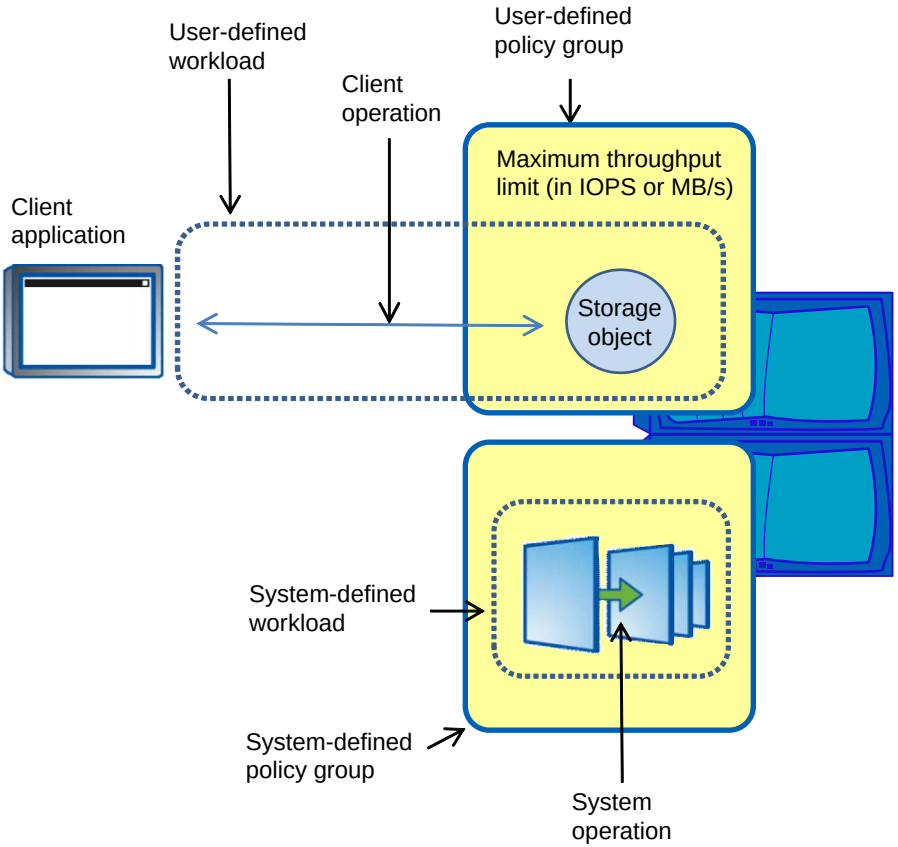
What workloads are

A workload represents work that the cluster performs. There are two types of workloads:

User-defined workload	Represents the input/output (I/O) operations from clients to a storage object that belongs to a policy group. A storage object is one of the following: • A Vserver with FlexVol volumes • A FlexVol volume • A LUN • A file (typically represents a virtual machine) I/O to storage objects that are not assigned to policy groups belongs to the "User-Default" workload.
System-defined workload	Represents internal work that the cluster performs. Storage QoS controls specific system operations to prevent them from interfering with client operations. Examples include storage efficiency operations and data replication operations.

You can view performance data for both types of workloads. The names of system-defined workloads start with an underscore.

The following illustration shows a user-defined policy group and a system-defined policy group. The user-defined policy group controls the user-defined workload, which represents the client operations from the application to the storage object. The system-defined policy group controls the system-defined workload, which represents the internal system operations that the cluster performs.



How the maximum throughput limit works

You can specify one service-level objective for a Storage QoS policy group: a maximum throughput limit. A maximum throughput limit, which you define in terms of IOPS or MB/s, specifies the throughput that the workloads in the policy group cannot collectively exceed.

When you specify a maximum throughput for a policy group, Storage QoS controls client operations to ensure that the aggregate throughput for all workloads in the policy group does not exceed the specified maximum throughput.

For example, you create the policy group "untested_apps" and specify a maximum throughput of 300 MB/s. You assign three volumes to the policy group. The aggregate throughput to those three volumes cannot exceed 300 MB/s.

> **Note:** The aggregate throughput to the workloads in a policy group might exceed the specified limit by up to 10%. A deviation might occur if you have a workload that experiences rapid changes in throughput (sometimes called a "bursty workload").

Note the following about specifying a maximum throughput:

- A throughput limit applies to all clients that access a storage object.
- Do not set the limit too low, because you might underutilize the cluster.
- Consider the minimum amount of throughput that you want to reserve for workloads that do not have limits.

  For example, you can ensure that your critical workloads get the throughput that they need by limiting non-critical workloads.
- You might want to provide room for growth.

  For example, if you see an average utilization of 500 IOPS, you might specify a limit of 1,000 IOPS.

How throttling a workload can affect non-throttled workload requests from the same client

In some situations, throttling a workload (I/O to a storage object) can affect the performance of non-throttled workloads if the I/O requests are sent from the same client.

If a client sends I/O requests to multiple storage objects and some of those storage objects belong to Storage QoS policy groups, performance to the storage objects that do not belong to policy groups might be degraded. Performance is affected because resources on the client, such as buffers and outstanding requests, are shared.

For example, this might affect a configuration that has multiple applications or virtual machines running on the same host.

This behavior is likely to occur if you set a low maximum throughput limit and there are a high number of I/O requests from the client.

If this occurs, you can increase the maximum throughput limit or separate the applications so they do not contend for client resources.

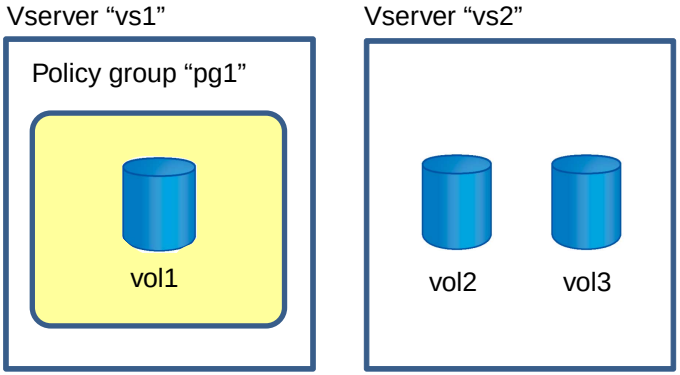
Rules for assigning storage objects to policy groups

You should be aware of rules that dictate how you can assign storage objects to Storage QoS policy groups.

Storage objects and policy groups must belong to the same Vserver

A storage object must be contained by the Vserver to which the policy group belongs. You specify the Vserver to which the policy group belongs when you create the policy group. Multiple policy groups can belong to the same Vserver.

In the following illustration, the policy group pg1 belongs to Vserver vs1. You cannot assign volumes vol2 or vol3 to policy group pg1 because those volumes are contained by a different Vserver.

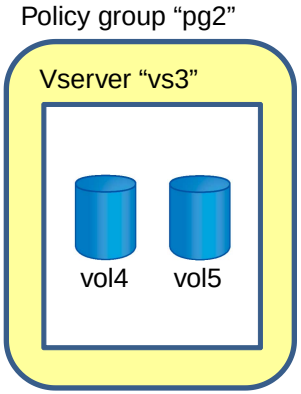


Nested storage objects cannot belong to policy groups

You cannot assign a storage object to a policy group if its containing object or its child objects belong to a policy group. The following table lists the restrictions.

If you assign a...	Then you cannot assign...
Vserver to a policy group	Any storage objects contained by the Vserver to a policy group
Volume to a policy group	The volume's containing Vserver or any child LUNs or files to a policy group
LUN to a policy group	The LUN's containing volume or Vserver to a policy group
File to a policy group	The file's containing volume or Vserver to a policy group

In the following illustration, the Vserver vs3 is assigned to policy group pg2. You cannot assign volumes vol4 or vol5 to a policy group because an object in the storage hierarchy (Vserver vs3) is assigned to a policy group.



Some types of volumes not supported with Storage QoS

You can assign FlexVol volumes to policy groups. Infinite Volumes are not supported with Storage QoS.

The following FlexVol volume variations are not supported with Storage QoS:

- Data protection mirrors
- Load-sharing mirrors
- Node root volumes
- FlexCache volumes

  Note: You can assign the origin volume to a policy group, which controls the origin volume and its FlexCache volumes.

How to monitor workload performance when using Storage QoS

To determine an appropriate throughput limit, you should monitor performance from the cluster. You should not use a tool on the host to monitor performance. A host can report different results than the cluster.

Storage QoS limits I/O to and from the cluster. The rate of I/O that the cluster experiences can be different from what an application experiences. For example, reads from the application can go to the file system buffer cache and not to the cluster.

Due to this behavior, you should monitor performance from the cluster and not from a host-side tool.

Supported number of Storage QoS policy groups and workloads

You can create up to 3,500 policy groups per cluster. You can assign up to 10,000 storage objects to those policy groups. Assigning a storage object to a policy group creates a workload. There are no other limits.

Controlling and monitoring workload performance

You control and monitor workload performance to address performance problems and to proactively limit workloads that have defined performance targets.

Before you begin

- You must be familiar with *How the maximum throughput limit works* on page 247.
- You must be familiar with *Rules for assigning storage objects to QoS policy groups* on page 248.

About this task

Storage QoS is supported on clusters that have up to eight nodes.

Steps

1. Identify the storage objects that you want to assign to Storage QoS policy groups.

   A best practice is to assign the same type of storage object to all policy groups.

2. Use the `qos policy-group create` command to create a new policy group or use the `qos policy-group modify` command to modify an existing policy group.

   You can specify a maximum throughput limit when you create the policy group or you can wait until after you monitor the workload. Monitoring the workload first can help you identify the limit that you need to set. If you do not specify a maximum throughput, the workloads get best-effort performance.

   #### Example

   The following command creates policy group pg-vs1 with a maximum throughput of 5,000 IOPS.

   ```
   cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
   throughput 5000iops
   ```

   #### Example

   The following command creates policy group pg-app2 without a maximum throughput.

   ```
   cluster1::> qos policy-group create pg-app2 -vserver vs2
   ```

3. To assign a storage object to a policy group, use the create or modify command for a Vserver, volume, LUN, or file.

Example

The following command assigns the Vserver vs1 to policy group pg-vs1.

```
cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
```

Example

The following command creates the volume app2 and assigns it to policy group pg-app2.

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr2 -
qos-policy-group pg-app2
```

4. To identify whether you are meeting your performance objectives, use the `qos statistics` commands to monitor policy group and workload performance.

   You should monitor performance from the cluster. You should not use a tool on the host to monitor performance.

   Example

   The following command shows the performance of policy groups.

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

   Example

   The following command shows the performance of workloads.

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

5. If necessary, use the `qos policy-group modify` command to adjust the policy group's maximum throughput limit.

Example

The following command modifies the maximum throughput for policy group pg-app2 to 20 MB/s.

```
cluster1::> qos policy-group modify pg-app2 -max-throughput 20mb/s
```

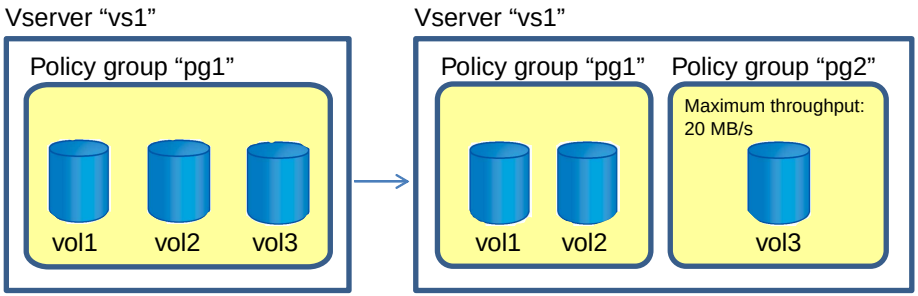
Related references

Commands for controlling and monitoring workloads on page 256

Example: Isolating a workload

You might have a workload that gets better performance than necessary, which affects the performance of other workloads. To address this problem, you use Storage QoS to throttle the workload, which frees cluster resources for other workloads. In this example, the workloads are at the volume level.

The following illustration shows three volumes. You place each volume in policy group pg1, but you do not set a maximum throughput because you want to monitor the workloads first. When you monitor the workloads, you find that vol3 is getting better performance than other workloads. To limit the workload's resource consumption, you move vol3 to policy group pg2. This should allow the other workloads to speed up.



Using the CLI to isolate a workload

The following command creates a policy group without a maximum throughput.

```
cluster1::> qos policy-group create pg1 -vserver vs1
```

The following command assigns three existing volumes to the policy group.

```
cluster1::> volume modify vol1,vol2,vol3 -vserver vs1 -qos-policy-
group pg1
```

The following command displays performance data for the workloads.

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    16645        64.77MB/s   411.00us
vol3-wid12459    12459    10063        39.31MB/s   410.00us
vol2-wid1445      1445     3505        13.69MB/s   437.00us
vol1-wid11344    11344     3007        11.75MB/s   277.00us
_USERSPACE_APPS     14       40        26.40KB/s     8.68ms
_Scan_Backgro..   5688       30            0KB/s        0ms
```

The vol3 workload is getting such good performance that other workloads cannot meet your performance objectives. You decide to move that workload to a new policy group that has a maximum throughput.

The following command creates a policy group with a maximum throughput.

```
cluster1::> qos policy-group create pg2 -vserver vs1 -max-
throughput 20mb/s
```

The following command assigns vol3 to the new policy group.

```
cluster1::> volume modify vol3 -vserver vs1 -qos-policy-group pg2
```

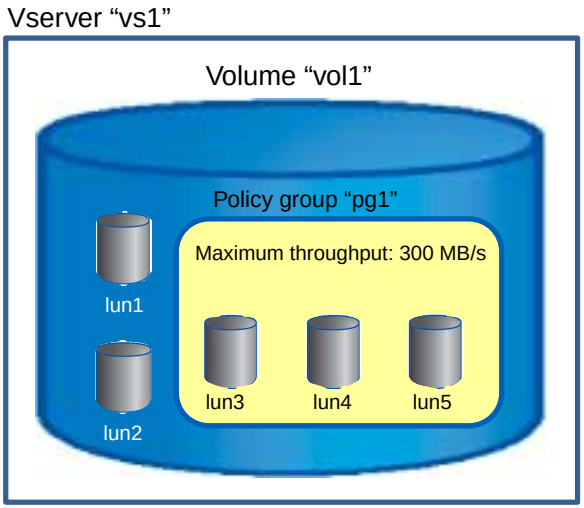
Displaying performance data for the workloads shows that limiting vol3 has allowed the other workloads to get better performance.

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    15691        61.17MB/s  1001.00us
vol1-wid11344    11344     6016        23.50MB/s   355.00us
vol3-wid12459    12459     5133        20.05MB/s     2.42ms
vol2-wid1445      1445     4462        17.43MB/s   253.00us
_USERSPACE_APPS     14       50       204.20KB/s   355.00us
_Scan_Backgro..   5688       30            0KB/s        0ms
```

Example: Proactively setting a limit on non-critical workloads

You might want to ensure that your critical workloads get the best performance possible, so you use Storage QoS to limit the throughput to non-critical workloads. In this example, the workloads are at the LUN level.

The following illustration shows five LUNs in volume vol1. lun1 and lun2 are used for critical applications. lun3, lun4, and lun5 are used for non-critical applications. You want lun1 and lun2 to get best effort performance, so you limit lun3, lun4, and lun5 by assigning them to a policy group with a maximum throughput limit.



Using the CLI to set a limit on non-critical workloads

The following command creates a policy group with a maximum throughput of 300 MB/s.

```
cluster1::> qos policy-group create pg1 -vserver vs1 -max-
throughput 300mb/s
```

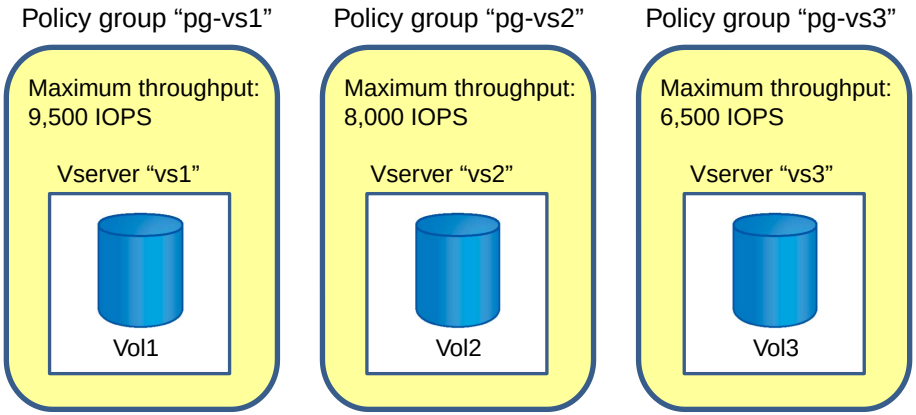
The following commands assign three new LUNs to the policy group.

```
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun3 -size
50GB -ostype windows_2008 -qos-policy-group pg1
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun4 -size
50GB -ostype windows_2008 -qos-policy-group pg1
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun5 -size
50GB -ostype windows_2008 -qos-policy-group pg1
```

Example: Proactively setting a limit on workloads in a shared storage infrastructure

If you have a shared storage infrastructure, you might need to ensure that each workload does not get better performance than necessary. In this example, you use Storage QoS policy groups to set a limit on each workload, all of which are at the Vserver level.

The following illustration shows three Vservers assigned to three separate policy groups. You assign each Vserver to a policy group because you know the performance objectives for each workload and you do not want one tenant taking system resources from other tenants.



Using the CLI to set a limit on workloads in a shared storage infrastructure

The following commands create three policy groups with maximum throughput limits.

```
cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
throughput 9500iops
cluster1::> qos policy-group create pg-vs2 -vserver vs2 -max-
throughput 8000iops
cluster1::> qos policy-group create pg-vs3 -vserver vs3 -max-
throughput 6500iops
```

The following commands assign three existing Vservers to the policy groups.

```
cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
cluster1::> vserver modify -vserver vs2 -qos-policy-group pg-vs2
cluster1::> vserver modify -vserver vs3 -qos-policy-group pg-vs3
```

Commands for controlling and monitoring workloads

You can use commands to manage Storage QoS policy groups, assign storage objects to policy groups, identify the storage objects that belong to policy groups, and monitor workload and policy group performance.

- *Commands for managing policy groups* on page 257
- *Commands for assigning storage objects to policy groups* on page 257
- *Commands for identifying the storage objects that belong to policy groups* on page 257
- *Commands for monitoring policy group performance* on page 258
- *Commands for monitoring workload performance* on page 258

For more information about these commands, see the man pages.

Commands for managing policy groups

Use the `qos policy-group` commands to manage policy groups. You use policy groups to control and monitor workload performance.

If you want to...	Use this command...
Create a policy group	`qos policy-group create`
Modify a policy group	`qos policy-group modify`
Rename a policy group	`qos policy-group rename`
View all user-defined policy groups	`qos policy-group show`
Delete a policy group	`qos policy-group delete`

Commands for assigning storage objects to policy groups

Use a storage object's create command or modify command to assign a storage object to a policy group. You assign a storage object to a policy group to control and monitor workload performance.

Note: To remove a storage object from a policy group, set the `-qos-policy-group` parameter to `none`.

If you want to assign...	Use this command with the `-qos-policy-group` parameter...
A Vserver with FlexVol volumes to a policy group	`vserver modify`
A new FlexVol volume to a policy group	`volume create`
An existing FlexVol volume to a policy group	`volume modify`
A new FlexClone volume to a policy group	`volume clone create`
A new LUN to a policy group	`lun create`
An existing LUN to a policy group	`lun modify`
A file to a policy group	`volume file modify`
A new clone of a file or LUN to a policy group	`volume file clone create`

Commands for identifying the storage objects that belong to policy groups

Use a storage object's show command to identify the storage objects that belong to policy groups.

If you want to identify the...	Use this command with the `-qos-policy-group` parameter...
Vservers with FlexVol volumes that belong to a policy group	`vserver show`
FlexVol volumes that belong to a policy group	`volume show`
LUNs that belong to a policy group	`lun show`
Files that belong to a policy group	`volume file show`

Commands for monitoring policy group and workload performance

Use the following commands to monitor policy group and workload performance in terms of IOPS, throughput, and latency.

If you want to view...	Use this command...
The collective performance of all workloads in a policy group	`qos statistics performance show`
The performance of individual workloads	`qos statistics workload performance show`

Commands for advanced monitoring of policy group performance

Use the following commands to view advanced performance data for policy groups. These commands show the collective performance of all workloads in a policy group.

If you want to view data about...	Use this command...
The client load as it enters the cluster, in terms of request size, read percentage, and concurrency	`qos statistics characteristics show`
Latency across Data ONTAP subsystems, which helps to determine why response time is slow	`qos statistics latency show`
CPU utilization	`qos statistics resource cpu show`
Disk utilization, in terms of the percentage of time spent on the disk during read and write operations	`qos statistics resource disk show`

Commands for advanced monitoring of workload performance

Use the following commands to view advanced performance data for individual workloads.

If you want to view data about...	Use this command...
The client load as it enters the cluster, in terms of request size, read percentage, and concurrency	`qos statistics workload characteristics show`
Latency across Data ONTAP subsystems, which helps to determine why response time is slow	`qos statistics workload latency show`
CPU utilization	`qos statistics workload resource cpu show`
Disk utilization, in terms of the percentage of time spent on the disk during read and write operations	`qos statistics workload resource disk show`

Increasing WAFL cache memory

You can increase Write Anywhere File Layout (WAFL) cache memory in a system that has a caching module installed (Performance Acceleration Module (PAM), Flash Cache module, or Flash Cache 2 module). To increase the WAFL cache memory, you use the WAFL external cache, a software component of Data ONTAP.

WAFL external cache provides extra WAFL cache memory to improve the performance of the storage system by reducing the number of disk reads. You can control how user data blocks are cached by changing the mode of operation for a caching module. You can keep the default mode (normal user data blocks) or you can choose metadata mode or low-priority blocks mode.

You should verify that the WAFL external cache functionality is enabled after you install a caching module.

Note: WAFL external cache does not require a separate license if your system is running Data ONTAP 8.1 or later.

Note: Not all systems have a caching module installed. Therefore, not all systems can utilize the WAFL external cache functionality.

WAFL external cache does not cache data that is stored in a RAID group composed of SSDs.

If you use WAFL external cache on storage systems with a high-availability configuration, you must ensure that the WAFL external cache options are the same on both nodes. Otherwise, a takeover can result in lower performance due to the lack of WAFL external cache on the remaining node.

Besides the Data ONTAP options that you can use to manage WAFL external cache, a diagnostic command is available for sanitizing a caching module. For more information, see the *Diagnostics Guide*.

How Flash Pools and Flash Cache compare

Both the Flash Pool technology and the family of Flash Cache modules (Flash Cache and Flash Cache 2) provide a high-performance cache to increase storage performance. However, there are differences between the two technologies that you should understand before choosing between them.

You can employ both technologies on the same system. However, data stored in volumes associated with a Flash Pool (or an SSD aggregate) is not cached by Flash Cache.

Criteria	Flash Pool	Flash Cache
Scope	A specific aggregate	All aggregates assigned to a node
Caching types supported	Read and write	Read
Cached data availability during and after takeover events	Cached data is available and unaffected by either planned or unplanned takeover events.	Cached data is not available during takeover events. After giveback for a planned takeover, previously cached data that is still valid is re-cached automatically.
PCIe slot on storage controller required?	No	Yes
Supported with array LUNs?	No	Yes

For more information about Flash Pools, see the *Clustered Data ONTAP Physical Storage Management Guide*.

Enabling and disabling WAFL external cache

You can enable or disable the WAFL external cache functionality for a storage system that has a caching module installed (Performance Acceleration Module, Flash Cache module, or Flash Cache 2 module). You should verify that the WAFL external cache functionality is enabled after you install a caching module.

About this task

The `flexscale.enable` option enables or disables the WAFL external cache functionality. If your storage system does not have a caching module installed, the `flexscale.enable` option enables or disables the Predictive Cache Statistics (PCS). PCS is supported on platforms that support caching modules.

WAFL external cache does not require a separate license if your system is running Data ONTAP 8.1 or later. PCS does not require a license.

This command is available through the nodeshell. You access the nodeshell by using the `system node run` command. For more information, see the man page.

Steps

1. To verify whether the WAFL external cache is enabled or disabled, enter the following command:

   `options flexscale.enable`

2. To enable or disable the WAFL external cache, enter the following command:

   `options flexscale.enable {on|off}`

Caching normal user data blocks

If you cache normal user data blocks, the WAFL external cache interprets this setting as the buffer cache policy of `keep` and saves normal user data blocks in the external cache.

About this task

This command is available through the nodeshell. You access the nodeshell by using the `system node run` command. For more information, see the man page.

Step

1. To enable or disable caching for normal user data blocks, enter the following command:

   `options flexscale.normal_data_blocks {on|off}`

   The default value is `on`.

   When the `flexscale.normal_data_blocks` option is set to `on`, the WAFL external cache interprets this setting as the buffer cache policy of `keep` and saves normal user data blocks in the external cache.

   If this option is set to `off`, only metadata blocks are cached.

Caching low-priority user data blocks

You can cache low-priority user data blocks that are not normally stored by WAFL external cache. Low-priority blocks include blocks read in large sequential scans that are not normally reused, and blocks that have been written to the storage system through the iSCSI, NFS, or CIFS protocols.

About this task

Caching low-priority user data blocks is useful if you have workloads that fit within WAFL external cache memory and if the workloads consist of either write followed by read or large sequential reads.

You can cache low-priority user data blocks (setting `flexscale.lopri_blocks` to `on`) only if you also cache normal user data blocks (by setting `flexscale.normal_data_blocks` to `on`).

This command is available through the nodeshell. You access the nodeshell by using the `system node run` command. For more information, see the man page.

Step

1. To control whether low-priority user data blocks are cached, enter the following command:

   `options flexscale.lopri_blocks {on|off}`

   The default value is `off`.

   Setting the option to `on` caches low-priority user data blocks.

Caching only system metadata

If the working set of the storage system is very large, such as a large e-mail server, you can cache only system metadata in WAFL external cache memory by turning off both normal user data block caching and low-priority user data block caching.

About this task

When you cache only system metadata, with both `flexscale.normal_data_blocks` and `flexscale.lopri_blocks` set to `off`, WAFL external cache interprets this setting as the buffer cache policy of `reuse` and does not save normal data blocks or low-priority blocks in the external cache.

These commands are available through the nodeshell. You access the nodeshell by using the `system node run` command. For more information, see the man page.

Steps

1. Enter the following command to turn off normal user data block caching:

   `options flexscale.normal_data_blocks off`

2. Enter the following command to turn off low-priority user data block caching:

   `options flexscale.lopri_blocks off`

Displaying the WAFL external cache configuration

Data ONTAP enables you to display configuration information for WAFL external cache.

About this task

This command is available through the nodeshell. You access the nodeshell by using the `system node run` command. For more information, see the man page.

Step

1. Enter the following command:

stats show -p flexscale

Displaying usage and access information for WAFL external cache

You can display usage and access information for WAFL external cache, have output produced periodically, and terminate the output after a specified number of iterations.

About this task

This command is available through the nodeshell. You access the nodeshell by using the `system node run` command. For more information, see the man page.

Step

1. Enter the following command:

   stats show -p flexscale-access [-i *interval*] [-n *num*]

   - If no options are used, a single one-second snapshot of statistics is used.
   - `-i` *`interval`* specifies that output is to be produced periodically, with an interval of *`interval`* seconds between each set of output.
   - `-n` *`num`* terminates the output after *`num`* number of iterations, when the `-i` option is also used.

     If no *`num`* value is specified, the output runs forever until a user issues a break.
   - Press Ctrl-c to interrupt output.

Example

The following example shows sample output from the `stats show -p flexscale-access` command:

```
Cache                                     Reads       Writes    Disk Read
Usage Hit Meta Miss Hit Evict Inval Insrt Chain Blcks Chain Blcks Replcd
   %   /s  /s   /s   %   /s    /s     /s    /s    /s    /s    /s    /s
   0  581   0   83  87    0   604   13961   579   581   218  13960   552
   0  777   0  133  85    0   121   21500   773   777   335  21494   744
   0  842   0   81  91    0  1105   23844   837   842   372  23845   812
   0  989   0  122  89    0     0   23175   981   989   362  23175   960
```

Example

The following command displays access and usage information for WAFL external cache once every 10 seconds for 5 times:

stats show -p flexscale-access -i 10 -n 5

Preserving the cache in the Flash Cache family of modules

The system does not serve data from a Flash Cache or Flash Cache 2 module when a node is shutdown. However, the WAFL external cache preserves the cache during a graceful shutdown and can serve "warm" data after giveback.

The WAFL external cache can preserve the cache in Flash Cache modules during a graceful shutdown. It preserves the cache through a process called "cache rewarming," which helps to maintain system performance after a graceful shutdown. For example, you might shut down a system to add hardware or upgrade software.

Cache rewarming is enabled by default if you have a Flash Cache or Flash Cache 2 module installed. Cache rewarming is available when both nodes in an HA pair are running Data ONTAP 8.1 or later.

Related concepts

Increasing WAFL cache memory on page 259

How cache rewarming works

WAFL external cache initiates the cache rewarming process during a reboot or a takeover and giveback. The process keeps the cache in Flash Cache and Flash Cache 2 modules "warm."

When a storage system powers down, the WAFL external cache takes a snapshot of the data in Flash Cache and Flash Cache 2 modules. When the system powers up, it uses the snapshot to rebuild the cache. After the process completes, the system can read data from the cache.

In an HA configuration, cache rewarming is more successful when minimal changes are made to data during takeover and giveback. When you initiate takeover and giveback, the takeover partner maintains a log of data written to the down partner's storage. If there are changes to a large amount of the data that is stored in the cache, then the cache rewarming process has more data to rewarm when the node comes back online. As a result, the cache may require additional warming time.

Note: Cache rewarming does not work if the WAFL external cache functionality is disabled.

Events that initiate cache rewarming

You can initiate cache rewarming when you shut down a node or when you initiate takeover and giveback.

The following commands initiate cache rewarming:

- `system node halt`
- `storage failover takeover ([-ofnode] | [-bynode]) node -option takeover_option`
- `cf takeover [-node]`
- `cf takeover [-f]`

Events that do not initiate cache rewarming

WAFL external cache does not initiate cache rewarming if the storage system crashes, if there is a sudden loss of power, or if you run certain commands.

The following commands do not initiate cache rewarming:

- `system node halt -dump`
- `system node reboot -dump`
- `cf forcetakeover [-f]`

Events that abort cache rewarming

After the cache rewarming process starts, some events can abort the entire process and some events can abort the process on specific aggregates.

The following events abort the entire cache rewarming process:

- You add, remove, or move a Flash Cache or Flash Cache 2 module after the WAFL external cache takes the snapshot, but before it rebuilds the cache.
- The takeover node crashes.
- The local node crashes as the WAFL external cache rebuilds the cache.
- After a node reboots, it shuts down before the WAFL external cache can rebuild the cache.
- You initiate a SnapRestore operation on the node's root aggregate before the WAFL external cache rebuilds the cache.
- The `wafliron` process mounts the root aggregate.

The following events abort cache rewarming on the affected aggregate:

- You initiate a SnapRestore operation on an aggregate before the WAFL external cache rebuilds the cache.
- An aggregate does not come online within 20 minutes after the WAFL external cache starts to rebuild the cache.
- The `wafliron` process mounts an aggregate.

Enabling and disabling cache rewarming

Cache "rewarming" is enabled by default if a Flash Cache or Flash Cache 2 module is installed. You can disable and then re-enable cache rewarming, if necessary. You should do this only under the guidance of technical support.

Before you begin

You can enable cache rewarming if the following is true:

- A Flash Cache or Flash Cache 2 module is installed.
- The WAFL external cache functionality is enabled.

About this task

Cache rewarming works at the node level. To ensure that cache rewarming works during a takeover and giveback, enable it on all nodes.

These commands are available through the nodeshell. You access the nodeshell by using the `system node run` command. For more information, see the man page.

Step

1. Enter one of the following commands:

If you want to...	Use this command:
Disable cache rewarming	`options flexscale.rewarm off`
Enable cache rewarming	`options flexscale.rewarm on`

Related tasks

Enabling and disabling WAFL external cache on page 260

Improving read performance

You can improve the read performance of your storage system by enabling read reallocation on volumes. Read reallocation is disabled by default.

What read reallocation is

For workloads that perform a mixture of random writes and large and multiple sequential reads, read reallocation improves file layout and sequential read performance. You can enable read reallocation on FlexVol volumes and Infinite Volumes.

Read reallocation analyzes the parts of the file that are read sequentially. If the associated blocks are not already largely contiguous, Data ONTAP updates the layout by rewriting those blocks to another location on disk. The rewrite improves the layout, thus improving the sequential read performance the next time that section of the file is read. However, read reallocation might result in a higher load on the storage system.

Read reallocation is not supported on compressed volumes and FlexCache volumes.

Commands for managing read reallocation

Use the `volume modify` and `volume show` commands to manage read reallocation.

If you want to...	Use this command...
Enable read reallocation on a volume	`volume modify` with the `-read-realloc` parameter set to `on` or `space-optimized` **Note:** `space-optimized` conserves space if you have Snapshot copies, but it can result in degraded read performance of Snapshot copies. `space-optimized` also rearranges the shared blocks in a deduplicated volume, where as `on` does not.
Disable read reallocation on a volume	`volume modify` with the `-read-realloc` parameter set to `off`
Identify whether read reallocation is enabled or disabled on volumes	`volume show -fields read-realloc`

For more information, see the man pages.

Improving write performance

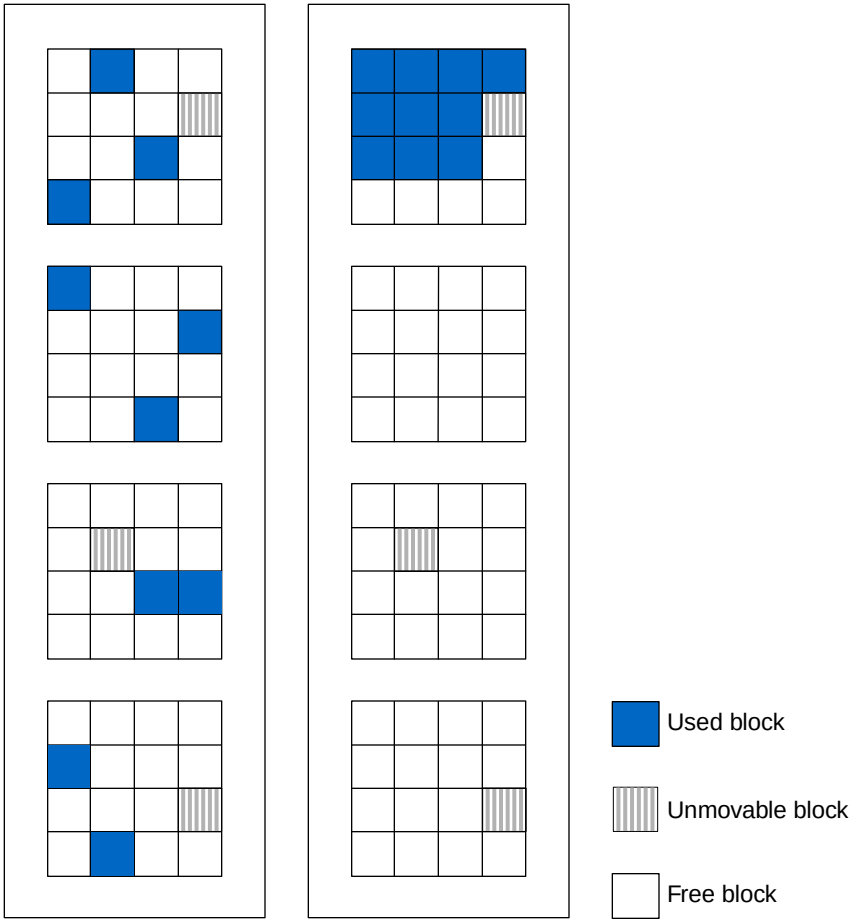
You can enable free space reallocation on aggregates to improve write performance. Free space reallocation improves write performance by optimizing the free space within an aggregate. Free space reallocation is disabled by default.

How free space reallocation optimizes free space

Free space reallocation optimizes the free space in an aggregate immediately before Data ONTAP writes data to the blocks in that aggregate.

Before Data ONTAP writes data to a segment of blocks in an aggregate, free space reallocation evaluates the layout of those blocks. If the layout is not optimal, the free space reallocation function rearranges the blocks. Rearranging the blocks increases the amount of contiguous free space available in the aggregate, which improves the performance of Data ONTAP writes to those blocks.

The following graphic illustrates how free space reallocation optimizes the free space in a segment of blocks:



Segment of blocks before free space reallocation runs

Segment of blocks after free space reallocation runs

When to enable free space reallocation

Free space reallocation works best on workloads that perform a mixture of small random overwrites and sequential or random reads. You can expect additional CPU utilization when you enable free space reallocation. You should not enable free space reallocation if your storage system has sustained, high CPU utilization.

Note: You can use the `statistics show-periodic` command to monitor CPU utilization.

For best results, you should enable free space reallocation when you create a new aggregate. If you enable free space reallocation on an existing aggregate, there might be a period where Data ONTAP performs additional work to optimize free space. This additional work can temporarily impact system performance.

When to use free space reallocation with other reallocation features

When you enable free space reallocation, you should also consider enabling read reallocation. Free space reallocation and read reallocation are complementary technologies that optimize data layout. Read reallocation optimizes the system for sequential reads, while free space reallocation optimizes for writes.

Related concepts

What read reallocation is on page 266

Types of aggregates that free space reallocation can and cannot optimize

Free space reallocation optimizes the free space in specific types of aggregates.

Free space reallocation optimizes free space in the following:

- Aggregates that provide storage to FlexVol volumes or Infinite Volumes
- The HDD RAID groups in an aggregate

Free space reallocation does not optimize free space in the following:

- The SSD RAID groups in an aggregate
- Read-only volumes such as load-sharing or data protection mirrors

Commands for managing free space reallocation

Use the `storage aggregate modify` and `storage aggregate show` commands to manage free space reallocation.

If you want to...	Use this command...
Enable free space reallocation on an aggregate	`storage aggregate modify` with the `-free-space-realloc` parameter set to `on`
Disable free space reallocation on an aggregate	`storage aggregate modify` with the `-free-space-realloc` parameter set to `off`
Identify whether free space reallocation is enabled or disabled on aggregates	`storage aggregate show -fields free-space-realloc`

For more information, see the man pages.

Managing peer relationships for data backup and recovery (cluster administrators only)

Establishing peer relationships between two clusters or two Vservers enables you to back up and recover the data on the clusters or Vservers.

Managing cluster peer relationships

You can create data protection mirroring relationships from one cluster to another and you can manage the jobs on a remote cluster from another cluster if you have cluster peer relationships.

Related concepts

Managing Vserver peer relationships on page 290

What a cluster peer is

The cluster peer feature allows two clusters to coordinate and share resources between them.

Connecting one cluster to another cluster in a peer relationship

You connect clusters together in a cluster peer relationship to share information and to provide access to operations on the peer cluster.

About this task

Connecting clusters together requires network ports, network interfaces configured with the intercluster role, and creating the cluster peer relationship.

Steps

1. *Cluster peer network topologies* on page 271
2. *What cluster peer intercluster networking is* on page 273
3. *Cluster peer intercluster networking requirements* on page 273
4. *Considerations when sharing data ports* on page 274
5. *Considerations when using dedicated ports* on page 275
6. *Configuring intercluster LIFs to share data ports* on page 275
7. *Configuring intercluster LIFs to use dedicated intercluster ports* on page 279
8. *Creating the cluster peer relationship* on page 284

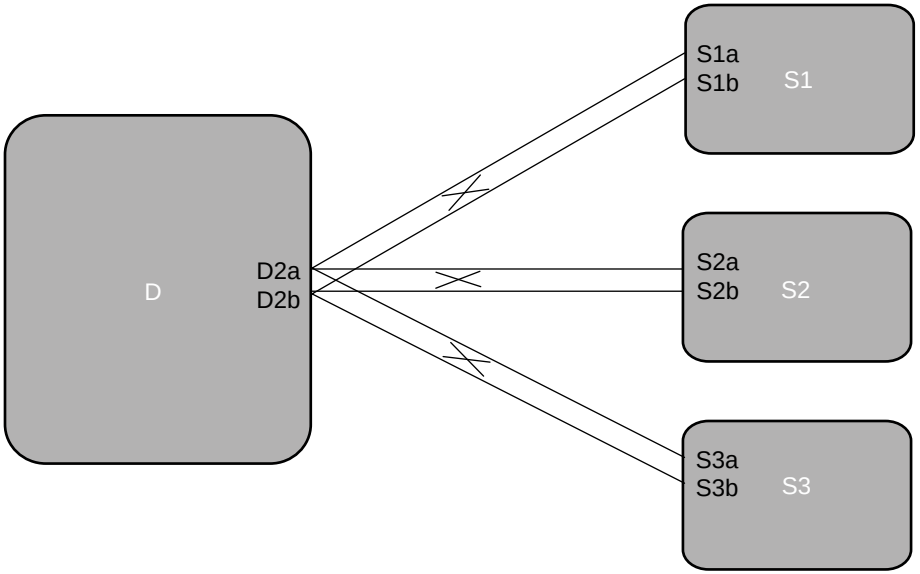
Cluster peer network topologies

You want to connect clusters together in such a way that the clusters in a peer relationship will always be able to communicate with each other.

The best network topology when you have multiple intercluster LIFs connecting clusters in a peering relationship is full mesh connectivity. Full mesh connectivity means that all of the intercluster LIFs of a cluster can communicate with all of the intercluster LIFs on all of the clusters to which you want it to communicate.

For example, Cluster D has the following LIF connections to Clusters S1, S2, and S3:

- D2a is connected to S1a and S1b, S2a and S2b, and S3a and S3b
- D2b is connected to S1a and S1b, S2a and S2b, and S3a and S3b



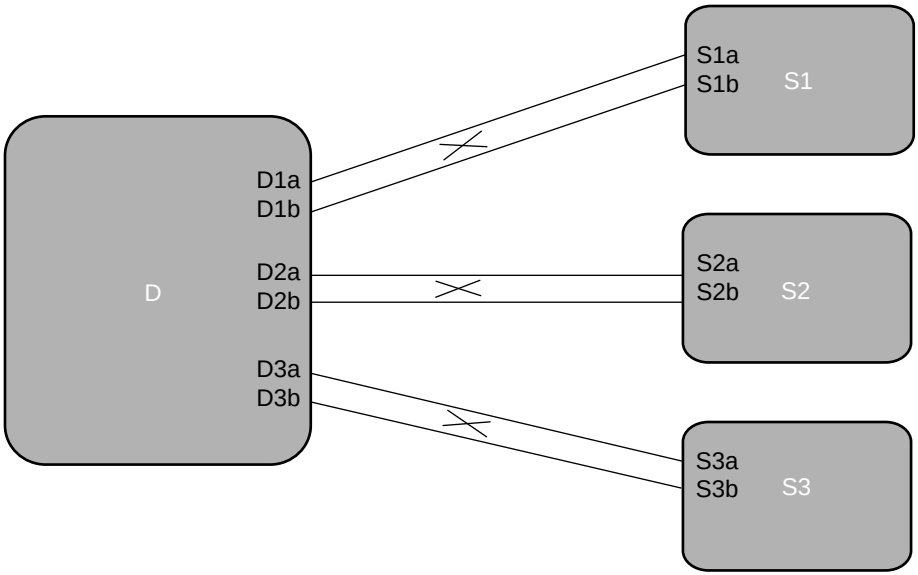
With this topology, there are no missing routes from Cluster D to Clusters S1, S2, and S3.

If, for some reason, you cannot configure full mesh connectivity between all of the LIFs of one cluster to other clusters, you can configure full mesh connections between some LIFs of one cluster to other clusters. This provides the full connectivity between clusters, but can result in an initial and temporary slowing in performance and in the systems issuing EMS warnings. The slowed performance can occur because Data ONTAP might need to define the route from one cluster to another before data can transfer.

For example, Cluster D has the following LIF connections to Clusters S1, S2, and S3:

- D1a is connected to S1a and S1b
- D1b is connected to S1a and S1b
- D2a is connected to S2a and S2b

- D2b is connected to S2a and S2b
- D3a is connected to S3a and S3b
- D3b is connected to S3a and S3b

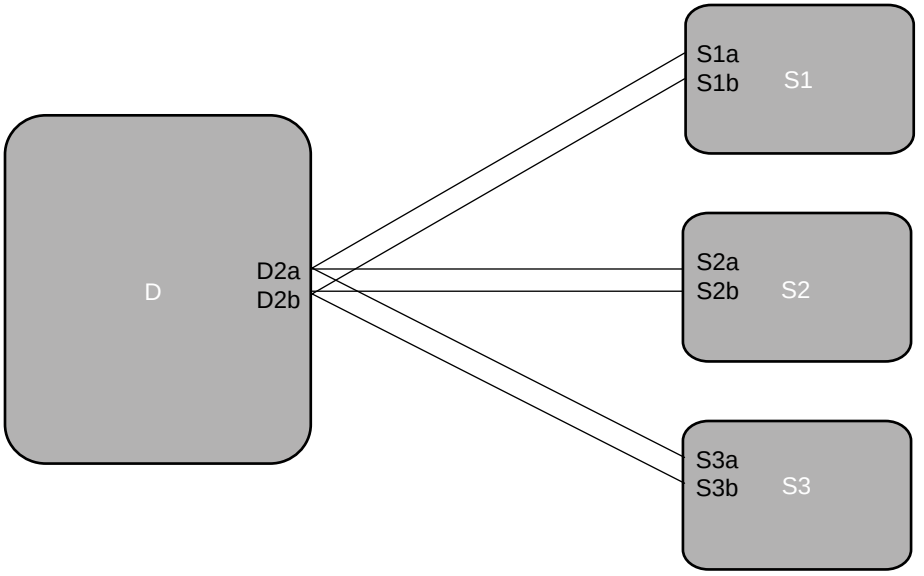


With this topology, routes in which LIFs are directly connected to each other are defined. If there is not a direct connection, for example, when data must go between D1a to S3b, a small amount of time is taken for Data ONTAP to determine a path between Cluster D and Cluster S3.

If the network topology used is not full mesh connectivity, the peer relationships will fail because not all of the possible routes between intercluster LIFs exist.

For example, Cluster D has the following LIF connections to Cluster S1, S2, and S3:

- D2a to S1a, S2a, and S3a
- D2b to S1b, S2b, and S3b



What cluster peer intercluster networking is

A cluster peer relationship, that is, two different clusters communicating with each other, requires an intercluster network on which the communication occurs. An intercluster network consists of intercluster logical interfaces (LIFs) that are assigned to network ports.

The intercluster network on which replication occurs between two different clusters is defined when the intercluster LIFs are created. Replication between two clusters can occur on the intercluster network only; this is true regardless of whether the intercluster network is on the same subnet as a data network in the same cluster.

The IP addresses assigned to intercluster LIFs can reside in the same subnet as data LIFs or in a different subnet. When an intercluster LIF is created, an intercluster routing group is automatically created on that node too. A gateway address for the intercluster routing group must be defined and the intercluster routing group must be routed to the defined gateway address.

Intercluster LIFs can be assigned to ports that have the role of data, which are the same ports used for CIFS or NFS access, or intercluster LIFs can be assigned to dedicated ports that have the role of intercluster. Each method has its advantages and disadvantages.

Cluster peer intercluster networking requirements

Your cluster peer intercluster network must fulfill requirements that include synchronized cluster time, number of intercluster LIFs, IP addresses for intercluster LIFs, maximum transmission units, and more.

The following are requirements of cluster peer intercluster networking:

- The time on the clusters that you want to connect using an intercluster network must be synchronized within 300 seconds (5 minutes).

Cluster peers can be in different time zones.

- At least one intercluster LIF must be created on every node in the cluster.
- Every intercluster LIF requires an IP address dedicated for intercluster replication.

  Note: The IPv6 communication protocol is not supported.

- The correct maximum transmission unit (MTU) value must be used on the network ports that are used for replication.

  The network administrator can identify which MTU value to use in the environment. The MTU value should be set to a value that is supported by the network end point to which it is connected. The default value of 1,500 is correct for most environments.
- All paths on a node used for intercluster networking should have equal performance characteristics.
- The intercluster network must provide connectivity among all intercluster LIFs on all nodes in the cluster peers.

  Every intercluster LIF on every node in a cluster must be able to connect to every intercluster LIF on every node in the peer cluster.

Considerations when sharing data ports

When determining whether sharing a data port for intercluster replication is the correct interconnect network solution, you should consider configurations and requirements such as LAN type, available WAN bandwidth, replication interval, change rate, and number of ports.

Consider the following aspects of your network to determine whether sharing data ports is the best interconnect network solution:

- For a high-speed network, such as a 10-Gigabit Ethernet (10-GbE) network, a sufficient amount of local LAN bandwidth might be available to perform replication on the same 10-GbE ports that are used for data access.

  In many cases, the available WAN bandwidth is far less than 10 GbE, which reduces the LAN network utilization to only that which the WAN is capable of supporting.
- All nodes in the cluster might have to replicate data and share the available WAN bandwidth, making data port sharing more acceptable.
- Sharing ports for data and replication eliminates the extra port counts required to dedicate ports for replication.
- If the replication interval is set to perform only after hours, when little or no client activity exists, then using data ports for replication during this time is acceptable, even without a 10-GbE LAN connection.
- Consider the data change rate and replication interval and whether the amount of data that must be replicated on each interval requires enough bandwidth that it might cause contention with data protocols if sharing data ports.
- When data ports for intercluster replication are shared, the intercluster LIFs can be migrated to any other intercluster-capable port on the same node to control the specific data port that is used for replication.

Considerations when using dedicated ports

When determining whether using a dedicated port for intercluster replication is the correct interconnect network solution, you should consider configurations and requirements such as LAN type, available WAN bandwidth, replication interval, change rate, and number of ports.

Consider the following aspects of your network to determine whether using a dedicated port is the best interconnect network solution:

- If the amount of available WAN bandwidth is similar to that of the LAN ports and the replication interval is such that replication occurs while regular client activity exists, then you should dedicate Ethernet ports for intercluster replication to avoid contention between replication and the data protocols.
- If the network utilization generated by the data protocols (CIFS, NFS, and iSCSI) is such that the network utilization is above 50 percent, then you should dedicate ports for replication to allow for nondegraded performance if a node failover occurs.
- When physical 10-GbE ports are used for data and replication, you can create VLAN ports for replication and dedicate the logical ports for intercluster replication.
- Consider the data change rate and replication interval and whether the amount of data that must be replicated on each interval requires enough bandwidth that it might cause contention with data protocols if sharing data ports.
- If the replication network requires configuration of a maximum transmission unit (MTU) size that differs from the MTU size used on the data network, then you must use physical ports for replication because the MTU size can only be configured on physical ports.

Configuring intercluster LIFs to share data ports

Configuring intercluster LIFs to share data ports enables you to use existing data ports to create intercluster networks for cluster peer relationships. Sharing data ports reduces the number of ports you might need for intercluster networking.

Before you begin

You should have reviewed the considerations for sharing data ports and determined that this is an appropriate intercluster networking configuration.

About this task

Creating intercluster LIFs that share data ports involves assigning LIFs to existing data ports and, possibly, creating an intercluster route. In this procedure, a two-node cluster exists in which each node has two data ports, e0c and e0d. These are the two data ports that are shared for intercluster replication. In your own environment, you replace the ports, networks, IP addresses, subnet masks, and subnets with those specific to your environment.

Steps

1. Check the role of the ports in the cluster by using the `network port show` command.

Example

```
cluster01::> network port show
                                      Auto-Negot  Duplex     Speed(Mbps)
Node   Port   Role         Link MTU   Admin/Oper  Admin/Oper Admin/Oper
------ ------ ------------ ---- ----- ----------- ---------- ----------
cluster01-01
       e0a    cluster      up   1500  true/true   full/full  auto/1000
       e0b    cluster      up   1500  true/true   full/full  auto/1000
       e0c    data         up   1500  true/true   full/full  auto/1000
       e0d    data         up   1500  true/true   full/full  auto/1000
cluster01-02
       e0a    cluster      up   1500  true/true   full/full  auto/1000
       e0b    cluster      up   1500  true/true   full/full  auto/1000
       e0c    data         up   1500  true/true   full/full  auto/1000
       e0d    data         up   1500  true/true   full/full  auto/1000
```

2. Create an intercluster LIF on each node in cluster01 by using the `network interface create` command.

Example

This example uses the LIF naming convention of *nodename*_icl# for the intercluster LIF.

```
cluster01::> network interface create -vserver cluster01-01 -lif
cluster01-01_icl01 -role intercluster -home-node cluster01-01 -home-
port e0c -address 192.168.1.201 -netmask 255.255.255.0
Info: Your interface was created successfully; the routing group
i192.168.1.0/24 was created

cluster01::> network interface create -vserver cluster01-02 -lif
cluster01-02_icl01 -role intercluster -home-node cluster01-02 -home-
port e0c -address 192.168.1.202 -netmask 255.255.255.0
Info: Your interface was created successfully; the routing group
i192.168.1.0/24 was created
```

3. Verify that the intercluster LIFs were created properly by using the `network interface show` command with the `-role intercluster` parameter.

Example

```
cluster01::> network interface show –role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster01-01
            cluster01-01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c     true
cluster01-02
            cluster01-02_icl01
                       up/up      192.168.1.202/24   cluster01-02  e0c     true
```

4. Verify that the intercluster LIFs are configured to be redundant by using the `network interface show` command with the `-role intercluster` and `-failover` parameters.

Example

The LIFs in this example are assigned the e0c port on each node. If the e0c port fails, the LIF can fail over to the e0d port because e0d is also assigned the data role.

The intercluster LIF is assigned to a data port; therefore, a failover group for the intercluster LIF is created automatically, and contains all ports with the data role on that node. Intercluster failover groups are node specific; therefore, if changes are required, they must be managed for each node because different nodes might use different ports for replication.

```
cluster01::> network interface show -role intercluster –failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Group Usage     Group
-------- --------------- --------------------- --------------- --------
cluster01-01
         cluster01-01_icl01 cluster01-01:e0c   system-defined
                             Failover Targets: cluster01-01:e0c,
                                               cluster01-01:e0d
cluster01-02
         cluster01-02_icl01 cluster01-02:e0c   system-defined
                             Failover Targets: cluster01-02:e0c,
                                               cluster01-02:e0d
```

5. Display routing groups by using the `network routing-group show` command with the `-role intercluster` parameter.

   An intercluster routing group is created automatically for the intercluster LIFs.

   Example

```
cluster01::> network routing-group show –role intercluster
          Routing
Vserver   Group     Subnet          Role         Metric
--------- --------- --------------- ------------ -------
cluster01-01
          i192.168.1.0/24
                    192.168.1.0/24  intercluster 40
cluster01-02
          i192.168.1.0/24
                    192.168.1.0/24  intercluster 40
```

6. Display the routes in the cluster by using the `network routing-group show` command to determine whether intercluster routes are available or you must create them.

   Creating a route is required only if the intercluster addresses in both clusters are not on the same subnet and a specific route is needed for communication between the clusters.

   Example

   In this example, no intercluster routes are available.

```
cluster01::> network routing-group route show
          Routing
Vserver   Group     Destination     Gateway         Metric
--------- --------- --------------- --------------- ------
```

```
cluster01
          c192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     20
cluster01-01
          n192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     10
cluster01-02
          n192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     10
```

7. If communication between intercluster LIFs in different clusters requires routing, create an intercluster route by using the `network routing-groups route create` command.

   The intercluster networks apply to each node; therefore, you must create an intercluster route on each node.

   Example

   In this example, 192.168.1.1 is the gateway address for the 192.168.1.0/24 network.

   Note: If the destination is specified as 0.0.0.0/0, then it becomes the default route for the intercluster network.

```
cluster01::> network routing-groups route create -server cluster01-01
-routing-group i192.168.1.0/24 -destination 0.0.0.0/0 -gateway
192.168.1.1 -metric 40

cluster01::> network routing-groups route create -server cluster01-02
-routing-group i192.168.1.0/24 -destination 0.0.0.0/0 -gateway
192.168.1.1 -metric 40
```

8. Display the newly created routes by using the `network routing-groups route show` command.

   Although the intercluster routes do not have an assigned role, they are assigned to the routing group i192.168.1.0/24, which is assigned the role of intercluster. These routes are only used for intercluster communication.

   Example

```
cluster01::> network routing-group route show
          Routing
Vserver   Group     Destination     Gateway         Metric
--------- --------- --------------- --------------- ------
cluster01
          c192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     20
cluster01-01
          n192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     10
          i192.168.1.0/24
                    0.0.0.0/0       192.168.1.1     40
cluster01-02
```

```
           n192.168.0.0/24
                     0.0.0.0/0       192.168.0.1     10
           i192.168.1.0/24
                     0.0.0.0/0       192.168.1.1     40
```

9. Repeat Steps 1 through 8 on the cluster to which you want to connect.

Configuring intercluster LIFs to use dedicated intercluster ports

Configuring intercluster LIFs to use dedicated data ports allows greater bandwidth than using shared data ports on your intercluster networks for cluster peer relationships.

About this task

In this example, a two-node cluster exists in which each node has two data ports, e0e and e0f, which are dedicated for intercluster replication. In your own environment, you would replace the ports, networks, IP addresses, subnet masks, and subnets with those specific to your environment.

Steps

1. Check the role of the ports in the cluster by using the `network port show` command.

Example

```
cluster01::> network port show
                                    Auto-Negot  Duplex     Speed(Mbps)
Node   Port   Role         Link MTU   Admin/Oper  Admin/Oper Admin/Oper
------ ------ ------------ ---- ----- ----------- ---------- ----------
cluster01-01
       e0a    cluster      up   1500  true/true   full/full  auto/1000
       e0b    cluster      up   1500  true/true   full/full  auto/1000
       e0c    data         up   1500  true/true   full/full  auto/1000
       e0d    data         up   1500  true/true   full/full  auto/1000
       e0e    data         up   1500  true/true   full/full  auto/1000
       e0f    data         up   1500  true/true   full/full  auto/1000
cluster01-02
       e0a    cluster      up   1500  true/true   full/full  auto/1000
       e0b    cluster      up   1500  true/true   full/full  auto/1000
       e0c    data         up   1500  true/true   full/full  auto/1000
       e0d    data         up   1500  true/true   full/full  auto/1000
       e0e    data         up   1500  true/true   full/full  auto/1000
       e0f    data         up   1500  true/true   full/full  auto/1000
```

2. Determine whether any of the LIFs are using ports that are dedicated for replication by using the `network interface show` command.

Example

```
cluster01::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster01
            cluster_mgmt up/up    192.168.0.xxx/24   cluster01-01  e0c     true
```

```
vs1
            vs1_lif1     up/up    192.168.0.151/24   cluster01-01  e0e     true
```

3. If a LIF is using one of the ports dedicated to replication, then migrate the LIF to another port by using the `network interface migrate` command.

   This is required because intercluster ports cannot host data LIFs. This migration is nondisruptive, assuming that the other data ports have been configured properly so that clients can access the LIF after migration.

   Example

```
cluster01::> network interface migrate -vserver vs1 -lif vs1_lif1 -dest-node
cluster01-01 -dest-port e0d

cluster01::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster01
            cluster_mgmt up/up    192.168.0.xxx/24   cluster01-01  e0c     true
vs1
            vs1_lif1     up/up    192.168.0.151/24   cluster01-01  e0d     false
```

4. If necessary, modify the newly migrated LIFs to the LIF home port by using the `network interface modify` command, so that the new port is the LIF home port.

   Example

```
cluster01::> network interface modify -vserver vserver1 -lif vs1_lif1 -home-node
dpg1-01 -home-port e0d

cluster01::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
vserver1
            vs1_lif1   up/up      192.168.0.151/24   cluster01-01  e0d     true
```

5. After all LIFs have been migrated off the ports dedicated for replication, change the role of the port used on each node to `intercluster` by using the `network port modify` command.

   Example

```
cluster01::> network port modify -node cluster01-01 -port e0e -role
intercluster

cluster01::> network port modify -node cluster01-01 -port e0f -role
intercluster

cluster01::> network port modify -node cluster01-02 -port e0e -role
intercluster

cluster01::> network port modify -node cluster01-02 -port e0f -role
intercluster
```

6. Verify that the roles of the correct ports have been changed to `intercluster` by using the `network port show` command with the `-role intercluster` parameter.

   Example

```
cluster01::> network port show –role intercluster
                                    Auto-Negot  Duplex     Speed(Mbps)
Node   Port   Role         Link MTU   Admin/Oper  Admin/Oper Admin/Oper
------ ------ ------------ ---- ----- ----------- ---------- ----------
cluster01-01
       e0e    intercluster up   1500  true/true   full/full  auto/1000
       e0f    intercluster up   1500  true/true   full/full  auto/1000
cluster01-02
       e0e    intercluster up   1500  true/true   full/full  auto/1000
       e0f    intercluster up   1500  true/true   full/full  auto/1000
```

7. Create an intercluster LIF on each node in cluster01 by using the `network interface create` command.

   Example

   This example uses the LIF naming convention *`nodename`*_icl# for intercluster LIF.

```
cluster01::> network interface create -vserver cluster01-01 -lif
cluster01-01_icl01 -role intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201 -netmask 255.255.255.0
Info: Your interface was created successfully; the routing group
i192.168.1.0/24 was created

cluster01::> network interface create -vserver cluster01-02 -lif
cluster01-02_icl01 -role intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202 -netmask 255.255.255.0
Info: Your interface was created successfully; the routing group
i192.168.1.0/24 was created
```

8. Verify that the intercluster LIFs are configured for redundancy by using the `network interface show` command with the `-role intercluster` and `-failover` parameters.

   Example

   The LIFs in this example are assigned the e0e home port on each node. If the e0e port fails, the LIF can fail over to the e0f port because e0f is also assigned the role of intercluster.

   The intercluster LIF is assigned to an intercluster port; therefore, a failover group is created automatically, and contains all ports with the intercluster role on that node. In this example, the failover group does not include any data ports. Intercluster failover groups are node specific; therefore, if changes are required, they must be managed for each node because different nodes might use different ports for replication.

```
cluster01::> network interface show -role intercluster –failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Group Usage     Group
-------- --------------- --------------------- --------------- --------
cluster01-01
         cluster01-01_icl01 cluster01-01:e0e   system-defined
```

```
                                Failover Targets: cluster01-01:e0e,
                                                  cluster01-01:e0f
cluster01-02
         cluster01-02_icl01 cluster01-02:e0e   system-defined
                                Failover Targets: cluster01-02:e0e,
                                                  cluster01-02:e0f
```

9. Verify that the intercluster LIFs were created properly by using the `network interface show` command.

Example

```
cluster01::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster01
            cluster_mgmt up/up    192.168.0.xxx/24   cluster01-01  e0c     true
cluster01-01
            cluster01-01_icl01
                       up/up    192.168.1.201/24   cluster01-01  e0e     true
            clus1      up/up    169.254.xx.xx/24   cluster01-01  e0a     true
            clus2      up/up    169.254.xx.xx/24   cluster01-01  e0b     true
            mgmt1      up/up    192.168.0.xxx/24   cluster01-01  e0c     true
cluster01-02
            cluster01-02_icl01
                       up/up    192.168.1.202/24   cluster01-02  e0e     true
            clus1      up/up    169.254.xx.xx/24   cluster01-02  e0a     true
            clus2      up/up    169.254.xx.xx/24   cluster01-02  e0b     true
            mgmt1      up/up    192.168.0.xxx/24   cluster01-02  e0c     true
```

10. Display routing groups by using the `network routing-group show` command with the `-role intercluster` parameter to determine whether the intercluster network needs intercluster routes.

An intercluster routing group is created automatically for the intercluster LIFs.

Example

```
cluster01::> network routing-group show –role intercluster
            Routing
Vserver     Group     Subnet          Role         Metric
--------- --------- --------------- ------------ -------
cluster01-01
            i192.168.1.0/24
                      192.168.1.0/24  intercluster 40
cluster01-02
            i192.168.1.0/24
                      192.168.1.0/24  intercluster 40
```

11. Display the routes in the cluster by using the `network routing-group show` command to determine whether intercluster routes are available or you must create them.

Creating a route is required only if the intercluster addresses in both clusters are not on the same subnet and a specific route is needed for communication between the clusters.

Example

In this example, no intercluster routes are available.

```
cluster01::> network routing-group route show
          Routing
Vserver   Group     Destination     Gateway         Metric
--------- --------- --------------- --------------- ------
cluster01
          c192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     20
cluster01-01
          n192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     10
cluster01-02
          n192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     10
```

12. If communication between intercluster LIFs in different clusters requires routing, create an intercluster route by using the `network routing-groups route create` command.

The intercluster networks apply to each node; therefore, you must create an intercluster route on each node.

Example

In this example, 192.168.1.1 is the gateway address for the 192.168.1.0/24 network.

Note: If the destination is specified as 0.0.0.0/0, then it becomes the default route for the intercluster network.

```
cluster01::> network routing-groups route create -server cluster01-01 -routing-
group i192.168.1.0/24 -destination 0.0.0.0/0 -gateway 192.168.1.1 -metric 40

cluster01::> network routing-groups route create -server cluster01-02 -routing-
group i192.168.1.0/24 -destination 0.0.0.0/0 -gateway 192.168.1.1 -metric 40
```

13. Display the newly created routes by using the `network routing-groups route show` command to confirm that you created the routes correctly.

Although the intercluster routes do not have an assigned role, they are assigned to the routing group i192.168.1.0/24, which is assigned the role of `intercluster`. These routes are only used for intercluster communication.

Example

```
cluster01::> network routing-group route show
          Routing
Vserver   Group     Destination     Gateway         Metric
--------- --------- --------------- --------------- ------
cluster01
          c192.168.0.0/24
```

```
                    0.0.0.0/0       192.168.0.1     20
cluster01-01
          n192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     10
          i192.168.1.0/24
                    0.0.0.0/0       192.168.1.1     40
cluster01-02
          n192.168.0.0/24
                    0.0.0.0/0       192.168.0.1     10
          i192.168.1.0/24
                    0.0.0.0/0       192.168.1.1     40
```

14. Repeat Steps 1 through 13 to configure intercluster networking in the other cluster.

15. Verify that the ports have access to the proper subnets, VLANs, and so on.

Dedicating ports for replication in one cluster does not require dedicating ports in all clusters; one cluster might use dedicated ports, while the other cluster shares data ports for intercluster replication.

Creating the cluster peer relationship

You create the cluster peer relationship using a set of intercluster designated logical interfaces to make information about one cluster available to the other cluster for use in cluster peering applications.

Before you begin

You should have the intercluster network configured.

Steps

1. Create the cluster peer relationship using the `cluster peer create` command.

Example

In the following example, cluster01 is peered with a remote cluster named cluster02. Cluster02 is a two-node cluster that has one intercluster LIF per node. The IP addresses of the intercluster LIFs created in cluster02 are 192.168.2.203 and 192.168.2.204. These IP addresses are used to create the cluster peer relationship.

```
cluster01::> cluster peer create -peer-addrs
192.168.2.203,192.168.2.204 –username admin
Password: *********
```

If DNS is configured to resolve host names for the intercluster IP addresses, you can use host names in the `–peer-addrs` option. It is not likely that intercluster IP addresses frequently change; however, using host names allows intercluster IP addresses to change without having to modify the cluster peer relationship.

2. Display the cluster peer relationship using the `cluster peer show` command with the `-instance` parameter.

   Example

```
cluster01::> cluster peer show –instance
Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.168.2.203,192.168.2.204
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.203,192.168.2.204
Cluster Serial Number: 1-80-000013
```

3. Preview the health of the cluster peer relationship using the `cluster peer health show` command.

   Example

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  --------------- --------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

Displaying a cluster peer relationship

You can see if a cluster is connected to another cluster if you want to make use of cluster peer features such as mirroring a volume from one cluster to another.

Step

1. To display information about a cluster to which you previously connected, use the `cluster peer show` command.

   This command displays only basic information about the other cluster. If you want to see more information about the other cluster, use the `cluster peer show -instance` command.

   The following example displays basic information about a cluster connected to a cluster named cluster_a:

```
cluster_a::>cluster peer show

Peer Cluster Name         Cluster Serial Number LIF Role     Availability
------------------------- --------------------- ------------ ---------------
cluster_b                  1-80-123456          intercluster Available
```

Modifying a cluster peer relationship

You can modify a cluster peer relationship if the name of the cluster you connected to, the logical interface you used, or the IP address you used when creating the cluster peer relationship changes. for example, the IP address of the cluster you used when creating the relationship changed.

Step

1. To change the configuration of a cluster peer relationship, use the `cluster peer modify` command.

The following example changes the IP address of the cluster peer configuration of a cluster named cluster_b to 172.19.7.3:

```
node::> cluster peer modify -cluster cluster_b -stable-addrs
172.19.7.3
```

Deleting a cluster peering relationship

You can delete a cluster peering relationship if the relationship is no longer needed. You must delete the cluster peering relationship from each of the clusters in the relationship.

Steps

1. To delete the cluster peering relationship from the cluster of which you are the administrator, use the `cluster peer delete` command.

   Note: This procedure assumes that you are the administrator of only one of the clusters in the cluster peering relationship.

Example

The following example deletes the cluster peering relationship with the cluster 2 cluster from the cluster1 cluster:

```
cluster1::> cluster peer delete -cluster cluster2
```

2. To delete the cluster peering relationship from the other cluster, an administrator of the other cluster uses the `cluster peer delete` command.

Example

The following example deletes the cluster peering relationship with the cluster 1 cluster from the cluster2 cluster:

```
cluster2::> cluster peer delete -cluster cluster1
```

Managing jobs on another cluster

From the local cluster, you can manage jobs that are running on the cluster to which the local cluster is connected. This is useful for monitoring and controlling cross cluster applications like a data protection mirror.

Viewing jobs on another cluster

From the local cluster, you can see jobs that are running on the cluster to which the local cluster is connected. This is useful for monitoring cross cluster applications like a data protection mirror.

Step

1. To view the jobs running on a cluster which is connected to the local cluster in a cross cluster relationship, complete the following step.

   `cluster peer job show -cluster` ***`cluster_name`***

The following example shows information about jobs running on a cluster named cluster_a connected to the local cluster in a cross cluster relationship:

```
cluster_b::cluster peer job show -cluster cluster_a
 Job ID     Name           State    Description
 ---------  -------------- -------- --------------------------
 Cluster: cluster_a
 5          Vol Create     Running  create striped-volume vol0
```

You can show detailed information using the `-instance` parameter of the `cluster peer job show` command. See the `cluster peer job show` command for details.

Monitoring progress of a job on another cluster

From the local cluster, you can monitor the progress of a job on the cluster to which the local cluster is connected.

About this task

The progress of the job is monitored until the job ends, terminates, or you interrupt its progress.

Step

1. To monitor a job on a cluster which is connected to the local cluster in a cross cluster relationship, complete the following step.

   cluster peer job watch-progress -cluster *cluster_a* -id *ID_number* -interval *integer*

The following example monitors the progress of a job whose job ID is 15. The progress is updated every 3 seconds.

```
cluster_b::cluster peer job watch-progress -cluster cluster_a -id 15
     -interval 3
```

See the `cluster peer job watch-progress` command for details.

Pausing jobs on another cluster

From the local cluster, you can pause jobs that are running on the cluster to which the local cluster is connected. If a job is consuming too many system resources, you can pause it until there is less demand on the system.

Step

1. To pause a job running on a cluster which is connected to the local cluster in a cross cluster relationship, complete the following step.

   cluster peer job pause -cluster *cluster_name* -id *ID_number*

The following example pauses a job whose job ID is 15:

```
cluster_b::cluster peer job pause -cluster cluster_a -id 15
```

See the `cluster peer job pause` command for details.

Resuming jobs on another cluster

From the local cluster, you can resume paused jobs on the cluster to which the local cluster is connected.

Step

1. To resume a paused job on a cluster which is connected to the local cluster in a cross cluster relationship, complete the following step.

   cluster peer job resume -cluster *cluster_name* -id *ID_number*

The following example resumes a job whose job ID is 15:

```
cluster_b::cluster peer job resume -cluster cluster_a -id 15
```

See the `cluster peer job resume` command for details.

Stopping a job on another cluster

From the local cluster, you can stop a job on the cluster to which the local cluster is connected.

About this task

If you stop a job, you cannot resume it using the `cluster peer job resume` command.

Step

1. To stop a job on a cluster which is connected to the local cluster in a cluster peer relationship, use the `cluster peer job stop` command.

The following example stops a job whose job ID is 15:

```
cluster_b::cluster peer job stop -cluster cluster_a -id 15
```

See the `cluster peer job stop` command for details.

Deleting a job on another cluster

From the local cluster, you can delete a job on the cluster to which the local cluster is connected.

Step

1. To delete a job on a cluster which is connected to the local cluster in a cluster peer relationship, use the `cluster peer job delete` command.

The following example deletes a job whose job ID is 15:

```
cluster_b::cluster peer job delete -cluster cluster_a -id 15
```

See the `cluster peer job delete` command for details.

Managing Vserver peer relationships

A cluster administrator can create and manage data protection mirroring relationships between two Vservers either existing within a cluster (intracluster) or in the peered clusters (intercluster) to provide an infrastructure for peering applications, such as SnapMirror.

Peered clusters and peered Vservers can be managed either by the same cluster administrator or different cluster administrators.

The cluster administrator can perform the following Vserver peer management tasks:

- Creating a Vserver peer relationship
- Accepting a Vserver peer relationship
- Rejecting a Vserver peer relationship
- Suspending a Vserver peer relationship
- Resuming a Vserver peer relationship
- Modifying a Vserver peer relationship
- Deleting a Vserver peer relationship
- Viewing the Vserver peer relationships
- Setting up SnapMirror relationship between the volumes of the peered Vservers

  Note: You cannot set up load-sharing SnapMirror relationship between the volumes of intercluster Vserver peers.

A Vserver administrator can perform only the following Vserver peer management tasks:

- Viewing the Vserver peer relationships to identify the peered Vservers
- Setting up SnapMirror relationship such as data protection relationship (DP), vault relationship (XDP), and transition relationship (TDP) between the volumes of the peered Vservers

For more information about setting up peering applications, see the *Clustered Data ONTAP Data Protection Guide*.

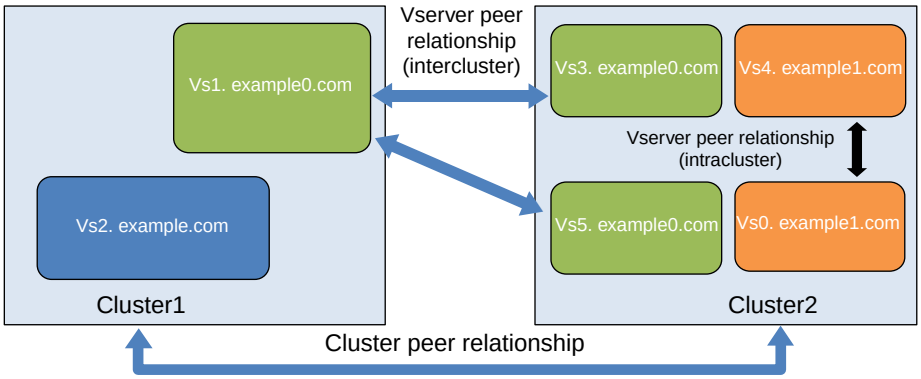
Related concepts

Managing cluster peer relationships on page 270

What Vserver peer relationship is

Vserver peer relationship is an authorization infrastructure that enables a cluster administrator to set up peering applications such as SnapMirror relationships between Vservers either existing within a cluster (intracluster) or in the peered clusters (intercluster). Only a cluster administrator can set up Vserver peer relationships.

The following illustration shows the intercluster and intracluster Vserver peer relationships:



Vserver peer infrastructure enables you to set up a backup and recovery mechanism between Vservers. You can set up mirroring relationship at volume level between peered Vservers. If a Vserver's volume becomes unavailable, the cluster administrator or a Vserver administrator can configure the respective mirrored volume of the peered Vserver to serve data.

One Vserver can be peered with multiple Vservers within a cluster or across clusters.

In clustered Data ONTAP 8.2, only SnapMirror data protection (DP), vault (XDP) and load-sharing relationship (LS) relationships can be set up by using the Vserver peer infrastructure.

States of Vserver peer relationships

A Vserver peer relationship can be in different states depending on the operation performed on the Vserver peer relationship. You must be aware of the states of the Vserver peer relationship to perform other operations such as SnapMirror data transfer between peered Vservers.

The following table lists the different states of a Vserver peer relationship and helps you understand when a Vserver peer relationship is in a particular state:

A Vserver peer relationship is in...	**When...**
`initializing` state on the local cluster	The local cluster is communicating with the peer cluster for initializing the Vserver peer relationship
`initiated` state on the local cluster `pending` state on the peered cluster	An intercluster Vserver peer relationship is requested from the local cluster
`peered` state on the local and peered clusters	An intercluster Vserver peer relationship is accepted from the peered cluster An intracluster Vserver peer relationship is established An intercluster or intracluster Vserver peer relationship is resumed

A Vserver peer relationship is in...	When...
`rejected` state on the local cluster	An intercluster Vserver peer relationship is rejected from the peered cluster
`suspended` state on the local and peered clusters	An intercluster or intracluster Vserver peer relationship is suspended from the local or peered cluster
`deleted` state	An intercluster Vserver peer relationship is deleted from any of the peered clusters

Creating a Vserver peer relationship

A cluster administrator can create a Vserver peer relationship to provide an authorization infrastructure for running Vserver peering applications between two Vservers by using the `vserver peer create` command. You can create a Vserver peer relationship between two Vservers existing either in a single cluster (intracluster) or existing in peered clusters (intercluster).

Before you begin

- If you want to create an intercluster Vserver peer relationship, you must have ensured that both the clusters are peered with each other.
- Vserver peer relationship that is in rejected or deleted state must be deleted if you want to re-create the Vserver peer relationship between the same Vservers.
- The admin state of the Vservers to be peered must not be `initializing` or `deleting`.
- The names of Vservers in the peered clusters must be unique across the two clusters. If they do not have unique names, you must rename one of the Vservers .

About this task

Peered clusters can be managed by a single cluster administrator or different cluster administrators. In clustered Data ONTAP 8.2, you can set up only SnapMirror relationships between the peered Vservers. If you do not specify the peering application as `SnapMirror`, a Vserver administrator cannot set up SnapMirror relationship between the peered Vservers.

You can create a Vserver peer relationship either between Vserver with FlexVol volumes or between Vserver with Infinite Volumes. You cannot create a Vserver peer relationship between Vserver with FlexVol volume and Vserver with Infinite Volume.

You can create only intercluster Vserver peer relationship for Vservers with Infinite Volumes.

Steps

1. Use the `vserver peer create` command to create a Vserver peer relationship.

Example

The following example illustrates how to create an intercluster Vserver peer relationship between vs1.example0.com and vs3.example0.com residing on cluster1 and cluster2 respectively:

```
cluster1::> vserver peer create -vserver vs1.example0.com -peer-
vserver vs3.example0.com -applications snapmirror -peer-cluster
cluster2

 Info: [Job 43] 'vserver peer create' job queued
```

At this point, the state of the intercluster Vserver peer relationship is `initiated`. A Vserver peer relationship is not established until the cluster administrator of the peered cluster accepts the Vserver peer request.

Example

The following example illustrates how to create an intracluster Vserver peer relationship between Vservers vs4.example1.com and vs0.example1.com residing on cluster2:

```
cluster2::> vserver peer create -vserver vs4.example1.com -peer-
vserver vs0.example1.com -applications snapmirror

Info: 'vserver peer create' command is successful.
```

An intracluster Vserver peer relationship is created when the command is executed. Authentication is not needed as the cluster is managed by a single cluster administrator. The state of the Vserver peer relationship is `peered`.

2. Use the `vserver peer show-all` command to view the status and other details of the Vserver peer relationship.

Example

The following example illustrates how to view the status and other details of the Vserver peer relationship:

```
cluster1::> vserver peer show-all
                    Peer              Peer                           Peering
Vserver             Vserver           State       Peer Cluster       Applications
------------        ------------      ----------  -------------- ----------------
vs1.example0.com    vs3.example0.com  initiated   Cluster2          snapmirror
```

```
Cluster2::> vserver peer show-all
                   Peer              Peer                   Peering
Vserver            Vserver           State   Peer Cluster   Applications
-----------       ---------------   --------- ------------ ---------------
vs3.example0.com  vs1.example0.com   pending   cluster1       snapmirror
vs4.example1.com  vs0.example1.com   peered    cluster2       snapmirror
```

For more information about these commands, see the man pages.

Note: You can use the `job show -fields state, completion -id` to view the status of the intercluster operations.

After you finish

If you have initiated an intercluster Vserver peer relationship, you must inform the cluster administrator of the remote cluster about the Vserver peer request. After the cluster administrator of the remote cluster accepts the Vserver peer request, the Vserver peer relationship is established.

Accepting a Vserver peer relationship

When a cluster administrator creates an intercluster Vserver peer relationship, the cluster administrator of the remote cluster can accept the Vserver peer request to establish the peer relationship between the Vservers by using the `vserver peer accept` command.

About this task

Peered clusters can be managed by a single administrator or different cluster administrators. If a single cluster administrator is managing the peered clusters, the cluster administrator has to accept the Vserver peer request on the peered cluster. If different administrators are managing the peered clusters, the cluster administrator who initiates the Vserver peer request has to notify the cluster administrator of the peered cluster about the incoming Vserver peer request through any channel such as email.

Steps

1. Use the `vserver peer show` command to view the Vserver peer requests.

Example

The following example illustrates how to view the Vserver peer requests on cluster2:

```
cluster2::> vserver peer show

                    Peer              Peer
Vserver             Vserver           State
-----------         -----------       ------------
vs3.example0.com    vs1.example0.com  pending
```

2. Use the `vserver peer accept` command to accept the Vserver peer request and establish the Vserver peer relationship

Example

The following example illustrates how to accept an incoming Vserver peer request to establish a Vserver peer relationship between vs1.example0.com and vs3.example0.com on cluster1 and cluster2 respectively:

```
cluster2::> vserver peer accept -vserver vs3.example0.com -peer-
vserver vs1.example0.com

Info: [Job 46] 'vserver peer accept' job queued
```

The Vserver peer relationship is established and state is `peered`.

3. Use the `vserver peer show` command on either of the peered clusters to view the state of the Vserver peer relationship

Example

The following example illustrates how to view to state of the Vserver peer relationships:

```
cluster2::> vserver peer show
                Peer              Peer
Vserver         Vserver           State
-----------     ---------------   ------------
vs3.example0.com vs1.example0.com    peered
```

For more information about these commands, see the man pages.

Result

A cluster or Vserver administrator can establish peering applications such as SnapMirror between the peered Vservers.

Rejecting a Vserver peer relationship

When a cluster administrator creates an intercluster Vserver peer relationship, the cluster administrator of the peered cluster can reject the Vserver peer request to prevent peer relationship between the Vservers by using the `vserver peer reject` command.

About this task

If the Vserver peer request is initiated with an unauthorized Vserver, then the cluster administrator of the peered cluster can reject the relationship. Other peering operations cannot be performed on the rejected peering relationship.

Steps

1. Use the `vserver peer show` command to view the Vserver peer requests on the peered cluster.

Example

The following example illustrates how to view the Vserver peer requests on cluster2:

```
cluster2::> vserver peer show
                Peer              Peer
```

```
Vserver          Vserver            State
-----------      -----------        ------------
vs5.example0.com vs1.example0.com    pending
```

2. Use the `vserver peer reject` command to reject the Vserver peer request.

   Example

   The following example illustrates how to reject an incoming Vserver peer request between vs1.example0.com and vs5.example0.com on cluster1 and cluster2 respectively:

```
cluster2::> vserver peer reject -vserver vs5.example0.com -peer-
vserver vs1.example0.com

Info: [Job 48] 'vserver peer reject' job queued
```

   The Vserver peer relationship is in rejected state.

3. Use the `vserver peer show` command on the cluster from which the Vserver peer request was created to view the state of the Vserver peer relationship.

   Example

   The following example illustrates how to view to state of the Vserver peer relationships:

```
cluster1::> vserver peer show
                  Peer               Peer
Vserver           Vserver            State
-----------       -----------        ------------
vs1.example0.com  vs5.example0.com   rejected
```

4. Use the `vserver peer delete` command to delete the rejected Vserver peer requests because when you create the Vserver relationship between the same Vservers again, it fails.

   Example

   The following example illustrates how to delete the rejected Vserver peer requests:

```
cluster1::> vserver peer delete -vserver vs1.example0.com -peer-
vserver vs5.example0.com

Info: 'vserver peer delete' command is successful.
```

   For more information about these commands, see the man pages.

Modifying a Vserver peer relationship

A cluster administrator can modify a Vserver peering application running on the Vserver peer relationship by using the `vserver peer modify` command. In clustered Data ONTAP 8.2, the

Vserver peering relationship can either have SnapMirror or no application. The default value is `snapmirror`.

About this task

If the value of the application parameter is " ", then a cluster or Vserver administrator cannot set up SnapMirror relationship between the peered Vservers.

Steps

1. Use the `vserver peer modify` command to modify the application on the Vserver peer relationship.

   #### Example

   The following example illustrates how to modify the application on the Vserver peer relationship:

   ```
   cluster2::> vserver peer modify -vserver vs4.example1.com -peer-
   vserver vs0.example1.com -applications " "

   Info: [Job 78] 'vserver peer modify' job queued
   ```

2. Use the `vserver peer show-all` to view the applications running on the Vserver peer relationship.

   #### Example

   The following example illustrates how to view the applications running on the Vserver peer relationship:

   ```
   cluster2::> vserver peer show-all

   Vserver            Vserver           State      Peer Cluster   Applications
   -----------        -----------       -------    ------------  ------------
   vs4.example1.com   vs0.example1.com  peered     cluster2          -
   ```

   For more information about these command, see the man pages.

Deleting a Vserver peer relationship

A cluster administrator can delete the Vserver peer relationship by using the `vserver peer delete` command when the relationship between two Vservers is no longer needed.

About this task

When you are deleting a Vserver peer relationship, you must delete the Vserver peer relationship from both the peered clusters.

Steps

1. Use the `vserver peer delete` command on both the clusters to delete a Vserver peer relationship.

   When the Vserver peer relationship is deleted from one cluster, the relationship is in deleted state on the other peered cluster.

2. Use the `vserver peer show` command on both the clusters to view if the relationship is deleted.

Example

The following example illustrates how to delete a Vserver peer relationship from both the clusters:

```
cluster1::> vserver peer delete -vserver vs1.example0.com -peer-
vserver vs3.example0.com

Info: [Job 47] 'vserver peer delete' job queued

cluster1::> vserver peer show
There are no Vserver peer relationships.
```

```
cluster2::> vserver peer show
                    Peer              Peer
Vserver             Vserver           State
-----------       -----------       ------------
vs3.example0.com  vs1.example0.com   deleted
vs4.example1.com  vs0.example1.com   peered
2 entries were displayed.

cluster2::> vserver peer delete -vserver vs3.example0.com -peer-
vserver vs1.example0.com

Info: 'vserver peer delete' command is successful.

cluster2::> vserver peer show
                    Peer              Peer
Vserver             Vserver           State
-----------         -----------       ------------
vs4.example1.com    vs0.example1.com  peered
```

For more information about these commands, see the man pages.

Suspending a Vserver peer relationship

A cluster administrator can suspend an established Vserver peer relationship whenever needed by using the `vserver peer suspend` command. For example, during the maintenance period, you might want to suspend the Vserver peer relationship.

About this task

When you suspend the Vserver peer relationship, any SnapMirror data transfer that was initiated before suspending a Vserver peer relationship is not affected and the operation is completed. Any data transfer that was scheduled to run during suspension period will not get initiated.

Steps

1. Use the `vserver peer suspend` command on either of the peered cluster to suspend an active Vserver peer relationship.

   #### Example

   The following example illustrates how to suspend a Vserver peer relationship:

   ```
   cluster2::> vserver peer suspend -vserver vs4.example1.com -peer-
   vserver vs0.example1.com

   Info: [Job 50] 'vserver peer suspend' job queued
   ```

   The Vserver peer relationship is in suspended state.

2. Use the `vserver peer show` command to verify the status of the Vserver peer relationship.

   #### Example

   The following example illustrates how to verify the status of the Vserver peer relationship:

   ```
   cluster2::> vserver peer show
                    Peer              Peer
   Vserver          Vserver           State
   -----------      -----------       ------------
   vs4.example1.com  vs0.example1.com   suspended
   ```

   For more information about these commands, see the man pages.

Resuming a Vserver peer relationship

A cluster administrator can resume a suspended Vserver peer relationship by using the `vserver peer resume` command. For example, after the maintenance is complete, you can resume the suspended Vserver peering relationship.

About this task

Any SnapMirror data transfer that was scheduled to run during the suspension period will not get initiated when you resume the Vserver peer relationship. You must manually initiate the data transfer.

Steps

1. Use the `vserver peer resume` command to resume a suspended Vserver peer relationship from either of the peered clusters.

   #### Example

   The following example shows how to resume a suspended Vserver peer relationship:

   ```
   cluster1::> vserver peer resume -vserver vs4.example1.com -peer-
   vserver vs0.example1.com

   Info: [Job 76] 'vserver peer resume' job queued
   ```

   The Vserver peer relationship is in peered state.

2. Use the `vserver peer show` command to verify the status of the Vserver peer relationship.

   #### Example

   The following example shows how to verify the status of the Vserver peer relationship:

   ```
   cluster1::> vserver peer show

                    Peer              Peer
   Vserver          Vserver           State
   -----------      -----------       ---------
   vs4.example1.com  vs0.example1.com   peered
   ```

   For more information about these commands, see the man pages.

Displaying information about Vserver peer relationships

Peer Vservers are fully functional Vservers which could be either local or remote. Cluster administrators and Vserver administrators can view the peers of the Vserver to set up peering

applications such as SnapMirror between volumes of the peer Vservers by using the `vserver peer show` command.

About this task

You can also view the status of the Vserver peer relationships and the applications running on the peer relationship.

Step

1. Use the appropriate command to view the details of Vserver peer relationships:

If you want to view information about...	Enter the following command...

Peered Vservers and the peer state	`vserver peer show`
	The following example illustrates how to view the information about the peered Vservers:
	`cluster1::> vserver peer show`
	`Vserver Peer Vserver Peer State`
	`vs1.example0.com vs3.example0.com peered`
	`vs1.example0.com vs5.example0.com rejected`
	`2 entries were displayed.`

The applications running on the Vserver peer relationship	`vserver peer show-all`
	The following example illustrates how to view the information about the peered Vservers:
	`cluster1::> vserver peer show-all`
	`Vserver Peer Vserver Peer State Peer Cluster Peering Applications`
	`vs1.example0.com vs5.example0.com peered cluster2 snapmirror`

For more information about this command, see the man pages.

Glossary

A

ACL — Access control list.

active/active configuration

- In the Data ONTAP 7.2 and 7.3 release families, a pair of storage systems or V-Series systems (sometimes called *nodes*) configured to serve data for each other if one of the two systems stops functioning. Also sometimes referred to as *active/active pairs*.
- In the Data ONTAP 8.x release family, this functionality is referred to as a *high-availability (HA) configuration* or an *HA pair*.
- In the Data ONTAP 7.1 release family and earlier releases, this functionality is referred to as a *cluster*.

address resolution — The procedure for determining an address corresponding to the address of a LAN or WAN destination.

admin Vserver — In clustered Data ONTAP, a Vserver that has overall administrative access to all objects in the cluster, including all objects owned by other Vservers, but does not provide data access to clients or hosts.

administration host — A client computer that is used to manage a storage system through a Telnet or Remote Shell connection.

Application Program Interface (API) — A language and message format used by an application program to communicate with the operating system or some other system, control program, or communications protocol.

authentication — The process of verifying the identity of a user who is logging in to a computer system.

AutoSupport — An integrated technology that triggers email messages from the customer site to technical support or another specified email recipient when there are any failures in Unified Manager services. These messages contain information such as feature usage metrics, configuration and user settings, system health, and so on.

B

big-endian — A binary data format for storage and transmission in which the most significant byte comes first.

C

caching module — A Flash Cache 2, Flash Cache, or Performance Acceleration Module (PAM) PCIe-based, memory module that optimizes the performance of random read-intensive workloads by functioning as an intelligent external read

cache. This hardware works in tandem with the WAFL External Cache software component of Data ONTAP.

CIFS share

- In Data ONTAP, a directory or directory structure that has been made available to network users and can be mapped to a drive letter on a CIFS client. Also known simply as a *share*.
- In OnCommand Insight (formerly SANscreen suite), a service exposed from a NAS device to provide file-based storage through the CIFS protocol. CIFS is mostly used for Microsoft Windows clients, but many other operating systems can access CIFS shares as well.

CLI

command-line interface. The storage system prompt is an example of a command-line interface.

client

A workstation or PC in a client-server architecture; that is, a computer system or process that requests services from and accepts the responses of another computer system or process.

cluster

- In clustered Data ONTAP 8.x, a group of connected nodes (storage systems) that share a namespace and that you can manage as a single virtual server or multiple virtual servers, providing performance, reliability, and scalability benefits.
- In the Data ONTAP 7.1 release family and earlier releases, a pair of storage systems (sometimes called *nodes*) configured to serve data for each other if one of the two systems stops functioning.
- In the Data ONTAP 7.3 and 7.2 release families, this functionality is referred to as an *active/active configuration*.
- For some storage array vendors, *cluster* refers to the hardware component on which host adapters and ports are located. Some storage array vendors refer to this component as a *controller*.

cluster Vserver

Previous name for a *data Vserver*. See *data Vserver*.

Common Internet File System (CIFS)

Microsoft's file-sharing networking protocol that evolved from SMB.

community

A logical relationship between an SNMP agent and one or more SNMP managers. A community is identified by name, and all members of the community have the same access privileges.

console

The physical or virtual terminal that is used to monitor and control a storage system.

Copy-On-Write (COW)

The technique for creating Snapshot copies without consuming excess disk space.

D

data Vserver	In clustered Data ONTAP, a virtual server that facilitates data access from the cluster; the hardware and storage resources of the cluster are dynamically shared by data Vservers within a cluster. Previously referred to as a *cluster Vserver*.
degraded mode	The operating mode of a storage system when a disk in the RAID group fails or the batteries on the NVRAM card are low.
disk ID number	The number assigned by the storage system to each disk when it probes the disks at startup.
disk sanitization	A multiple write process for physically obliterating existing data on specified disks in such a manner that the obliterated data is no longer recoverable by known means of data recovery.
disk shelf	A shelf that contains disk drives and is attached to a storage system.
E	
emulated storage system	A software copy of a failed storage system that is hosted by its takeover storage system. The emulated storage system appears to users and administrators to be a functional version of the failed storage system. For example, it has the same name as the failed storage system.
Ethernet adapter	An Ethernet interface card.
expansion card	A SCSI card, NVRAM card, network card, hot-swap card, or console card that plugs into a storage system expansion slot. Sometimes called an *adapter*.
expansion slot	The slots on the storage system board into which you insert expansion cards.
F	
failed storage system	A physical storage system that has ceased operating. In a high-availability configuration, it remains the failed storage system until a giveback succeeds.
Flash Cache module	A PCIe-based, solid state memory module that optimizes the performance of random read-intensive workloads by functioning as an intelligent external read cache. The Flash Cache 2 module is the successor of the Flash Cache module, which is the successor of the Performance Acceleration Module (PAM). This hardware works in tandem with the WAFL External Cache software component of Data ONTAP.
G	
giveback	The technology that enables two storage systems to return control of each other's data after the issues that caused a controller failover are resolved.
global namespace	See *namespace*.
group	In Data ONTAP operating in 7-Mode, a group of users defined in the storage system's `/etc/group` file.

Group ID (GID) The number used by UNIX systems to identify groups.

H

HA (high availability)
- In Data ONTAP 8.x, the recovery capability provided by a pair of nodes (storage systems), called an *HA pair*, that are configured to serve data for each other if one of the two nodes stops functioning.
- In the Data ONTAP 7.3 and 7.2 release families, this functionality is referred to as an *active/active configuration*.

HA pair
- In Data ONTAP 8.x, a pair of nodes whose controllers are configured to serve data for each other if one of the two nodes stops functioning. Depending on the system model, both controllers can be in a single chassis, or one controller can be in one chassis and the other controller can be in a separate chassis.
- In the Data ONTAP 7.3 and 7.2 release families, this functionality is referred to as an *active/active configuration*.

heartbeat A repeating signal transmitted from one storage system to the other that indicates that the storage system is in operation. Heartbeat information is also stored on disk.

hot swap The process of adding, removing, or replacing a disk while the storage system is running.

hot swap adapter An expansion card that makes it possible to add or remove a hard disk with minimal interruption to file system activity.

I

inode A data structure containing information about files on a storage system and in a UNIX file system.

interrupt switch A switch on some storage system front panels used for debugging purposes.

L

LAN Emulation (LANE) The architecture, protocols, and services that create an Emulated LAN using ATM as an underlying network topology. LANE enables ATM-connected end systems to communicate with other LAN-based systems.

M

Maintenance mode An option when booting a storage system from a system boot disk. Maintenance mode provides special commands for troubleshooting hardware and configuration.

MultiStore In Data ONTAP operating in 7-Mode, an optional software product that enables you to partition the storage and network resources of a single storage system so that it appears as multiple storage systems on the network.

N

namespace	In network-attached storage (NAS) environments, a collection of files and path names to the files.
NDMP	Network Data Management Protocol. A protocol that allows storage systems to communicate with backup applications and provides capabilities for controlling the robotics of multiple tape backup devices.
network adapter	An Ethernet, FDDI, or ATM card.
node Vserver	In clustered Data ONTAP, a Vserver that is restricted to operation in a single node of the cluster at any one time, and provides administrative access to some objects owned by that node. A node Vserver does not provide data access to clients or hosts.
normal mode	The state of a storage system when there is no takeover in the high-availability configuration.
NVMEM	nonvolatile memory.
NVRAM cache	Nonvolatile RAM in a storage system, used for logging incoming write data and NFS requests. Improves system performance and prevents loss of data in case of a storage system or power failure.
NVRAM card	An adapter that contains the storage system's NVRAM cache.
NVRAM mirror	A synchronously updated copy of the contents of the storage system NVRAM (nonvolatile random access memory) contents kept on the partner storage system.

P

PAM (Performance Acceleration Module)	A PCIe-based, DRAM memory module that optimizes the performance of random read-intensive workloads by functioning as an intelligent external read cache. This hardware is the predecessor of the Flash Cache module and works in tandem with the WAFL External Cache software component of Data ONTAP.
panic	A serious error condition causing the storage system or V-Series system to halt. Similar to a software crash in the Windows system environment.
parity disk	The disk on which parity information is stored for a RAID4 disk drive array. In RAID groups using RAID-DP protection, two parity disks store the parity and double-parity information. Used to reconstruct data in failed disk blocks or on a failed disk.
partner mode	The method you use to communicate through the command-line interface with a virtual storage system during a takeover.
partner node	From the point of view of the local node (storage system), the other node in a high-availability configuration.

Performance Acceleration Module (PAM) — See *PAM (Performance Acceleration Module)*.

POST — Power-on self-tests. The tests run by a storage system after the power is turned on.

Q

qtree — A special subdirectory of the root of a volume that acts as a virtual subvolume with special attributes.

R

RAID — Redundant Array of Independent Disks. A technique that protects against disk failure by computing parity information based on the contents of all the disks in an array. Storage systems use either RAID4, which stores all parity information on a single disk, or RAID-DP, which stores all parity information on two disks.

RAID disk scrubbing — The process in which a system reads each disk in the RAID group and tries to fix media errors by rewriting the data to another disk area.

S

SCSI adapter — An expansion card that supports SCSI disk drives and tape drives.

SCSI address — The full address of a disk, consisting of the disk's SCSI adapter number and the disk's SCSI ID, such as 9a.1.

SCSI ID — The number of a disk drive on a SCSI chain (0 to 6).

serial adapter — An expansion card for attaching a terminal as the console on some storage system models.

serial console — An ASCII or ANSI terminal attached to a storage system's serial port. Used to monitor and manage storage system operations.

SFO — See *storage failover (SFO)*.

SID — Security identifier used by the Windows operating system.

Snapshot copy — An online, read-only copy of an entire file system that protects against accidental deletions or modifications of files without duplicating file contents. Snapshot copies enable users to restore files and to back up the storage system to tape while the storage system is in use.

storage failover (SFO) — In clustered Data ONTAP, the method of ensuring data availability by transferring the data service of a failed node to another node in an HA pair. Transfer of data service is often transparent to users and applications. In Data ONTAP 7.2 and later, and in Data ONTAP operating in 7-Mode, the failover method is called *controller failover*.

T

takeover — The emulation of the failed node identity by the takeover node in a high-availability configuration; the opposite of *giveback.*

takeover mode — The method you use to interact with a node (storage system) when it has taken over its partner. The console prompt indicates when the node is in takeover mode.

takeover node — A node (storage system) that remains in operation after the other node stops working and that hosts a virtual node that manages access to the failed node disk shelves and network connections. The takeover node maintains its own identity and the virtual node maintains the failed node identity.

trap — An asynchronous, unsolicited message sent by an SNMP agent to an SNMP manager indicating that an event has occurred on the storage system.

U

UID — user identification number.

Unicode — A 16-bit character set standard. It was designed and is maintained by the nonprofit consortium Unicode Inc.

V

vFiler unit — In Data ONTAP operating in 7-Mode, a virtual storage system that you create using MultiStore, which enables you to partition the storage and network resources of a single storage system so that it appears as multiple storage systems on the network.

volume — A file system.

Vserver — In clustered Data ONTAP, a virtual storage server that provides network access through unique network addresses, that might serve data out of a distinct namespace, and that is separately administrable from the rest of the cluster. There are three types of Vservers—*admin*, *node*, and *cluster* ("cluster Vserver" is called "data Vserver" in Data ONTAP 8.2 and later)—but unless there is a specific need to identify the type of Vserver, Vserver usually refers to the cluster/data Vserver.

W

WAFL — Write Anywhere File Layout. A file system designed for the storage system to optimize write performance.

WAFL External Cache — On a storage system that has a Performance Acceleration Module (PAM), Flash Cache, or Flash Cache 2 module installed, this cache improves storage system performance by reducing the number of disk reads. Sometimes referred to as *WAFL extended cache*.

WINS — Windows Internet Name Service.

workgroup A collection of computers running Windows NT or Windows for Workgroups that is grouped for browsing and sharing.

Copyright information

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at *www.ibm.com/legal/copytrade.shtml*.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *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.

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

B

C

D

E

F

H

I

J

O

P

Q

R

S

T

U

V

W