Contents

Copyright information ........................................................................................................ 11
Trademark information .................................................................................................... 13
About this guide .................................................................................................................. 15
  Audience .......................................................................................................................... 15
  Terminology ..................................................................................................................... 15
  Where to enter commands .............................................................................................. 17
  Keyboard and formatting conventions ............................................................................. 17
  Special messages .............................................................................................................. 18
  How to send your comments .......................................................................................... 18
What the management interface is .................................................................................. 21
  Command availability ....................................................................................................... 21
  Different shells that are available ................................................................................... 22
  Types of privilege levels .................................................................................................. 22
  The diagnostic account and the systemshell ................................................................. 22
Management interface basics .......................................................................................... 25
  How to use the command-line interface ....................................................................... 25
    How to navigate CLI command directories .................................................................. 25
    How to specify values in the CLI ............................................................................... 26
    How to reissue CLI commands ............................................................................... 27
    Keyboard shortcuts to edit CLI commands .............................................................. 27
    Setting the privilege level in the CLI ....................................................................... 28
    Setting display preferences in the CLI ...................................................................... 29
  How to access the Web interface .................................................................................... 29
    How to navigate the Web interface ............................................................................ 30
    Setting the privilege level in the Web interface ....................................................... 31
  How to use queries, patterns, and wildcards ............................................................... 31
    How to use extended queries ................................................................................. 32
  Exiting the management interface ............................................................................... 33
How Data ONTAP Cluster-Mode works with disks ......................................................... 35
  How Data ONTAP reports disk types ....................................................................... 35
  Disk connection protocols, topologies, and types ....................................................... 37
    Fibre Channel-Arbitrated Loop (FC-AL) disk connection type ................................. 37
Assigning ownership of array LUNs on nodes running Cluster-Mode .......... 60
Modifying assignment of spare array LUNs in Cluster-Mode ..................... 62
Why you might change the checksum type of an array LUN ...................... 63
Changing the checksum type of an array LUN ........................................... 63
Prerequisites to reconfiguring a LUN on the storage array ...................... 64
Changing array LUN size or composition .................................................. 65
Removing one array LUN from use by Data ONTAP .................................. 66
Removing a storage system using array LUNs from service ...................... 67

**Reusing disks configured for software-based disk ownership ............ 69**
Manually erasing software-based disk ownership information ................. 69
Automatically erasing disk ownership information .................................... 70

**Disk management .................................................................................. 73**
Displaying information about disks .......................................................... 73
Modifying disk attributes ............................................................................ 74
Failing a disk ............................................................................................... 75
Displaying disk-option settings .................................................................... 75
Modifying disk-option settings .................................................................... 76
Reassigning disks to another node .............................................................. 77
Removing ownership from a disk ............................................................... 77
Zeroing spare disks ....................................................................................... 78
Downloading disk, ACP processor, and shelf firmware ......................... 78
Commands for manually updating disk, ACP processor, and disk shelf
  firmware .................................................................................................... 79
Controlling disk LEDs .................................................................................. 80

**How Data ONTAP uses RAID to protect your data and data**
**availability ................................................................................................ 81**
RAID protection levels for disks ................................................................. 81
  What RAID-DP protection is ................................................................. 82
  What RAID4 protection is ................................................................. 82
RAID protection for third-party storage ....................................................... 82
RAID disk types ......................................................................................... 83
How Data ONTAP RAID groups work ....................................................... 83
  How RAID groups are named ............................................................. 84
  About RAID group size ....................................................................... 84
Considerations for sizing RAID groups for disks ........................................ 84
Considerations for Data ONTAP RAID groups for array LUNs .......... 85
How Data ONTAP works with hot spare disks ......................................................... 86
How many hot spares you should have ............................................................. 86
What disks can be used as hot spares ............................................................... 86
What a matching spare is .............................................................................. 87
What an appropriate hot spare is ................................................................... 87
About degraded mode ................................................................................... 87
How Data ONTAP handles a failed disk with a hot spare ........................................ 88
How Data ONTAP handles a failed disk that has no available hot spare ................. 88
How RAID-level disk scrubs verify data integrity ................................................... 89

Controlling the impact of RAID operations on system performance .... 91
Controlling the performance impact of RAID data reconstruction ..................... 92
Controlling the performance impact of RAID-level scrubbing ............................. 93

How you use aggregates to provide storage to your volumes ............... 95
Aggregate types ..................................................................................................... 95
How unmirrored aggregates work ................................................................. 96
Rules for mixing disk types in aggregates ....................................................... 97
Rules for mixing array LUNs in an aggregate .................................................. 98
Checksum rules for adding storage to an aggregate .......................................... 99
What happens when you add larger disks to an aggregate ............................... 100

Aggregate management ...................................................................................... 101
Creating an aggregate ..................................................................................... 101
Displaying information about aggregates ....................................................... 102
   About aggregate states ................................................................................ 103
Adding disks to an aggregate ........................................................................... 104
Modifying an aggregate .................................................................................. 104
Renaming an aggregate ................................................................................... 105
Scrubbing an aggregate for errors .................................................................... 105
   Displaying status information about aggregate scrubs ............................... 106
Deleting an aggregate ...................................................................................... 106

Storage failover management ............................................................................. 107
What an HA pair is .......................................................................................... 107
Benefits of HA pairs ........................................................................................ 107
Characteristics of nodes in an HA pair ............................................................ 108
Displaying information about an HA pair ......................................................... 109
Modifying an HA pair ..................................................................................... 110
Taking over partner node storage ................................................................... 111
How to protect your data ................................................................. 165
How Snapshot copies work .............................................................. 167
How many Snapshot copies you can have ...................................... 168
Creating a single Snapshot copy ..................................................... 168
Creating a Snapshot policy ............................................................. 172
How mirrors work ........................................................................... 175
Types of mirrors you can create ....................................................... 175
Mirror location in the global namespace ......................................... 176
Pattern matching path names .......................................................... 176
Replicating between two virtual servers requires the same language settings .... 177
Mirror limitations ............................................................................. 177
SnapMirror configuration limit ......................................................... 178
Active transfer limits ...................................................................... 178
SnapMirror fanout limits ................................................................. 179
Maximum number of Snapshot copies for volumes that are mirrored ...... 180
Cannot automatically delete Snapshot copies on destination volumes ...... 180
Load-sharing mirror management .................................................... 180
Mounting a volume that has load-sharing mirrors for NFS clients ...... 181
Mounting a volume that has load-sharing mirrors for CIFS clients ...... 181
Restriction when modifying the source volume ............................... 181
Creating a set of load-sharing mirrors ............................................. 182
Adding a load-sharing mirror to a set of load-sharing mirrors .......... 184
Updating a set of load-sharing mirrors .......................................... 185
Aborting an update to a load-sharing mirror .................................. 186
Scheduling SnapMirror transfers .................................................... 186
Changing mirroring relationship schedules .................................... 187
Listing the schedule state of a mirroring relationship ..................... 188
Listing the status of a particular load-sharing mirror ...................... 188
Determining whether load-sharing mirrors are up-to-date ................ 188
Managing data protection mirror .................................................... 189
Uses for data protection mirrors .................................................... 190
Creating a data protection mirror .................................................. 190
Managing mirroring relationships .................................................. 191
Deleting a mirror .......................................................................... 193
Copyright information

Copyright © 1994–2011 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).
Trademark information

All applicable trademark attribution is listed here.

NetApp; the NetApp logo; the Network Appliance logo; Bycast; Cryptainer; Cryptoshred; DataFabric; Data ONTAP; Decru; Decru DataFort; FAServer; FilerView; FlexCache; FlexClone; FlexShare; FlexVol; FPolicy; gFiler; Go further, faster; Manage ONTAP; MultiStore; NearStore; NetCache; NOW (NetApp on the Web); ONTAPI; RAID-DP; SANscreen; SecureShare; Simulate ONTAP; SnapCopy; SnapDrive; SnapLock; SnapManager; SnapMirror; SnapMover; SnapRestore; SnapValidator; SnapVault; Spinnaker Networks; Spinnaker Networks logo; SpinAccess; SpinCluster; SpinFlex; SpinFS; SpinHA; SpinMove; SpinServer; SpinStor; StorageGRID; StoreVault; SyncMirror; Topio; vFiler; VFM; and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. Network Appliance, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The StoreVault logo, ApplianceWatch, ApplianceWatch PRO, ASUP, AutoSupport, ComplianceClock, DataFort, Data Motion, FlexScale, FlexSuite, Lifetime Key Management, LockVault, NOW, MetroCluster, OpenKey, ReplicatorX, SecureAdmin, Shadow Tape, SnapDirector, SnapFilter, SnapMigrator, SnapSuite, Tech OnTap, Virtual File Manager, VPolicy, and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. Get Successful and Select are service marks of NetApp, Inc. in the U.S.A.

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 http://www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. 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 U.S.A. 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.

NetCache is certified RealSystem compatible.
About this guide

This document helps you to use the product that it describes. You can do that more effectively when you understand the intended audience and the conventions that this document uses to present information.

This document describes how to configure, operate, and manage the storage resources for storage systems that run Data ONTAP software. It discusses disks, RAID, aggregates, volumes, and qtrees that are used to organize and manage data. In addition, this document provides information about how to protect your data by using Snapshot copies, mirrors, storage failover, and tape backups.

Next topics

- Audience on page 15
- Terminology on page 15
- Where to enter commands on page 17
- Keyboard and formatting conventions on page 17
- Special messages on page 18
- How to send your comments on page 18

Audience

This document is written with certain assumptions about your technical knowledge and experience.

This document is for storage administrators who need to configure and maintain a storage system running Data ONTAP 8 Cluster-Mode. It assumes that you are familiar with UNIX commands.

Terminology

To understand the concepts in this document, you might need to know how certain terms are used.

Storage terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>array LUN</td>
<td>The storage that third-party storage arrays provide to storage systems running Data ONTAP software. One array LUN is the equivalent of one disk on a native disk shelf.</td>
</tr>
<tr>
<td>LUN (logical unit number)</td>
<td>A logical unit of storage identified by a number.</td>
</tr>
<tr>
<td>native disk</td>
<td>A disk that is sold as local storage for storage systems that run Data ONTAP software.</td>
</tr>
</tbody>
</table>
native disk shelf  A disk shelf that is sold as local storage for storage systems that run Data ONTAP software.

storage controller  The component of a storage system that runs the Data ONTAP operating system and controls its disk subsystem. Storage controllers are also sometimes called controllers, storage appliances, appliances, storage engines, heads, CPU modules, or controller modules.

storage system  The hardware device running Data ONTAP that receives data from and sends data to native disk shelves, third-party storage, or both. Storage systems that run Data ONTAP are sometimes referred to as filers, appliances, storage appliances, V-Series systems, or systems.

third-party storage  The back-end storage arrays, such as IBM, Hitachi Data Systems, and HP, that provide storage for storage systems running Data ONTAP.

Cluster and high-availability terms

cluster  • In Data ONTAP 8.x Cluster-Mode, a group of connected nodes (storage systems) that share a global 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.

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 (storage systems) 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.
Where to enter commands

You can use your product more effectively when you understand how this document uses command conventions to present information.

You can perform common administrator tasks in one or more of the following ways:

- You can enter commands on the system console, or from any client computer that can obtain access to the storage system using a Telnet or Secure Shell (SSH) session.
  In examples that illustrate command execution, the command syntax and output might differ, depending on your version of the operating system.
- You can use the ClusterView graphical user interface.
  For information about accessing your system with ClusterView and about ClusterView Help, which explains Data ONTAP features and how to work with them in ClusterView, see the Data ONTAP System Administration Guide.
- You can enter Windows, ESX, HP-UX, AIX, Linux, and Solaris commands on a client console.
  Your product documentation provides specific command options you can use.
- You can use the client graphical user interface.
  Your product documentation provides details about how to use the graphical user interface.
- You can enter commands on the switch console or from any client that can obtain access to the switch using a Telnet session.
  In examples that illustrate command execution, the command syntax and output might differ, depending on your version of the operating system.

Keyboard and formatting conventions

You can use your product more effectively when you understand how this document uses keyboard and formatting conventions to present information.

Keyboard conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>The NOW site</td>
<td>Refers to NetApp On the Web at now.netapp.com/</td>
</tr>
<tr>
<td>Enter, enter</td>
<td>• Used to refer to the key that generates a carriage return; the key is named Return on some keyboards.</td>
</tr>
<tr>
<td></td>
<td>• Used to mean pressing one or more keys on the keyboard and then pressing the Enter key, or clicking in a field in a graphical interface and then typing information into the field.</td>
</tr>
</tbody>
</table>
### Formatting conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Italic font</strong></td>
<td>• Words or characters that require special attention.</td>
</tr>
<tr>
<td></td>
<td>• Placeholders for information you must supply.</td>
</tr>
<tr>
<td></td>
<td>For example, if the guide says to enter the <code>arp -d hostname</code> command,</td>
</tr>
<tr>
<td></td>
<td>you enter the characters &quot;arp -d&quot; followed by the actual name of the host.</td>
</tr>
<tr>
<td></td>
<td>• Book titles in cross-references.</td>
</tr>
<tr>
<td><strong>Monospaced font</strong></td>
<td>• Command names, option names, keywords, and daemon names.</td>
</tr>
<tr>
<td></td>
<td>• Information displayed on the system console or other computer monitors.</td>
</tr>
<tr>
<td></td>
<td>• Contents of files.</td>
</tr>
<tr>
<td></td>
<td>• File, path, and directory names.</td>
</tr>
<tr>
<td><strong>Bold monospaced font</strong></td>
<td>Words or characters you type. What you type is always shown in lowercase</td>
</tr>
<tr>
<td></td>
<td>letters, unless your program is case-sensitive and uppercase letters are</td>
</tr>
<tr>
<td></td>
<td>necessary for it to work properly.</td>
</tr>
</tbody>
</table>

### Special messages

This document might contain the following types of messages to alert you to conditions that you need to be aware of.

**Note:** A note contains important information that helps you install or operate the system efficiently.

**Attention:** An attention notice contains instructions that you must follow to avoid a system crash, loss of data, or damage to the equipment.

### 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 e-mail to
doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the name of your product and the applicable operating system. For example, FAS6070—Data ONTAP 7.3, or Host Utilities—Solaris, or Operations Manager 3.8—Windows.
What the management interface is

The management interface enables you to administer the storage system.

Data ONTAP Cluster-Mode provides two kinds of management interfaces, the command-line interface (CLI) and the Web interface. The CLI provides a command-based mechanism that is similar to the UNIX tcsh shell in that it provides tab completion and advanced queries and UNIX-style patterns and wildcards. The Web interface provides a model with which you can interact by using a Web browser.

Regardless of the interface you use (CLI or Web), a set of similar objects is displayed as rows in a table. Each object or row is identified by a set of key values, which occupy the first fields. The rest of the rows are occupied by values of other parameters.

Data ONTAP Cluster-Mode commands are organized hierarchically into command sets by directories. Command directories can contain other directories. The commands contained within the directories enable you to manage the components of a Data ONTAP Cluster-Mode storage system.

Next topics

Command availability on page 21
Different shells that are available on page 22
Types of privilege levels on page 22
The diagnostic account and the systemshell on page 22

Command availability

All commands are available in either operational mode or maintenance mode.

Operational mode commands are available during normal operation of a Data ONTAP Cluster-Mode storage system, after it has been initialized and configured. Almost all commands are available in operational mode.

Maintenance mode commands are available when a Data ONTAP Cluster-Mode storage system is running but has not yet been initialized or configured, or when the system has failed and is not yet fully operational. You can use maintenance-mode commands to initialize and configure a system, and to diagnose and resolve problems. Most maintenance-mode commands are also available in operational mode, but a few commands are available only in maintenance mode.
Different shells that are available

The Data ONTAP Cluster-Mode CLI provides three different shells in which you can execute different commands.

The native shell in which you can execute commands is referred to as the clustershell. This is the shell that is started automatically when you log in to a filer. It provides all of the commands you need to configure, manage, monitor, and maintain your cluster.

In addition, a special shell exists that enables you to run a subset of 7-Mode commands from the Cluster-Mode. This special shell is called the nodeshell. The standard way to access the nodeshell is by typing the single verb `run`. However, the full syntax of this command is `system node run` and it is documented as such in the Data ONTAP Cluster-Mode Administration Reference. For more information about using the nodeshell and which networking, storage, and system administrative commands are supported, see the Data ONTAP Cluster-Mode Administration Reference.

The systemshell is a low-level shell used for diagnostic and troubleshooting purposes. The systemshell is not intended for general administrative purposes. Use it only with guidance from technical support. For more information about using the `system node systemshell` command, see the Data ONTAP Cluster-Mode Administration Reference.

Related concepts

Storage commands that are available in the nodeshell on page 219

Types of privilege levels

Data ONTAP Cluster-Mode commands are classified into three privilege levels: admin, advanced, and diagnostic.

- admin—Most commands fall into this category. These commands are used for routine tasks.
- advanced—Commands in this category are used infrequently, require advanced knowledge to use, and can cause problems if used inappropriately. You should use advanced-level commands and parameters only with the advice of support personnel.
- diagnostic—Commands in this category are potentially disruptive tools that are used only by support personnel to diagnose and fix serious problems. Diagnostic commands are the highest privilege commands available to customers.

The diagnostic account and the systemshell

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

The diagnostic account is the only account that can be used to access the systemshell, through the advanced command `system node systemshell`. The diagnostic account is disabled by default. You must enable the account and set up its password before using it. Neither the diagnostic account nor the systemshell is intended for general administrative purposes.

For more information about how to use the `system node systemshell` command and how to set the initial password for the diagnostic account, see the *Data ONTAP Cluster-Mode Administration Reference*. 
Management interface basics

To manage a Data ONTAP Cluster-Mode storage system, you need to know about using the CLI and Web interface; about using queries, patterns, and wildcards in commands; about setting the command privilege level; and about exiting the management interface.

Next topics

- How to use the command-line interface on page 25
- How to access the Web interface on page 29
- How to use queries, patterns, and wildcards on page 31
- Exiting the management interface on page 33

How to use the command-line interface

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

You can access the CLI from a terminal that is connected directly to a node's console port, or you can use secure shell (ssh) or Telnet to access a node and use the CLI to interact with the management interface remotely.

The CLI's command prompt is represented as node::> in the documentation. On a running Data ONTAP Cluster-Mode storage system, the prompt shows the node name. For example, on a node named hr_data11, the CLI prompt is hr_data11::>.

Next topics

- How to navigate CLI command directories on page 25
- How to specify values in the CLI on page 26
- How to reissue CLI commands on page 27
- Keyboard shortcuts to edit CLI commands on page 27
- Setting the privilege level in the CLI on page 28
- Setting display preferences in the CLI on page 29

How to navigate 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 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:

```
node::> storage
node:::storage> disk
node:::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 previous example, you can enter `st d sh`. You can 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.

### How to specify 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 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 double quoted. 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 double quotes.

The clustershell CLI interprets a question mark (?) as the command to display help information for a particular command. As a result, when you want a question mark in a command to be interpreted literally, you must type Esc+?.

Some text that you enter in the CLI, like command names, parameters, and certain values, is case-insensitive. For example, when entering parameter values for the `vserver cifs` commands, capitalization is ignored. However, most parameter values, like the names of nodes, virtual servers, 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 ("-").

In the following example, a virtual server is created with a text comment. The virtual server is then modified to delete the comment.

```
node::> vserver create -vserver vs0 -rootvolume root_vs0 -aggregate aggr0 -ns-switch nis -nm-switch file -language en_US -rootvolume-security-style
```
How to reissue CLI commands

Each CLI session keeps a history of all commands issued in it. You can view the command history and reissue previous commands by using the `history` and `redo` commands, respectively.

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 vol` command to reexecute the command.
- The numeric ID of a previous command, as listed by the `history`; for example, you can use the `redo 4` command to reexecute 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 reexecute 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 enter the following command:

```
node::> redo -3
```

Keyboard shortcuts to edit CLI commands

The command at the current command prompt is the current active command. You can edit the command by using the following key combinations. These key combinations are similar to those of the UNIX `tcsh` shell and the Emacs editor. In the following table, a caret (^) indicates that you must press the Ctrl key with the specified key.

<table>
<thead>
<tr>
<th>Edit Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>^b</td>
<td>Move the cursor back one character.</td>
</tr>
<tr>
<td>^f</td>
<td>Move the cursor forward one character.</td>
</tr>
<tr>
<td>^a</td>
<td>Move the cursor to the beginning of the line.</td>
</tr>
<tr>
<td>^e</td>
<td>Move the cursor to the end of the line.</td>
</tr>
<tr>
<td>^k</td>
<td>Remove the contents of the edit buffer, from the cursor to the end of the line, and save it in the cut buffer.</td>
</tr>
<tr>
<td>^y</td>
<td>Yank the contents of the cut buffer, pushing it into the edit buffer at the cursor.</td>
</tr>
<tr>
<td>ESC b</td>
<td>Move the cursor back one word.</td>
</tr>
<tr>
<td>ESC f</td>
<td>Move the cursor forward one word.</td>
</tr>
<tr>
<td>Edit Command</td>
<td>Action</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
</tr>
<tr>
<td>ESC d</td>
<td>Cut the contents of the edit buffer, beginning at the cursor and continuing to the end of the following word.</td>
</tr>
<tr>
<td>ESC Backspace</td>
<td>Delete the word before the cursor.</td>
</tr>
<tr>
<td>^h</td>
<td>Delete the character before the cursor.</td>
</tr>
<tr>
<td>Backspace</td>
<td>Delete the character before the cursor.</td>
</tr>
<tr>
<td>^d</td>
<td>Delete the character after the cursor.</td>
</tr>
<tr>
<td>^p</td>
<td>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.</td>
</tr>
<tr>
<td>^n</td>
<td>Replace the current contents of the edit buffer with the next entry on the history buffer.</td>
</tr>
<tr>
<td>Down arrow</td>
<td>Down history.</td>
</tr>
<tr>
<td>Up arrow</td>
<td>Up history.</td>
</tr>
<tr>
<td>Back arrow</td>
<td>Go backward one character.</td>
</tr>
<tr>
<td>Forward arrow</td>
<td>Go forward one character.</td>
</tr>
<tr>
<td>^q</td>
<td>TTY start output.</td>
</tr>
<tr>
<td>^s</td>
<td>TTY stop output.</td>
</tr>
<tr>
<td>^u</td>
<td>Clear the current edit buffer.</td>
</tr>
<tr>
<td>^v</td>
<td>Escapes a special mapping for the following character. For instance, to enter a question mark into a command's arguments, press ^v, then press ?.</td>
</tr>
<tr>
<td>?</td>
<td>Display context-sensitive help.</td>
</tr>
</tbody>
</table>

**Setting the privilege level in the CLI**

You can set the privilege level in the CLI by using the `set` command.

**Step**

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

**Example**

The following example sets the privilege level to advanced and then to admin:
Setting display preferences in the CLI

You can use the `set` command and `rows` command to set CLI display preferences.

Step

1. To set CLI display preferences, use the `set` command, the `rows` command, or both.
   - Use the `set` command with one or more of the following parameters:
     - `-confirmations {on | off}`—Specifies whether confirmations are issued for potentially disruptive commands. The default is on.
     - `-showallfields {true | false}`—Specifies whether `show` commands display all fields by default. The default is false.
     - `-showseparator separator`—Specifies an alternative field separator for `show` commands. The separator can be from one to three characters in length. When using this parameter, specify the separator in double quotation marks.
     - `-units {auto | raw | B | KB | MB | GB | TB | PB}`—Specifies a default data-size unit. The default is auto.
   - Use the `rows` command to specify the number of rows for the current CLI session.
     - 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.

Example

For example, to have fields separated by a comma and use GB as the default data-size unit and to set the number of rows to 50, run the following commands:

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

How to access the Web interface

The Web interface provides a browser-based view of the management interface. You select commands from a menu of options, and command results are displayed in tables.

You access the Web interface by pointing a supported Web browser to a node—for example, http://node1 or http://192.168.12.1. You enter a valid administrative user name and password into the appropriate fields and then click Login.
Note: To access the Web interface through a firewall or by using VPN, port 80 must be available and included in the URL when pointing your Web browser to a node—for example, http://node1:80 or http://192.168.12.1:80.

Next topics

- How to navigate the Web interface on page 30
- Setting the privilege level in the Web interface on page 31

How to navigate the Web interface

Commands in the Web interface are organized in the same hierarchy used by the CLI.

The left-most pane, also called the *navigation pane*, of the browser lists the available command directories. Command directories can be expanded to show their commands and subdirectories; you expand directories by clicking the plus sign (+). If a command directory is expanded, a minus sign (-) is displayed in the box to the left of the directory name; you can collapse the directory listing by clicking the minus sign. Clicking a command displays the command's objects or parameters in the right-most pane, also called the *action pane*, of the browser. You can then perform the following actions:

- To display a command's current objects and to perform operations on one or more of them, you click *manage*, then use the table and commands that are displayed in the action pane.
- To display a list of objects that match specific criteria, you click *Query Table*. You enter the appropriate values into the fields that you want to query and then click *Show Matches*.
- To create a new object, you select *Create* from the *Actions* menu, enter the appropriate values, and then click *Create Entry*.

  **Note:** All of the objects that you can create by using the CLI, you can also create by using the Web interface. In addition, you can "duplicate" an object in the Web interface. When you duplicate an object, the initial values for the new object are inherited from the existing one. Note that the fields of duplicated object initially include all of the attributes of the original object, including object names and other attributes that might or might not apply to the final duplicated object. Therefore, if you use the "duplicate" option, be sure to change the duplicated object's name and any other attributes that are different from the original object's.

- To perform an operation on an existing object, you select the appropriate command from the *Actions* menu and click on the object's name in the table (by default, linked names are displayed in blue text). Specific values for the object are displayed in the action pane. You make the appropriate changes and then click *Run Command* or the equivalent button to run the command.

The Web interface has links to many of the attributes in a table. You can use these links to navigate to different command directories. For example, if you are viewing the virtual server table, you can click on the link for a virtual server's root volume to go to the volume table. From the volume table, you can click on the root volume's aggregate link to go to the aggregate table. From the aggregate table, you can click on the aggregate's disk link to go to the disk table, which displays the names of the disks on which the aggregate is located.
Setting the privilege level in the Web interface

You can set the privilege level in the Web interface by using the PREFERENCES command.

About this task

See the reference page for the set command for information about setting other preferences.

Steps

1. Click PREFERENCES in the navigation pane.
   The Web Preferences panel is displayed in the action pane.
2. Select the appropriate privilege level from the Privilege Level menu, then click Apply Changes.
3. If you are setting the privilege level to a level other than admin, a warning page is displayed; click Please Continue to confirm the change.

How to use queries, patterns, and wildcards

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

The query operators in the following table are supported.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Wildcard that matches all entries.</td>
</tr>
<tr>
<td>!</td>
<td>NOT operator. Indicates a value that is not to be matched; for example, !vs0 indicates not to match the value vs0.</td>
</tr>
<tr>
<td></td>
<td>OR operator. Separates two values that are to be compared; for example, vs0</td>
</tr>
<tr>
<td>..</td>
<td>Range operator. For example, 5 . 10 matches any value from 5 to 10, inclusive.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less-than operator. For example, &lt;20 matches any value that is less than 20.</td>
</tr>
</tbody>
</table>
Operator Description

> Greater-than operator. For example, >5 matches any value that is greater than 5.

<= Less-than-or-equal-to operator.

>= Greater-than-or-equal-to operator.

{query} Extended query.

For example, to display a list of all volumes whose names include the string tmp, you run the command shown in the following example:

```
node::> volume show -volume *tmp*
```

**Note:** 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 anti-virus policies that contain the characters ^.*$, you must enclose these characters in double quotes ("^.*$") for the correct results to be returned.

**How to use extended queries**

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

Extended queries are specified 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:

```
node::> 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.

**Note:** 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 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:

```
node::> system 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:
Exiting the management interface

When you are finished using the current management session, log out to prevent unauthorized access to the management interface.

Step

1. To exit from the management interface, use one of the following methods.
   - To exit from a CLI session, enter the `exit` command.
   - To exit from a Web-interface session, click LOG OUT.
How Data ONTAP Cluster-Mode works with disks

Disks provide the basic unit of storage for storage systems running Data ONTAP. Understanding how Data ONTAP uses and classifies disks will help you manage your storage more effectively.

Next topics

- How Data ONTAP reports disk types on page 35
- Disk connection protocols, topologies, and types on page 37
- Available disk capacity by disk size on page 37
- Disk speeds on page 39
- Disk formats on page 40
- Disk names on page 40
- RAID disk types on page 41
- How disk sanitization works on page 42
- How Data ONTAP monitors disk performance and health on page 44
- How Data ONTAP uses ACP to increase storage availability on page 48
- How you use SSDs to increase storage performance on page 51

How Data ONTAP reports disk types

Data ONTAP associates a type with every disk. This type is used to determine whether a disk can be used as a matching spare or added to an aggregate. Data ONTAP reports some disk types differently than the industry standards.

When this guide refers to a disk type, it is the type used by Data ONTAP unless otherwise specified.

The following table shows Data ONTAP disk types and how they map to industry standard disk types.

**Note:** Data ONTAP disk types are different from RAID disk types.

<table>
<thead>
<tr>
<th>Data ONTAP disk type</th>
<th>Disk connection type</th>
<th>Industry standard disk type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA</td>
<td>FC-AL</td>
<td>SATA</td>
<td></td>
</tr>
<tr>
<td>Data ONTAP disk type</td>
<td>Disk connection type</td>
<td>Industry standard disk type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------</td>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>BSAS</td>
<td>SAS</td>
<td>SATA</td>
<td>Bridged SAS–SATA disks with added hardware to enable them to be plugged into a SAS shelf.</td>
</tr>
<tr>
<td>FCAL</td>
<td>FC-AL</td>
<td>FC</td>
<td>A logical storage device backed by third-party storage and used by Data ONTAP as a disk. In this document, these LUNs are referred to as <em>array LUNs</em> to distinguish them from the LUNs that Data ONTAP serves to clients.</td>
</tr>
<tr>
<td>LUN</td>
<td>FC (point-to-point or switched)</td>
<td>LUN</td>
<td>A logical storage device backed by third-party storage and used by Data ONTAP as a disk. In this document, these LUNs are referred to as <em>array LUNs</em> to distinguish them from the LUNs that Data ONTAP serves to clients.</td>
</tr>
<tr>
<td>SAS</td>
<td>SAS</td>
<td>SAS</td>
<td>Available only as internal disks for the 20xx systems.</td>
</tr>
<tr>
<td>SATA</td>
<td>SAS</td>
<td>SATA</td>
<td>Available only as internal disks for the 20xx systems.</td>
</tr>
<tr>
<td>SSD</td>
<td>SAS</td>
<td>SSD</td>
<td>Solid-state disks</td>
</tr>
</tbody>
</table>

For a specific configuration, the disk types supported depend on the storage system model, the disk shelf type, and the I/O modules installed in the system. For more information about the types of disks supported by your configuration, see the *System Configuration Guide*.

For information about best practices for working with different types of disks, see *Technical Report 3437: Storage Best Practices and Resiliency Guide*.

**Related information**

- *TR 3437: Storage Best Practices and Resiliency Guide*
- *System Configuration Guide: now.netapp.com/NOW/knowledge/docs/hardware/NetApp/syscfg/*
Disk connection protocols, topologies, and types

Data ONTAP supports two disk connection protocols: serial-attached SCSI (SAS) and Fibre Channel (FC). The Fibre Channel protocol supports three topologies: arbitrated loop, switched, and point-to-point.

- SAS, BSAS, and SATA disks use the SAS disk connection protocol.
- FC and ATA disks use the Fibre Channel protocol with an arbitrated loop topology, or FC-AL.
- Array LUNs use the FC protocol, with either the point-to-point or switched topology.

You cannot combine different disk connection types in the same loop or stack.

Next topics

Fibre Channel-Arbitrated Loop (FC-AL) disk connection type on page 37
Serial-attached SCSI (SAS) disk connection type on page 37

Fibre Channel-Arbitrated Loop (FC-AL) disk connection type

For the FC-AL disk connection type, disk shelves are connected to the controller in a loop.

Devices must arbitrate for the chance to communicate over the loop to avoid collisions on the loop. If connectivity is lost somewhere along the loop and a redundant path is not available, the controller loses the ability to communicate with some devices on the loop.

You cannot combine disk shelves containing FC disks and DS14 disk shelves containing ATA disks in the same loop.

Serial-attached SCSI (SAS) disk connection type

The SAS disk connection type is a point-to-point architecture. This means that the controller can communicate with more than one device at once.

Disk shelves are connected to the controller on a daisy chain called a stack.

For information about combining different disk types within a stack, see the Installation and Service Guide for your SAS disk shelf.

Available disk capacity by disk size

To maintain compatibility across brands of disks, Data ONTAP rounds down ("right-sizes") the amount of space available for user data.

Because of right-sizing, informational commands such as `sysconfig` show a lower number for available space than the disk's rated capacity (you use rated capacity if you specify disk size when creating an aggregate). The available disk space is rounded down as shown in the following table.
**Note:** For this table, GB = 1,000 MB.

The capacity numbers in this table do not take into account the 10 percent of disk space that Data ONTAP reserves for its own use.

<table>
<thead>
<tr>
<th>Disk size</th>
<th>Right-sized capacity</th>
<th>Available blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FC disks</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36 GB</td>
<td>34.5 GB</td>
<td>70,656,000</td>
</tr>
<tr>
<td>72 GB</td>
<td>68 GB</td>
<td>139,264,000</td>
</tr>
<tr>
<td>144 GB</td>
<td>136 GB</td>
<td>278,528,000</td>
</tr>
<tr>
<td>300 GB</td>
<td>272 GB</td>
<td>557,056,000</td>
</tr>
<tr>
<td>450 GB</td>
<td>418 GB</td>
<td>856,064,000</td>
</tr>
<tr>
<td>600 GB</td>
<td>560 GB</td>
<td>1,146,880,000</td>
</tr>
<tr>
<td><strong>ATA disks—FC connected</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>250 GB</td>
<td>211 GB</td>
<td>432,901,760</td>
</tr>
<tr>
<td>320 GB</td>
<td>274 GB</td>
<td>561,971,200</td>
</tr>
<tr>
<td>500 GB</td>
<td>423 GB</td>
<td>866,531,584</td>
</tr>
<tr>
<td>750 GB</td>
<td>635 GB</td>
<td>1,301,618,176</td>
</tr>
<tr>
<td>1 TB</td>
<td>847 GB</td>
<td>1,735,794,176</td>
</tr>
<tr>
<td>2 TB</td>
<td>1,695 GB</td>
<td>3,472,315,904</td>
</tr>
<tr>
<td><strong>SAS disks—SAS connected</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>144 GB</td>
<td>136 GB</td>
<td>278,528,000</td>
</tr>
<tr>
<td>300 GB</td>
<td>272 GB</td>
<td>557,056,000</td>
</tr>
<tr>
<td>450 GB</td>
<td>418 GB</td>
<td>856,064,000</td>
</tr>
<tr>
<td>600 GB</td>
<td>560 GB</td>
<td>1,146,880,000</td>
</tr>
<tr>
<td><strong>SATA disks—SAS connected</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>250 GB</td>
<td>211 GB</td>
<td>432,901,760</td>
</tr>
<tr>
<td>500 GB</td>
<td>423 GB</td>
<td>866,531,584</td>
</tr>
<tr>
<td>750 GB</td>
<td>635 GB</td>
<td>1,301,618,176</td>
</tr>
<tr>
<td>1 TB</td>
<td>847 GB</td>
<td>1,735,794,176</td>
</tr>
<tr>
<td>2 TB</td>
<td>1,695 GB</td>
<td>3,472,315,904</td>
</tr>
</tbody>
</table>
### Disk speeds

For hard disk drives, which use rotating media, speed is measured in revolutions per minute (RPM). Faster disks provide more disk input/output operations per second (IOPS) and faster response time.

It is best to use disks of the same speed in an aggregate.

Data ONTAP supports the following rotational speeds for disks:

- FCAL disks (FC-AL connected)
  - 10K RPM
  - 15K RPM
- ATA disks (FC-AL connected)
  - 5.4K RPM
  - 7.2K RPM
- SAS disks (SAS-connected)
  - 15K RPM
- SATA disks (SAS-connected)
  - 7.2K RPM
- BSAS disks (SAS-connected)
  - 7.2K RPM

Solid-state disks, or SSDs, are flash memory-based devices and therefore the concept of rotational speed does not apply to them. SSDs provide more IOPS and faster response times than rotating media.

For more information about supported disk speeds, see the *System Configuration Guide*.

**Related information**

*TR 3285: 15,000 RPM Fibre Channel Disk Drives: A Best-Practice Guide for Optimizing System Performance*

[System Configuration Guide: now.netapp.com/NOW/knowledge/docs/hardware/NetApp/syscfg/](now.netapp.com/NOW/knowledge/docs/hardware/NetApp/syscfg/)
Disk formats

The disk format determines how much of the disk’s raw capacity can be used for data storage. Some disk formats cannot be combined in the same aggregate.

Most disks used in storage systems are block checksum disks (BCS disks).

The amount of space available for data depends on the bytes per sector (bps) of the disk:

- Disks that use 520 bps provide 512 bytes per sector for data. 8 bytes per sector are used for the checksum.
- Disks that use 512 bps use some sectors for data and others for checksums. For every 9 sectors, 1 sector is used for the checksum, and 8 sectors are available for data.

The disk formats by Data ONTAP disk type are as follows:

- FCAL and SAS BCS disks use 520 bps.
- ATA, SATA, and BSAS BCS disks use 512 bps.
- SSD BCS disks use 512 bps.

Disk names

Each disk has a name that differentiates it from all other disks for a storage system. Disk names have different formats, depending on the disk connection type (FC-AL or SAS) and whether the disk is directly attached to the storage system or attached to a switch.

Each disk has a universal unique identifier (UUID) that differentiates it from all other disks in the cluster.

The same disk can have multiple disk names, depending on how the disk is connected. For example, a disk known to a node named alpha as alpha:1a.19 can be known to a node named beta as beta:0b.37. All names are listed in the output of queries and are equally valid. To determine a disk's unique identity, run a detailed query and look for the disk's universal unique identifier (UUID) or serial number.

The following table shows the various formats for disk names, depending on how they are connected to the storage system.

Note: For internal disks, the slot number is zero, and the internal port number depends on the system model.
Loop IDs for FC-AL connected disks

For disks connected using Fibre Channel-Arbitrated Loop (FC-AL or FC), the loop ID is an integer between 16 and 126. The loop ID identifies the disk within its loop, and is included in the disk name, which identifies the disk uniquely for the entire system.

The loop ID corresponds to the disk shelf number and the bay in which the disk is installed. The lowest loop ID is always in the far right bay of the first disk shelf. The next higher loop ID is in the next bay to the left, and so on. You can view the device map for your disk shelves with the `fcadmin device_map` command.

For more information about the loop ID map for your disk shelf, see the hardware guide for the disk shelf.

RAID disk types

Data ONTAP classifies disks as one of four types for RAID: data, hot spare, parity, or dParity. The RAID disk type is determined by how RAID is using a disk.

- **Data disk**  Holds data stored on behalf of clients within RAID groups (and any data generated about the state of the storage system as a result of a malfunction).
Spare disk  Does not hold usable data, but is available to be added to a RAID group in an aggregate. Any functioning disk that is not assigned to an aggregate but is assigned to a system functions as a hot spare disk.

Parity disk  Stores data reconstruction information within RAID groups.

dParity disk  Stores double-parity information within RAID groups, if RAID-DP is enabled.

How disk sanitization works

Disk sanitization is the process of physically obliterating data by overwriting disks with specified byte patterns or random data so that recovery of the original data becomes impossible. You use the disk sanitize command to ensure that no one can recover the data on the disks. This command is available through the nodeshell.

The disk sanitize command uses three successive default or user-specified byte overwrite patterns for up to seven cycles per operation. Depending on the disk capacity, the patterns, and the number of cycles, the process can take several hours. Sanitization runs in the background. You can start, stop, and display the status of the sanitization process.

After you enter the disk sanitize start command, Data ONTAP begins the sanitization process on each of the specified disks. The process consists of a disk format operation, followed by the specified overwrite patterns repeated for the specified number of cycles.

**Note:** The formatting phase of the disk sanitization process is skipped on ATA disks.

If the sanitization process is interrupted by power failure, system panic, or a user-invoked disk sanitize abort command, the disk sanitize command must be re-invoked and the process repeated from the beginning in order for the sanitization to take place.

When the sanitization process is complete, the specified disks are in a sanitized state. You designate the sanitized disks as spare disks by using the disk sanitize release command.

**Note:** You must install the disk sanitization license before you can perform disk sanitization.

Next topics

- Disk sanitization limitations on page 43
- What happens if disk sanitization is interrupted on page 43
- How selective disk sanitization works on page 44
- Tips for creating and backing up aggregates containing data that will be sanitized on page 44
Disk sanitization limitations

Installing the disk sanitization license disables certain Data ONTAP commands. In addition, disk sanitization cannot be used with all configurations, models and disk drives.

Installing the disk sanitization license prohibits the following commands from being used on the storage system with that license:

- `dd` (to copy blocks of data)
- `dumpblock` (to print dumps of disk blocks)
- `setflag wafl_metadata_visible` (to allow access to internal WAFL files)

The disk sanitization process has the following limitations:

- It is not supported in takeover mode for systems in an HA configuration. (If a storage system is disabled, it remains disabled during the disk sanitization process.)
- It cannot be carried out on disks that were failed due to readability or writability problems.
- It does not perform its formatting phase on ATA drives.
- If you are using the random pattern, it cannot be performed on more than 100 disks at one time.
- It is not supported on array LUNs.
- It is not supported on SSDs.
- If you sanitize both SES disks in the same ESH shelf at the same time, you see errors on the console about access to that shelf, and shelf warnings are not reported for the duration of the sanitization. However, data access to that shelf is not interrupted.

What happens if disk sanitization is interrupted

Disk sanitization can take time to complete. If disk sanitization is interrupted by user intervention or an unexpected event such as a power outage, Data ONTAP takes certain actions to prevent corrupted disks if necessary.

If the sanitization process is interrupted by power failure, system panic, or a user-invoked `disk sanitize abort` command, the `disk sanitize` command must be re-invoked and the process repeated from the beginning in order for the sanitization to take place.

If the formatting phase of disk sanitization is interrupted, Data ONTAP attempts to reformat any disks that were corrupted by the interruption. After a system reboot and once every hour, Data ONTAP checks for any sanitization target disk that did not complete the formatting phase of its sanitization. If such a disk is found, Data ONTAP attempts to reformat that disk, and writes a message to the console informing you that a corrupted disk has been found and will be reformatted. After the disk is reformatted, it is designated as a hot spare. You can then rerun the `disk sanitize` command on that disk.
How selective disk sanitization works

Selective disk sanitization consists of physically obliterating data in specified files or volumes while preserving all other data located on the affected aggregate for continued user access. Because a file can be stored on multiple disks, there are three parts to the process.

To selectively sanitize data contained in an aggregate, you must carry out three general tasks:

1. Delete the files, directories or volumes that contain the data you want to sanitize from the aggregate that contains them.

2. Migrate the data that you want to preserve to a new set of disks in a destination aggregate on the same storage system.
   
   You can migrate data using the `ndmpcopy` command or `qtree` SnapMirror.

3. Destroy the original aggregate and sanitize all the disks that were RAID group members in that aggregate.

Tips for creating and backing up aggregates containing data that will be sanitized

If you are creating or backing up aggregates to contain data that might need to be sanitized, following some simple guidelines will reduce the time it takes to sanitize your data.

- Make sure your aggregates containing sensitive data are not larger than they need to be. If they are larger than needed, sanitization requires more time, disk space, and bandwidth.

- When you back up aggregates containing sensitive data, avoid backing them up to aggregates that also contain large amounts of nonsensitive data. This will reduce the resources required to move nonsensitive data before sanitizing sensitive data.

How Data ONTAP monitors disk performance and health

Data ONTAP continually monitors disks to assess their performance and health. When Data ONTAP encounters certain errors or behaviors from a disk, it takes the disk offline temporarily or takes the disk out of service to run further tests.

Next topics

* [When Data ONTAP takes disks offline temporarily](#) on page 45
* [How Data ONTAP reduces disk failures using Rapid RAID Recovery](#) on page 45
* [How the maintenance center works](#) on page 46
* [How Data ONTAP uses continuous media scrubbing to prevent media errors](#) on page 47
When Data ONTAP takes disks offline temporarily

Data ONTAP temporarily stops I/O activity to a disk and takes a disk offline when Data ONTAP is updating disk firmware in background mode or when disks become non-responsive. While the disk is offline, Data ONTAP performs a quick check on it to reduce the likelihood of forced disk failures.

While the disk is offline, Data ONTAP reads from other disks within the RAID group while writes are logged. When the offline disk is ready to come back online, Data ONTAP re-synchronizes the RAID group and brings the disk online. This process generally takes a few minutes and incurs a negligible performance impact.

Note: The disk offline feature is only supported for spares and data disks within RAID-DP and mirrored-RAID4 aggregates. A disk can be taken offline only if its containing RAID group is in a normal state and the plex or aggregate is not offline.

How Data ONTAP reduces disk failures using Rapid RAID Recovery

When Data ONTAP determines that a disk has exceeded its error thresholds, Data ONTAP can perform Rapid RAID Recovery by removing the disk from its RAID group for testing and, if necessary, failing the disk. Spotting disk errors quickly helps prevent multiple disk failures and allows problem disks to be replaced.

By performing the Rapid RAID Recovery process on a suspect disk, Data ONTAP avoids three problems that occur during sudden disk failure and the subsequent RAID reconstruction process:

- Rebuild time
- Performance degradation
- Potential data loss due to additional disk failure during reconstruction

During Rapid RAID Recovery, Data ONTAP performs the following tasks:

1. Places the suspect disk in pre-fail mode.
2. Selects a hot spare replacement disk.

   Note: If no appropriate hot spare is available, the suspect disk remains in pre-fail mode and data continues to be served. However, a suspect disk performs less efficiently. Impact on performance ranges from negligible to worse than degraded mode. For this reason, make sure hot spares are always available.

3. Copies the suspect disk’s contents to the spare disk on the storage system before an actual failure occurs.
4. After the copy is complete, attempts to put the suspect disk into the maintenance center, or else fails the disk.

   Note:
   Tasks 2 through 4 can only occur when the RAID group is in normal (not degraded) mode.
If the suspect disk fails on its own before copying to a hot spare disk is complete, Data ONTAP starts the normal RAID reconstruction process.

How the maintenance center works

When a disk is in the maintenance center, it is subjected to a number of tests. If the disk passes all of the tests, it is redesignated as a spare. Otherwise, Data ONTAP fails the disk.

You can access the options and commands to control the maintenance center by using the nodeshell. For more information about the nodeshell, see the information about the system node run command in the Data ONTAP Cluster-Mode Administration Reference.

The maintenance center is controlled by the disk.maint_center.enable option. It is on by default.

Data ONTAP puts disks into the maintenance center only if there are two or more spares available for that disk.

You can control the number of times a disk is allowed to go to the maintenance center using the disk.maint_center.allowed_entries option. The default value for this option is 1, which means that if the disk is ever sent back to the maintenance center, it is automatically failed.

Data ONTAP informs you of these activities by sending messages to the following destinations:

- The console

For information about best practices for working with the maintenance center, see Technical Report 3437: Storage Best Practices and Resiliency Guide.

Next topics

When Data ONTAP can put a disk into the maintenance center on page 46
Putting a disk into the maintenance center manually on page 47

Related information

TR 3437: Storage Best Practices and Resiliency Guide

When Data ONTAP can put a disk into the maintenance center

When Data ONTAP detects certain disk errors, it tries to put the disk into the maintenance center for testing. Certain requirements must be met for the disk to be put into the maintenance center.

If a disk experiences more errors than are allowed for that disk type, Data ONTAP takes one of the following actions:

- If the disk.maint_center.spares_check option is set to on (the default) and two or more spares are available, Data ONTAP takes the disk out of service and assigns it to the maintenance center for data management operations and further testing.
• If the `disk.maint_center.spares_check` option is set to `on` and fewer than two spares are available, Data ONTAP does not assign the disk to the maintenance center. It simply fails the disk and designates the disk as a broken disk.

• If the `disk.maint_center.spares_check` option is set to `off`, Data ONTAP assigns the disk to the maintenance center without checking the number of available spares.

  **Note:** The `disk.maint_center.spares_check` option has no effect on putting disks into the maintenance center from the command-line interface.

Data ONTAP does not put SSDs into the maintenance center.

### Putting a disk into the maintenance center manually

You can put a disk into the maintenance center by using the `disk maint start` command. This command is available through the nodeshell.

**About this task**

Manually running maintenance tests on a disk does not count toward the number of times a disk is sent to the maintenance center by Data ONTAP.

For more information about the nodeshell, see the information about the `system node run` command in the *Data ONTAP Cluster-Mode Administration Reference*.

**Step**

1. Enter the following command:

   ```bash
disk maint start [-i] disk_list
   ```

   If you select a disk that is part of an active file system, the selected disk is marked as prefailed but is not put into the maintenance center until an appropriate spare is found and the disk is copied to the spare using Rapid RAID Recovery. If you want the testing to begin immediately, use the `-i` option. With the `-i` option, the RAID group that contains the disk goes into degraded mode until a spare is located and the disk is reconstructed onto the spare.

### How Data ONTAP uses continuous media scrubbing to prevent media errors

The purpose of the continuous media scrub is to detect and correct media errors in order to minimize the chance of storage system disruption due to a media error while a storage system is in degraded or reconstruction mode.

By default, Data ONTAP runs continuous background media scrubbing for media errors on all storage system disks. If a media error is found, Data ONTAP uses RAID to reconstruct the data and repairs the error.
Media scrubbing is a continuous background process. Therefore, you might observe disk LEDs blinking on an apparently idle storage system. You might also observe some CPU activity even when no user workload is present.

**Note:** You can disable continuous media scrubbing for disks in use in aggregates by using the `raid.media_scrub.enable` option. In addition, you can disable continuous media scrubbing for spare disks by using the `raid.media_scrub.spares.enable` option. However, you are advised not to disable continuous media scrubbing, especially for SATA or ATA disks and disks used in RAID4 aggregates.

You access the options and commands to control media scrubs by using the nodeshell. For more information about the nodeshell, see the information about the `system node run` command in the *Data ONTAP Cluster-Mode Administration Reference*. For more information about the `raid.media_scrub` options, see the `na_options(1)` man page.

**Next topics**

- *How continuous media scrub impacts system performance* on page 48
- *Why continuous media scrubbing should not replace scheduled RAID-level disk scrubs* on page 48

**How continuous media scrub impacts system performance**

Because continuous media scrubbing searches only for media errors, the impact on system performance is negligible. In addition, the media scrub attempts to exploit idle disk bandwidth and free CPU cycles to make faster progress. However, any client workload results in aggressive throttling of the media scrub resource.

If needed, you can further decrease the CPU resources consumed by a continuous media scrub under a heavy client workload by increasing the maximum time allowed for a media scrub cycle to complete. You can do this by using the `raid.media_scrub.rate` option.

**Why continuous media scrubbing should not replace scheduled RAID-level disk scrubs**

Because the continuous media scrub process scrubs only media errors, you should continue to run the storage system’s scheduled complete RAID-level scrub operation. The RAID-level scrub finds and corrects parity and checksum errors as well as media errors.

**How Data ONTAP uses ACP to increase storage availability**

ACP, or Alternate Control Path, is a protocol that enables Data ONTAP to manage and control a SAS disk shelf storage subsystem. It uses a separate network (alternate path) from the data path, so management communication is not dependent on the data path being intact and available.

You do not need to actively manage the SAS disk shelf storage subsystem. Data ONTAP automatically monitors and manages the subsystem without operator intervention. However, you
must provide the required physical connectivity and configuration parameters to enable the ACP functionality.

**Note:** You can install SAS disk shelves without configuring ACP. However, for maximum storage availability and stability, you should always have ACP configured and enabled.

After you enable ACP, you can use the `storage show acp` and `acpadmin list all` commands to display information about your ACP subsystem.

Because ACP communication is on a separate network, it does not affect data access in any way.

**Next topics**

*Enabling ACP* on page 49  
*The ACP subnet* on page 50

### Enabling ACP

ACP can increase your storage availability when you use SAS disk shelves. To get the benefits of ACP, you must configure and enable ACP on your storage system.

**Before you begin**

ACP must be cabled before beginning this procedure. For more information, see the *Installation and Service Guide* for your disk shelf.

**Note:** If your storage system model has a dedicated port for ACP, then ACP is enabled by default. In this case, you do not need to explicitly enable ACP in Data ONTAP.

If you have not previously configured the network connectivity for ACP, and your platform does not have a dedicated ACP port, you must gather the following network configuration information for the ACP connection:

- **Network interface**
  An unused network interface you want to use for ACP traffic (unless your storage system has a dedicated ACP port)

- **Domain for network interface**
  The network name (an IP address ending in 0) for the private subnet to be used exclusively by ACP (if you do not choose to use the default value)

- **Netmask for network interface**
  The network mask for the ACP subnet (if you do not want to use the default value)

**Step**

1. At the Data ONTAP command line, enter the following command:

   ```
   acpadmin configure
   ```
If you have not previously configured the networking information for ACP, you are prompted for that information.

**Example**

For example, if you select e0b as the interface for ACP traffic, 198.15.1.0 as the ACP domain, and 255.255.255.0 as the network mask for the ACP subnet, the `storage show acp` command output looks similar to the following example:

```
my-sys-1> storage show acp

  Alternate Control Path: enabled
  Ethernet Interface:      e0b
  ACP Status:              Active
  ACP IP address:          198.168.1.212
  ACP domain:              198.168.1.0
  ACP netmask:             255.255.255.0
  ACP Connectivity Status: Full Connectivity

<table>
<thead>
<tr>
<th>Shelf Module</th>
<th>Reset Cnt</th>
<th>IP address</th>
<th>FW Version</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>7a.001.A</td>
<td>002</td>
<td>198.15.1.145</td>
<td>01.05</td>
<td></td>
</tr>
<tr>
<td>IOM6</td>
<td></td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7a.001.B</td>
<td>003</td>
<td>198.15.1.146</td>
<td>01.05</td>
<td></td>
</tr>
<tr>
<td>IOM6</td>
<td></td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7c.002.A</td>
<td>000</td>
<td>198.15.1.206</td>
<td>01.05</td>
<td></td>
</tr>
<tr>
<td>IOM6</td>
<td></td>
<td>active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7c.002.B</td>
<td>001</td>
<td>198.15.1.204</td>
<td>01.05</td>
<td></td>
</tr>
<tr>
<td>IOM6</td>
<td></td>
<td>active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**After you finish**

If you want to change your ACP configuration parameters later, you can use the `acpadmin configure` command to do so.

**The ACP subnet**

The ACP subnet is a private Ethernet network that enables the ACP processor in the SAS module to communicate both with Data ONTAP and with the SAS IOMs in the disk shelves.

The ACP subnet is separate from the I/O data path that connects the disk shelves to the HBA on the storage controller. When you configure ACP on one of the system's network interfaces, you must supply a private domain name that conforms to the standard for private internet addresses (RFC1918). You can use the system default domain, 198.15.1.0, or another network name (that is, an IP address ending in 0) that conforms to the standard.

If you are configuring ACP for disk shelves attached to an HA pair, you must supply the same ACP domain name and network mask for both systems.
Attention: Do not connect the ACP port to a routed network, and do not configure switches or hubs between the ACP port and the designated Ethernet port. Doing so is not supported and causes interruptions in service.

After you select a domain name and network mask for the interface, Data ONTAP automatically assigns IP addresses for the ACP interface on the storage controller and both I/O modules on each disk shelf on the ACP subnet.

You can use the `sysconfig -v` command to check whether your ACP subnet is cabled correctly. If ACP is disabled, `sysconfig` shows ACP connectivity as "NA".

### How you use SSDs to increase storage performance

Solid-state disks, or SSDs, are flash memory-based storage devices that provide better overall performance than hard disk drives, or HDDs, which are mechanical devices using rotating media.

You can manage aggregates created with SSDs, and the volumes they contain, the same way you manage aggregates created with standard disks. However, there are some differences in the way you manage SSDs from the way you manage disks. In addition, some Data ONTAP capabilities are not available on SSDs.

Next topics

- SSD life cycle on page 51
- Limitations of SSDs on page 52

### SSD life cycle

Solid-state disks (SSDs) have a different life cycle than rotating media (hard disk drives, or HDDs). Data ONTAP monitors and manages SSDs to maximize storage performance and availability.

In the absence of a mechanical failure, rotating media can serve data almost indefinitely. This is not true for SSDs, which can accept only a finite (though very large) number of write operations.

Because some blocks are written to more often than others, SSDs provide a set of internal spare capacity, called spare blocks, that can be used to replace blocks that have reached their write operation limit. After all of the spare blocks have been used, the next block that reaches its limit causes the disk to fail.

Because a drive failure is an undesirable occurrence, Data ONTAP replaces SSDs before they reach their limit. When the percentage of spare blocks that have been used reaches a predetermined threshold, Data ONTAP performs the following actions:

1. Sends an AutoSupport message.
2. If a spare SSD is available, starts a disk copy to that spare.
3. If no spare is available, starts a periodic check for a spare so that the disk copy can be started when a spare becomes available.
4. When the disk copy finishes, fails the disk.

   **Note:** You do not need to replace SSDs before they are failed by Data ONTAP. However, it is important to ensure that spares are available as SSDs approach the end of their lifetimes.

**Limitations of SSDs**

SSDs and standard disks cannot be used interchangeably. In addition, some Data ONTAP functionality is not available for aggregates made up of SSDs.

SSDs cannot be combined with standard disks within the same aggregate or stack. When you replace an SSD in an aggregate, you must replace it with another SSD. Similarly, when you physically replace an SSD within a shelf, you must replace it with another SSD.

The following capabilities of Data ONTAP are not available for SSDs or aggregates made up of SSDs:

- Disk sanitization
- The maintenance center

Data stored in an SSD aggregate is not cached in WAFL extended cache. WAFL extended cache is reserved for data stored on slower performance storage (hard disk drives). For more information about WAFL extended cache, see the *Data ONTAP 7-Mode System Administration Guide*.

An SSD-only configuration is not supported. Your system must include some HDD-based storage.

SSDs are supported only on some hardware platforms. For more information, see the *System Configuration Guide*.

Other than these limitations, you manage SSDs the same as standard disks, including firmware updates, scrubs, and zeroing.

**Related information**

[System Configuration Guide: now.netapp.com/NOW/knowledge/docs/hardware/NetApp/syscfg/](now.netapp.com/NOW/knowledge/docs/hardware/NetApp/syscfg/)
How ownership for disks and array LUNs works

Disk and array LUN ownership determines which node owns a disk or array LUN and what pool a disk or array LUN is associated with. Understanding how ownership works enables you to maximize storage redundancy and manage your hot spares effectively.

Data ONTAP stores ownership information directly on the disk or array LUN.

Next topics

- Why you assign ownership of disks and array LUNs on page 53
- What it means for Data ONTAP to own an array LUN on page 53
- Why you might assign array LUN ownership after installation on page 54
- How disks and array LUNs become available for use on page 55
- How ownership autoassignment works for disks on page 56
- Examples showing when Data ONTAP can use array LUNs on page 57

Why you assign ownership of disks and array LUNs

Storage system ownership must be assigned for disks and array LUNs before they become an effective part of your system. You must explicitly assign ownership for array LUNs. Disks can be automatically or manually assigned.

You assign ownership of a disk or array LUN to accomplish the following actions:

- Associate the disk or array LUN with a specific storage system.
  
  For a stand-alone system, all disks and array LUNs are owned by that system. In an HA pair, the disks and array LUNs could be owned by either system.

- Enable the disk or array LUN to be used and managed by the system that owns it.
  
  Unowned disks cannot be used as spares and do not receive the automatic firmware updates that owned disks do.

What it means for Data ONTAP to own an array LUN

Data ONTAP cannot use an array LUN presented to it by a storage array until you have configured a logical relationship in Data ONTAP that identifies a specific system running Data ONTAP as the owner of the array LUN.

A storage array administrator creates LUNs and makes them available to specified FC initiator ports of storage systems running Data ONTAP. (The process for how to do this varies among storage array vendors.) When you assign an array LUN to a system running Data ONTAP, Data ONTAP writes
data to the array LUN to identify that system as the *owner* of the LUN. Thereafter, Data ONTAP ensures that only the owner can write data to and read data from the LUN.

From the perspective of Data ONTAP, this logical relationship is referred to as *disk ownership* because Data ONTAP considers an array LUN to be a virtual disk. From the perspective of Data ONTAP, you are assigning disks to a storage system.

An advantage of the disk ownership scheme is that you can make changes through the Data ONTAP software that, on typical hosts, must be done by reconfiguring hardware or LUN access controls. For example, through Data ONTAP you can balance the load of requests among a group of systems running Data ONTAP by moving data service from one system to another, and the process is transparent to most users. You do not need to reconfigure hardware or the LUN access controls on the storage array to change which system running Data ONTAP is the owner and, therefore, servicing data requests.

**Attention:** The Data ONTAP software-based scheme provides ownership control only for storage systems running Data ONTAP; it does not prevent a different type of host from overwriting data in an array LUN owned by a system running Data ONTAP. Therefore, if multiple hosts are accessing LUNs through the same storage array port, be sure to use LUN security on your storage array to prevent the systems from overwriting each other's array LUNs.

LUN reconfiguration, such as resizing the LUN, must be done from the storage array. Before such activities can occur, you must release Data ONTAP ownership of the LUN.

**Why you might assign array LUN ownership after installation**

For a V-Series system ordered with disk shelves, you are not required to set up third-party storage during initial installation. For a V-Series system using only third-party storage, you need to assign only two array LUNs during initial installation.

If you ordered your V-Series system with disk shelves, you do not need to assign any array LUNs initially because the factory installs the root volume on a disk for you. If you are using only third-party storage, you must configure one array LUN for the root volume and one array LUN as a spare for core dumps during initial installation. In either case, you can assign ownership of additional array LUNs to your system at any time after initial installation.

After initial configuration of your system, you might assign ownership of an array LUN in circumstances such as the following:

- You ordered your V-Series system with native disk shelves and you did not set up your system to work with third-party storage initially
- You left some LUNs that the storage array presented to Data ONTAP unowned and you now need to use the storage
- Another system released ownership of a particular array LUN and you want this system to be able to use the LUN
- The storage array administrator had not made the LUNs available to Data ONTAP when you initially configured your system and you now want to use the storage

**How disks and array LUNs become available for use**

When you add a disk or array LUN to a system running Data ONTAP, the disk or array LUN goes through several stages before it can be used by Data ONTAP to store data or parity information.

The process for making a disk available for use differs slightly from the process for making an array LUN available for use. Both processes are shown in the following diagram.

The process for disks includes the following actions:

1. The administrator physically installs the disk into a disk shelf. Data ONTAP can see the disk but the disk is still unowned.
2. If the system is configured to support disk autoassignment, Data ONTAP assigns ownership for the disk. Otherwise, the administrator must use the `disk assign` command to assign ownership for the disk manually. The disk is now a spare disk.
3. The administrator or Data ONTAP adds the disk to an aggregate.
The disk is now in use by that aggregate. It could contain data or parity information.

The process for array LUNs includes the following actions:

1. The administrator uses the third-party storage array to create the array LUN and make it available to Data ONTAP.
   Data ONTAP can see the array LUN but the array LUN is still unowned.

2. The administrator uses the `disk assign` command to assign ownership for the array LUN.
   The array LUN is now a spare array LUN.

3. The administrator adds the array LUN to an aggregate.
   The array LUN is now in use by that aggregate and is used to contain data.

### How ownership autoassignment works for disks

If your configuration follows some basic rules to avoid ambiguity, Data ONTAP can automatically assign ownership and pool membership for disks. Autoassignment is not available for array LUNs.

If you decide to change the way Data ONTAP has assigned the disks, you can do so at any time.

**Note:** You can disable disk autoassignment using the `storage disk option modify` command.

### Next topics

*What autoassignment does* on page 56

*When autoassignment is invoked* on page 56

### What autoassignment does

When disk autoassignment runs, Data ONTAP looks for any unassigned disks and assigns them to the same system and pool as all other disks on their loop or stack.

**Note:** If a single loop or stack has disks assigned to multiple systems or pools, Data ONTAP does not perform autoassignment on that loop or stack. To avoid this issue, always follow the disk assignment guidelines.

### When autoassignment is invoked

Disk ownership autoassignment does not happen immediately after disks are introduced into the storage system.

Disk autoassignment is invoked at the following times:

- Every five minutes during normal system operation
- Ten minutes after the initial system initialization

This delay allows the person configuring the system enough time to finish the initial disk assignments so that the results of the autoassignment are as expected.
• Whenever you enter the `disk assign auto` command. This command is available through the nodeshell. For more information about the nodeshell, see the information about the `system node run` command in the *Data ONTAP Cluster-Mode Administration Reference*.

### Examples showing when Data ONTAP can use array LUNs

After an array LUN has been assigned to a storage system, it can be added to an aggregate and used for storage or it can remain a spare LUN until it is needed for storage.

#### No storage system owns the LUNs yet

In this example, the storage array administrator made the array LUNs available to Data ONTAP. However, system vs1 has not yet been configured to "own" any of the LUNs. Therefore, it cannot read data from or write data to any array LUNs on the storage array.

![Diagram of storage array and LUNs available for Data ONTAP](image)

#### Only some array LUNs are owned

In this example, vs1 was configured to own array LUNs 1 and 2, but not array LUNs 3 and 4. LUNs 3 and 4 are still available to Data ONTAP, however, and can be assigned to a storage system later.

Data ONTAP used the smallest of the two array LUNs, LUN 1, for the root volume. System vs1 can read data from and write data to LUN 1, because LUN 1 is in an aggregate. LUN 2 remains a spare LUN because it has not yet been added to an aggregate. System vs1 cannot read data from and write data to LUN 2 while it is a spare.

![Diagram of storage array and LUNs available for Data ONTAP](image)
After you perform initial setup of the storage system, you could configure vs1 to also own LUN 3, LUN 4, both, or neither, depending on your storage needs.

**Ownership of LUNs in an HA pair**

In this example, two storage systems running Data ONTAP are configured in an HA pair. In an HA pair, only one node can be the owner of a particular LUN, but both nodes must be able to see the same LUNs so that the partner can take over if the owning node becomes unavailable.

LUN 1 through LUN 4 were created on the storage array and mapped to the ports on the storage array to which the storage systems are connected. All four LUNs are visible to each node in the HA pair.

Assume that during initial setup vs1 was assigned ownership of LUN 1 and LUN 2. LUN 1 was automatically added to the root volume, so LUN 1 is now "in use" by vs1. LUN 2 remains a spare until it is explicitly added to an aggregate on vs1. Similarly, assume that during initial setup vs2 was assigned ownership of LUN 3 and LUN 4, with LUN 3 assigned to the root volume. LUN 4 remains a spare LUN until it is explicitly added to an aggregate.

The key points of this example are as follows:

- By deploying the storage systems in an HA pair, one system can take over services for its partner if the partner becomes unavailable.
- Only one storage system can own a specific array LUN. However, all array LUNs assigned to a node in an HA pair must be visible to—but not assigned to or owned by—the other node in the HA pair.
- By deploying two switches, if one switch fails, the other switch provides the alternate path to the storage array.
- Both switches must be zoned correctly so that each storage system in the HA pair can see the array LUNs owned by its partner.
Managing array LUNs through Data ONTAP

Before a storage array administrator can reconfigure an array LUN that was assigned to a V-Series system, you must remove the information that Data ONTAP wrote to that LUN when it was assigned.

Certain storage management tasks must always be done on the storage array—for example, creating the LUNs, mapping them to Data ONTAP, and reconfiguring them (for example, to resize them). Other storage management tasks are done through Data ONTAP—for example, creating volumes and aggregates. Depending on what you need to do, you might need to coordinate storage management activities with the storage array administrator.

For example, you need to remove information that Data ONTAP has written to a LUN before the storage array administrator can reconfigure the LUN on the storage array to resize it or use it for a different host. The reason is that Data ONTAP disk ownership information still exists in the disk label.

Next topics

- Array LUN name format on page 59
- Assigning ownership of array LUNs on nodes running Cluster-Mode on page 60
- Modifying assignment of spare array LUNs in Cluster-Mode on page 62
- Why you might change the checksum type of an array LUN on page 63
- Changing the checksum type of an array LUN on page 63
- Prerequisites to reconfiguring a LUN on the storage array on page 64
- Changing array LUN size or composition on page 65
- Removing one array LUN from use by Data ONTAP on page 66
- Removing a storage system using array LUNs from service on page 67

Array LUN name format

The array LUN name is a path-based name that includes the devices in the path between the V-Series system and the storage array.

By looking at the array LUN name as it is displayed in Data ONTAP output, you can identify devices in the path between the storage system and the storage array, ports used, and the LUN identifier that the storage array presents externally for mapping to hosts. The format of the array LUN name depends on whether the system that runs Data ONTAP connects directly to the storage array or whether it connects through a switch.

The format for an array LUN name for a direct-attached configuration is as follows:

\[ \text{node-name.adapter.id lun-id} \]
node-name is the name of the Cluster-Mode node. The node name is prepended to the LUN name so that the path-based name will be unique within the cluster.

adapter is the adapter on the storage system that runs Data ONTAP.

id is the channel adapter port on the storage array.

lun-id is the array LUN number that the storage array presents to hosts.

Example: node1.0a.0L0

The format for an array LUN name for a switch-attached configuration is as follows:

node-name.switch-name:port.idlun-id

node-name is the name of the Cluster-Mode node. The node name is prepended to the LUN name so that the path-based name will be unique within the cluster.

switch-name is the name of the switch.

port is the switch port that is connected to the target port (the end point).

id is the device ID.

lun-id is the array LUN number that the storage array presents to hosts.

Example: node1.mcdata3:6.127L0

These names consist of a path component and the SCSI LUN id on that path. For example, in the array LUN name example for a fabric-attached configuration, mcdata3:6.127 is the path component and L0 is the SCSI LUN ID.

On a V-Series system, there are two names for each LUN because there are two paths to each LUN—for example, node1.mcdata3:6.127L0 and node1.brocade15:6.127L0.

See the V-Series Installation Requirements and Reference Guide for details about how to use the array LUN names when you are checking paths to array LUNs.

Assigning ownership of array LUNs on nodes running Cluster-Mode

Array LUNs must be owned by a node before they can be used in an aggregate. You must use the disk assign command via node shell to assign ownership of an array LUN so that you can specify the checksum type for the LUN.

Before you begin

The storage array administrator must make array LUNs available to Data ONTAP before you can see them in Data ONTAP and assign them to a node running Data ONTAP.

About this task

Use this procedure to assign ownership of array LUNs that are currently unowned. If you want to change the ownership of array LUNs that are already owned by a node, use the procedure for changing ownership for array LUNs.
Steps

1. Enter the following to access the nodeshell:

   system run -node node_name

   *node_name* is the name of this node.

2. Use the `disk show -n` command to view all array LUNs that do not have assigned owners.

   **Note:** You must make array LUNs available to Data ONTAP before they can be assigned to a node.

3. Use the following command to assign the array LUNs that are labeled `Not Owned` to a node.

   ```
   disk assign {disk_list | all | [-T storage_type] -n count|auto} [-p pool] [-o owner_name] [-s sysid] [-c block | zoned] [-f]
   ```

   You can specify the array LUNs to be assigned in the following ways:
   - Use the `disk_list` parameter to specify one or more array LUN names. This is the most specific way to specify array LUNs. However, you must manually enter each name.
   - Use the `disk_list` parameter with the wildcard character (`*`) to specify a group of array LUN names.
   - Use the `all` keyword to specify all unowned array LUNs.
   - Use the `-n count` option to specify a number of unassigned array LUNs to be assigned.
   - Use the `-T` option with the disk type `LUN` to identify that you are assigning an array LUN. Specific disk types are available to be used with disks. If you have both disks and array LUNs on your node, always use the `-T` option with the `LUN` disk type to ensure that Data ONTAP uses the array LUNs that you expect. Without this option, Data ONTAP uses the type of disk or array LUN with the most spares.
   - Use the `-c` option to specify the checksum type for the array LUNs to be assigned. You can specify block or zoned. The default checksum type is block. For more information about checksums, see the *V-Series Installation Requirements and Reference Guide*.

   You use the following options to specify the node to own the array LUNs you are assigning.

   **Note:** If you do not specify a node to own the array LUNs, they are assigned to the local node.
   - The `-o owner_name` option specifies the name of the node to which you want to assign the array LUNs.
   - The `-s sysid` specifies the ID of the node that the array LUNs are assigned to. This is an alternative to specifying the system ID.
   - The `-f` option is used only for changing ownership for an array LUN that is already owned by a node.

4. You can use the `disk show -v` command to verify the assignments that you just made.

5. Enter the following to exit nodeshell:
Modifying assignment of spare array LUNs in Cluster-Mode

You can change the ownership of a spare array LUN to another node.

Before you begin

For an array LUN that is part of an aggregate, you must first remove the LUN from the aggregate, which changes the state of the array LUN to spare. To remove an array LUN from an aggregate, you must destroy the aggregate.

About this task

Steps

1. At the console of the node that owns the array LUN that you want to reassign, enter the following to access the nodeshell:

   system run -node node_name

   node_name is the name of this node.

2. At the console of the node that owns the array LUN that you want to reassign, enter the following to see a list of spare array LUNs on the node:

   aggr status -s

3. On the node that owns the spare array LUN you want to reassign, enter either of the following commands to reassign ownership of the array LUN:

   disk assign LUN-name -o new_owner_name -f
   or

   disk assign LUN-name -s sysID-of-receiving_system -f

   -o is the name of the node that you want to be the new owner of the array LUN.

   -s is the ID of the node that you want to be the new owner of the array LUN. You can obtain the system ID of the destination node by running sysconfig on the destination node

   -f is required to force the change.

4. Enter the following command to verify that the ownership of the spare array LUN moved to the other node: aggr status -s

   The spare array LUN that you moved should no longer appear in the list of spares.

5. On the destination node, enter the following command to verify that the spare array LUN whose ownership you changed is listed as a spare owned by the destination node: aggr status -s
6. Enter the following command to exit nodeshell:

   `exit`

**After you finish**

You must add the array LUN to an aggregate before you can use it for storage.

---

**Why you might change the checksum type of an array LUN**

All array LUNs in an aggregate must be the same checksum type. If necessary, you can change the checksum type of an array LUN to be able to add it to an aggregate.

Data ONTAP formats array LUNs in a special way to store checksum information that is used for data integrity checking on READs. The major factor that determines the usable space in an array LUN is the checksum type. For array LUNs, Data ONTAP supports both block (BCS) checksum and zoned (ZCS) checksum types. You specify a checksum type when you assign ownership of an array LUN to a storage system (or accept the default of BCS).

You might need to change the checksum type associated with an array LUN after you have assigned the LUN to a system running Data ONTAP, for example, because your remaining array LUNs are BCS and you want to add them to an aggregate that is ZCS type. Before changing the checksum type of an array LUN, you should review the tradeoffs between performance in certain types of workloads and storage capacity utilization of each checksum type.

- **Block checksums**
  With block checksums, Data ONTAP reserves 12.5 percent of the space of the array LUN is used for checksum. Data ONTAP uses BCS by default because it provides better performance in certain workloads.

- **Zoned checksums**
  Zoned checksums have better storage capacity utilization. However, at certain workloads ZCS LUNs have a performance impact. Random-read intensive workloads are affected the most.

See the *V-Series Installation Requirements and Reference Guide* for more information about checksums. Contact your Sales Engineer for more details about using checksums.

---

**Changing the checksum type of an array LUN**

Sometimes you need to change the checksum type that you assigned to an array LUN, for example, because a LUN that you want to add to an aggregate is a different checksum type than the aggregate.

**About this task**

For array LUNs, you can change the checksum type of an array LUN from block checksum type (BCS) to zoned checksum type (ZCS), or the reverse. For example, if your remaining array LUNs are...
BCS type and the aggregate that you need to add them to is ZCS type, you would need to change the checksum type of those LUNs before you can add them to the aggregate.

**Note:** Data ONTAP automatically assigns a BCS type to native disks. You cannot change the checksum type of native disks.

**Steps**

1. Enter the following to access the nodeshell:

   ```bash
   system run -node node_name
   ```

   *node_name* is the name of this system.

2. Enter the following command:

   ```bash
   disk remove -w LUN-name
   ```

   *LUN name* is the name of the array LUN whose checksum type you want to change.

3. Enter the following command:

   ```bash
   disk assign LUN-name -c new_checksum_type
   ```

   *LUN name* is the name of the array LUN whose checksum type you want to change.

   *new_checksum_type* can be *block* or *zoned*.

   The checksum type of the array LUN is changed to the new checksum type you specified.

4. Enter the following to exit nodeshell:

   ```bash
   exit
   ```

**Prerequisites to reconfiguring a LUN on the storage array**

If an array LUN has already been assigned (through Data ONTAP) to a particular storage system, you must ensure that the information Data ONTAP wrote to the LUN is removed before the storage administrator attempts to reconfigure the LUN on the storage array.

When the storage array presents a LUN to Data ONTAP, Data ONTAP collects information about the LUN (for example, its size) and writes that information to the LUN. Data ONTAP cannot dynamically update information that it wrote to an array LUN. Therefore, before the storage array administrator reconfigures a LUN, you must use Data ONTAP to change the state of the LUN to **unused**. (The LUN is unused from the perspective of Data ONTAP.)

While changing the state of the LUN to unused, Data ONTAP does the following:

- Terminates I/O operations to the LUN.
- Removes the label for RAID configuration information and the persistent reservations from the LUN, which makes the array LUN unowned by any V-Series system.

After you run `disk remove -w` on a LUN, you can do the following on the storage array:
• Remove the mapping of the LUN to Data ONTAP and make the LUN available to other hosts. No Data ONTAP information remains in the LUN.

• Resize the LUN or change its composition.

• If you want Data ONTAP to use the LUN again, present the LUN to Data ONTAP again. When the LUN is presented again to Data ONTAP after it is reconfigured, Data ONTAP is aware of the new LUN size or composition. Thereafter, in Data ONTAP you can assign the LUN to a V-Series system again.

   **Note:** You need to assign the LUN to a V-Series system again because all ownership information was removed from the LUN when you ran `disk remove -w`.

### Changing array LUN size or composition

Reconfiguration of array LUN size or composition must be done on the storage array. If a LUN has already been assigned to a storage system running Data ONTAP, you must change the state of a LUN to unused, through Data ONTAP, before the storage array administrator can reconfigure the LUN.

#### Before you begin

If the LUN that the storage administrator wants to reconfigure is in an aggregate, you must take the aggregate to which the LUN belongs offline and destroy the aggregate before starting this procedure. Taking the aggregate offline and destroying it changes the LUN from a data LUN to a spare LUN.

#### About this task

Using the `disk remove -w` command on a LUN removes the information that Data ONTAP wrote to the LUN to identify which system running Data ONTAP is the assigned owner of the LUN. After the ownership information is removed, the LUN cannot be used by any system running Data ONTAP unless the LUN is assigned again to a system.

#### Steps

1. On the system running Data ONTAP, enter the following to access the nodeshell:
   
   ```
   system run -node node_name
   ```

   `node_name` is the name of this system.

2. On the system running Data ONTAP, enter the following command to remove ownership information:

   ```
   disk remove -w LUNfullname
   ```

3. On the storage array, complete the following steps:

   a. Unmap (unpresent) the array LUN from the systems in the V-Series neighborhood so that they can no longer see the LUN.
b. Change the size or composition of the array LUN.

c. Present the array LUN to the systems running Data ONTAP again.

At this point, the LUN is visible to the FC initiator ports to which the LUN was presented, but it cannot be used by any systems running Data ONTAP yet.

4. On the system that you want to be the owner of the LUN, use the `disk assign` command, through nodeshell, to assign the ownership of the LUN to the storage system.

You can leave the LUN as a spare or add it to an aggregate. The LUN cannot be used for storage until after it has been added to an aggregate.

5. Enter the following command to exit nodeshell:

   `exit`

Removing one array LUN from use by Data ONTAP

If you no longer want to use an array LUN for Data ONTAP, you must remove the information that Data ONTAP wrote to the LUN before you can reconfigure the LUN from the storage array for use by another host.

Before you begin

If the LUN that you no longer want Data ONTAP to use is in an aggregate, you must take the aggregate to which the LUN belongs offline and destroy the aggregate before starting this procedure. Taking an aggregate offline and destroying it changes the LUN from a data LUN to a spare LUN.

About this task

When Data ONTAP sees an array LUN, it writes information that it discovers about that LUN to that LUN. Additionally, Data ONTAP writes ownership information to a LUN when (through Data ONTAP) you assign a particular system to be the owner of the LUN. If you no longer want to use a LUN for Data ONTAP, you must use a Data ONTAP command to remove that information from the LUN before you reconfigure the LUN on the storage array. Otherwise that LUN is not available for other hosts.

   **Note:** If you want a different V-Series system to own the LUN, use the `disk assign -s` or `disk assign -o` command to reassign the LUN to the other V-Series system.

Perform this procedure from the command line of your storage system running Data ONTAP.

Steps

1. Enter the following to access the nodeshell:

   `system run -node node_name`

   `node_name` is the name of this system.
2. Enter the following command:

   `disk remove -w LUNfullname`

   LUNfullname is the full name of the array LUN.

3. Enter the following to exit nodeshell:

   `exit`

Removing a storage system using array LUNs from service

You must release the persistent reservations on all array LUNs assigned to the storage system running Data ONTAP before removing the system from service.

**About this task**

When you assign Data ONTAP ownership of an array LUN, Data ONTAP places persistent reservations (ownership locks) on that array LUN to identify which V-Series system owns the LUN. If you want the array LUNs to be available for use by other types of hosts, you must remove the persistent reservations that Data ONTAP put on those array LUNs. The reason is that some arrays do not allow you to destroy a reserved LUN if you do not remove the ownership and persistent reservations that Data ONTAP wrote to that LUN.

For example, the Hitachi USP storage array does not have a user command for removing persistent reservations from LUNs. If you do not remove persistent reservations through Data ONTAP before removing the V-Series system from service, you must call Hitachi technical support to remove the reservations.

Contact Technical Support for instructions about how to remove persistent reservations from LUNs before removing a V-Series system from service.

**Note:** If the system that you want to remove is part of an HA pair, you must remove the high availability software and interconnect cabling before you can remove the system from service. See the *Data ONTAP Cluster-Mode High-Availability Configuration Guide* for more information.
Reusing disks configured for software-based disk ownership

If you plan to reuse disks from storage systems that have been configured for software-based disk ownership, you should remove the software information from the disks first.

**Attention:** If disks with unerased software-based ownership information are installed in an unbooted storage system that does not use software-based disk ownership, the storage system will not boot.

You can use the following methods to remove software-based disk ownership information, as appropriate:

- You can transfer the disks to the target storage system while that storage system is in operation, thus automatically erasing their disk ownership information.
- You can manually erase the disk ownership information for a disk before removing it from its original storage system.

**Note:** If you accidentally cause a boot failure by installing software-assigned disks, you can recover by running the `disk remove_ownership` command in maintenance mode.

**Next topics**

- [Manually erasing software-based disk ownership information](#) on page 69
- [Automatically erasing disk ownership information](#) on page 70

Manually erasing software-based disk ownership information

If you are moving disks from a storage system using software-based disk ownership to a system that does not, and the target system is running a version of Data ONTAP earlier than 6.5.1, you should erase all software-based disk ownership information on the disks before moving them.

**Steps**

1. At the prompt of the storage system whose disks you want to transfer, enter the following command to list all the storage system disks and their RAID status:
   ```bash
   aggr status -r
   ```
2. Note the names of the disks you plan to transfer; you will erase the disk ownership information from these disks.
In most cases (unless you plan to physically move an entire aggregate of disks to a new storage system), you should plan to transfer only disks listed as hot spare disks.

3. Enter the following command to enter advanced privilege mode:
   ```
   priv set advanced
   ```

4. For each disk that you want to remove, enter the following commands:
   ```
   disk remove_ownership disk_name
   disk remove disk_name
   ```
   **Note:** You can use the wildcard character ("*") to specify multiple disks for the `disk remove_ownership` command.

5. Enter the following command to return to administrative privilege mode:
   ```
   priv set
   ```

6. Enter the following command to confirm the removal of the disk ownership information from the specified disk:
   ```
   disk show -v
   ```
   Any disk that is labeled “Not Owned” no longer contains disk ownership information and is ready to be moved to another storage system.

### Automatically erasing disk ownership information

If you physically transfer disks from a storage system that uses software-based disk ownership to a running storage system that does not, you can do so without using the `disk remove_ownership` command if the storage system you are transferring to is running Data ONTAP 6.5.1 or higher.

**Steps**

1. Do not shut down the target storage system.

2. On the target storage system, enter the following command to confirm the version of Data ONTAP on the target storage system:
   ```
   version
   ```

3. If the Data ONTAP version on the target storage system is earlier than 6.5.1, do not continue this procedure. Instead, erase the software-based disk ownership information on the source storage system manually.

4. Enter the following command for each of the disks you plan to remove to spin down the disks:
   ```
   disk remove disk_name
   ```

5. Remove the disks from their original storage system and physically install them in the running target storage system.
**Result**

The running target storage system automatically erases any existing software-based disk ownership information on the transferred disks.

**After you finish**

On the target storage system, you can use the `aggr status -r` command to verify that the disks you have added are successfully installed.
Disk management

This section describes the tasks you can perform to manage disks.

Next topics

Displaying information about disks on page 73
Modifying disk attributes on page 74
Failing a disk on page 75
Displaying disk-option settings on page 75
Modifying disk-option settings on page 76
Reassigning disks to another node on page 77
Removing ownership from a disk on page 77
Zeroing spare disks on page 78
Downloading disk, ACP processor, and shelf firmware on page 78
Commands for manually updating disk, ACP processor, and disk shelf firmware on page 79
Controlling disk LEDs on page 80

Displaying information about disks

You can display information about disks in an aggregate.

Step

1. Use the `storage disk show` command to display information about the disks that comprise aggregates.

By default, the command displays the following information about all disks:

- Disk name.
- Size of the disk, in MB.
- Number of the disk shelf on which the disk is located.
- Number of the bay in which the disk is located.
- Disk state. Possible values include partner, broken, zeroing, spare, copy, pending, reconstructing, and present.
- RAID type. Possible values include pending, parity, dparity, or data.
- Aggregate name.
- Name of the node that owns the disk.

Other information is displayed in a detailed view and if other parameters are specified. See the reference page for the command for details.
Example
The following example displays information about all disks in all aggregates:

```
node::> storage disk show
Disk          UsedSize(MB) Shelf Bay State     RAID Type  Aggregate Owner
------------  ------------ ----- --- --------- ---------- --------- --------
node0:0a.16   271979           1   0 partner   -          -         node2
node0:0a.17   271979           1   1 partner   -          -         node2
node0:0a.18   271979           1   2 partner   -          -         node2
node0:0a.19   271979           1   3 partner   -          -         node2
node0:0a.20   271979           1   4 partner   -          -         node2
node0:0a.21   271979           1   5 partner   -          -         node2
node0:0a.22   271979           1   6 partner   -          -         node2
node0:0a.23   271979           1   7 partner   -          -         node2
node0:0a.24   271979           1   8 partner   -          -         node2
node0:0a.25   271979           1   9 partner   -          -         node2
node0:0a.26   271979           1  10 partner   -          -         node2
node0:0a.27   271979           1  11 partner   -          -         node2
node0:0a.28   271979           1  12 partner   -          -         node2
node0:0a.29   271979           1  13 partner   -          -         node2
node0:0a.32   271979           2   0 partner   -          -         node2
node0:0a.33   271979           2   1 partner   -          -         node2
node0:0a.34   271979           2   2 partner   -          -         node2
node0:0a.35   271979           2   3 partner   -          -         node2
node0:0a.36   271979           2   4 partner   -          -         node2
node0:0a.37   271979           2   5 partner   -          -         node2
[...]```

Modifying disk attributes

You can change the owning node and state of a disk.

Step

1. Use the `storage disk modify` command to modify the owning node, the state, or both of a disk.

   The command prompts you for confirmation before proceeding.

Example

The following example sets a disk’s state to spare.

```
node::> storage disk modify -disk node1b:0c.27 -state spare
```

Related tasks

* Failing a disk on page 75
* Failing a disk on page 75
Failing a disk

You can manually fail a disk.

Steps

1. Use the `storage disk fail` command to manually fail a disk.

   The command prompts you for confirmation before proceeding.

   Example

   The following example fails a disk named node0:1a.16 immediately:

   ```
   node::> storage disk fail -disk node0:1a.16 -i true
   WARNING: The system will not prefail the disk and its contents will not be
   copied to a replacement disk before being failed out. Do you want to
   fail out the disk immediately? {y|n}: y
   ```

2. Use the `storage disk modify` command to unfail a disk.

Related tasks

   * [Modifying disk attributes](#) on page 74
   * [Modifying disk attributes](#) on page 74

Displaying disk-option settings

You can display the settings of disk options.

Step

1. Use the `storage disk option show` command to display the settings of disk options.

   The command displays the settings of the following disk options:

   - Background firmware update
   - Automatic copying of data to a spare in the event of a predictive failure
   - Automatic assignment of disks

   Example

   The following example displays the disk-option settings for all nodes.

   ```
   node::> storage disk option show
   Node       Bkg. FW Upg.    Auto Copy   Auto Assign
   node0a     on             on          on
   node0b     on             on          on
   node1a     on             on          on
   ```
Modifying disk-option settings

You can modify the settings of disk options.

Step

1. Use the `storage disk option modify` command to modify the settings of disk options.

   You can use the command to modify the following disk options:

   - `[-bkg-firmware-update {on | off}]`—Specifies whether firmware updates run in the background. The default setting is on, meaning that firmware updates to spares and file system disks within RAID-DP, mirrored RAID-DP, and mirrored RAID4 volumes is performed nondisruptively via a background process. Firmware updates for disks within RAID4 volumes are performed at system startup. If the option is turned off, automatic firmware updates occur at system startup or during disk insertion.

   - `[-autocopy {on | off}]`—Specifies whether data is automatically copied to a spare in the event of a predictive failure. The default setting is on. It is sometimes possible to predict a disk failure based on a pattern of recovered errors that have occurred. In such cases, the disk reports a predictive failure. If this option is set to on, the system initiates Rapid RAID Recovery to copy data from the failing disk to an available spare. When data is copied, the disk is marked as failed and placed in the pool of broken disks. If a spare is not available, the node continues to use the disk until it fails. If the option is set to off, the disk is immediately marked as failed and placed in the pool of broken disks. A spare is be selected and data from the missing disk is reconstructed from other disks in the RAID group. The disk is not failed if the RAID group is already degraded or reconstructing, thereby preventing another disk failure from leading to the failure of the whole RAID group.

   - `[-autoassign {on | off}]`—Specifies whether unowned disks are automatically assigned. The default setting is on.

By default, all of these options are set to on.

Example

The following example disables background firmware upgrades for disks on all nodes:

```
node::> storage disk option modify -node * -bkg-firmware-update off
```
Reassigning disks to another node

You can reassign disks from one node to another.

Step

1. You can use the `storage disk reassign` command to reassign a node's disks to a different node.

   You can specify the nodes either by their names or by their serial numbers. If the a node's disks have been taken over by the node's failover partner, specify the `-force true` parameter to force the reassignment operation. This command requires the advanced privilege level or higher.

   Example
   In the following example, the disks for a node named `node0a` are reassigned to a node named `node0b`. The node named `node0b` is `node0a`'s failover partner and has taken over `node0a`'s disks. To assign `node0a`'s disks to `node0b`, ensure that `node0b` is running, and enter the following command:

   ```
   node::*> storage disk reassign -home node0a -newhome node0b -force true
   node0a:1a.11, node0a:1a.12, node0a:1a.13, node0a:1a.14, node0a:1a.15, node0a:1a.16, node0a:1a.23 and node0a:1a.24 were reassigned to new owner node0b.
   ```

Removing ownership from a disk

You can remove ownership from a disk.

About this task

When you remove ownership from a disk, the data that's stored on the disk remains intact. You can then assign the disk to the same node or a different node and continue reading and writing data.

Step

1. Use the `storage disk removeowner` command to remove ownership from a disk.

   After a disk's ownership is removed, another node can take ownership of it.

   Example
   The following example removes ownership from a disk named `node0a:0a.10`.

   ```
   node::*> storage disk removeowner -disk node0a:0a.10
   ```
### Zeroing spare disks

You can zero (that is, overwrite all data on the disk with zeroes) all spare disks owned by a node.

**Step**

1. Use the `storage disk zerospares` command to zero all spare disks owned by a node.

Zeroing a disk means to overwrite all data on it with zeroes. This needs to be done if you have spare disks that were previously contained in an aggregate or volume. Spare disks should be zeroed so that the hot spare can come online rapidly when needed.

**Example**

The following example zeroes all spare disks owned by a node named node1b.

```
node::> storage disk zerospares -owner node1b
```

### Downloading disk, ACP processor, and shelf firmware

You can download disk, ACP processor, and shelf firmware to update the versions of this firmware currently running on the nodes in your cluster.

**Before you begin**

Downloading firmware requires you to be logged in at the advanced privilege level.

**Steps**

1. Use the `storage firmware download` command and the `-package-type` parameter with a value of `disk` to download disk firmware from a URL or URI to a specified node.

**Example**

The following example downloads a package containing all updates for disks from http://now.netapp.com/path_to_fw/all.tgz to a node named node0a.

```
node::*> storage firmware download -node node0a -package-type disk
    -package http://now.netapp.com/path_to_fw/all.tgz
```

**Example**

The following example downloads a specific file containing an update for disks from http://now.netapp.com/path_to_fw/file_name.LOD to a node named node0a.

```
node::*> storage firmware download -node node0a -package-type disk
    -package http://now.netapp.com/path_to_fw/file_name.LOD
```

2. Use the `storage firmware download` command and the `-package-type` parameter with a value of `shelf` to download disk shelf firmware from a URL or URI to a specified node.
3. Use the `storage firmware download` command and the `-package-type` parameter with a value of `acpp` to download **ACP processor firmware** from a URL or URI to a specified node.

**Example**

The following example downloads a package containing all updates for the ACP processor from `http://now.netapp.com/path_to_fw/all_shelf_fw.tar` to a node named `node0a`.

```bash
code
node::*> storage firmware download -node node0a -package-type acpp
                          -package http://now.netapp.com/path_to_fw/all_shelf_fw.tar
```

**Example**

The following example downloads a file containing an update for the ACP processor from `http://now.netapp.com/path_to_fw/file_name.SFW` to a node named `node0a`.

```bash
code
node::*> storage firmware download -node node0a -package-type acpp
                          -package http://now.netapp.com/path_to_fw/file_name.SFW
```

4. Repeat these steps on each node in your cluster.

**After you finish**

After you have downloaded the packages needed to update disk, ACP processor, and shelf firmware, you can initiate an automatic update by restarting each node. If you prefer to avoid restarting the nodes in your cluster, you can manually update each type of firmware by using the commands in the section *Commands for updating disk ACP and disk shelf firmware* on page 79.

**Commands for manually updating disk, ACP processor, and disk shelf firmware**

There are different advanced privilege-level commands you use to manually update disk, ACP processor, and disk shelf firmware.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update disk firmware</td>
<td><code>storage disk updatefirmware</code></td>
</tr>
</tbody>
</table>
Controlling disk LEDs

You can control disk LEDs. This is useful for locating disks on one or more disk shelves.

**Step**

1. Use the `storage disk setled` command to control disk LEDs.

   You can turn LEDs on or off or cause them to blink or stop blinking. When you run the command, you specify a disk name or name pattern, the state to which the LED or LEDs are to be set, and the time, in minutes, that the LED or LEDs are to remain in the specified state.

   **Example**

   The following example causes the LEDs on all disks whose names match the pattern `node1b*` to turn on:

   ```
   node::> storage disk setled -disk node1b* -action on
   ```
How Data ONTAP uses RAID to protect your data and data availability

RAID protects your data and data availability. Understanding how RAID provides this protection can help you administer your storage systems more effectively.

For native storage, Data ONTAP uses RAID-DP (double-parity) or RAID Level 4 (RAID4) protection to ensure data integrity within a group of disks even if one or two of those disks fail. Parity disks provide redundancy for the data stored in the data disks. If a disk fails (or, for RAID-DP, up to two disks), the RAID subsystem can use the parity disks to reconstruct the data in the drive that failed.

For third-party storage, Data ONTAP stripes across the array LUNs using RAID0. The storage arrays, not Data ONTAP, provide the RAID protection for the array LUNs that they make available to Data ONTAP.

Next topics
- RAID protection levels for disks on page 81
- RAID protection for third-party storage on page 82
- RAID disk types on page 41
- How Data ONTAP RAID groups work on page 83
- How Data ONTAP works with hot spare disks on page 86
- How Data ONTAP handles a failed disk with a hot spare on page 88
- How Data ONTAP handles a failed disk that has no available hot spare on page 88
- How RAID-level disk scrubs verify data integrity on page 89

RAID protection levels for disks

Data ONTAP supports two levels of RAID protection for disks in native disk shelves, RAID-DP and RAID4. RAID-DP can protect against double-disk failures or failures during reconstruction. RAID4 can protect against single-disk failures. You assign RAID level on a per-aggregate basis.

For more information about choosing RAID protection levels, see Technical Report 3437: Storage Best Practices and Resiliency Guide.

Next topics
- What RAID-DP protection is on page 82
- What RAID4 protection is on page 82
Related information

TR 3437: Storage Best Practices and Resiliency Guide

What RAID-DP protection is

If an aggregate is configured for RAID-DP protection, Data ONTAP reconstructs the data from one or two failed disks within a RAID group and transfers that reconstructed data to one or two spare disks as necessary.

RAID-DP provides double-parity disk protection when the following conditions occur:

- There is a single-disk or double-disk failure within a RAID group.
- There are media errors on a block when Data ONTAP is attempting to reconstruct a failed disk.

The minimum number of disks in a RAID-DP group is three: at least one data disk, one regular parity disk, and one double-parity (or dParity) disk.

If there is a data-disk or parity-disk failure in a RAID-DP group, Data ONTAP replaces the failed disk in the RAID group with a spare disk and uses the parity data to reconstruct the data of the failed disk on the replacement disk. If there is a double-disk failure, Data ONTAP replaces the failed disks in the RAID group with two spare disks and uses the double-parity data to reconstruct the data of the failed disks on the replacement disks.

RAID-DP is the default RAID type for all aggregates.

What RAID4 protection is

RAID4 provides single-parity disk protection against single-disk failure within a RAID group. If an aggregate is configured for RAID4 protection, Data ONTAP reconstructs the data from a single failed disk within a RAID group and transfers that reconstructed data to a spare disk.

The minimum number of disks in a RAID4 group is two: at least one data disk and one parity disk.

If there is a single data or parity disk failure in a RAID4 group, Data ONTAP replaces the failed disk in the RAID group with a spare disk and uses the parity data to reconstruct the failed disk’s data on the replacement disk. If no spare disks are available, Data ONTAP goes into degraded mode and alerts you of this condition.

**Attention:** With RAID4, if there is a second disk failure before data can be reconstructed from the data on the first failed disk, there will be data loss. To avoid data loss when two disks fail, you can select RAID-DP. This provides two parity disks to protect you from data loss when two disk failures occur in the same RAID group before the first failed disk can be reconstructed.

RAID protection for third-party storage

Third-party storage arrays provide the RAID protection for the array LUNs they make available to systems running Data ONTAP.

Data ONTAP supports a variety of RAID types used by storage arrays, but imposes restrictions on storage arrays using RAID0 for the LUNs that they make available to Data ONTAP. Data ONTAP
uses RAID0 to stripe across the array LUNs, which splits data evenly across two or more array LUNs. Performance is maximized because more disk spindles are used.

RAID0 provides no data protection. Therefore, when creating "RAID groups" on storage arrays, follow the best practices of the storage array vendor to ensure that there is an adequate level of protection on the storage array so that disk failure does not result in loss of data or loss of access to data.

**Note:** A "RAID group" on a storage array is the arrangement of disks that together form the defined RAID level. Each RAID group supports only one RAID type. The number of disks that you select for a RAID group determines the RAID type that a particular RAID group supports. Different storage array vendors use different terms to describe this entity—RAID groups, parity groups, disk groups, Parity RAID groups, and other terms.

Starting in Data ONTAP 7.3, V-Series systems support native disk shelves as well as third-party storage. Data ONTAP supports RAID4 and RAID-DP on the native disk shelves connected to a V-Series system but does not support RAID4 and RAID-DP with array LUNs.

See the V-Series implementation guide for your vendor to determine whether there are specific requirements or limitations about RAID types in configurations with storage systems running Data ONTAP.

### RAID disk types

Data ONTAP classifies disks as one of four types for RAID: data, hot spare, parity, or dParity. The RAID disk type is determined by how RAID is using a disk.

- **Data disk** Holds data stored on behalf of clients within RAID groups (and any data generated about the state of the storage system as a result of a malfunction).
- **Spare disk** Does not hold usable data, but is available to be added to a RAID group in an aggregate. Any functioning disk that is not assigned to an aggregate but is assigned to a system functions as a hot spare disk.
- **Parity disk** Stores data reconstruction information within RAID groups.
- **dParity disk** Stores double-parity information within RAID groups, if RAID-DP is enabled.

### How Data ONTAP RAID groups work

A RAID group consists of one or more data disks or array LUNs, across which client data is striped and stored, and up to two parity disks, depending on the RAID level of the aggregate that contains the RAID group.

RAID-DP uses two parity disks to ensure data recoverability even if two disks within the RAID group fail.

RAID4 uses one parity disk to ensure data recoverability if one disk within the RAID group fails.
RAID0 does not use any parity disks; it does not provide data recoverability if any disks within the RAID group fail.

For native storage, Data ONTAP uses RAID-DP or RAID4 groups to provide parity protection. For third-party storage, Data ONTAP uses RAID0 groups to optimize performance and storage utilization. The storage arrays provide the parity protection for third-party storage.

Next topics

- How RAID groups are named on page 84
- About RAID group size on page 84
- Considerations for sizing RAID groups for disks on page 84
- Considerations for Data ONTAP RAID groups for array LUNs on page 85

How RAID groups are named

Within each aggregate, RAID groups are named rg0, rg1, rg2, and so on in order of their creation. You cannot specify the names of RAID groups.

About RAID group size

A RAID group has a maximum number of disks or array LUNs that it can contain. This is called its maximum size, or its size. A RAID group can be left partially full, with fewer than its maximum number of disks or array LUNs, but storage system performance is optimized when all RAID groups are full.

Considerations for sizing RAID groups for disks

Configuring an optimum RAID group size for an aggregate made up of disks requires a trade-off of factors. You must decide which factor—speed of recovery, assurance against data loss, or maximizing data storage space—is most important for the aggregate that you are configuring.

In most cases, the default RAID group size is the best size for your RAID groups. However, you can change the maximum size of your RAID groups.

Note: You change the size of RAID groups on a per-aggregate basis. You cannot change the size of an individual RAID group.

Configuring an optimum RAID group size for an aggregate requires a trade-off of factors. Adding more data disks to a RAID group increases the striping of data across those disks, which typically improves I/O performance. Additionally, a smaller percentage of disks is used for parity rather than data. However, with more disks in a RAID group, there is a greater risk that one of the disks might fail.

Note: With RAID-DP, you can use larger RAID groups because they offer more protection. A RAID-DP group is more reliable than a RAID4 group that is half its size, even though a RAID-DP group has twice as many disks. Thus, the RAID-DP group provides better reliability with the same parity overhead.

Large RAID group configurations offer the following advantages:
• More data drives available. An aggregate configured into a few large RAID groups requires fewer drives reserved for parity than that same aggregate configured into many small RAID groups.

• Small improvement in storage system performance. Write operations are generally faster with larger RAID groups than with smaller RAID groups.

Small RAID group configurations offer the following advantages:

• Shorter disk reconstruction times. In case of disk failure within a small RAID group, data reconstruction time is usually shorter than it would be within a large RAID group.

• Decreased risk of data loss due to multiple disk failures. The probability of data loss through double-disk failure within a RAID4 group or through triple-disk failure within a RAID-DP group is lower within a small RAID group than within a large RAID group.

### Considerations for Data ONTAP RAID groups for array LUNs

Setting up Data ONTAP RAID groups for array LUNs requires planning and coordination with the storage array administrator so that the administrator makes the number and size of array LUNs you need available to Data ONTAP.

For array LUNs, Data ONTAP uses RAID0 RAID groups to determine where to allocate data to the LUNs on the storage array. The RAID0 RAID groups are not used for RAID data protection. The storage arrays provide the RAID data protection.

**Note:** Data ONTAP RAID groups are similar in concept to what storage array vendors call RAID groups, parity groups, disk groups, Parity RAID groups, and other terms.

Follow these steps when planning your Data ONTAP RAID groups for array LUNs:

1. Plan the size of the aggregate that best meets your data needs.

2. Plan the number and size of RAID groups that you need for the size of the aggregate.

   Follow these guidelines:

   • RAID groups in the same aggregate should be the same size with the same number of LUNs in each RAID group. For example, you should create four RAID groups of 8 LUNs each, not three RAID groups of 8 LUNs and one RAID group of 6 LUNs.

   • Use the default RAID group size for array LUNs, if possible. The default RAID group size is adequate for most organizations.

      **Note:** The default RAID group size is different for array LUNs and disks.

3. Plan the size of the LUNs that you need in your RAID groups.

   • To avoid a performance penalty, all array LUNs in a particular RAID group should be the same size.

   • The LUNs should be the same size in all RAID groups in the aggregate.

4. Ask the storage array administrator to create the number of LUNs of the size you need for the aggregate.
The LUNs should be optimized for performance, according to the instructions in the storage array vendor documentation.

5. Create all the RAID groups in the aggregate at the same time.

   **Note:** Do not mix array LUNs from storage arrays with different characteristics in the same Data ONTAP RAID group.

   **Note:** If you create a new RAID group for an existing aggregate, be sure that the new RAID group is the same size as the other RAID groups in the aggregate, and that the array LUNs are the same size as the LUNs in the other RAID groups in the aggregate.

### How Data ONTAP works with hot spare disks

A hot spare disk is a disk that is assigned to a storage system but is not in use by a RAID group. It does not yet hold data but is ready for use. If a disk failure occurs within a RAID group, Data ONTAP automatically assigns hot spare disks to RAID groups to replace the failed disks.

**Next topics**

- How many hot spares you should have on page 86
- What disks can be used as hot spares on page 86
- What a matching spare is on page 87
- What an appropriate hot spare is on page 87
- About degraded mode on page 87

### How many hot spares you should have

At a minimum, you should have at least one matching or appropriate hot spare available for each kind of disk installed in your storage system. However, having two available hot spares for all disks provides the best protection against disk failure.

Having at least two available hot spares for all disks provides the following benefits:

- At least two hot spares must be available in order to put a disk into the maintenance center.
- Having two hot spares means that when a disk fails, you still have a spare available if another disk fails before you replace the first failed disk.

   **Note:** One disk can be the hot spare for multiple disks.

### What disks can be used as hot spares

A disk must conform to certain criteria to be used as a hot spare for a particular data disk.

For a disk to be used as a hot spare for another disk, it must conform to the following criteria:

- It must be either an exact match for the disk it is replacing or an appropriate alternative.
- The spare must be owned by the same system as the disk it is replacing.
What a matching spare is
A matching hot spare exactly matches a data disk for several characteristics.

A matching spare is a disk that exactly matches a data disk for all of the following criteria:

- Type (FC, SAS, ATA, BSAS, SSD, or SATA)
  
  **Note:** On systems with the `raid.disktype.enable` option set to `off`, FC and SAS disks are considered to be the same type and SATA, ATA, and BSAS disks are considered to be the same type.

- Size
- Speed (RPM)
- Checksum type (BCS or ZCS)

What an appropriate hot spare is
If a disk fails and no hot spare disk that exactly matches the failed disk is available, Data ONTAP uses the best available spare.

Data ONTAP picks a non-matching hot spare based on the following criteria:

- If the available hot spares are not the correct size, Data ONTAP uses one that is the next size up if possible.
  
  **Note:** The replacement disk is downsized to match the size of the disk it is replacing; the extra capacity is not available.

- If the hot spares are not the correct speed, Data ONTAP uses one that is a different speed.
  
  **Note:** Using drives with different speeds within the same aggregate is not optimal. Replacing a disk with a slower disk can cause performance degradation, and replacing with a faster disk is not a cost-effective solution.

- The hot spare must be of the same disk type (FC, SAS, and so on) as the failed disk, or of a type that is considered to be equivalent.

- If the hot spares are ZCS disks, they can be added only to zoned checksum aggregates. ZCS disks cannot be added to block checksum aggregates.

About degraded mode
When a disk fails, Data ONTAP can continue to serve data, but it must reconstruct the data from the failed disk using RAID parity. When this happens, the affected RAID group is said to be in **degraded mode**. The performance of a storage system with one or more RAID groups in degraded mode is decreased.

A RAID group goes into degraded mode in the following scenarios:

- A single disk fails in a RAID4 group.
  
  After the failed disk is reconstructed to a spare, the RAID group returns to normal mode.

- One or two disks fail in a RAID-DP group.
If two disks have failed in a RAID-DP group, the RAID group goes into \textit{double-degraded mode}.

- A disk in a RAID4 group is taken offline by Data ONTAP. After the offline disk is brought back online, the RAID group returns to normal mode.

\textbf{Note:} If another disk fails in a RAID-DP group in double-degraded mode or a RAID4 group in degraded mode, data loss could occur (unless the data is mirrored). For this reason, always minimize the amount of time a RAID group is in degraded mode by ensuring that appropriate hot spares are available.

\section*{How Data ONTAP handles a failed disk with a hot spare}

Using an available matching hot spare, Data ONTAP can use RAID to reconstruct the missing data from the failed disk onto the hot spare disk with no data service interruption.

If a disk fails and a matching or appropriate spare is available, Data ONTAP performs the following tasks:

- Replaces the failed disk with a hot spare disk. If RAID-DP is enabled and double-disk failure occurs in the RAID group, Data ONTAP replaces each failed disk with a separate spare disk.
- In the background, reconstructs the missing data onto the hot spare disk or disks.
  
  \textbf{Note:} During reconstruction, the system is in degraded mode, and file service might slow down.

  - Logs the activity to the event log, which you can view by using the \texttt{event log show} command.
  - Sends an AutoSupport message.

\textbf{Attention:} After Data ONTAP is finished reconstructing data, replace the failed disk or disks with new hot spare disks as soon as possible, so that hot spare disks are always available in the storage system.

\textbf{Note:} If the available spare disks are not the correct size, Data ONTAP chooses a disk of the next larger size and restricts its capacity to match the size of the disk it is replacing.

\section*{How Data ONTAP handles a failed disk that has no available hot spare}

When a failed disk has no appropriate hot spare available, Data ONTAP puts the affected RAID group into degraded mode indefinitely and the storage system automatically shuts down within a specified time period.

If the maximum number of disks have failed in a RAID group (two for RAID-DP, one for RAID4), the storage system automatically shuts down in the period of time specified by the \texttt{raid.timeout} option. The default timeout value is 24 hours.
To ensure that you are aware of the situation, Data ONTAP sends an AutoSupport message whenever a disk fails. In addition, it logs a warning message to the event log once per hour after a disk fails.

**Attention:** If a disk fails and no hot spare disk is available, contact technical support.

**How RAID-level disk scrubs verify data integrity**

RAID-level scrubbing means checking the disk blocks of all disks in use in aggregates (or in a particular aggregate, plex, or RAID group) for media errors and parity consistency. If Data ONTAP finds media errors or inconsistencies, it uses RAID to reconstruct the data from other disks and rewrites the data.

RAID-level scrubs help improve data availability by uncovering and fixing media and checksum errors while the RAID group is in a normal state (for RAID-DP, RAID-level scrubs can also be performed when the RAID group has a single-disk failure).

RAID-level scrubs can be scheduled or run manually.
Controlling the impact of RAID operations on system performance

You can reduce the impact of RAID operations on system performance by decreasing the speed of RAID operations.

About this task

You can control the speed of the following RAID operations with RAID options:

- RAID data reconstruction
- Disk scrubbing
- Plex resynchronization
- Synchronous mirror verification

The speed that you select for each of these operations might affect the overall performance of the storage system. However, if the operation is already running at the maximum speed possible and it is fully utilizing one of the three system resources (the CPU, disks, or the disk-to-controller connection bandwidth), changing the speed of the operation has no effect on the performance of the operation or the storage system.

If the operation is not yet running, you can set a speed that minimally slows storage system network operations or a speed that severely slows storage system network operations. For each operation, use the following guidelines:

- If you want to reduce the performance impact on client access to the storage system, change the specific RAID option from medium to low. Doing so also causes the operation to slow down.
- If you want to speed up the operation, change the RAID option from medium to high. Doing so might decrease the performance of the storage system in response to client access.

Next topics

Controlling the performance impact of RAID data reconstruction on page 92
Controlling the performance impact of RAID-level scrubbing on page 93
Controlling the performance impact of RAID data reconstruction

Because RAID data reconstruction consumes CPU resources, increasing the speed of data reconstruction sometimes slows storage system network and disk operations. You can control the speed of data reconstruction with the `raid.reconstruct.perf_impact` option.

About this task

When RAID data reconstruction and plex resynchronization are running at the same time, Data ONTAP limits the combined resource utilization to the greater impact set by either operation. For example, if `raid.resync.perf_impact` is set to `medium` and `raid.reconstruct.perf_impact` is set to `low`, the resource utilization of both operations has a medium impact.

These options are available through the nodeshell. For more information about the nodeshell, see the information about the `system node run` command in the Data ONTAP Cluster-Mode Administration Reference.

Step

1. Enter the following command:

   ```
   options raid.reconstruct.perf_impact impact
   ```

   `impact` can be `high`, `medium`, or `low`.

   high means that the storage system uses most of the system resources—CPU time, disks, and disk-to-controller bandwidth—available for RAID data reconstruction; this setting can heavily affect storage system performance. However, reconstruction finishes faster, reducing the time that the storage system is running in degraded mode.

   low means that the storage system uses very little of the system resources; this setting lightly affects storage system performance. However, reconstruction takes more time to complete, increasing the time that the storage system is running in degraded mode.

   The default speed is `medium`.

   **Note:** The setting for this option also controls the speed of Rapid RAID recovery.
Controlling the performance impact of RAID-level scrubbing

When Data ONTAP performs a RAID-level scrub, it checks the disk blocks of all disks on the storage system for media errors and parity consistency. You can control the impact this operation has on system performance with the `raid.verify.perf_impact` option.

**About this task**

When RAID-level scrubbing and mirror verification are running at the same time, Data ONTAP limits the combined resource utilization to the greater impact set by either operation. For example, if `raid.verify.perf_impact` is set to medium and `raid.scrub.perf_impact` is set to low, the resource utilization by both operations has a medium impact.

**Note:** If there are times during the day where the load on your storage system is decreased, you can also limit the performance impact of the automatic RAID-level scrub by changing the start time or duration of the automatic scrub.

These options are available through the nodeshell. For more information about the nodeshell, see the information about the `system node run` command in the *Data ONTAP Cluster-Mode Administration Reference*.

**Step**

1. Enter the following command:

   ```
   options raid.scrub.perf_impact impact
   ```

   `impact` can be high, medium, or low.

   **high** means that the storage system uses most of the system resources—CPU time, disks, and disk-to-controller bandwidth—available for scrubbing; this setting can heavily affect storage system performance, but the scrub will complete in less time.

   **low** means that the storage system uses very little of the system resources; this setting lightly affects storage system performance, and the scrub will take longer to complete.

   The default value for `impact` is **low**.
How you use aggregates to provide storage to your volumes

To support the differing security, backup, performance, and data sharing needs of your users, you group the physical data storage resources on your storage system into one or more aggregates. These aggregates provide storage to the volume or volumes that they contain.

Each aggregate has its own RAID configuration, plex structure, and set of assigned disks or array LUNs. You create an aggregate to hold one or more FlexVol volumes—the logical file systems that share the physical storage resources, RAID configuration, and plex structure of that common containing aggregate.

Aggregates can be mirrored or unmirrored. An unmirrored aggregate has only one plex; a mirrored aggregates have two plexes. For Data ONTAP 8 Cluster-Mode, only unmirrored aggregates are supported at this time.


Next topics

*Aggregate types* on page 95
*How unmirrored aggregates work* on page 96
*Rules for mixing disk types in aggregates* on page 97
*Rules for mixing array LUNs in an aggregate* on page 98
*Checksum rules for adding storage to an aggregate* on page 99
*What happens when you add larger disks to an aggregate* on page 100

Related information

*TR 3437: Storage Best Practices and Resiliency Guide*

Aggregate types

Starting with Data ONTAP 8.0, you can create aggregates that are either 32-bit or 64-bit. 32-bit and 64-bit aggregates can coexist on the same storage system.

The following list outlines the differences between the two types of aggregates:

- 32-bit aggregates have a maximum size of 16 TB, while 64-bit aggregates have a maximum size of up to 100 TB, depending on the storage system model.
- FlexVol volumes contained by 32-bit aggregates are called 32-bit volumes, while FlexVol volumes contained by 64-bit aggregates are called 64-bit volumes.
You decide the type of an aggregate when you create it. You cannot change the type of an aggregate after it is created.

All aggregates created using versions of Data ONTAP earlier than 8.0 are 32-bit aggregates.

You can determine whether an aggregate is a 32-bit aggregate or a 64-bit aggregate by using the `aggr status` command.

**How unmirrored aggregates work**

Unmirrored aggregates have a single copy of their data, or *plex*, which contains all of the RAID groups belonging to that aggregate. Mirrored aggregates are not currently supported in Data ONTAP Cluster-Mode.

The following diagram shows an unmirrored aggregate with disks, with its one plex.

![Diagram of an unmirrored aggregate with disks and its plex]

The following diagram shows an unmirrored aggregate with array LUNs, with its one plex.
Rules for mixing disk types in aggregates

You can mix disks from different loops or stacks within the same aggregate. Depending on the value of the `raid.disktype.enable` option, you might be able to mix certain types of disks within the same aggregate.

The following table shows what types of disks can be mixed within an aggregate when the `raid.disktype.enable` option is set to off:

<table>
<thead>
<tr>
<th></th>
<th>SAS disks in DS4243 disk shelves</th>
<th>SATA disks in DS4243 disk shelves</th>
<th>FC disks in DS14mk2 FC or DS14mk4 FC disk shelves</th>
<th>ATA disks in DS14mk2 FC or DS14mk4 FC disk shelves</th>
<th>SSDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal SAS disks</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Internal SATA disks</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>SAS disks in DS4243 disk shelves</td>
<td>Y</td>
<td>N</td>
<td>Y*</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>SATA disks in DS4243 disk shelves</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y*</td>
<td>N</td>
</tr>
</tbody>
</table>
FC disks in DS14mk2 FC or DS14mk4 FC disk shelves | Y* | N | Y | N | N
ATA disks in DS14mk2 FC or DS14mk4 FC disk shelves | N | Y* | N | Y | N
SSDs | N | N | N | N | Y

*Data ONTAP does not prevent these combinations. However, due to the large difference in performance between the two disk types, you should avoid these combinations.

BSAS disks are considered to be the same as SATA disks in this table.

SAS and SATA disks are not allowed in the same aggregate.

If the raid.disktype.enable option is set to on, all aggregates must contain disks of a single type.

Note: If you set the raid.disktype.enable option to on for a system that already contains aggregates with disks of mixed type, those mixed aggregates continue to function normally and accept both types of disks. However, no other aggregates will accept mixed disk types as long as the raid.disktype.enable option is set to on.

For information about best practices for working with different types of disks, see Technical Report 3437: Storage Best Practices and Resiliency Guide.

Related information

_TR 3437: Storage Best Practices and Resiliency Guide_

Rules for mixing array LUNs in an aggregate

Data ONTAP does not support mixing different types of storage in the same aggregate because it causes performance degradation.

There are restrictions on the types of array LUNs that you can mix in the same aggregate, which you must observe when you add array LUNs to an aggregate. Data ONTAP does not prevent you from mixing different types of array LUNs.

Note: Data ONTAP prevents you from mixing native disks and array LUNs in the same aggregate.

For aggregates for third-party storage, you cannot mix the following storage types in the same aggregate:
- Array LUNs from storage arrays from different vendors
- Array LUNs from storage arrays from the same vendor but from different storage array families

**Note:** Storage arrays in the same family share the same characteristics---for example, the same performance characteristics. See the V-Series implementation guide for your vendor for information about how Data ONTAP defines family members for the vendor.

- Array LUNs from storage arrays with 4-Gb HBAs and array LUNs from storage arrays with 2-Gb HBAs
- Array LUNs from Fibre Channel and SATA drives

You can deploy Fibre Channel and SATA drives behind the same V-Series system. However, you cannot mix array LUNs from SATA disks and Fibre Channel disks in the same aggregate, even if they are from the same series and the same vendor. Before setting up this type of configuration, consult your authorized reseller to plan the best implementation for your environment.

### Checksum rules for adding storage to an aggregate

If you have disks or array LUNs of both checksum types (blocks and zoned) in your storage system, you must follow the checksum type rules when you add storage to an aggregate.

Data ONTAP enforces the following rules when creating aggregates or adding storage to existing aggregates:

- An aggregate can have only one checksum type, and it applies to the entire aggregate.
- To use block checksum storage when you create a new aggregate, you must have at least the number of block checksum spare disks or array LUNs available that you specified in the `aggr create` command.
- When you add storage to an existing aggregate, the following rules apply:
  - You can add block checksum storage to either a block checksum aggregate or a zoned checksum aggregate.
  - You cannot add zoned checksum storage to a block checksum aggregate.

The following table shows the types of storage that you can add to an existing aggregate of each type.

<table>
<thead>
<tr>
<th>Storage checksum type</th>
<th>Block checksum aggregate</th>
<th>Zoned checksum aggregate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block checksum</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Zoned checksum</td>
<td>Not allowed</td>
<td>OK</td>
</tr>
</tbody>
</table>
What happens when you add larger disks to an aggregate

What Data ONTAP does when you add disks to an aggregate that are larger than the existing disks depends on the RAID level (RAID4 or RAID-DP) of the aggregate.

- When an aggregate configured for RAID4 protection is created, Data ONTAP assigns the role of parity disk to the largest disk in each RAID group. When an existing RAID4 group is assigned an additional disk that is larger than the group’s existing parity disk, then Data ONTAP reassigns the new disk as parity disk for that RAID group.
- When an aggregate configured for RAID-DP protection is created, Data ONTAP assigns the role of dParity disk and regular parity disk to the largest and second largest disk in the RAID group. When an existing RAID-DP group is assigned an additional disk that is larger than the group’s existing dParity disk, then Data ONTAP reassigns the new disk as the regular parity disk for that RAID group and restricts its capacity to be the same size as the existing dParity disk. Note that Data ONTAP does not replace the existing dParity disk, even if the new disk is larger than the dParity disk.

**Note:** Because the smallest parity disk limits the effective size of disks added to a RAID-DP group, you can maximize available disk space by ensuring that the regular parity disk is as large as the dParity disk.

**Note:** If needed, you can replace a capacity-restricted disk with a more suitable (smaller) disk later, to avoid wasting disk space. However, replacing a disk already in use in an aggregate with a larger disk does not result in any additional usable disk space; the new disk is capacity-restricted to be the same size as the smaller disk it replaced.
Aggregate management

This section describes the tasks you can perform to manage aggregates.

Next topics

Creating an aggregate on page 101
Displaying information about aggregates on page 102
Adding disks to an aggregate on page 104
Modifying an aggregate on page 104
Renaming an aggregate on page 105
Scrubbing an aggregate for errors on page 105
Deleting an aggregate on page 106

Creating an aggregate

You can create an aggregate to hold volumes.

About this task

A 32-bit aggregate can grow to a maximum of 16 TB and contains FlexVol volumes that are called 32-bit volumes. All aggregates created by using Data ONTAP 8.0 and earlier are 32-bit aggregates. A 64-bit aggregate's maximum size, up to 100 TB, depends on your storage system model. FlexVol volumes contained by 64-bit aggregates are called 64-bit volumes. If you create an aggregate without using this parameter, a 32-bit aggregate is created by default. You cannot modify the block type of an aggregate after it is created.

Step

1. Use the storage aggregate create command to create an aggregate.

When you create an aggregate, you specify a name for the aggregate and the number of disks or array LUNs to be added to the aggregate. If the RAID type of the aggregate you are creating is RAID 4, a minimum of two disks is required. If the RAID type of the aggregate is RAID-DP, a minimum of three disks is required.

In addition, you can optionally specify the:

- aggregate's home node (that is, the node on which the aggregate is located unless the aggregate fails over to the node's storage failover partner)
- list of specific disks or array LUNs that are to be added to the aggregate
- the RAID type for RAID groups on the aggregate
- maximum number of disks or array LUNs that can be included in a RAID group
- volume style
- whether disks with different RPM are allowed
- block type (32-bit or 64-bit to contain 32-bit or 64-bit FlexVol volumes, respectively)

**Note:** If you create 64-bit aggregates and volumes by using Data ONTAP 8.0.1 Cluster-Mode, you cannot revert to Data ONTAP 8.0 Cluster-Mode.

**Example**
The following example creates an aggregate named aggr2 on a home node named node1b. The aggregate includes 30 disks and uses RAID-DP. The maximum number of disks in a RAID group on the aggregate is 10, and disk with different RPM are allowed. The aggregate contains FlexVol volumes that are 32-bit volumes.

```
node::> storage aggregate create -aggregate aggr2 -node node1b
   -diskcount 30 -raidtype raid_dp -maxraidsize 10 -allow-mixed true -
   block-type 32-bit
```

### Displaying information about aggregates

You can display information about aggregates.

**Step**

1. Use the `storage aggregate show` command to display information about aggregates.

By default, the command displays the following information about all aggregates:

- Aggregate name
- Size
- Available size
- Percentage used
- State (creating, failed, offline, online, partial, restrict, or unknown)
- Number of volumes
- Node or nodes on which the aggregate is located
- RAID status

Other information is displayed in a detailed view and if other parameters are specified. See the reference page for the command for details.

**Example**
The following example displays information about all aggregates.

```
node::> storage aggregate show
Aggregate   Size   Available  Used%  State     #Vols  Nodes      RAID Status
----------   ------  ---------  -----  -------   -----  ----------  ---------------
aggr0       6.21TB  1.78TB    71%   online  49 node0      raid_dp
aggr1       6.65TB  6.42TB    3%    online  4 node1      raid_dp
```
Aggregates can be in one of several states. You can determine an aggregate's state by using the `storage aggregate show` command.

The following table displays the possible states for aggregates.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>online</td>
<td>Read and write access to volumes hosted on this aggregate is allowed.</td>
</tr>
<tr>
<td>creating</td>
<td>The aggregate is being created.</td>
</tr>
<tr>
<td>mounting</td>
<td>The aggregate is being mounted.</td>
</tr>
<tr>
<td>quiesced</td>
<td>The aggregate is quiesced.</td>
</tr>
<tr>
<td>quiescing</td>
<td>The aggregate is being quiesced.</td>
</tr>
<tr>
<td>unmounted</td>
<td>The aggregate is offline.</td>
</tr>
<tr>
<td>unmounting</td>
<td>The aggregate is being taken offline.</td>
</tr>
<tr>
<td>destroying</td>
<td>The aggregate is being destroyed.</td>
</tr>
<tr>
<td>partial</td>
<td>At least one disk was found for the aggregate, but two or more disks are</td>
</tr>
<tr>
<td></td>
<td>missing.</td>
</tr>
<tr>
<td>frozen</td>
<td>The aggregate is (temporarily) not serving requests.</td>
</tr>
<tr>
<td>reverted</td>
<td>The revert of an aggregate is completed.</td>
</tr>
<tr>
<td>restricted</td>
<td>Some operations, such as parity reconstruction, are allowed, but data</td>
</tr>
<tr>
<td></td>
<td>access is not allowed.</td>
</tr>
<tr>
<td>inconsistent</td>
<td>The aggregate has been marked corrupted; contact technical support.</td>
</tr>
<tr>
<td>iron_restricted</td>
<td>Diagnostic tools cannot be run on the aggregate.</td>
</tr>
<tr>
<td>unknown</td>
<td>The aggregate's state is not known.</td>
</tr>
<tr>
<td>offline</td>
<td>No access to the aggregate is allowed.</td>
</tr>
<tr>
<td>failed</td>
<td>The aggregate cannot be brought online.</td>
</tr>
</tbody>
</table>
Adding disks to an aggregate

You can add disks or array LUNs to an existing aggregate.

Step

1. Use the `storage aggregate add-disks` command to add disks or array LUNs to an aggregate.

   You must specify the number of disks or array LUNs that are to be added to the aggregate. You can optionally specify a list of specific disks or array LUNs that are to be added to the aggregate; the number of disks or array LUNs in the list must match the number of disks or array LUNs specified by the value of the `-diskcount` parameter. You can also optionally specify a RAID group to which to assign the disks or array LUNs and to allow disk types that have different RPM to be added.

   **Example**
   The following example adds 20 disks to an aggregate named aggr2.

```
node::> storage aggregate add-disks -aggregate aggr2 -diskcount 20
```

Modifying an aggregate

You can modify an existing aggregate.

Step

1. Use the `storage aggregate modify` command to modify the attributes of an aggregate:

   You can modify the following attributes:

   - **State**, which can be one of the following:
     - online—Immediately sets the aggregate online. All volumes on the aggregate are set to the state they were in when the aggregate was taken offline or restricted.
     - restrict—Restricts the aggregate. You cannot restrict an aggregate if any of its volumes are online. Administrative operations are permitted on a restricted aggregate, but data access is not enabled.
   - **RAID type**
   - **Maximum number of disks or array LUNs in a RAID group**
   - **HA policy**—This optionally specifies the high-availability policy to be used in the context of a root recovery procedure. Do not modify this setting unless directed to do so by a customer support representative.

   **Note:** To change an aggregate's name, use the `storage aggregate rename` command.
Example
The following example modifies all RAID groups on an aggregate named aggr1 to use RAID-DP and to have a maximum of 25 disks per RAID group.

node::> storage aggregate modify -aggregate aggr1 -raidtype raid_dp -maxraidsize 25

Related tasks
Renaming an aggregate on page 105

Renaming an aggregate
You can rename an aggregate.

Step
1. Use the `storage aggregate rename` command to rename an aggregate. The following example renames an aggregate named aggr2 to the name aggr3.

Example
node::> storage aggregate rename -aggregate aggr2 -newname aggr3

Related tasks
Modifying an aggregate on page 104

Scrubbing an aggregate for errors
You can scrub an aggregate to detect and fix parity errors on the aggregate.

Step
1. Use the `storage aggregate scrub` command to control the scrubbing of an aggregate for parity errors.

You can optionally specify a single RAID group to be scrubbed on the aggregate. The command enables you to start, stop, pause, restart, and display status information about scrubbing.

Example
The following examples start a scrub of a storage aggregate named aggr3.

node::> storage aggregate scrub -aggregate aggr3 -action start
Displaying status information about aggregate scrubs

You can display information about the status of aggregate scrubs.

**Step**

1. Use the `storage aggregate show-scrub-status` command to display status information about aggregate scrubs.

**Example**
The following example displays information about aggregate scrubs:

```
node::> storage aggregate show-scrub-status
```

<table>
<thead>
<tr>
<th>Aggregate</th>
<th>RAID Groups</th>
<th>Suspended?</th>
<th>Percentage</th>
<th>Last Scrub Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggr0</td>
<td>/aggr0/plex0/rg0</td>
<td>false</td>
<td></td>
<td>7/9/2006 02:32:51</td>
</tr>
<tr>
<td>aggr3</td>
<td>/aggr3/plex0/rg0</td>
<td>false</td>
<td>13</td>
<td>7/12/2006 01:46:21</td>
</tr>
</tbody>
</table>

Deleting an aggregate

You can delete an aggregate.

**Before you begin**

You must remove all volumes from an aggregate before you can delete it.

**Steps**

1. Use the `storage aggregate delete` command to delete an aggregate.

   The command fails if any volumes exist on the aggregate. The command prompts you for confirmation before running.

   **Example**
The following example deletes an aggregate named aggr3.

   ```
   node::> storage aggregate delete -aggregate aggr3
   WARNING: Are you sure you want to destroy this aggregate? (y or n): y
   ```

2. Use the `storage aggregate show` command to verify that the aggregate was deleted.
Storage failover management

The storage failover (SFO) commands allow you to manage HA pairs. An HA pair provides an additional level of security among nodes in an that data continues to be served in the event of a hardware failure and certain software failures such as panics.

Next topics

What an HA pair is on page 107
Benefits of HA pairs on page 107
Characteristics of nodes in an HA pair on page 108
Displaying information about an HA pair on page 109
Modifying an HA pair on page 110
Taking over partner node storage on page 111
Limitations on performing commands on the taken-over root aggregate on page 112
Giving back storage on page 112
Displaying information about mailbox disks on page 113
Displaying information about storage failover interconnections on page 114
Displaying internal options for storage failover configurations on page 114

What an HA pair is

An HA pair is two storage systems (nodes) whose controllers are connected to each other directly.

You can configure the HA pair so that each node in the pair shares access to a common set of storage, subnets, and tape drives, or each node can own its own distinct set of storage.

The nodes are connected to each other through an NVRAM adapter, or, in the case of systems with two controllers in a single chassis, through an internal interconnect. This allows one node to serve data that resides on the disks of its failed partner node. Each node continually monitors its partner, mirroring the data for each other’s nonvolatile memory (NVRAM or NVMEM).

Benefits of HA pairs

HA pairs provide fault tolerance and the ability to perform nondisruptive upgrades and maintenance.

Configuring storage systems in an HA pair provides the following benefits:

• Fault tolerance
  When one node fails or becomes impaired a takeover occurs, and the partner node continues to serve the failed node’s data.
• Nondisruptive software upgrades
  When you halt one node and allow takeover, the partner node continues to serve data for the
  halted node while you upgrade the node you halted.
  For more information about nondisruptive software upgrades, see the Data ONTAP 7-Mode
  Upgrade Guide.
• Nondisruptive hardware maintenance
  When you halt one node and allow takeover, the partner node continues to serve data for the
  halted node while you replace or repair hardware in the node you halted.

Characteristics of nodes in an HA pair

To configure and manage nodes in an HA pair, you should be familiar with the characteristics that all
 types of HA pairs have in common.
• They are connected to each other either through an HA interconnect consisting of adapters and
cable, or, in systems with two controllers in the same chassis, through an internal interconnect.
The nodes use the interconnect to do the following tasks:
  • Continually check whether the other node is functioning
  • Mirror log data for each other’s NVRAM
  • Synchronize each other’s time
• They use two or more disk shelf loops, or third-party storage, in which the following conditions
apply:
  • Each node manages its own disks or array LUNs.
  • Each node in takeover mode manages its partner’s disks or array LUNs. For third-party
    storage, the partner node takes over read/write access to the array LUNs owned by the failed
    node until the failed node becomes available again.
  
  Note: Disk ownership is established by Data ONTAP or the administrator, rather than by
which disk shelf the disk is attached to.
• They own their spare disks, spare array LUNs, or both and do not share them with the other node.
• They each have mailbox disks or array LUNs on the root volume:
  • Two if it is a FAS system.
  • One if it is a V-Series system.
The mailbox disks or LUNs are used to do the following tasks:
  • Maintain consistency between the pair
  • Continually check whether the other node is running or whether it has performed a takeover
  • Store configuration information that is not specific to any particular node
• They can reside on the same Windows domain or on different domains.
Displaying information about an HA pair

You can display information about an HA pair.

Step

1. Use the `storage failover show` command to display information about HA pairs.

   By default, the command displays the following information:

   - Node name.
   - Partner node name.
   - Whether storage failover is enabled.
   - Whether storage failover is possible.
   - Whether the storage failover interconnection is available.
   - The current state of storage failover. Possible values include the following:
     - connected
     - takeover
     - giveback_partial_waiting
     - giveback_partial_connected
     - waiting

   Other information is displayed in a detailed view and if other parameters are specified. See the reference page for the command for details.

Example

The following example displays information about all HA pairs.

```
ha40::storage failover> show
Takeover InterConn
Node    Partner      Enabled  Possible  Up        State
-------- --------- -------- -------- -------- ------------
ha40     ha41       true     true     true      connected
ha41     ha40       true     true     true      connected

ha40::storage failover> show
Takeover InterConn
Node    Partner      Enabled  Possible  Up        State
-------- --------- -------- -------- -------- ------------
ha40     ha41       true     false    false    takeover
```

Modifying an HA pair

You can modify an HA pair.

Step

1. Use the `storage failover modify` command to modify the HA attributes of a node in an HA pair.

You can use the command to modify the following attributes:

- Whether storage failover is enabled. The default is true.
- Whether automatic giveback operations are enabled. An automatic giveback operation is invoked when one filer in a failover pair is in takeover mode and the failed node is repaired and restarts. When the repaired node restarts, the node in takeover mode detects this and initiates a giveback operation. The default is false.
- Whether long-running jobs such as NDMP operations and volume operations are terminated when an automatic giveback operation is initiated. If this option is set to true (the default), the automatic giveback operation is deferred until the long-running jobs have completed.
- Whether the node checks its partner's readiness before initiating a giveback operation that was invoked by using the `storage failover giveback` command. The default is true, which reduces downtime caused by a giveback operation.
- The number of seconds that the node remains unresponsive before its partner initiates a takeover operation. The default is 15 seconds; possible values range from 10 to 180 seconds.
- Whether the node automatically takes over for its partner if the partner panics. The default is true. Setting this option on one node automatically makes the same setting on its partner node.
- Whether the node automatically takes over for its partner if the partner reboots. This automatic takeover, and the automatic giveback that follows after the reboot is complete, can reduce the outage during which the storage belonging to the rebooting system is unavailable. The default is true.
- Whether the node automatically takes over for its partner if the partner fails. The default is true. Setting this option requires the advanced privilege level or higher.
- Whether the node takes over for its partner if the partner fails within a default 60 seconds of starting up. The default is true. Setting this option requires the advanced privilege level or higher.
• The number of seconds, used by the previous option, before the node takes over for its partner if the partner fails within the specified number of seconds after starting up. The default is 60 seconds. Setting this option requires the advanced privilege level or higher.

• The number of seconds after takeover before the node attempts automatic giveback operations. The default value is 300; possible values range from 0 to 600 seconds. Setting this option requires the advanced privilege level or higher.

• The number of times the node attempts an automatic giveback operation within a default 10 minutes. The default value is three attempts. Setting this option requires the advanced privilege level or higher.

• The number of minutes, used by the previous option, during which the node attempts automatic giveback operations. The default value is 10 minutes. Setting this option requires the advanced privilege level or higher.

• Whether storage failover status is propagated via mailbox disks. The default is true. Setting this option requires the advanced privilege level or higher.

• How frequently the node reads its partner's status from the mailbox disks. The default is five seconds. Setting this option requires the advanced privilege level or higher.

• How frequently the node writes its status to the mailbox disks. The default is five seconds. Setting this option requires the advanced privilege level or higher.

Example
The following example enables the storage failover service, automatic giveback operations, and partner-readiness checks on a node named node1b.

```
node::> storage failover modify -node node1b -enabled true
      -auto-giveback true -check-partner true
```

Related tasks

*Giving back storage* on page 112

Taking over partner node storage

You can initiate a takeover of a partner node's storage in an HA pair.

Step

1. Use the `storage failover takeover` command to initiate a takeover of the partner node's storage.

When you run the command, specify the name of the node that is taking over the partner's storage, not the name of the partner. You can optionally specify the style of takeover operation; possible styles include the following:

• normal—Specifies a normal takeover operation; that is, the partner is given the time to close its storage resources gracefully before the takeover operation proceeds. This is the default value.
- **Immediate**—Specifies an immediate takeover. In an immediate takeover, the takeover operation is initiated before the partner is given the time to close its storage resources gracefully.
- **Allow-Version-Mismatch**—If this value is specified, the takeover operation is initiated even if the partner is running a version of Data ONTAP that is incompatible with the version running on the node. In this case, the partner must be cleanly halted. Use this value as part of a non-disruptive upgrade procedure.
- **Force**—If this value is specified, the takeover operation is initiated even if the node detects an error that normally prevents a takeover operation from occurring. Setting this option requires the advanced privilege level or higher.

**Note:** Regardless of the takeover style you specify, it is important to not interrupt the takeover operation. For example, attempting to restart the system during takeover can cause one of the filers in a failover pair to panic.

**Example**
The following example causes a node named node1b to initiate an immediate takeover of its partner's storage.

```
node::> storage failover takeover -bynode node1b -option immediate
```

In this example, the failover partner of node1b restarts and waits for a giveback operation to occur.

**Limitations on performing commands on the taken-over root aggregate**

Aside from the `storage aggregate` command, you cannot issue any `storage aggregate` commands on the partner node's root aggregate while the partner is taken over. You can, however, use the `partner aggr` command in the nodeshell to perform such operations.

**Note:** You cannot rename the partner's root aggregate while the partner is taken over.

For more information about the nodeshell, see the information about the `system node run` command in the *Data ONTAP Cluster-Mode Administration Reference*.

**Giving back storage**

You can return storage that has failed over to a node's partner back to the home node.

**Step**

1. Use the `storage failover giveback` command to return storage that has failed over to a node's partner back to the home node.
The root aggregate is given back at the start of the giveback operation (as it is required for the taken over system to boot). The other aggregates are given back one at a time after the taken over node completes booting up.

The command fails if other resource-intensive operations (for example, system dumps) are running, thereby making the giveback operation potentially dangerous or disruptive. When you run the command, specify the name of the node that currently holds the storage, not the node to which the storage is being returned.

You can specify options to control whether or not:

- Storage is given back only if the partner is available to take back the storage. The default is true, so that if the partner is not available to take back its storage, the storage failover giveback command fails.
- The system overrides partner veto votes during a giveback operation. The default is false.

**Example**
The following example gives back storage that is currently held by a node named node1b. The partner must be available for the giveback operation to occur.

```
node::> storage failover giveback -fromnode node1b -require-partner-waiting true
```

**Related tasks**

*Modifying an HA pair* on page 110

**Displaying information about mailbox disks**

Storage failover uses mailbox disks to communicate status between the nodes in an HA pair. You can display information about mailbox disks.

**Step**

1. Use the `storage failover mailbox-disk show` command to display information about mailbox disks.

   This information is not useful for the daily administration; use it only with the advice of support personnel. The command requires the advanced privilege level or higher.
Displaying information about storage failover interconnections

Storage failover operations occur over an Infiniband interconnection between the nodes of an HA pair. You can display the status of the interconnection.

Step

1. Use one or more of the following commands to display the status of SFO interconnections.

   These commands are available only at the advanced privilege level. Use the commands only with the advice of support personnel. For detailed information about these commands, see the reference pages.

   • `storage failover interconnect link`—Displays information about the interconnection link.
   • `storage failover interconnect queue`—Displays information about the interconnection's send and receive queues.
   • `storage failover interconnect status`—Displays the state of the interconnection and any active logical links
   • `storage failover interconnect statistics performance basic`—Displays basic performance statistics for the interconnection
   • `storage failover interconnect statistics performance per-interface`—Displays performance statistics for the interconnection on a per-interface basis

   Example

   The following example displays information about the interconnection link:

   ```
   node::*> storage failover interconnect link
   ```

Displaying internal options for storage failover configurations

You can display information about the internal options used by HA pairs.

Step

1. Use the `storage failover internal-options show` command to display information about HA pairs' internal options.

   Depending on the parameters specified with it, the command displays some or all of the following information. See the reference for the command for details. The command is available only at the advanced privilege level or higher.
- Node name
- Whether automatic giveback is enabled
- Whether partner checking is enabled
- Takeover detection time, in seconds
- Whether takeover on failover is enabled
- Whether takeover on panic is enabled
- Whether takeover on reboot is enabled
- Whether storage failover occurs when all cluster ports are down (detailed view only)
- Interval before storage failover when all cluster ports are down (detailed view only)
- Automatic giveback delay time, in seconds (detailed view only)
- Whether takeover on short uptime is enabled (detailed view only)
- Short uptime interval, in seconds (detailed view only)
- Number of giveback attempts (detailed view only)
- Giveback attempt interval, in minutes (detailed view only)
- Whether status is propagated through SFO mailboxes (detailed view only)
- Status read interval, in seconds (detailed view only)
- Status write interval, in seconds (detailed view only)

**Example**
The following example displays general information about internal options on all HA pairs:

```bash
node:*> storage failover internal-options show

<table>
<thead>
<tr>
<th>Node</th>
<th>Auto Giveback</th>
<th>Check Partner</th>
<th>Detection Time (secs)</th>
<th>Takeover On Failure</th>
<th>Takeover On Panic</th>
<th>Takeover On Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>node12</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node13</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node14</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node15</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node16</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node17</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node18</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node19</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node20</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node21</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node22</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node23</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node24</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node25</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node26</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node27</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node28</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node29</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>node30</td>
<td>true</td>
<td>true</td>
<td>15</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
</tbody>
</table>

16 entries were displayed.
Multipath Storage concepts

Multipath Storage provides redundancy for the path from each node to every disk shelf in the HA pair.

An HA pair without Multipath Storage has only one path from each node to every disk, but an HA pair with Multipath Storage has two paths from each node to each disk, regardless of which node owns the disk.

By providing two paths from each controller to every disk shelf, Multipath Storage provides the following advantages:

• The loss of a disk shelf module, connection, or host bus adapter (HBA) does not require a failover. The same storage system can continue to access the data by using the redundant path.
• The loss of a single disk shelf module, connection, or HBA does not prevent a successful failover. The takeover node can access its partner’s disks by using the redundant path.
• You can replace modules without having to initiate a failover.

Multipath Storage for HA pairs requires twice as many Fibre Channel ports. Without Multipath Storage, you need one Fibre Channel port for each node for each loop in the configuration. With Multipath Storage, you need two Fibre Channel ports for each loop.

**Note:** Multipath Storage is for use with native disks only. You cannot use Multipath Storage with third-party storage attached to a V-Series system.

For maximum protection, cable all loops for Multipath Storage. If any loop in your SFO configuration is cabled for Multipath Storage, cable every loop for Multipath Storage. This is the recommended best practice.

**Next topics**

*Boot environment variable requirement for V-Series systems* on page 117
*About redundant pathing* on page 118
*Determining Multipath Storage pathing* on page 118
*Cabling for Multipath Storage* on page 120
*Adding storage to a Multipath Storage configuration* on page 121

**Boot environment variable requirement for V-Series systems**

The `fc-nonarray-adapter-list` environment variable is required if you want to use Multipath Storage with native disks connected to V-Series systems.
To use Multipath Storage with native disks connected to a V-Series system, you must configure the fc-nonarray-adapter-list environment variable for each new loop before you connect and configure the disk shelf for Multipath Storage.

See the V-Series Systems Implementation Guide for Native Disk Shelves for details about using native disk shelves with V-Series systems.

About redundant pathing

HA pairs that use Multipath Storage are redundant-path configurations.

Some HA pairs have two paths from each controller to each of their disk shelves; this configuration is called a redundant-path or multipath configuration. HA pairs that use Multipath Storage are redundant-path configurations.

If you want to remove a module from your HA pair, you need to know whether the path you will disrupt is redundant. If it is, you can remove the module without interfering with the storage system’s ability to serve data. On the other hand, if that module provides the only path to any of the disks in your HA pair, you must take action to ensure that you do not incur system downtime.

Determining Multipath Storage pathing

You can determine whether any module in your system provides the only path to any disk.

Step

1. Use the storage disk show -port command to display pathing information for all disks in the HA pair.

   The command displays the following information:

   - Primary port
   - Secondary port
   - Disk shelf
   - Bay

Example

The following example displays information about all disk paths in a redundant-path HA pair.

```
node::> storage disk show -port

<table>
<thead>
<tr>
<th>Primary</th>
<th>Port</th>
<th>Secondary</th>
<th>Port</th>
<th>Type</th>
<th>Shelf</th>
<th>Bay</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1a:0a.16</td>
<td>A</td>
<td>node1a:0d.16</td>
<td>B</td>
<td>FCAL</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>node1a:0a.18</td>
<td>A</td>
<td>node1a:0d.18</td>
<td>B</td>
<td>FCAL</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>node1a:0a.19</td>
<td>A</td>
<td>node1a:0d.19</td>
<td>B</td>
<td>FCAL</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>node1a:0a.21</td>
<td>A</td>
<td>node1a:0d.21</td>
<td>B</td>
<td>FCAL</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>node1a:0a.22</td>
<td>A</td>
<td>node1a:0d.22</td>
<td>B</td>
<td>FCAL</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>node1a:0a.23</td>
<td>A</td>
<td>node1a:0d.23</td>
<td>B</td>
<td>FCAL</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>node1a:0a.25</td>
<td>A</td>
<td>node1a:0d.25</td>
<td>B</td>
<td>FCAL</td>
<td>1</td>
<td>9</td>
</tr>
</tbody>
</table>
```
Notice that every disk has two ports active: one for A and one for B (for example, 0a.16/0d.16). The presence of the redundant path means that you do not need to fail over one system before removing modules from the system.

**Caution:** When examining the command output, ensure that every disk has two paths. Even in an HA pair that uses redundant paths, a hardware or configuration problem can cause one or more disks to have only one path. If any disk in the HA pair has only one path, you must treat its loop as if it were in a single-path HA pair when removing modules.

**Note:** Disk names reported by `storage disk show` are based on the primary path. On a single-path system, if a loop is re-connected to a different HBA, then names of the disks connected on that loop change as the primary path changes. On a Multipath Storage system, the primary path and hence the disk name may change due to path failure or load balancing.

**Example**
The following example displays information about all disk paths in an HA pair that does not use redundant paths.

```
node2a:0a.16 A - Port Secondary Type Shelf Bay
node2a:0a.17 A - - FCAL 1 0
node2a:0a.18 A - - FCAL 1 1
node2a:0a.19 A - - FCAL 1 2
node2a:0a.20 A - - FCAL 1 3
node2a:0a.21 A - - FCAL 1 4
node2a:0a.22 A - - FCAL 1 5
node2a:0a.23 A - - FCAL 1 6
node2a:0a.24 A - - FCAL 1 7
node2a:0a.25 A - - FCAL 1 8
node2a:0a.26 A - - FCAL 1 9
node2a:0a.27 A - - FCAL 1 10
node2a:0a.28 A - - FCAL 1 11
node2a:0a.29 A - - FCAL 1 12
node2a:0a.30 A - - FCAL 1 13
node2a:0b.16 B - - FCAL 1 0
node2a:0b.17 B - - FCAL 1 1
node2a:0b.18 B - - FCAL 1 2
node2a:0b.19 B - - FCAL 1 3
node2a:0b.20 B - - FCAL 1 4
node2a:0b.21 B - - FCAL 1 5
node2a:0b.22 B - - FCAL 1 6
node2a:0b.23 B - - FCAL 1 7
node2a:0b.24 B - - FCAL 1 8
```
For this HA pair, there is only one path to each disk. This means that you cannot remove a module from the configuration, thereby disabling that path, without first manually performing a storage-failover operation.

Use the following commands to display additional information about paths in the configuration:

- storage disk show -primaryport
- storage disk show -secondaryport
- storage disk show -instance

Cabling for Multipath Storage

You can cable an HA pair for Multipath Storage.

Before you begin

To use Multipath Storage on native disks connected to a V-Series system, you must configure the fc-non-array-adapter-list environment variable for each new loop before you connect and configure the disk shelf for Multipath Storage.

About this task

For instructions about connecting disk shelves, see the hardware documentation for your disk shelf. For detailed instructions about adding HBAs to your node, see the hardware documentation for your system model.

Steps

1. Display the current, nonredundant disk paths by entering the following command:
   
   storage disk show -port

2. Pick a loop on one node (Node 1) for Channel A (the cable is connected to the A port on the disk shelves), and trace the cables from the node to the last disk shelf in the loop.

   The last disk shelf has no cable connected to the Channel A Output port.

3. Use the correct cable type for a disk shelf-to-node connection to connect the Channel A Output port to a Fibre Channel port on the partner node (Node 2).

   When possible, do not connect the same HBA to both the primary and redundant path of the same loop. For example, if an HBA is connected to Channel B for a loop, do not use another port on
that HBA for the redundant connection for Channel A of that same loop. Otherwise, the failure of the HBA could prevent the controller from accessing that loop.

Adjacent pairs of on-board ports share hardware; consider them to be the same as a single HBA. For example, do not use port 0a and port 0b for the primary and redundant paths of the same loop.

4. From the same disk shelf, use the correct cable type for a disk shelf-to-node connection to connect the Channel B Output port to a Fibre Channel port on the first node (node 1).

5. Repeat Steps 3 and 4 for every loop connected to Node 1.

6. Repeat Steps 2 through 5 for Node 2.

   Ensure that there is a cable in every Input and Output port of each disk shelf.

7. Ensure that there are two paths listed for every disk in the output of the following command:

   `storage disk show -port`

**Adding storage to a Multipath Storage configuration**

You can add storage to an HA pair that uses Multipath Storage.

**Before you begin**

You must be using AT-FCX modules that support Multipath Storage.

**Steps**

1. *Determining whether your AT-FCX modules support Multipath Storage* on page 121

2. *Adding a disk shelf to a Multipath Storage configuration* on page 122

**Determining whether your AT-FCX modules support Multipath Storage**

To use an AT-FCX module with Multipath Storage for HA pairs, the module must be the right version.

**About this task**

Modules shipped prior to December 2005 do not support Multipath Storage for HA pairs. If you are unsure whether your module is the correct version, use the following procedure.

This procedure requires that you run the `fcadmin` command in the nodeshell. For more information about the nodeshell, see the information about the `system node run` command in the *Data ONTAP Cluster-Mode Administration Reference*.

**Steps**

1. Determine the disk address of the target SES device for the AT-FCX module by entering the following command:
**fcadmin device_map**

**Example**

```
node1> fcadmin device_map
Loop Map for channel 3b:
Translated Map: Port Count 17
 7 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61
Shelf mapping:
Shelf 3: 61 60 59 58 57 56 55 54 53 52 51 50 49 48
Target SES devices on this loop:
Shelf 3: 46 47
```

The device map is displayed, including the SES target device IDs.

2. Set the privilege level to advanced by entering the following command:

```
priv set advanced
```

3. Enter the following command:

```
fcadmin bridge cmd_cemi -d target_SES_device -c "cpld"
```

**Example**

```
node1*> fcadmin bridge cmd_cemi -d 3b.46 -c "cpld"
21h45m11s SelID:3(255).MA IMS601550001296 8b.03 pfuID=32
? RegisterCount: 20
Drive 00:80 Drive 01:80 Drive 02:80 Drive 03:80
Drive 04:80 Drive 05:80 Drive 06:00 Drive 07:80
Drive 08:80 Drive 09:80 Drive 10:80 Drive 11:80
Drive 12:80 Drive 13:80 Drive 14:00 Drive 15:80
HOST:20 HwId:0f SFP Reg2:52 SFP Reg1:22
Revision:24 MISC:00 0 8067:2c 1 8067:2e
Fan control:96 Controller:98 ThumbCtlrId:57 Fan status:00
PSU0:0e PSU1:0e Status:08 Control:2d
```

Several columns of information about the disk shelf are displayed.

4. Find the Revision value in the output of the fcadmin bridge command. If this value is 24 or higher, your AT-FCX module supports Multipath Storage for HA pairs.

5. Return the privilege level to administrative by entering the following command:

```
priv set
```

**Adding a disk shelf to a Multipath Storage configuration**

You can add storage to an HA pair that uses Multipath Storage.

**About this task**

For detailed instructions about connecting disk shelves, see the hardware documentation for your disk shelf.
Steps

1. Confirm that there are two paths to every disk by entering the following command:
   
   `storage disk show -port`

   **Note:** If there are not two paths listed for every disk, this procedure can potentially result in a data-service outage. Before proceeding, address any issues so that all paths are redundant.

2. Install the new disk shelf in your cabinet or equipment rack, as described in the *DiskShelf14, DiskShelf14mk2, or DiskShelf14mk4 FC Hardware Guide*.

3. Find the last disk shelf in the loop for which you want to add the new disk shelf.

   **Note:** The Channel A Output port of the last disk shelf in the loop is connected back to one of the controllers.

4. Disconnect the SFP and cable coming from the Channel A Output port of the last disk shelf.

   **Note:** Leave the other ends of the cable connected to the controller.

   **Note:** When you disconnect the cable from the disk shelf, the system displays messages about adapter resets and eventually indicates that the loop is down. These messages are normal within the context of this procedure.

5. Use the correct cable for a shelf-to-shelf connection to connect the Channel A Output port of the last disk shelf to the Channel A Input port of the new disk shelf.

6. Connect the cable and SFP you removed in Step 4 to the Channel A Output port of the new disk shelf.

7. Repeat Step 4 through Step 6 for Channel B.

   **Note:** The Channel B Output port is connected to the other node in the HA pair.

8. Ensure that there are two paths listed for every disk in the output of the following command:

   `storage disk show -port`
How volumes work

A volume is the basic unit of storage within an aggregate.

More specifically, a volume is a file system that holds user data and is accessible to clients through a virtual server that is configured with one or more access protocols such as NFS and CIFS. A volume in Cluster-Mode is equivalent to a FlexVol volume in 7-Mode.

A volume provides a conceptual container for a set of logically related directories and files. Volumes create a single logical storage area that can be seamlessly managed across diverse platform types and geographically dispersed locations. The global namespace for a virtual server is created by mounting volumes to the virtual server's root volume and to one another. You mount volumes by using junctions, which are similar to UNIX mount points. A junction from one volume to another can be active (that is, the volume appears in the global namespace) or inactive (that is, any volume without an active junction does not appear in the global namespace).

Next topics

How 32-bit and 64-bit volumes differ on page 125
How you determine the type of a volume on page 126
Interoperability between 32-bit and 64-bit volumes on page 126
How you move data between 32-bit and 64-bit volumes on page 127
Differences among volume features on page 127
Creating a volume on page 128
Displaying information about volumes on page 129
Mounting a volume on page 130
Modifying a volume on page 131
How moving a volume works on page 133
How copying a volume works on page 134
Renaming a volume on page 135
Making a volume the root volume of its virtual server on page 136
Deleting a volume on page 137

How 32-bit and 64-bit volumes differ

Starting in Data ONTAP 8.0, FlexVol volumes are one of two types: 32-bit or 64-bit, depending on the type of their containing aggregate. A 64-bit volume has a larger maximum size than a 32-bit volume.

A 32-bit volume has a maximum size of 16 TB. The maximum size of a 64-bit volume is determined by the size of its containing aggregate—up to 100 TB, depending on the storage system model.
**Note:** In both types of volumes, the maximum size for LUNs and files is 16 TB. (The term LUNs in this context refer to the LUNs that Data ONTAP serves to clients, not to the array LUNs used for storage on a storage array.)

For best performance, if you want to create a large number of small files in a volume, you should use a 32-bit volume.

All FlexVol volumes created in versions of Data ONTAP earlier than 8.0 are 32-bit volumes.

### How you determine the type of a volume

The type of a FlexVol volume is determined by the type of its containing aggregate. To determine what type a FlexVol volume is, you use the `aggr status` command on its containing aggregate.

The type of a volume becomes important when you create a relationship between two volumes (for example, a volume SnapMirror relationship) that requires that both volumes be of the same type.

### Interoperability between 32-bit and 64-bit volumes

Some Data ONTAP features use two volumes that might be contained by different aggregates. Some of these features can interoperate between different types of volumes, but some cannot.

<table>
<thead>
<tr>
<th>Data ONTAP feature</th>
<th>Interoperates between 32-bit and 64-bit?</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexCache</td>
<td>Y</td>
</tr>
<tr>
<td>ndmpcopy</td>
<td>Y</td>
</tr>
<tr>
<td>Qtree SnapMirror</td>
<td>Y</td>
</tr>
<tr>
<td>Synchronous SnapMirror</td>
<td>N</td>
</tr>
<tr>
<td>vol copy</td>
<td>N</td>
</tr>
<tr>
<td>Volume SnapMirror</td>
<td>N</td>
</tr>
</tbody>
</table>
How you move data between 32-bit and 64-bit volumes

If you want to use Data ONTAP to move data between a 32-bit volume and a 64-bit volume, you must use `ndmpcopy` or `qtree SnapMirror`. You cannot use the `vol copy` command or volume SnapMirror between a 32-bit volume and a 64-bit volume.

Differences among volume features

There are differences among Snapshot copies, copies, mirrors, and moved volumes.

The following table summarizes the differences.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Access type (read-write or read-only)</th>
<th>Automatically mounted?</th>
<th>Full copy or shared blocks?</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot copy</td>
<td>Read-only</td>
<td>Yes</td>
<td>Shared blocks (same volume as parent)</td>
<td>Same aggregate and node</td>
</tr>
<tr>
<td>Copy</td>
<td>Same as the original volume (read-write or read-only)</td>
<td>No</td>
<td>Full copy</td>
<td>Same or different aggregate; same or different node</td>
</tr>
<tr>
<td>Mirror</td>
<td>Read-only</td>
<td>No</td>
<td>Full copy</td>
<td>Same or different aggregate; same or different node</td>
</tr>
<tr>
<td>Move</td>
<td>Same as the original volume (read-write or read-only)</td>
<td>Yes</td>
<td>Full move, then deletion of original</td>
<td>Different aggregate; same or different node</td>
</tr>
</tbody>
</table>

All of these volume operations must occur within the context of the same virtual server. For instance, you cannot move a volume from a virtual server named vs0 to a virtual server named vs1. However, a virtual server can span multiple nodes and multiple aggregates.

You can schedule regular occurrences of Snapshot copies and mirrors by creating schedules.

Volume operations can take a long time to complete, depending on the size of the volume and the load on the cluster. For instance, moving a 1-TB volume might take several hours to complete.
Volume limitations

There are limitations to the use of volumes.

The following limitations apply to volumes:

- Up to 500 volumes can be created on each node in a cluster; if more than one aggregate is located on a particular node, the total number of volumes on those aggregates cannot exceed 500.
  
  **Note:** This limit assumes that you are using storage failover (SFO). If you are not using SFO, up to 1,000 volumes can be created per node; however, without SFO, those volumes become unavailable if the node fails.

- A cluster can contain up to 60,000 volumes and Snapshot copies. Be sure to account for all Snapshot copies as well as their parent volumes when tracking the total number of volume and Snapshot copies in your cluster.

- A volume can contain up to 100,000 directories; however, two of these directories are links to the current directory (.) and the parent directory (..), so the effective limit is 99,998 directories per volume.

Creating a volume

You can create a volume and specify its properties.

**Before you begin**

A virtual server and an aggregate must exist before you can create a volume.

**Step**

1. Use the `volume create` command to create a volume.

   When you create a volume, you must specify, at a minimum, the virtual server on which the volume is to be located, the volume name, and the aggregate that is to hold the volume. Note that a volume's name must be 203 or fewer characters in length.

   You can optionally specify additional information when the volume is created, including its state, type, the export policy that applies to it, its user and group IDs, its security style (UNIX mode bits, CIFS ACLs, or mixed NFS and CIFS permissions), the default UNIX permissions for files located on it, its junction path, and its size and space-guarantee style. Some attributes can be specified only at the advanced privilege level and higher. For a complete list of possible attributes, see the reference page for the command.

   **Note:** When a mirror is created or replicated, you might encounter a short delay before the mirror becomes available for use.

**Example**

The following example creates a new volume named dept_eng on a virtual server named vs1 and an aggregate named aggr2. The volume is initially in the online state. It uses the export policy
named default. The owner of the volume's root is a user named george whose primary group is named eng. The volume's junction is /dept/eng. The volume is 750 GB in size, and space for the entire volume is guaranteed on the aggregate.

```
node::> volume create -vserver vs1 -volume dept_eng
-aggregate aggr2 -state online -policy default -user george
-group eng -junction-path /dept/eng -size 750g -space-guarantee volume
```

**Related tasks**

*Creating a qtree* on page 141

**Volume names**

It is important to have a consistent volume-naming scheme.

Each volume must be labeled with a name that is unique to its virtual server; you use this name in commands to manage the volume. You need to give some thought to the names you choose so that when other volumes are added to the virtual server, the names are orderly and recognizable. For example, if you are deploying a software-development project on a Data ONTAP system, you might choose to create the following volumes:

- A volume named `user_user_name` for each user
- A volume named `src_component` for source code for each component
- A volume named `build_component` for compiled images of each component

Uniform naming schemes make it easier to manage large number of volumes.

Volume names must conform to the following rules:

- The first character in the volume name must be an alphabetic character (a to z or A to Z).
- Characters in a name can include alphanumeric characters (a to z, A to Z, and 0 (zero) to 9) and the underscore character (_). Other characters and symbols are not permitted.
- Volume names can be from 1 to 203 characters in length. If a volume name exceeds 203 characters in length, Snapshot copies and mirror volumes do not work correctly.

The root volume for a virtual server is automatically created and mounted when the virtual server is created. The root volume is given the name specified by the value of the `-rootvolume` parameter of the `vserver create` command. The volume is mounted at / (root).

**Displaying information about volumes**

You can display information about volumes.

**Step**

1. Use the `volume show` command to display information at volumes.

   The command displays, at minimum, the following information:
- Virtual server name
- Volume name
- Aggregate name
- State (online, offline, or restricted)
- Type (RW for read-write, LS for a load-sharing mirror, DP for a disaster-protection mirror)
- Size
- Available size
- Percentage of space used

Other information is displayed in a detailed view and if other parameters are specified. See the reference page for the command for details.

**Example**
The following example displays information about volumes named dept*:

```
node::> volume show -volume dept*
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Aggregate</th>
<th>State</th>
<th>Type</th>
<th>Size</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>dept</td>
<td>node14_aggr1</td>
<td>online</td>
<td>RW</td>
<td>500MB</td>
<td>399.89MB</td>
</tr>
<tr>
<td>vs0</td>
<td>dept_hr</td>
<td>node14_aggr1</td>
<td>online</td>
<td>RW</td>
<td>500MB</td>
<td>399.87MB</td>
</tr>
<tr>
<td>vs0</td>
<td>dept_eng</td>
<td>node14_aggr1</td>
<td>online</td>
<td>RW</td>
<td>100GB</td>
<td>99.87GB</td>
</tr>
</tbody>
</table>

**Mounting a volume**

You can manually mount a volume.

**Step**

1. Use the `volume mount` command to mount the volume. To mount a volume, you specify the volume name and a junction path. You can optionally specify whether the parent volume's export policy overrides the mounted volume's export policy.

**Example**
The following example mounts a volume named dept on a virtual server named vs0. The volume is mounted on the path /dept.

```
node::> volume mount -vserver vs0 -volume dept
         -junction-path /dept
```

**Related tasks**

- *Copying a volume* on page 134
- *Making a volume the root volume of its virtual server* on page 136
Unmounting a volume

You can unmount a volume.

Step

1. Use the `volume unmount` command to unmount a volume.

   To unmount a volume, specify the volume and its virtual server. After you unmount a volume, you can remount it at another location.

   **Note:** Even though a volume can be unmounted by using the `volume unmount` command, the volume is still in an online state and some clients might still be able to access data. Unmounting a volume is not sufficient for preventing access to the volume. To fully restrict access to a volume, use the `volume modify` command to take the volume offline.

Example

The following example unmounts a volume named `eng_ecns` on a virtual server named `vs1`:

```
node::> volume unmount -vserver vs1 -volume eng_ecns
```

Related tasks

- *Deleting a volume* on page 137
- *Making a volume the root volume of its virtual server* on page 136

Modifying a volume

You can modify a volume's properties.

Step

1. Use the `volume modify` command to modify a volume.

   The command enables you to modify the following properties of a volume:

   - State (online, offline, or restricted)
   - Export policy
   - User ID
   - Group ID
   - Security style (UNIX mode bits, CIFS ACLs, or mixed NFS and CIFS permissions)
   - Default UNIX permissions for files on the volume
   - Whether the junction path is active (advanced privilege level or higher only)
   - Comment
   - Size
   - Total number of files permitted on the volume
• Space guarantee style (none or volume)
• Snapshot policy
• Whether the modification operation is forced

At the advanced privilege level and higher, the command enables you to change additional volume attributes. See the reference page for the command for details.

To change a volume's aggregate, use the `volume move` command. To change a volume's name, use the `volume rename` command. To change a mirror volume to a read-write volume, use the `snapmirror promote` command. To make a volume the root volume of its virtual server, use the `volume make-vsroot`.

**Example**
The following example modifies a volume named `dept_eng` on a virtual server named `vs1`. The volume's default user is changed to `ralph` and the size is changed to 15 TB.

```
node::> volume modify -vserver vs1 -volume dept_eng -user ralph -size 15t
```

**Related tasks**
- *Moving a volume* on page 133
- *Renaming a volume* on page 135
- *Making a volume the root volume of its virtual server* on page 136
- *Deleting a volume* on page 137
- *Deleting a Snapshot policy* on page 174

### Increasing the maximum directory size
Increasing the maximum directory size as the limit is approached can help avoid performance degradation.

**About this task**

Messages in the form `wafl.dir.size.warning: Directory /vol/data/images/ is approaching the maxdirsize limit. Reduce the number of files or use the vol options command to increase this limit can indicate that the directory is reaching the maximum directory (maxdir) size limit.

**Steps**

1. Use the `set` command to set the privilege level to advanced.

   **Example**
The following example sets the privilege level to advanced.

   ```
   node::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them
   ```
only when directed to do so by NetApp personnel. Do you want to continue? {y|n}: y

2. Use the `volume modify` command with the `-maxdir-size` parameter to gradually increase the maximum directory size.

The maximum directory size is specified in KB, and the default is 10240 KB (10 MB).

Because increasing the maximum directory size also increases the memory requirements for the volume, increase the size in small increments until the system stops issuing the warning messages.

**Example**
The following example set a maximum directory size of 20480 KB (20 MB) for a volume named images on a virtual server named vs1.

```
node::*> volume modify -vserver vs1 -volume images -maxdir-size 20480
```

**How moving a volume works**
You can move a volume from one aggregate or node to another within the same virtual server.

Moving a volume occurs in multiple phases. First, a copy of the volume you're moving is made. This copy is moved to the new location with the same name and junction, while the original volume remains intact. After the copy is safely transferred to its new location, the original volume is deleted.

The capability to move volumes is useful for managing space and balancing workloads within your cluster. For instance, if one aggregate holds 500 volumes with similar sizes and another aggregate of the same size holds only 200 volumes of the same approximate sizes, you can move volumes from the first aggregate to the second to balance the workload and improve performance.

**Related concepts**

*About moving a volume that contains quotas* on page 161

**Moving a volume**

You can move a FlexVol volume to a different aggregate, node, or both within the same virtual server.

**Before you begin**

If you are moving a data protection mirror, it must be initialized by using the `snapmirror initialize` before you can move it.

**About this task**

Moving a volume has the following limitations:

- You can move FlexVol volumes only.
The volume move operation can affect existing CIFS client sessions. Before you perform this operation, you might consider scheduling the volume move during an outage window, taking the volume offline, or disabling CIFS during the operation.

Steps

1. Use the `volume move` command to move a volume.

   **Example**
   The following example moves a volume named `user_max` on a virtual server named `vs2` to an aggregate named `node12a_aggr3`. The move runs as a foreground process.

   ```bash
   node::> volume move -vserver vs2 -volume user_max -destination-aggregate node12a_aggr3 -foreground true
   ```

2. Use the `job show` command to determine the command’s job ID and to display the job’s status.

Related concepts

   *About moving a volume that contains quotas* on page 161

Related tasks

   *Modifying a volume* on page 131
   *Initializing a data protection mirror* on page 0

How copying a volume works

A volume copy is a full copy of the original volume with the same access (read-only or read-write) as the original volume.

A volume copy does not share blocks with the original volume; thus, a copy of a 2-GB volume uses 2 GB of disk space, unlike a Snapshot copy of a volume, which might use only a few kilobytes of disk space because of shared blocks. After the copy is made, no operations made on the copy or on the original affect the other. For instance, if you write data to the original volume, the data is not written to the copy. A volume copy is not automatically mounted when it is created. A volume copy must occur within the context of the same virtual server.

Copying a volume

Copying a volume creates a standalone copy of a volume that can be used for a variety of purposes such as testing.

About this task

Copying a volume has the following limitations:
You can copy a volume within a cluster only.
• You can copy a FlexVol volume to a FlexVol volume only.

Steps

1. To create a standalone copy of a volume, use the `volume copy` command.

   The copy can be made on the same aggregate as the original or on a different aggregate. When the copy is complete, it has no relation to its source volume; changes made to one volume are not propagated to the other. The copy is not automatically mounted; mount it by using the `volume mount` command.

   **Example**

   The following example creates a copy of a volume named `src_builds` on a virtual server named `vs0`. The copy is named `builds` and is located on an aggregate named `aggr4`. The copy operation runs as a background process.

   ```bash
   node::> volume copy -vserver vs0 -volume src_builds -destination-volume builds -destination-aggregate aggr4 -foreground false
   ```

2. Use the the `job show` command to determine the command’s job ID and to display the job’s status.

Related tasks

*Mounting a volume* on page 130

---

**Renaming a volume**

You can rename a volume.

Steps

1. Use the `volume rename` command to rename a volume.

   The volume's new name must be unique among other volume names on the same virtual server. Also, a volume's name must be 203 or fewer characters in length.

   **Example**

   The following example renames a volume named `dept_it` as `dept_helpdesk` on a virtual server named `vs1`:

   ```bash
   node::> volume rename -vserver vs1 -volume dept_it -newname dept_helpdesk
   ```

2. Verify your change by using the `volume show` command.
Example
The following example displays the renamed volume dept_helpdesk on the virtual server named vs1:

```
node::> volume show
```

<table>
<thead>
<tr>
<th>Virtual Server</th>
<th>Volume</th>
<th>Aggregate</th>
<th>State</th>
<th>Type</th>
<th>Size</th>
<th>Available</th>
<th>Used%</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>dept_eng</td>
<td>aggr1</td>
<td>online</td>
<td>RW</td>
<td>20MB</td>
<td>15.80MB</td>
<td>20%</td>
</tr>
<tr>
<td>vs1</td>
<td>dept_finance</td>
<td>aggr1</td>
<td>online</td>
<td>DP</td>
<td>20MB</td>
<td>15.80MB</td>
<td>20%</td>
</tr>
<tr>
<td>vs1</td>
<td>dept_helpdesk</td>
<td>aggr1</td>
<td>online</td>
<td>DP</td>
<td>20MB</td>
<td>15.89MB</td>
<td>20%</td>
</tr>
<tr>
<td>vs1</td>
<td>dept_hr</td>
<td>aggr1</td>
<td>online</td>
<td>LS</td>
<td>20MB</td>
<td>15.82MB</td>
<td>20%</td>
</tr>
</tbody>
</table>

Related tasks

*Modifying a volume* on page 131

Making a volume the root volume of its virtual server

If the root volume of a virtual server becomes unavailable, you can promote another of the virtual server's volumes to be the virtual server's root.

About this task

A virtual server's root volume must be a FlexVol volume. You can promote a load-sharing or data-protection mirror to be the root volume as long as the volume is initialized.

Steps

1. Use the `set` command to set the privilege level to advanced.

   **Example**
   The following example sets the privilege level to advanced.

   ```
   node::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

2. Use the `volume make-vsroot` command to promote another of the virtual server's volumes to be the virtual server root volume.

   The command renames the volume as root__virtual_server_name. For instance, if you run this command on a volume named mirror_root_vs0 that is located on a virtual server named vs0, the volume is made the root volume of the virtual server and given the name root_vs0.

   **Example**
   The following example makes a volume named backup_vs1 the root volume of a virtual server named vs1. The command renames the volume to root_vs1.

   ```
   node:*> volume make-vsroot -vserver vs1 -volume backup_vs1
   ```
3. Unmount all volumes that were mounted below the previous root volume and remount them below the new root volume.

Related tasks

- Modifying a volume on page 131
- Unmounting a volume on page 131
- Mounting a volume on page 130

Deleting a volume

Deleting a volume deletes all of its files and directories.

Steps

1. Use the `volume unmount` command to unmount any volumes that are children of the volume you want to delete.
   
   **Example**
   
   The following example unmounts a volume named `user_scott` from a virtual server named `vs1`:
   
   ```bash
   node::> volume unmount -vserver vs1 -volume users_scott
   ```

2. Use the `volume unmount` command to unmount the volume that you want to delete.
   
   **Example**
   
   The following example unmounts a volume named `users` from a virtual server named `vs1`:
   
   ```bash
   node::> volume unmount -vserver vs1 -volume users
   ```

3. Use the `snapmirror delete` command to delete SnapMirror relationships.
   
   **Example**
   
   The following example deletes the destination endpoint named `//vs1/users_mirror4`:
   
   ```bash
   node::> snapmirror delete -destination-path //vs1/users_mirror4
   ```

4. Use the `volume modify` command to change the state of the volume you want to delete to offline.
   
   **Example**
   
   The following example modifies a volume named `users` on a virtual server named `vs1` to be in the offline state:
   
   ```bash
   node::> volume modify -vserver vs1 -volume users -state offline
   ```

5. Use the `volume delete` command to delete a volume and all of its files and directories, including Snapshot copies and associated qtree and quota policies.
Example
The following example deletes a volume named users from a virtual server named vs1. Also deleted as part of this operation is the child volume named users_scott:

```
node::> volume delete -vserver vs1 -volume users
```

Related tasks

- *Unmounting a volume* on page 131
- *Modifying a volume* on page 131
When you use qtrees

You use qtrees to partition your data. You might create qtrees to organize your data, or to manage one or more of the following factors: quotas, security style, and CIFS oplocks setting.

The following list describes examples of qtree usage strategies:

- **Quotas**
  You can limit the size of the data used by a particular project, by placing all of that project's files into a qtree and applying a tree quota to the qtree.

- **Security style**
  If you have a project that needs to use NTFS-style security, because the members of the project use Windows files and applications, you can group the data for that project in a qtree and set its security style to NTFS, without requiring that other projects also use the same security style.

- **CIFS oplocks settings**
  If you have a project using a database that requires CIFS oplocks to be off, you can set CIFS oplocks to Off for that project's qtree, while allowing other projects to retain CIFS oplocks.

Next topics

- How many qtrees you can have on page 140
- Where you can create qtrees on page 140
- How qtrees compare with volumes on page 140
- How 7-Mode and Cluster-Mode qtree features compare on page 141
- About the CIFS oplocks setting on page 141
- Creating a qtree on page 141
- Modifying a qtree on page 144
- Displaying statistics about qtrees on page 145
- Deleting an empty qtree on page 146
How many qtrees you can have

You can have a maximum of 4,995 qtrees in any volume. There is no maximum for the storage system as a whole.

Where you can create qtrees

You can create qtrees only at the top level of a FlexVol volume. You cannot create qtrees within other qtrees.

How qtrees compare with volumes

In general, qtrees are similar to volumes. However, they have some key differences.

The following table compares qtrees and FlexVol volumes.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Qtree</th>
<th>FlexVol volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables organizing user data</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enables grouping users with similar needs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Accepts a security style</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Accepts oplocks configuration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can be resized</td>
<td>Yes (using quota limits)</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Snapshot copies</td>
<td>No (qtree data can be extracted from volume Snapshot copies)</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports quotas</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can be cloned</td>
<td>No (except as part of a FlexVol volume)</td>
<td>Yes</td>
</tr>
<tr>
<td>Can serve as the root of a vserver</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can serve as a junction</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can be exported using NFS</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
How 7-Mode and Cluster-Mode qtree features compare

Different qtree features are supported, depending on whether you use 7-Mode or Cluster-Mode.

Table 2: How 7-Mode and Cluster-Mode qtree features compare

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Supported in 7-Mode?</th>
<th>Supported in Cluster-Mode?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS opportunistic locking</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Quotas</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security style settings</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Statistics collection and display</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UNIX permissions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

About the CIFS oplocks setting

Usually, you should leave CIFS oplocks on for all volumes and qtrees. This is the default setting. However, you might turn CIFS oplocks off under certain circumstances.

CIFS oplocks (opportunistic locks) enable the redirector on a CIFS client in certain file-sharing scenarios to perform client-side caching of read-ahead, write-behind, and lock information. A client can then work with a file (read or write it) without regularly reminding the server that it needs access to the file. This improves performance by reducing network traffic.

You might turn CIFS oplocks off on a volume or a qtree under either of the following circumstances:

- You are using a database application whose documentation recommends that CIFS oplocks be turned off.
- You are handling critical data and cannot afford even the slightest data loss.

Otherwise, you can leave CIFS oplocks on.

For more information about CIFS oplocks, see the CIFS section of the *Clustered Network and File Access Management Guide*.

Creating a qtree

You can create a qtree and specify its security, locking, and permissions properties.

Before you begin

A virtual server and a volume must exist before you can create a qtree.
Steps

1. Use the `volume qtree create` command to create a qtree.

   When you create a qtree, you must specify the virtual server and volume on which the qtree is to be located.

   **Note:** A qtree name cannot contain a forward slash (/) and must be less than 65 characters in length.

   You can optionally specify the following attributes of a qtree when you create it:

   - Security style—You can use the `-security-style` parameter to specify the security style for the qtree. Possible values include `unix` (for UNIX mode bits), `ntfs` (for CIFS ACLs), and `mixed` (for mixed NFS and CIFS access).
   - Whether opportunistic locking is enabled—You can use the `-oplock-mode` parameter to specify whether oplocks are enabled for the qtree.
   - UNIX permissions—You can use the `-unix-permissions` parameter to specify the default UNIX permissions for the qtree when the `-security-style` is set to `unix` or `mixed`. You can specify UNIX permissions either as a four-digit octal value (for example, 0700) or in the style of the UNIX `ls` command (for example, `-rwxr-x---`). For information on UNIX permissions, see the UNIX or Linux documentation.

   If you do not specify a value for an optional attribute, the qtree you're creating inherits it from the volume on which you're creating the qtree.

   **Example**
   The following example creates a qtree named qtree1. The virtual server name is vs0 and the volume containing the qtree is named is vol0. The qtree has a mixed security style. Its other attributes are inherited from volume vol0.

   ```bash
   node::> volume qtree create -vserver vs0 -volume vol0 -qtree qtree1 -security-style mixed
   ```

2. Use the `job show` command to monitor the progress of the `volume qtree create` operation.

3. Use the `volume qtree show` command to display information about the new qtree.

Next topics

*Displaying information about qtrees* on page 143
*Renaming a qtree* on page 144

Related tasks

*Creating a volume* on page 128
*Creating a quota policy rule* on page 156
Displaying information about qtrees

You can display information about qtrees for volumes that are online.

Steps

1. Use the `volume qtree show` command to display information about qtrees.

   The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information about all qtrees:

   - **Qtree0**—When you create a volume, a special qtree referred to as "qtree0" is automatically created for the volume. It represents all of the data stored in a volume that isn't contained in a qtree. In the CLI output, qtree0 is denoted by empty quotation marks (""") and has the ID zero (0). The qtree called qtree0 cannot be manually created or deleted.
   - **Virtual server name**
   - **Volume name**
   - **Qtree name**
   - **Security style (UNIX mode bits, CIFS ACLs, or mixed NFS and CIFS permissions)**
   - **Whether opportunistic locking is enabled**
   - **Status**

Example

The following example displays default information about all qtrees along with each qtree ID. Note that on vs0, no qtrees have been manually created, so only the qtrees referred to as qtree 0 are shown. On vs1, the volume named vs1_vol1 contains qtree 0 and two manually created qtrees, qtree1 and qtree2.

```
node::> volume qtree show -id

<table>
<thead>
<tr>
<th>Virtual Server</th>
<th>Volume</th>
<th>Qtree</th>
<th>Style</th>
<th>Oplocks</th>
<th>Status</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>vs0_vol1</td>
<td>&quot;&quot;</td>
<td>unix</td>
<td>enable</td>
<td>readonly</td>
<td>0</td>
</tr>
<tr>
<td>vs0</td>
<td>vs0_vol2</td>
<td>&quot;&quot;</td>
<td>unix</td>
<td>enable</td>
<td>normal</td>
<td>0</td>
</tr>
<tr>
<td>vs0</td>
<td>vs0_vol3</td>
<td>&quot;&quot;</td>
<td>unix</td>
<td>enable</td>
<td>readonly</td>
<td>0</td>
</tr>
<tr>
<td>vs0</td>
<td>vs0_vol4</td>
<td>&quot;&quot;</td>
<td>unix</td>
<td>enable</td>
<td>readonly</td>
<td>0</td>
</tr>
<tr>
<td>vs0</td>
<td>root_vs_vs0</td>
<td>&quot;&quot;</td>
<td>unix</td>
<td>enable</td>
<td>normal</td>
<td>0</td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_vol1</td>
<td>&quot;&quot;</td>
<td>unix</td>
<td>enable</td>
<td>normal</td>
<td>0</td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_vol1</td>
<td>qtree1</td>
<td>unix</td>
<td>disable</td>
<td>normal</td>
<td>1</td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_vol1</td>
<td>qtree2</td>
<td>unix</td>
<td>enable</td>
<td>normal</td>
<td>2</td>
</tr>
<tr>
<td>vs1</td>
<td>root_vs_vs1</td>
<td>&quot;&quot;</td>
<td>unix</td>
<td>enable</td>
<td>normal</td>
<td>0</td>
</tr>
</tbody>
</table>
9 entries were displayed.
```

2. To display detailed information about a single qtree, execute the command with the `-instance` and `-qtree` parameters. The detailed view provides information about UNIX permissions, the qtree ID, and the qtree status.

Related concepts

*About mirroring a volume that contains quotas* on page 162
Renaming a qtree

You can rename a qtree.

Steps

1. Use the `volume qtree rename` command to rename a qtree.

   When you rename a qtree, you must specify the virtual server name, volume on which the qtree is located, existing qtree name, and new qtree name.

   **Note:** A qtree name cannot contain a forward slash (/) and must be less than 65 characters in length.

   **Example**
   The following example rename a qtree named qtree3 to qtree4. The virtual server name is vs0 and the volume containing the qtree is named is vol0.

   ```
   node::> volume qtree modify -vserver vs0 -volume vol0 -qtree qtree3 -newname qtree4
   ```

2. Use the `volume qtree show` command to display information about the renamed qtree.

Modifying a qtree

You can modify an existing qtree to change its security, locking, and permissions properties.

Steps

1. Use the `volume qtree modify` command to modify an existing qtree.

   When you modify a qtree, you must specify the virtual server, volume, and name of the qtree that you want to modify. You can modify the attributes of the default qtree referred to as qtree0 by omitting the `-qtree` parameter from the command or by specifying the value `""` for the `-qtree` parameter.

   You can modify the following attributes of a qtree:

   - **Security style**—You can use the `-security-style` parameter to specify the security style for the qtree. Possible values include `unix` (for UNIX mode bits), `ntfs` (for CIFS ACLs), and `mixed` (for mixed NFS and CIFS access).
   - Whether opportunistic locking is enabled—You can use the `-oplock-mode` parameter to specify whether oplocks are enabled for the qtree.
   - **UNIX permissions**—You can use the `-unix-permissions` parameter to specify the default UNIX permissions for the qtree when the `-security-style` is set to `unix` or `mixed`. You can specify UNIX permissions either as a four-digit octal value (for example, 0700) or in the style of the UNIX `ls` command (for example, `-rwxr-x---`). For information on UNIX
permissions, see the UNIX or Linux documentation. If you do not specify UNIX permissions for the qtree, it inherits the UNIX permissions of the volume on which you're creating it.

**Note:** You cannot apply a quota policy or quota policy rule to qtree0.

If you do not specify a value for an optional attribute, the qtree inherits it from the volume on which it exists.

**Example**
The following example modifies a qtree named qtree1. The virtual server name is vs0 and the volume containing the qtree is named is vol0. The qtree now has a UNIX security style and oplocks are enabled.

```
node::> volume qtree modify -vserver vs0 -volume vol0 -qtree qtree1 -security-style unix -oplocks enabled
```

2. Use the `volume qtree show` command to display information about the qtree you modified.

**Displaying statistics about qtrees**

You can display statistical information about qtrees.

**Step**

1. Use the `volume qtree statistics` command to display statistical information about qtrees.

   **Note:** Qtree statistics are available only when the volume containing the qtree is online. Statistics can be collected from the time the volume is created, when the volume state is set to online, or when the statistics have been reset by using the `volume qtree statistics-reset` command. Also, qtree statistics are not persistent. If you restart a node, if a storage takeover and giveback occurs, or if is volume is set to offline and then online, these statistics are set to zero.

The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following statistics information about all qtrees:

- Virtual server name
- Volume name
- Qtree name
- NFS operations
- CIFS operations
- Operations since statistics were last reset (advanced privilege level and higher)
- NFS operations since the volume was created (advanced privilege level and higher)
- CIFS operations since the volume was created (advanced privilege level and higher)
- Operations since the volume was created (advanced privilege level and higher)
Example
The following example displays statistics information for all qtrees on the virtual server named vs0.

```
node::> volume qtree statistics -vserver vs0
```

<table>
<thead>
<tr>
<th>Virtual Server</th>
<th>Volume</th>
<th>Qtree</th>
<th>NFS Ops</th>
<th>CIFS Ops</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>vol0</td>
<td>qtree1</td>
<td>10876</td>
<td>2678</td>
</tr>
<tr>
<td>vs0</td>
<td>vol1</td>
<td>qtree1a</td>
<td>16543</td>
<td>0</td>
</tr>
<tr>
<td>vs0</td>
<td>vol2</td>
<td>qtree2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>qtree2a</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

4 entries were displayed.

Resetting qtree statistics

You can reset qtree statistics for a volume.

Step

1. Use the `volume qtree statistics-reset` command to reset qtree statistics for a volume.

   When you reset qtree statistics, you must specify the virtual server and volume name.

Example
The following example resets statistics for all qtrees on the the volume named vol0 on the virtual server named vs0.

```
node::> volume qtree statistics-reset -vserver vs0 -volume vol0
```

Deleting an empty qtree

You can delete an empty qtree.

Steps

1. Use the `volume qtree delete` command to delete an empty qtree.

   When you delete a qtree, you must specify the virtual server name, volume on which the qtree is located, and the qtree name.

   Note: You cannot delete the special qtree referred to a qtree 0, which in the CLI is denoted by empty quotation marks (""") and has the ID zero (0).

   Note: If there is a quota policy or quota policy rule associated with a qtree, it is deleted when you delete the qtree.
Example
The following example deletes a qtree named qtree4. The virtual server name is vs0 and the volume containing the qtree is named is vol0.

```
node::> volume qtree delete -vserver vs0 -volume vol0 -qtree qtree4
```

2. Use the `volume qtree show` command to display information about the remaining qtrees.

Deleting a qtree that contains files
You can force-delete a qtree that contains files.

Steps

1. Use the `set` command to set the privilege level to advanced.

Example
The following example sets the privilege level to advanced.

```
node::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

2. Use the `volume qtree delete` command with the `-force` parameter to delete a qtree that contains files.

When you delete a qtree, you must specify the virtual server name, volume on which the qtree is located, and the qtree name.

**Note:** You cannot delete the special qtree referred to a qtree 0, which in the CLI is denoted by empty quotation marks (""") and has the ID zero (0).

**Note:** If there is a quota policy or quota policy rule associated with a qtree, it is deleted when you delete the qtree.

Example
The following example deletes a qtree named qtree5, which contains files. The virtual server name is vs0 and the volume containing the qtree is named is vol0.

```
node::> volume qtree delete -vserver vs0 -volume vol0 -qtree qtree4 -force true
```

3. Use the `volume qtree show` command to display information about the remaining qtrees.
Why you use quotas

You can use quotas to limit resource usage, to provide notification when resource usage reaches specific levels, or simply to track resource usage.

You specify a quota for the following reasons:

• To limit the amount of disk space or the number of files that can be used by a user or group, or that can be contained by a qtree
• To track the amount of disk space or the number of files used by a user, group, or qtree, without imposing a limit
• To warn users when their disk usage or file usage is high

Next topics

Overview of the quota process on page 149
How 7-Mode and Cluster-Mode quota features compare on page 150
Special kinds of quotas on page 150
How derived quotas work on page 150
How tree quotas work on page 151
Differences among hard, soft, and threshold quotas on page 151
About activating or reinitializing quotas on page 151
How qtree changes affect quotas on page 152
Creating a quota policy on page 152
Assigning a quota policy to a virtual server on page 155
Creating a quota policy rule on page 156
Activating and deactivating quota rules for a volume on page 160
Displaying a quota report on page 161
About moving a volume that contains quotas on page 161
About mirroring a volume that contains quotas on page 162
About restoring Snapshot copies of a volume that contains quotas on page 163

Overview of the quota process

Quotas can cause Data ONTAP to send a notification (soft quota) or to prevent a write operation from succeeding (hard quota) when quotas are exceeded.

When Data ONTAP receives a request to write to a volume, it checks to see whether quotas are activated for that volume. If so, Data ONTAP determines whether any quota for that volume (and, if the write is to a qtree, for that qtree) would be exceeded by performing the write operation. If any
hard quota would be exceeded, the write operation fails, and a quota notification is sent. If any soft quota would be exceeded, the write operation succeeds, and a quota notification is sent.

**How 7-Mode and Cluster-Mode quota features compare**

Different quota features are supported, depending on whether you use 7-Mode or Cluster-Mode.

**Table 3: How 7-Mode and Cluster-Mode quota features compare**

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Available in 7-Mode?</th>
<th>Available in Cluster-Mode?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derived quotas</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group quotas</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EMS and SNMP notifications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Quota for the default qtree</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Tree quotas</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User quotas</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Special kinds of quotas**

You use default, explicit, derived and tracking quotas to manage disk usage in the most efficient manner.

**How derived quotas work**

A quota applied as a result of a default quota, rather than an explicit quota (a quota with a specific target), is referred to as a derived quota.

Data ONTAP derives the quota information from the default quota and applies it if a write request affects the disk space or number of files used by an instance of the quota target. Derived quotas are applied unless an explicit quota is in effect for that target.

Data ONTAP tracks disk and file usage for quota targets of derived quotas, which means you can change the specifications of these derived quotas by resizing rather than having to perform a full quota reinitialization.
How tree quotas work

You can create a quota with a qtree as its target to limit how large the target qtree can become. These quotas are also called tree quotas.

When you apply a quota to a qtree, the result is similar to a disk partition, except that you can change the qtree's maximum size at any time by changing the quota. When applying a tree quota, Data ONTAP limits the disk space and number of files in the qtree, regardless of their owners. No users, including root and members of the BUILTIN\Administrators group, can write to the qtree if the write operation causes the tree quota to be exceeded.

Note: The size of the quota does not guarantee any specific amount of available space. The size of the quota can be larger than the amount of free space available to the qtree. You can use the volume quota report command to determine the true amount of available space in the qtree.

Differences among hard, soft, and threshold quotas

Hard quotas (disk-limit and file-limit parameters) impose a hard limit on system resources; any operation that would result in exceeding the limit fails. The soft quotas (threshold, soft-disk-limit, and soft-file-limit parameters) send a warning message when resource usage reaches a certain level, but do not affect data access operations, so you can take appropriate action before the quota is exceeded.

Threshold quotas (quotas specified using the threshold parameter) are equivalent to quotas specified using the soft-disk-limit parameter, except for how notifications are handled.

About activating or reinitializing quotas

You use the volume quota modify command to activate or reinitialize quotas, which causes all quotas for that volume to be recalculated. Knowing how quota initialization works can help you manage your quotas less disruptively.

The following list outlines some facts you should know about activating or reinitializing quotas:

- Changes to quotas do not take effect until quotas are either reinitialized or resized.
- You activate or reinitialize quotas for only one volume at a time.
- Quota reinitialization can take some time, during which storage system data is available, but quotas are not enforced for the specified volume.
- Quota reinitialization is performed in the background by default; other commands can be performed while the reinitialization is proceeding.

Note: Errors or warnings from the reinitialization process could be interspersed with the output from other commands.
• Quota reinitialization can be invoked in the foreground with the -foreground option; this is useful if you are reinitializing from a script.
• Errors and warnings from the reinitialization process are logged to the console as well as to /etc/messages.
• Quota activation persists across halts and reboots.

How qtree changes affect quotas

When you delete, rename, or change the security style of a qtree, the quotas applied by Data ONTAP might change, depending on the current quotas being applied.

Next topics

How deleting a qtree affects tree quotas on page 152
How renaming a qtree affects quotas on page 152

How deleting a qtree affects tree quotas

When you delete a qtree, all quotas applicable to that qtree, whether they are explicit or derived, are no longer applied by Data ONTAP.

If you create a new qtree with the same name as the one you deleted, the quotas previously applied to the deleted qtree are not applied automatically to the new qtree until you reinitialize quotas. If a default tree quota exists, Data ONTAP creates new derived quotas for the new qtree.

If you don't create a new qtree with the same name as the one you deleted, you can delete the quotas that applied to that qtree to avoid getting errors when you reinitialize quotas.

How renaming a qtree affects quotas

When you rename a qtree using Data ONTAP, the quota rules for that qtree are automatically updated. If you rename a qtree using your CIFS or NFS client, you must update any quota rules for that qtree with the new name before you reinitialize quotas to ensure that those quota continue to be applied.

Creating a quota policy

You can create a quota policy for volumes on a virtual server.

Before you begin

A cluster virtual server must exist before you can create a quota policy.

Steps

1. Use the `volume quota policy create` command to create a quota policy.
When you create a quota policy, you must specify the virtual server name and quota policy name.

**Note:** A quota policy name cannot exceed 32 characters in length. In addition, you can create a quota policy only for a cluster virtual server, not a node or admin virtual server.

**Example**
The following example creates a quota policy named quota_policy_vs1 for the virtual server named vs1.

```bash
node::> volume quota policy create -vserver vs1 -policy-name quota_policy_vs1
```

2. **Use the** `volume quota policy show` **command to display information about the new quota policy.**

**Next topics**

- [Displaying information about quota policies](#) on page 153
- [Copying a quota policy](#) on page 154
- [Renaming a quota policy](#) on page 154
- [Deleting a quota policy](#) on page 155

**Displaying information about quota policies**

You can display information about quota policies.

**Steps**

1. **Use the** `volume quota policy show` **command to display information about quota policies.**

   If no parameters are specified, the command displays the following information about all quota policies:
   - Virtual server name
   - Policy name
   - When the policy was last modified

**Example**
The following example displays default information about all quota policies.

```bash
node::> volume quota policy show
Virtual Server     Policy Name           Last Modified
---------------    --------------------   ----------------
vs0                quota_policy_vs0       10/16/2008 17:40:05
vs1                quota_policy_vs1       10/16/2008 17:47:45
vs2                quota_policy_vs2       10/16/2008 17:44:13
vs3                quota_policy_vs3       10/16/2008 17:44:13
4 entries were displayed.
```

2. **To display information about the quota policy assigned to a specific virtual server, execute the command with the -vserver parameter.**
3. To display information about a single quota policy, execute the command with the -policy-name parameter.

Copying a quota policy

You can copy an existing quota policy.

About this task

Because only a single, uniquely named quota policy can be associated with each virtual server, you can copy a quota policy to save time and effort. Copy a quota policy, give it a new name, assign it to a different virtual server, and modify the quota policy rules as needed.

Steps

1. Use the `volume quota policy copy` command to copy an existing quota policy.

   When you copy a quota policy, you must specify the virtual server name, the name of the quota policy you're copying, and a new name for the copy.

   **Note:** A quota policy name cannot exceed 32 characters in length.

   **Example**

   The following example copies a quota policy named `quota_policy_vs1` on a virtual server named `vs1`. The name of the copy is `quota_policy_vs2`.

   ```
   node::> volume quota policy copy -vserver vs1 -policy-name quota_policy_vs1 -new-policy-name quota_policy_vs2
   ```

   2. Use the `volume quota policy show` command to display information about the original quota policy and its copy.

   3. Use the `vserver modify` command to assign the new quota policy to a virtual server.

Related tasks

*Assigning a quota policy to a virtual server* on page 155

Renaming a quota policy

You can rename an existing quota policy.

Steps

1. Use the `volume quota policy rename` command to rename an existing quota policy.

   When you rename a quota policy, you must specify the virtual server name, the name of the quota policy you're renaming, and a new name for the quota policy.

   **Note:** A quota policy name cannot exceed 32 characters in length.
Example
The following example renames a quota policy named quota_policy_vs1 on a virtual server named vs1. The new name of the quota policy is quota_policy_vs1_old.

```
node::> volume quota policy copy -vserver vs1 -policy-name quota_policy_vs1
   -new-policy-name quota_policy_vs1_old
```

2. Use the `volume quota policy show` command to display information about the renamed quota policy.

Deleting a quota policy
You can delete a quota policy.

Steps
1. Use the `volume quota policy delete` command to delete an existing quota policy.

   When you delete a quota policy, you must specify the virtual server name and the name of the quota policy you're deleting.

Example
The following example deletes a quota policy named quota_policy_vs1_old on a virtual server named vs1.

```
node::> volume quota policy copy -vserver vs1 -policy-name quota_policy_vs1_old
```

2. Use the `volume quota policy show` command to verify that the quota policy has been deleted.

Assigning a quota policy to a virtual server
You can assign a quota policy to a virtual server and all of the volumes it contains.

Before you begin
A virtual server and a quota policy must exist before you can assign a quota policy to a virtual server.

Steps
1. Use the `vserver modify` command to assign a quota policy to a virtual server.

   When you assign a quota policy to a virtual server, you must specify the virtual server name and name of the quota policy. Only a single, uniquely named quota policy can be associated with each virtual server.
Example
The following example assigns a quota policy named quota__policy_vs1 to the virtual server named vs1.

node::> vserver modify -vserver vs1 -policy-name quota_policy_vs1

2. Use the vserver show command to display information about the virtual server and quota policy.

Related tasks
Copying a quota policy on page 154

Creating a quota policy rule
You can create a quota policy rule for a quota policy.

Before you begin
A quota policy must exist before you can create a quota policy rule.

Steps
1. Use the volume quota policy rule create command to create a quota policy rule.

   When you create a quota policy, you must specify the virtual server and name of the quota policy. A single quota policy can be associated with a single virtual server.

   • Virtual server name
   • Quota policy name
   • Volume name
   • Quota target type—This parameter specifies the type of the quota target (tree, user, or group) for which you are creating a rule.

   Note: Note that quota policy rules are supported only for tree quota types at this time.

   • Target to which the rule applies—This parameter specifies the name of the qtree to which the quota policy rule applies.

You can optionally specify the following additional attributes for the quota policy rule:

• Hard disk limit—This attribute specifies a hard limit for the disk space that can consumed by the quota target. When the hard disk space limit is reached, no additional disk space can be consumed by the specified target. The value that you specify for this parameter should be greater than or equal to the threshold and soft disk limit.

• Hard file limit—This attribute specifies a hard limit for the number of files permitted on the quota target. When the hard number of files limit is reached, no additional files can be added
to the specified target. The value that you specify for this parameter should be greater than or equal to the soft file limit.

- Threshold for limits—This attribute specifies the disk limit threshold for the quota target. The value that you specify for this parameter should be greater than or equal to the soft disk limit and equal to or less than the disk limit.

- Soft disk limit—This attribute specifies a soft limit for the disk space that can be consumed by the quota target. The value that you specify for this parameter should be equal to or less than the threshold and the disk limit.

- Soft file limit—This attribute specifies a soft limit for the number of files permitted on the quota target. The value that you specify for this parameter should be equal to or less than the file limit.

**Example**

The following example creates a quota policy rule on virtual server vs1 for the quota policy named quota_policy_vs1. This quota policy applies to the qtree named qtree1 on volume vol1.

```
node::> volume quota policy rule create -vserver vs1 -policy-name quota_policy_vs1 -volume vol1 -type tree -target qtree1
```

2. Use the `volume quota policy rule show` command to display information about the new quota policy rule.

**Next topics**

- Displaying information about quota policy rules on page 157
- Modifying a quota policy rule on page 158
- Deleting a quota policy rule on page 159

**Related tasks**

- Creating a qtree on page 141
- Creating a qtree on page 141

**Displaying information about quota policy rules**

You can display information about quota policy rules.

**Step**

1. Use the `volume quota policy rule show` command to display information about quota policy rules.

   If you do not specify any parameters, the command displays the following information about quota policy rules:

   - Virtual server name
   - Quota policy name
   - Volume name
• Type of quota policy rule
• Target of the quota policy rule
• Qtree name
• Hard disk limit
• Soft disk limit
• Hard file limit
• Soft file limit
• Threshold

**Example**
The following example displays information about a quota policy rule for a tree quota. It exists on virtual server vs5 for the quota policy named quota_policy_5. This quota policy applies to the target qtree5 on volume vol5.

```bash
node::> volume quota policy rule show
Virtual Server: vs5     Policy: quota_policy_5       Volume: vol5

<table>
<thead>
<tr>
<th>Type</th>
<th>Target</th>
<th>Qtree</th>
<th>Disk Limit</th>
<th>Soft Disk Limit</th>
<th>Files Limit</th>
<th>Soft Files Limit</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>tree</td>
<td>qtree5</td>
<td>&quot; &quot;</td>
<td>20GB</td>
<td>18GB</td>
<td>100000</td>
<td>80000</td>
<td>16GB</td>
</tr>
</tbody>
</table>
```

**Modifying a quota policy rule**
You can modify an existing quota policy rule.

**Steps**

1. Use the `volume quota policy rule modify` command to modify a quota policy rule.

   When you modify a quota policy rule, you must specify the virtual server and name of the quota policy. A single quota policy can be associated with a single virtual server.

   • Virtual server name
   • Quota policy name
   • Volume name
   • Quota target type
   • Target to which the rule applies.

   You can then modify the following attributes for the quota policy rule:

   • Hard disk limit—This attribute specifies a hard limit for the disk space that can be consumed by the quota target. When the hard disk space limit is reached, no additional disk space can be consumed by the specified target. The value that you specify for this parameter should be greater than or equal to the threshold and soft disk limit.
   • Hard file limit—This attribute specifies a hard limit for the number of files permitted on the quota target. When the hard number of files limit is reached, no additional files can be added
to the specified target. The value that you specify for this parameter should be greater than or equal to the soft file limit.

- Threshold for limits—This attribute specifies the disk limit threshold for the quota target. The value that you specify for this parameter should be greater than or equal to the soft disk limit and equal to or less than the disk limit.
- Soft disk limit—This attribute specifies a soft limit for the disk space that can be consumed by the quota target. The value that you specify for this parameter should be equal to or less than the threshold and the disk limit.
- Soft file limit—This attribute specifies a soft limit for the number of files permitted on the quota target. The value that you specify for this parameter should be equal to or less than the file limit.

**Example**
The following example modifies a quota policy rule for the quota policy named quota_policy_0. This quota policy exists on virtual server vs0 and applies to the qtree named qtree1 on volume vol0. The hard disk limit is set to 20 GB and the hard file limit is set to 100,000 files.

```
node::> volume quota policy rule modify -vserver vs0 -policy-name quota_policy_0 -volume vol0 -type tree -target qtree1 -disk-limit 20GB -file-limit 100000
```

2. Use the `volume quota policy rule show` command to display information about the modified quota policy rule.

### Deleting a quota policy rule
You can delete a quota policy rule.

**Steps**

1. **Use the `volume quota policy rule delete` command to delete a quota policy rule.**
   
   You must enter the following information to delete a quota policy rule:

   - Virtual server name
   - Quota policy name
   - Volume name
   - Quota target type
   - Target to which the rule applies

   **Example**
The following example deletes a quota policy rule on virtual server vs1 for the quota policy named quota_policy_1. This quota policy applies to the qtree named qtree1 on volume vol1.

   ```
   node::> volume quota policy rule delete -vserver vs1 -policy-name quota_policy_1 -volume vol1 -type tree -target qtree1
   ```

2. Use the `volume quota policy rule show` command to verify that the quota policy rule has been deleted.
Activating and deactivating quota rules for a volume

You can change the quota state and other quota attributes of a volume.

**Before you begin**

A volume must have a quota policy rule associated with it before you can modify the volume's quota attributes.

**Steps**

1. Use the `volume quota modify` command to change the quota state or other quota attributes of a volume.

   When you change the quota attributes of a volume, you must specify the virtual server name and name of the volume whose quota attributes you want to change. You can change the following attributes:
   - Quota state
   - Whether quota messages are logged or not
   - Frequency with which messages are sent

2. Use the `-state` parameter to deactivate, activate, or resize a quota for a volume.

   - **off**—Setting the quota state to `off` indicates that quotas are deactivated for the specified volume.
   - **on**—Setting the quota state to `on` indicates that quotas are activated for the specified volume.
   - **resize**—Setting the quota state to `resize` indicates that the quota limit and threshold will be resized according to the quota policy you've defined.

**Example**

The following example activates quotas on the volume named `vol1`, which exists on `vserver vs1`. Also, logging is enabled and messages are sent every hour and a half.

```
node::> volume quota modify -vserver vs1 -volume vol1 -state on -
    logging on -logging-interval 90m
```

3. Use the `job show` and `job watch-progress` commands, respectively, to monitor the progress of the modify operation.

4. Use the `volume quota show` command to display information about a volume's quota states.

**Related concepts**

*About mirroring a volume that contains quotas* on page 162
Displaying a quota report

You can display a quota report that includes quota file and disk space usage information.

**Step**

1. Use the `volume quota report` command to display quota file and disk space usage information for all online volumes on a virtual server.

   The command output depends on the parameter or parameters specified with the command. If no parameters are specified, the command displays the following information:

   - Virtual server name
   - Volume name
   - Qtree name
   - Quota type
   - Quota target ID
   - Disk space used
   - Disk space limit
   - Files used
   - File limit
   - Quota specifier

**Example**

The following example displays a quota report for the virtual server named vs0.

```
node::> volume quota report

Virtual Server: vs0

<table>
<thead>
<tr>
<th>Volume</th>
<th>Tree</th>
<th>Type</th>
<th>ID</th>
<th>Used</th>
<th>Limit</th>
<th>Used</th>
<th>Limit</th>
<th>Specifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>vol1</td>
<td>-</td>
<td>tree *</td>
<td></td>
<td>0</td>
<td>200G</td>
<td>0</td>
<td>2500</td>
<td>*</td>
</tr>
<tr>
<td>vol1</td>
<td>qtree1</td>
<td>tree 1</td>
<td></td>
<td>100G</td>
<td>500G</td>
<td>1022</td>
<td>5000</td>
<td>qtree1</td>
</tr>
<tr>
<td>vol2</td>
<td>-</td>
<td>tree *</td>
<td></td>
<td>0</td>
<td>200G</td>
<td>0</td>
<td>2500</td>
<td>*</td>
</tr>
<tr>
<td>vol2</td>
<td>qtree2</td>
<td>tree 5</td>
<td></td>
<td>353G</td>
<td>500G</td>
<td>2034</td>
<td>5000</td>
<td>qtree2</td>
</tr>
<tr>
<td>vol2</td>
<td>qtree3</td>
<td>tree 10</td>
<td></td>
<td>750G</td>
<td>1500G</td>
<td>3035</td>
<td>5000</td>
<td>qtree3</td>
</tr>
<tr>
<td>vol2</td>
<td>qtree4</td>
<td>tree 11</td>
<td></td>
<td>550G</td>
<td>-</td>
<td>1099</td>
<td>-</td>
<td>qtree4</td>
</tr>
</tbody>
</table>
```

**About moving a volume that contains quotas**

You can move a volume that contains quotas.

You can move a volume that contains quotas from one aggregate or node to another within the same virtual server. All of the existing quota policies, quota policy rules, and attributes are replicated from the original location and to the new location. The following caveats apply to modifying a quota while moving the volume that contains it:
• After you initiate a volume move, you cannot activate or deactivate a quota until the move operation is complete.

• You can, however, resize a quota on the source volume that contains it after initiating a request to move that volume. In this scenario, the updated quota rules are replicated to the new volume location after the move operation is complete.

Related concepts

How moving a volume works on page 133

Related tasks

Moving a volume on page 133

About mirroring a volume that contains quotas

You can create load sharing and data-protection mirrors of a parent volume that contains quotas.

You can create load sharing and data-protection mirrors of a parent volume that contains quotas just as you would for a volume that doesn't.

The following caveats apply to creating load sharing and data-protection mirrors of volumes that contain quotas:

• Because you cannot write data to a load sharing mirror, no quota accounting occurs for the mirror. No quota accounting occurs for data-protection mirrors, either.

• For mirrors of volumes that contain quotas, quota policies and rules are not replicated to the mirror.

• When you promote a mirror of a volume that contains quotas, you must use the volume quota policy modify command to explicitly activate quotas on the promoted volume.

• You can display information about qtrees that exist within a mirror of a volume that contains quotas. However, you cannot manage (create, modify, or delete) the qtrees on the mirror. Note that information displayed about the qtrees (including name, security style, oplock mode, and other attributes) may not be synchronized between the read-write volume and the mirror, depending on the mirror's replication schedule. But after the read-write volume is replicated to the mirror, qtree information is synchronized.

Related concepts

How to protect your data on page 165

Related tasks

Activating and deactivating quota rules for a volume on page 160

Displaying information about qtrees on page 143
About restoring Snapshot copies of a volume that contains quotas

You can create and restore Snapshot copies of a volume that contains quotas.

You can create and restore Snapshot copies of a volume that contains quotas just as you would for a volume that doesn't. The following caveats apply to managing Snapshot copies of volumes that contain quotas:

- You cannot manage Snapshot copies of quotas or quota policies and their rules independently of the volume that contains them. You can only manage the volume itself and its Snapshot copies.
- When restoring a Snapshot copy of a volume, the quota state contained in Snapshot copy becomes the state of the restored volume. This means that the quota rules enforced for the restored volume can be different from the rules enforced for the volume before you restored it. Therefore, after restoring a Snapshot copy of a volume that contain quotas, run the `volume quota report` command and resize or reinitialize the quota as needed.

Related tasks

- Restoring the contents of a volume from a Snapshot copy on page 170
- Restoring the contents of a volume from a Snapshot copy on page 170
Data ONTAP Cluster-Mode provides several mechanisms to protect your data.

A disaster is a situation in which data from one source is temporarily or permanently lost and must be restored from a backup location. An example of a disaster is a power failure on a disk shelf; in this case; data that is stored on the shelf cannot be retrieved until power is restored. If the data is duplicated on mirrors or tape backups, it can be accessed while the primary disk shelf is unavailable.

Cluster-Mode provides the following mechanisms for backing up data:

- **Snapshot copies.** Users can copy individual files out of Snapshot copies, or an administrator can promote the contents of a Snapshot to the read-write volume.
- **Mirrors.** An administrator can promote a load-sharing or data protection mirror to be the parent read-write volume of a volume family.
- **Tape backups of aggregates.** See the *Release Notes* for the list of supported NDMP-compliant tape backup products.

The following table lists the differences between the components of a complete disaster recovery setup.

**Table 4: Comparison of Backup Types**

<table>
<thead>
<tr>
<th></th>
<th>Snapshot copies</th>
<th>Mirrors</th>
<th>Tape backup</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Creation speed</strong></td>
<td>Fast</td>
<td>Medium</td>
<td>Slow</td>
</tr>
<tr>
<td>Snapshot copies</td>
<td>are located on the source volume.</td>
<td>Initial creation involves copying all data in the volume; only changed data is propagated on subsequent replications.</td>
<td></td>
</tr>
<tr>
<td><strong>Retrieval speed of single file</strong></td>
<td>Fast</td>
<td>Fast</td>
<td>N/A</td>
</tr>
<tr>
<td>Users can retrieve previous versions of their own files.</td>
<td>Assumes the mirror is mounted at a user-visible location; otherwise, an administrator must intervene.</td>
<td>It is usually inefficient to restore a single file from tape.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Snapshot copies</td>
<td>Mirrors</td>
<td>Tape backup</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Retrieval speed of</td>
<td>Fast</td>
<td>Fast</td>
<td>Medium</td>
</tr>
<tr>
<td>entire volume</td>
<td>You can promote the contents of the Snapshot copy to read-write status.</td>
<td>You can remove the mirror from the mirror group and convert it to read-write access.</td>
<td>Dependent on speed of tape drive and amount of data.</td>
</tr>
<tr>
<td>Available if primary</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>aggregate fails?</td>
<td>Snapshot copies cannot be accessed if the source volume is offline.</td>
<td>Data can be restored from a mirror on other aggregate.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**: The performance of Snapshot copies and mirrors is dependent on the performance and reliability of the underlying media. For instance, Fibre Channel-backed SCSI disk arrays have better performance and greater mean time between failure (MTBF) for disk drives than do ATA disk arrays.

**Next topics**

*How Snapshot copies work* on page 167
*How mirrors work* on page 175
*Types of mirrors you can create* on page 175
*Mirror location in the global namespace* on page 176
*Pattern matching path names* on page 176
*Replicating between two virtual servers requires the same language settings* on page 177
*Mirror limitations* on page 177
*Load-sharing mirror management* on page 180
*Managing data protection mirror* on page 189
*Recovering a lost source volume from a mirror* on page 193
*Deleting a mirror* on page 193

**Related concepts**

*How Snapshot copies work* on page 167
*How mirrors work* on page 175
*About mirroring a volume that contains quotas* on page 162

**Related tasks**

*Restoring the contents of a volume from a Snapshot copy* on page 170
How Snapshot copies work

A Snapshot copy is a lightweight copy of a volume representing the volume's contents at a particular point in time.

A Snapshot copy of a volume is located on the parent volume but has read-only access. It represents the contents of the original volume at a particular point in time. A parent volume and a Snapshot copy of it share disk space for all blocks that have not been modified between the creation of the volume and the time the Snapshot copy is made, thereby making Snapshot copies lightweight. Similarly, two Snapshot copies share disk space for those blocks that were not modified between the times that the two Snapshot copies were created. A chain of Snapshot copies can be created to represent the state of a volume at a number of points in time. Snapshot copies can be accessed online, enabling users to retrieve their own data from past copies, rather than asking a system administrator to restore data from tape. Administrators can restore the contents of a volume from a Snapshot copy.

Each volume has a .snapshot directory that is accessible to NFS users by using the ls command and to CIFS users by double-clicking the ~snapshot folder. The contents of the .snapshot directory are a set of subdirectories, labeled by type, date, and time, resembling the following:

```
$ ls .snapshot
daily.2006-05-14_0013/          hourly.2006-05-15_1306/
hourly.2006-05-15_1106/         weekly.2006-05-14_0019/
hourly.2006-05-15_1206/         
```

Each subdirectory of the .snapshot directory includes a list of the parent volume's files and directories. If users accidentally delete or overwrite a file, they can locate it in the most recent Snapshot directory and restore it to their main read-write volume simply by copying it back to the main directory. The following example shows how an NFS user can locate and retrieve a file named my.txt from the .snapshot directory:

```
$ ls .snapshot
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
$ ls my.txt
$ ls .snapshot/hourly.2006-05-15_1506/my.txt
$ ls my.txt
my.txt
```

Note that, unlike in Data ONTAP 7G or earlier, the .snapshot directory is always visible to NFS clients and available from within the volume, and not visible but still available from any other volume. In Data ONTAP 7G or earlier, you can customize the behavior of the .snapshot directory.
In Data ONTAP Cluster-Mode, you can have a maximum of 128 Snapshot copies of a regular FlexVol parent volume.

If a volume has reached the maximum number of Snapshot copies, use the `volume snapshot delete` command to delete unused copies.

**Creating a single Snapshot copy**

You can manually create a single Snapshot copy of a volume.

**Step**

1. Use the `volume snapshot create` command to create a single Snapshot copy.

   Specify a virtual server name, source volume name, and Snapshot copy name. You can optionally specify a comment for the Snapshot copy.

   **Example**
   
   The following example creates a Snapshot copy named `user_anna_snap_1` of a source volume named `user_anna` on a virtual server named `vs1`:

   `node::> volume snapshot create -vserver vs1 -volume user_anna -snapshot user_anna_snap_1`
Modifying a Snapshot copy

You can change the comment associated with a Snapshot copy.

**Step**

1. Use the `volume snapshot modify` command to change the comment associated with a Snapshot copy.

**Example**
The following example adds a comment named "Anna's snapshot" to a Snapshot copy named `user_anna_snap_1` of a source volume named `user_anna` on a virtual server named `vs1`.

```
node::> volume snapshot modify -vserver vs1 -volume user_anna -snapshot user_anna_snap_1 -comment "Anna's snapshot"
```

Displaying information about Snapshot copies

You can display information about Snapshot copies.

**Step**

1. Use the `volume snapshot show` command to display information about Snapshot copies.

   The command displays the following information about Snapshot copies:
   
   • Virtual server name  
   • Volume name  
   • Snapshot copy name  
   • Size  
   • Total number of blocks  
   • Number of used blocks

   Other information is displayed in a detailed view and if other parameters are specified. See the reference page for the command for details.

**Example**
The following example displays information about all Snapshot copies of a volume named `user_raoul`:

```
node::> volume snapshot show -volume user_raoul
---Blocks---
<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Snapshot</th>
<th>Size</th>
<th>Total%</th>
<th>Used%</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>user_raoul</td>
<td>daily.2006-10-12_0011</td>
<td>1.95MB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>daily.2006-10-13_0011</td>
<td>928KB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hourly.2006-10-13_0606</td>
<td>188KB</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
```
Restoring the contents of a volume from a Snapshot copy

You can restore the contents of a volume from a Snapshot copy to quickly recover lost or damaged data.

**Step**

1. The `volume snapshot promote` command restores the contents of a volume from a Snapshot copy.

   The command requires the advanced privilege level or higher.

   **Note:** NetApp recommends that you manually replicate all mirrors of a volume immediately after you promote its Snapshot copy. Not doing so can result in unusable mirrors that must be deleted and recreated.

**Example**

The following example restores data to a volume named `src_os` from a Snapshot copy named `src_os_snap_3` on a virtual server named `vs0`:

```
node::> volume snapshot promote -vserver vs0 -volume src_os -snapshot src_os_snap_3
```

**Related concepts**

- How to protect your data on page 165
- How Snapshot copies work on page 167
- About restoring Snapshot copies of a volume that contains quotas on page 163
- About restoring Snapshot copies of a volume that contains quotas on page 163

Renaming a Snapshot copy

You can rename a Snapshot copy.

**Step**

1. Use the `volume snapshot rename` command to rename a Snapshot copy.

   **Note:** You cannot rename a Snapshot copy that is created as a reference copy during execution of the `volume copy` or `volume move` commands.
Example
The following example renames a Snapshot copy named dept_acctg_backup to dept_acctg_snap. The Snapshot copy is of a volume named dept_acctg on a virtual server named vs0.

node::> volume snapshot rename -vserver vs0 -volume dept_acctg -snapshot dept_acctg_backup -newname dept_acctg_snap

Deleting a Snapshot copy

You can delete a Snapshot copy.

Step

1. Use the `volume snapshot delete` command to delete a Snapshot copy.

Example
The following example deletes a Snapshot copy named user_joy_snap_3 of a volume named user_joy on a virtual server named vs1.

node::> volume snapshot delete -vserver vs1 -volume user_joy -snapshot user_joy_snap_3

Related concepts

*How many Snapshot copies you can have* on page 168

Computing reclaimable space for Snapshot copies

You can calculate the amount of disk space that can be reclaimed if Snapshot copies are deleted.

Step

1. Use the `volume snapshot compute-reclaimable` command to calculate the amount of disk space that can be reclaimed if specified Snapshot copies are deleted.

The command is available only at the advanced privilege level and higher.

This command draws heavily on resources; using it can reduce the performance of the system for client requests and other system processes. Queries that use wildcards such as `*` are therefore disabled for this command. If specifying more than one Snapshot copy, use a comma-separated list of Snapshot copies with no spaces after the commas. You should specify no more than three Snapshot copies in a single query.

Example
The following example calculates the amount of space that can be reclaimed on a volume named dept_eng, on a virtual server named vs1, if the Snapshot copies named weekly.2006-01-08_0017 and daily.2006-01-09_0013 are deleted.

node::> set -priv advanced
node::*> volume snapshot compute-reclaimable -vserver vs1 -volume dept_eng -snapshots weekly.2006-01-08_0017,daily.2006-01-09_0013
Creating a Snapshot policy

You can create a Snapshot policy to specify the frequency and maximum number of automatically created Snapshot copies.

Step

1. Use the `volume snapshot policy create` command to create a Snapshot policy.

   When applied to a volume, a Snapshot policy specifies a schedule or schedules on which Snapshot copies are taken and the maximum number of Snapshot copies that each schedule can take. A Snapshot policy can include from one to five schedules. To create schedules that can be used in Snapshot policies, use the `job schedule cron create` or `job schedule interval create` commands.

Example

The following example creates a Snapshot policy named `policy2`. It runs on two schedules: a schedule named `8hrs` with a maximum of three Snapshot copies, and a schedule named `6am` with a maximum of two Snapshot copies. The policy is enabled.

```
node::> volume snapshot policy create -policy policy2 -enabled true -schedule1 8hrs -count1 3 -schedule2 6am -count2 2
```

Next topics

- Modifying a Snapshot policy on page 172
- Displaying information about Snapshot policies on page 173
- Adding a schedule to a Snapshot policy on page 173
- Deleting a Snapshot policy on page 174

Modifying a Snapshot policy

You can change the description associated with a Snapshot policy.

Step

1. Use the `volume snapshot policy modify` command to modify the description associated with a Snapshot policy.

Example

The following example adds the comment "For user volumes" to the Snapshot policy named `policy2`.

```
node::> volume snapshot policy modify -policy policy2 -comment "For user volumes"
```
Displaying information about Snapshot policies

You can display information about Snapshot policies.

Step

1. Use the `volume snapshot policy show` command to display information about Snapshot policies.

Example

The following example displays information about the Snapshot policy named policy2:

```
node::> volume snapshot policy show -policy policy2
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Number Of Schedules</th>
<th>Is Enabled</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>3</td>
<td>true</td>
<td>Default policy with hourly, daily &amp; weekly</td>
</tr>
<tr>
<td></td>
<td>Schedule: hourly</td>
<td></td>
<td>Count: 6</td>
</tr>
<tr>
<td></td>
<td>daily</td>
<td></td>
<td>Count: 2</td>
</tr>
<tr>
<td></td>
<td>weekly</td>
<td></td>
<td>Count: 2</td>
</tr>
<tr>
<td>none</td>
<td>0</td>
<td>false</td>
<td>Policy for no automatic snapshots.</td>
</tr>
<tr>
<td></td>
<td>Schedule: -</td>
<td></td>
<td>Count: -</td>
</tr>
<tr>
<td>nosnapshot</td>
<td>1</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Schedule: hourly</td>
<td></td>
<td>Count: 2</td>
</tr>
</tbody>
</table>

3 entries were displayed.

Adding a schedule to a Snapshot policy

You can add a schedule to an existing Snapshot policy.

Step

1. You can add a schedule to an existing Snapshot policy by using the `volume snapshot policy add-schedule` command.

Example

The following example adds a schedule named halfhour with a maximum count of five Snapshot copies to a Snapshot policy named policy2:

```
node::> volume snapshot policy add-schedule -policy policy2
-schedule halfhour -count 5
```

Next topics

- Modifying the maximum number of Snapshot copies for a Snapshot policy’s schedule on page 174
- Removing a schedule from a Snapshot policy on page 174
Modifying the maximum number of Snapshot copies for a Snapshot policy's schedule

You can change the maximum number of Snapshot copies for a Snapshot policy's schedule.

Step

1. Use the `volume snapshot policy modify-schedule` command to modify the maximum number of Snapshot copies for a Snapshot policy's schedule.

   Example
   The following example changes the maximum number of Snapshot copies to four for a schedule named halfhour on a Snapshot policy named policy2.

   ```
   node::> volume snapshot policy modify-schedule -policy policy2 -schedule halfhour -count 4
   ```

Removing a schedule from a Snapshot policy

You can remove a schedule from a Snapshot policy.

Step

1. Use the `volume snapshot policy remove-schedule` command to remove a schedule from a Snapshot policy.

   Example
   The following example removes a schedule named 8hrs from a Snapshot policy named policy2.

   ```
   node::> volume snapshot policy remove-schedule -policy policy2 -schedule 8hrs
   ```

Deleting a Snapshot policy

You can delete a Snapshot policy.

Step

1. Use the `volume snapshot policy delete` command to delete a Snapshot policy.

   If you delete a Snapshot policy that is being used by one or more volumes, Snapshot copies of the volume or volumes are no longer taken according to the deleted policy. Before you delete a Snapshot policy, you should use the `volume modify` command to dissociate the Snapshot policy from each volume that uses it.

   Example
   The following example deletes a Snapshot policy named policy2.

   ```
   node::> volume snapshot policy delete -policy policy2
   ```
How mirrors work

You create a mirroring relationship between a source volume and a destination volume. The source volume is a read-write volume that clients can access and modify. The destination volume is a read-only volume that exports a Snapshot copy to clients for read-only access.

Snapshot copies are used by the source volume to update destination volumes. Snapshot copies are transferred from the source volume to the destination volume using an automated schedule or manually; therefore, mirrors are updated asynchronously. You use the set of snapmirror commands to create and manage mirroring relationships.

Data ONTAP updates a mirror using logical transfers. Logical mirroring transfers incremental differences between Snapshot copies on the source volume to the destination volume to update the mirror. Logical mirroring transfers use the following process:

1. Create a base Snapshot copy on the source volume.
2. Find the newest Snapshot copy on the destination volume that is common to both the source volume and destination volume. Typically, the latest Snapshot copy on the destination is the newest common Snapshot copy.
3. Starting from the newest common Snapshot copy on the source volume, transfer incremental differences between succeeding Snapshot copies to the destination volume.
4. After the base Snapshot copy on the source volume has been transferred to the destination volume, export that Snapshot copy on the destination volume to clients for read-only access.

Types of mirrors you can create

You can create either a load-sharing mirror or a data protection mirror.

A set of load-sharing mirrors consists of a source volume that can fan out to one or more destination volumes. Each load-sharing mirror in the set must belong to the same virtual server as their source volume. The load-sharing mirrors should also be created on different aggregates and accessed by different nodes in the cluster to achieve proper load balancing of client requests.

Note: A source volume can have only one set of load-sharing mirrors.

A load-sharing mirror is mounted in the same area of the virtual server namespace as it source volume to provide additional read-only access to clients. This is useful for frequently read, but infrequently updated data, such as shared binary files. For example, you can set up one or more load-
sharing mirrors to a source volume that is mounted at the /bin directory. Client requests to read the binaries on that volume are routed to the load-sharing mirrors, not to the source volume.

A data protection mirror has a one-to-one relationship with a source volume. It can be created on the same aggregate as the source volume and on the same virtual server or on a different virtual server. You should create the data protection mirror on a different aggregate in order to recover from the failure of the source volume’s aggregate and the same virtual server is required to failover from the source volume.

A data protection mirror can be used for limited disaster recovery, off-loading tape backup, data distribution, and taking production data offline for research, such as data mining.

**Mirror location in the global namespace**

A mirror's location in the global namespace depends on its type, whether it is a load-sharing mirror or a data protection mirror.

A load-sharing mirror is a read-only volume and is automatically mounted with the same junction path as its source volume. If a source volume has one or more load-sharing mirrors, client requests are automatically routed to the load-sharing mirror or mirrors to reduce the load on the source volume.

A data protection mirror can be located on a different virtual server from the source read-write volume. It must be mounted at a different location from its source volume.

**Pattern matching path names**

You can use pattern matching when you use `snapmirror` commands to have the command work on selected mirroring relationships.

The `snapmirror` commands use fully qualified path names in the following format:

```
cluster://vserver/volume
```

You can abbreviate the path name by not entering the cluster or vserver parts. If you do this, the `snapmirror` command assumes the local cluster and vserver context of the user.

Assuming the cluster is called cluster1, the virtual server is called vserver1, and the volume is called vol1, the fully qualified path name is the following.

```
cluster1://vserver1/vol1
```

You can make the `snapmirror` commands work on the same volume by excluding the cluster name from the path name because the command assumes the local cluster to be cluster1.

```
//vserver1/vol1
```

Likewise, you can exclude the cluster name and virtual server name from the path name because the command assumes the local cluster to be cluster 1 and the vserver context to be vserver1.

```
vol1
```
You can use the asterisk (*) in paths as a wildcard to select matching, fully-qualified path names. The following table lists examples of using the wildcard to select a range of volumes.

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches all paths.</td>
</tr>
<tr>
<td>*volA</td>
<td>Matches all virtual servers and volumes with cluster names ending in volA.</td>
</tr>
<tr>
<td>aClus*</td>
<td>Matches all virtual servers and volumes with cluster names beginning with aClus.</td>
</tr>
<tr>
<td><em>/vol</em></td>
<td>Matches all clusters and virtual servers with volume names beginning with vol.</td>
</tr>
</tbody>
</table>
| //vol*| Does not match anything because no fully qualified path name begins with //.

**Replicating between two virtual servers requires the same language settings**

Problems accessing data from NFS or CIFS clients can occur if the source volume and destination volume of a mirroring relationship have different language settings.

This is not a problem if the source and destination volumes are located on the same virtual server because the language is set on the virtual server. If you plan to create a mirroring relationship between volumes on two different virtual servers, ensure that the language setting on the virtual servers is the same.

**Mirror limitations**

There are some limitations of which you should be aware when working with load-sharing or data protection mirrors.

The following limitations apply to mirrors:

- If a read-write volume has no load-sharing mirrors, you can mount it normally and client requests are always directed to it. However, when a read-write volume has a load-sharing mirror (or mirrors), client requests are directed to the mirror only after the mirror has been initialized (has a Snapshot copy exported to clients for read-only access). As a result, it may take several minutes before client requests are directed to a newly created load-sharing mirror.
- When a load-sharing mirror is removed, or when the last one is removed if there are multiple load-sharing mirrors, all clients are immediately directed to the read-write volume. If a client requires read-write access to a read-write volume that has one or more load-sharing mirrors, you must mount it through the /.admin link at the root of the virtual server.
- If a Windows client performs a CIFS create or a UNIX client performs an NFS mount to a source volume with load-sharing mirrors, ensure that you manually update the load-sharing mirrors first. If you do not, newly written data on the source volume will not be visible to clients unless they access the source volume through the /.admin link.
• You can create a fan out of both load-sharing mirrors and data protection mirrors from a common source volume, but you cannot cascade mirrors. For example, you cannot mirror a data protection mirror to another data protection mirror.

Next topics

SnapMirror configuration limit on page 178
Active transfer limits on page 178
SnapMirror fanout limits on page 179
Maximum number of Snapshot copies for volumes that are mirrored on page 180
Cannot automatically delete Snapshot copies on destination volumes on page 180

SnapMirror configuration limit

You can have a total of 500 SnapMirror relationships configured on one cluster.

A SnapMirror relationship consists of a source volume and a destination volume. For example, if you have a set of load-sharing mirrors that consists of a source volume and five destination volumes, you have five SnapMirror relationships.

The SnapMirror relationships can be for load-sharing mirrors, data protection mirrors, or both.

Active transfer limits

There are limits to the number of active transfers allowed at one time.

Active transfers refer to the total number of SnapMirror transfers, volume move transfers, volume member move transfers, and volume copy transfers. Depending on the configuration, the lower of the following two limits could be the applicable limit.

• 100 concurrently active endpoints in any given cluster. An endpoint is a flexible volume.
• 50 concurrently active flexible volumes on a node. An active flexible volume is one that is either a source or a destination of a transfer.

This limit applies to the case in which no volumes are in a taken over state, that is, a storage failover has not occurred. In the case where storage is temporarily taken over, 100 concurrently active flexible volumes on a node are allowed because the system still has to function when a single node is controlling the storage that usually belongs to two nodes.

Each endpoint of a SnapMirror relationship is counted as an endpoint, even if the endpoint is shared with other SnapMirror relationships.

Example of endpoint count for shared SnapMirror relationships

The following output from the `snapmirror show` command is used for all of the following examples.

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Source Status</th>
<th>Destination Type</th>
<th>Destination Path</th>
<th>Mirror State</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Healthy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

node::> snapmirror show
For the output shown, if transfers were active for all of the shown relationships, there are five source endpoints and five destination endpoints, even though src1 and src2 are shared by multiple destination endpoints.

### Example of determining the number of endpoints

The number of endpoints for the relationships are as follows:

- If only an update from src1 to dest1 were running, there would be two endpoints (1 source and 1 destination).
- If an update from src1 to dest1 and from src1 to dest2 were running, there would be 4 endpoints (2 source and 2 destination).
- If an update from src2 to ls13, ls14, and ls15 were running, there would be 6 endpoints (3 source and 3 destination)

### SnapMirror fanout limits

There are limits to the number of destination volumes a single source volume can have.

The fanout limits depend on the type of mirror that you want to fan out from a single source volume.

- A maximum of one destination volume on a node for a single source volume can be fanned out for load-sharing mirrors. Data ONTAP supports up to 24 nodes in a cluster; therefore, a maximum of 24 destination volumes can be fanned out from a single source volume.
- A maximum of four destination volumes can be fanned out from a single data protection source volume.
- A single source volume can have both one load-sharing destination volume on a node and four data protection destination volumes.
Maximum number of Snapshot copies for volumes that are mirrored

Data ONTAP has a limit to the number of Snapshot copies a volume that is to be mirrored can contain.

A volume that will be mirrored cannot contain more than 128 Snapshot copies.

Whenever an update to a data protection mirror or set of load-sharing mirrors occurs, Data ONTAP creates one new Snapshot copy. This should be considered as you manage the number of Snapshot copies on the source volume. You need to keep the limit far enough below the 128 Snapshot copy limit such that you do not exceed the limit when mirrors update.

Cannot automatically delete Snapshot copies on destination volumes

You cannot automatically delete old Snapshot copies on destination volumes of mirroring relationships.

You might want to try using the `snap autodelete` command to automatically delete Snapshot copies from a destination volume to remove older Snapshot copies, but this is not allowed. The command will fail if you try.

Load-sharing mirror management

Load-sharing mirror management consists of activities such as creating sets of load-sharing mirrors for source volumes, adding load-sharing mirrors to already established sets of load-sharing mirrors, creating or changing the schedule for when a set of load-sharing mirrors are updated, and monitoring load-sharing mirror status.

Next topics

- Mounting a volume that has load-sharing mirrors for NFS clients on page 181
- Mounting a volume that has load-sharing mirrors for CIFS clients on page 181
- Restriction when modifying the source volume on page 181
- Creating a set of load-sharing mirrors on page 182
- Adding a load-sharing mirror to a set of load-sharing mirrors on page 184
- Updating a set of load-sharing mirrors on page 185
- Aborting an update to a load-sharing mirror on page 186
- Scheduling SnapMirror transfers on page 186
- Changing mirroring relationship schedules on page 187
- Listing the schedule state of a mirroring relationship on page 188
- Listing the status of a particular load-sharing mirror on page 188
- Determining whether load-sharing mirrors are up-to-date on page 188
Mounting a volume that has load-sharing mirrors for NFS clients

If you are mounting a volume that has one or more load-sharing mirrors from an NFS client that must have access to the source read-write volume (for instance, to make changes to it), you must mount it through the .admin link at the root of the virtual server.

Step

1. Mount the volume using the /./admin link. The /./admin link routes requests to the parent read-write volume regardless of whether the volume has any mirrors.

Example

For example, if you are mounting a client that requires read-write access to a mirrored volume mounted at /dept/eng/sandbox on a virtual server named engdata, use the following command:

```
# mount -t nfs engdata:/./admin/dept/eng/sandbox mountpoint
```

If you are mounting a client that does not require read-write access to the same volume, use the following command:

```
# mount -t nfs engdata:/dept/eng/sandbox mountpoint
```

Mounting a volume that has load-sharing mirrors for CIFS clients

If you are mounting a volume that has one or more load-sharing mirrors from a CIFS client that must have access to the parent read-write volume (for instance, to make changes to it), you must create a new CIFS share.

Step

1. Use the vserver cifs share create command to maintain access to the parent read-write volume.

Example

For example, if you are mounting a client that requires read-write access to a mirrored volume mounted at /dept/eng/sandbox on a virtual server named engdata, use the following command:

```
node::> vserver cifs share create -vserver engdata -share-name engdata -path /./admin/dept/eng/sandbox
```

Restriction when modifying the source volume

If you create or mount a new volume on a mirrored source volume, or delete or unmount a volume from a mirrored source volume, be sure to manually replicate the source volume's to the load-sharing mirror or mirrors immediately after you mount or unmount the volume.

Failure to do so has the following results:
If you create or mount a new volume on a source volume without replicating the load-sharing mirrors, the new or mounted volume is not visible unless you access it through the / . admin link.

If you delete or unmount a volume on a source volume without replicating the load-sharing mirrors, a client can hang if it attempts to do a directory listing at the read-only mount point of the load-sharing mirrors.

Creating a set of load-sharing mirrors

You can create a set of one or more load-sharing mirrors to a read-write volume to reduce the amount of work that a volume would otherwise have to do.

About this task

This is useful for frequently read but infrequently updated data. An example might be shared binary files. You can set up one or more load-sharing mirrors to a volume that is mounted at the / bin directory. Client requests to read the binaries on that volume are routed to the load-sharing mirrors, not to the read-write volume.

Steps

1. Creating a volume for load-sharing on page 182
2. Creating load-sharing mirror relationships on page 183
3. Creating a baseline for a set of load-sharing mirrors on page 184

Creating a volume for load-sharing

You must create a volume and designate it as a load-sharing mirror before you can create mirror relationships for load-sharing.

Steps

1. Enter the following command to create a volume that will become the load-sharing mirror:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size volume_size -state online -type DP -unixpermissions 777
   ```

   Example

   The following example creates a load-sharing mirror volume named dept_eng_ls_mirror1. The mirror volume is located on a virtual server named vs0. The mirror volume is located on an aggregate named aggr3.

   ```
   node::> volume create -vserver vs0 -volume dept_eng_ls_mirror1 -aggregate aggr3 -type DP
   ```

   See the Data ONTAP Cluster-Mode Administration Reference for details about the volume create command.

2. Repeat the previous step for each load-sharing mirror that you want.
Creating load-sharing mirror relationships

Before you can replicate data from the source read-write volume to the load-sharing mirrors, you create the mirror relationship using the `snapmirror create` command.

Steps

1. Enter the following command to create a load-sharing mirror relationship between the source endpoint and a destination endpoint:

   ```
   snapmirror create -source-path source_endpoint -destination-path destination_endpoint -type LS
   ```

   Example
   The following example creates a load-sharing mirror of the source volume named `dept_eng`. The source volume and the mirrors are located on a virtual server named `vs0`.

   ```
   node::> snapmirror create -source-path //vs0/dept_eng -destination-path //vs0/dept_eng_ls_mirror1 -type LS
   
   [Job 171] Job is queued: snapmirror create the relationship with destination //v
   
   [Job 171] Job succeeded: SnapMirror: done
   ```

   **Note:** You can use one of the available default cron jobs or you can create your own SnapMirror schedule using the `job schedule cron create` command.

   When you create a relationship for a load-sharing mirror, the attributes for that load-sharing mirror (throttles, update schedules, and so on) are shared by all of the load-sharing mirrors in the group.

2. Repeat Step 1 to add load-sharing mirror relationships to the source volume, up to the maximum number allowed for a load-sharing mirror fanout.

   Example
   The following example creates load-sharing mirror relationships between the source volume named `dept_eng` and the destination volumes `dept_eng_ls_mirror2` and `dept_eng_ls_mirror3`.

   ```
   node::> snapmirror create -source-path //vs0/dept_eng -destination-path //vs0/dept_eng_ls_mirror1 -type LS
   
   [Job 172] Job is queued: snapmirror create the relationship with destination //v
   
   [Job 172] Job succeeded: SnapMirror: done
   ```

   ```
   node::> snapmirror create -source-path //vs0/dept_eng -destination-path //vs0/dept_eng_ls_mirror2 -type LS
   
   [Job 173] Job is queued: snapmirror create the relationship with destination //v
   
   [Job 173] Job succeeded: SnapMirror: done
   ```

   ```
   node::> snapmirror create -source-path //vs0/dept_eng -destination-path //vs0/dept_eng_ls_mirror3 -type LS
   ```
Creating a baseline for a set of load-sharing mirrors

You initialize the set of load-sharing mirrors to replicate data on a source volume to the load-sharing mirrors.

Step

1. Enter the following command to initialize all of the load-sharing mirrors in the set:

   `snapmirror initialize-ls-set -source-path source_endpoint`

   **Note:** Do not use the `snapmirror initialize` command to initialize a set of load-sharing mirrors. The `snapmirror initialize` command is for initializing individual volumes.

Example

The following example creates a baseline copy of the source volume named `dept_eng` to all of the load-sharing mirrors created for the source volume. The source volume is located on a virtual server named `vs0`.

```
node::> snapmirror initialize-ls-set //vs0/dept_eng
```

Adding a load-sharing mirror to a set of load-sharing mirrors

You might want to add a load-sharing mirror to a set of load-sharing mirrors if the current number of load-sharing mirrors in that set continually has a large number of requests for data.

About this task

When you add a load-sharing mirror to a load-sharing set, you create the volume that will be the load-sharing mirror, you create the SnapMirror relationship between the source volume and the new load-sharing mirror, and then you initialize the load sharing mirror to the same Snapshot copy of data that every other load sharing mirror in the set has.

Initializing an individual load-sharing mirror

You add a load-sharing mirror to the load-sharing set by initializing the load-sharing mirror. Clients cannot access the added load-sharing mirror until you initialize it.

Before you begin

You must have done the following tasks before you can initialize a load-sharing mirror and add it to the set of load-sharing mirrors:
• Have a set of load-sharing mirrors to which you want to add. That is, you have already created the set of load-sharing mirrors by creating destination volumes, SnapMirror relationships, and initializing those relationships using the `snapmirror initialize-ls-set` command.

• Created the destination volume of the load-sharing mirror you want to add by specifying the DP type option of the `volume create` command.

About this task
Initializing a load-sharing mirror creates a baseline copy of the source volume's data that is equivalent to the most up-to-date copies on the other load-sharing mirrors in the set.

Step

1. Enter the following command to initialize the volume that you are adding to the load-sharing set:

   ```
   snapmirror initialize -source-path source_volume -destination-path destination_volume -type LS
   ```

   **Note:** Do not use the `snapmirror initialize-ls-set` command. The `snapmirror initialize-ls-set` command is for initializing volumes for an entire set of load-sharing mirrors, not for initializing an individual volume.

Example
The following example adds a load-sharing mirror named `dept_eng_ls_mirror4` to a set of load-sharing mirrors of a source volume named `dept_eng`. The source volume and load-sharing mirrors are on the virtual server named `vs0`.

```
node::> snapmirror initialize -source-path node://vs0/dept_eng
   -destination-path //vs0/dept_eng_ls_mirror4 -type LS

[Job 187] Job is queued: snapmirror initialize of destination //vs0/dept_eng_ls_mirror4.
```

After this initial copy, Data ONTAP sees the new load-sharing mirror as part of the set of load-sharing mirrors and will update the set when a scheduled update or manual update of the set occurs.

Updating a set of load-sharing mirrors
You can update a set of load-sharing mirrors if you think an update is necessary before the next scheduled update.

Step

1. Enter the following command to update all of the load-sharing mirrors in the set:

   ```
   snapmirror update-ls-set -source-path source_endpoint
   ```
Example
The following example updates all of the load-sharing mirrors created for the source volume named dept_eng on the virtual server named vs0.

node::> snapmirror update-ls-set -source-path clus1://vs0/dept_eng
[Job 193] Job is queued: snapmirror load-share update for source clus1://vs0/dept_eng.

Abort an update to a load-sharing mirror
You can end an update to a set of load-sharing mirrors if the update started, but did not finish.

About this task
Load-sharing mirrors are either up to date and serving data to clients, or they are lagging and not serving data to clients. If you are aborting an up-to-date load-sharing mirror, transfers to associated up-to-date load-sharing mirrors in the set of load-sharing mirrors are also aborted. If you are aborting a lagging load-sharing mirror, then only the SnapMirror transfer associated with the lagging load-sharing mirror is aborted.

Step
1. Enter the following command to stop replicating data to a particular load-sharing mirror:

snapmirror abort -source-path source_endpoint -destination-path destination_endpoint

Note: You can use the snapmirror abort command on other load-sharing mirrors in the set if those load-sharing mirrors also prevent updates to other load-sharing mirrors in the set

Example
The following example ends the update to the load-sharing mirror named dept_eng_ls_mirror2 on a virtual server named vs0.

node::> snapmirror abort -source-path //vs0/dept_eng -destination-path //vs0/dept_eng_ls_mirror2
[Job 184] Job is queued: snapmirror abort for the relationship with destination
[Job 184] Job succeeded: SnapMirror: done

Scheduling SnapMirror transfers
Unless you created and implemented a schedule for SnapMirror transfers, you are limited to manually updating destination volumes of mirroring relationships.

About this task
You can add a schedule to a mirroring relationship either when you create the relationship or after you create the relationship.
When you add a schedule to a load-sharing mirror, Data ONTAP implements the schedule on the relationships of all the load-sharing mirrors in the group. Data ONTAP determines the load-sharing mirror group by the virtual server and source volume specified by the command.

**Steps**

1. Create the schedule you want to implement using the `job schedule cron create` command.
2. Apply the schedule to the mirroring relationship.

<table>
<thead>
<tr>
<th>If you are applying the schedule...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you created and initialized the mirroring relationship.</td>
<td>Use the <code>-schedule</code> option of the <code>snapmirror modify</code> command.</td>
</tr>
<tr>
<td>When you create the mirroring relationship</td>
<td>Use the <code>-schedule</code> option of the <code>snapmirror create</code> command.</td>
</tr>
</tbody>
</table>

**Changing mirroring relationship schedules**

You can change a schedule that updates mirroring relationships if the schedule impacts other backups or updates.

**About this task**

When you change a schedule to a load-sharing mirror relationship, Data ONTAP makes the change to the relationships of all the load-sharing mirrors in the group. Data ONTAP determines the load-sharing mirror group by the virtual server and source volume specified by the command.

**Steps**

1. Create the new schedule using the `job schedule cron create` command. Creating a schedule is described in the cron job creation section of the *Data ONTAP Cluster-Mode System Administration Guide*. The `job schedule cron create` command is described in the *Data ONTAP Cluster-Mode Administration Reference*.
2. Enter the following command to change a schedule for a mirroring relationship:

```
snapmirror modify -source-path source_endpoint -destination-path destination_endpoint -schedule sched
```

**Example**

The following example changes the update schedule used by a group of load-sharing mirrors for a source volume named dept_eng to a schedule named dept_eng_mirror_sched.

```
node::> snapmirror modify -source-path clus1://vs0/dept_eng
-destination-path clus1://vs0/dept_eng_ls1 -schedule
dept_eng_mirror_sched
```
Listing the schedule state of a mirroring relationship

You might want to see what state a scheduled transfer for a mirroring relationship is in to ensure jobs are running as they should.

Step

1. To see the state of scheduled jobs, enter the following command:

   `job show`

   **Note:** The state of a scheduled job might be dormant. The dormant state means that the job is waiting for the scheduled start time to begin the transfer. There is nothing wrong with the job and you need to do nothing.

Listing the status of a particular load-sharing mirror

You can list the status of a particular load-sharing mirror if you are uncertain of it state. For example, you might want to check the status of a load-sharing mirror if you are synchronizing it with other load-sharing mirrors in a group and you want to know if Data ONTAP is done synchronizing.

Step

1. Enter the following command to list the status of a particular load-sharing mirror:

   `snapmirror show -fields status -destination-volume volume_name`

**Example**

The following example lists the relationship for the load-sharing mirror named `dept_eng_ls_mirror2`.

```
node::> snapmirror show -fields status -destination-volume dept_eng_ls_mirror2
source-path          destination-path                    status
-------------------- ----------------------------------- ------
clus1://vs1/dept_eng clus1://vs1/dept_eng_ls_mirror2     Idle
```

**Note:** You can use one or more `snapmirror show` command options to list more specific information about a load-sharing mirror relationship. See the `snapmirror show` command page for more information.

Determining whether load-sharing mirrors are up-to-date

If you think you might have a problem when updating a set of load-sharing mirrors or you want to update a set of load-sharing mirrors manually and want to ensure that all of the load-sharing mirrors
in the set get updated, you can determine if load-sharing mirrors are up to date using the
\texttt{snapmirror show} command and looking at the exported-snapshot field.

**About this task**

If a load-sharing mirror is lagging behind the most up-to-date load-sharing mirror in the set, the
exported-snapshot field will show a dash (-).

**Step**

1. Enter the following command to list the status of load-sharing mirrors for a particular source
volume:

\texttt{snapmirror show -fields type,exported-snapshot -S source_endpoint}

**Example**
The following example lists the load-sharing mirrors for the source volume named dept_eng and
shows the load-sharing mirrors that are lagging behind the up-to-date mirrors.

\begin{verbatim}
node::> snapmirror show -fields type,exported-snapshot
-S clus1://vs1/dept_eng

source-path           destination-path          type exported-snapshot
--------------------- ------------------------- ---- -----------------
clus1://vs1/dept_eng  clust1://vs1/dept_eng_ls1 LS   -
clus1://vs1/dept_eng  clust1://vs1/dept_eng_ls2 LS   -
clus1://vs1/dept_eng  clust1://vs1/dept_eng_ls3 LS   -
clus1://vs1/dept_eng  clust1://vs1/dept_eng_ls4 LS snapmirror.5_2147484688.2010-04-16_173522
clus1://vs1/dept_eng  clust1://vs1/dept_eng_ls5 LS   -
clus1://vs1/dept_eng  clust1://vs1/dept_eng_ls6 LS snapmirror.5_2147484688.2010-04-16_173522
clus1://vs1/dept_eng  clust1://vs1/dept_eng_ls7 LS   -

7 entries were displayed.
\end{verbatim}

**Note:** You can use one or more \texttt{snapmirror show} command options to list more specific
information about a set of load-sharing mirrors. See the \texttt{snapmirror show} command in the
\textit{Data ONTAP Cluster-Mode System Administration Guide} for more information.

**Managing data protection mirror**

Data protection mirror management consists of activities such as creating data protection mirrors for
source volumes, modifying data protection mirrors, and monitoring data protection mirror status.

**Next topics**

- \textit{Uses for data protection mirrors} on page 190
- \textit{Creating a data protection mirror} on page 190
- \textit{Managing mirroring relationships} on page 191
- \textit{Deleting a mirror} on page 193
Uses for data protection mirrors
You can create data protection mirrors to solve a number of storage administration tasks to protect your data.

After creating a data protection mirror, you can perform any of the following actions:

- Provide users immediate access to mirrored data in case the source goes down.
- Restore the data to the source to recover from disaster or user error.
- Archive the data to tape.
- Balance resource loads.

Creating a data protection mirror
You can protect data by replicating it to data protection mirrors. Data protection mirrors can be used to recover data when a disaster occurs.

Before you begin
You must have a SnapMirror license installed to create mirroring relationships.

Steps
1. Create a destination volume that will become the data protection mirror using the following command:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -type DP
   ```

   **Example**
   The following example creates a data protection mirror volume named dept_eng_dr_mirror1 of a source volume named dept_eng. The source volume and mirror volume are located on a vserver named vs0. The mirror volume is located on an aggregate named aggr3.

   ```
   node::> volume create -vserver vs0 -volume dept_eng_dr_mirror1 -aggregate aggr3 -type DP
   ```

2. Create a data protection mirror relationship using the following command:

   ```
   snapmirror create -destination-path path -source-path path
   ```

   **Example**
   The following example creates a data protection mirror named dept_eng_dp_mirror1 of the source volume named dept_eng. The source cluster is named clus1 and the mirror is located on a virtual server named vs0.
node::> snapmirror create -destination-path clus1://vs0/dept_eng_dp_mirror1 -source-path clus1://vs0/dept_eng

Data ONTAP creates the data protection mirror relationship, but the relationship is left in an uninitialized state.

3. Initialize the data protection mirror using the following command:

```
snapmirror initialize -destination-path cluster_name://vserver_name/volume_name -source-path cluster_name://vserver_name/volume_name
```

Example
The following example adds a data protection mirror named dept_eng_dr_mirror4 of a source volume named dept_eng. The source volume and data protection mirror are on the virtual server named vs0 on a cluster named clus1.

```
node::> snapmirror initialize -destination-path clus1://vs0/dept_eng_dr_mirror4 -source-path clus1://vs0/dept_eng
```

Managing mirroring relationships
You manage mirroring relationships to optimize the performance of those relationships.

Next topics
- Listing the schedule state of a mirroring relationship on page 188
- Scheduling SnapMirror transfers on page 186
- Changing mirroring relationship schedules on page 187

Listing the schedule state of a mirroring relationship
You might want to see what state a scheduled transfer for a mirroring relationship is in to ensure jobs are running as they should.

Step
1. To see the state of scheduled jobs, enter the following command:

```
job show
```

Note: The state of a scheduled job might be dormant. The dormant state means that the job is waiting for the scheduled start time to begin the transfer. There is nothing wrong with the job and you need to do nothing.
Scheduling SnapMirror transfers

Unless you created and implemented a schedule for SnapMirror transfers, you are limited to manually updating destination volumes of mirroring relationships.

About this task

You can add a schedule to a mirroring relationship either when you create the relationship or after you create the relationship.

When you add a schedule to a load-sharing mirror, Data ONTAP implements the schedule on the relationships of all the load-sharing mirrors in the group. Data ONTAP determines the load-sharing mirror group by the virtual server and source volume specified by the command.

Steps

1. Create the schedule you want to implement using the `job schedule cron create` command.
2. Apply the schedule to the mirroring relationship.

<table>
<thead>
<tr>
<th>If you are applying the schedule...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you created and initialized the mirroring relationship.</td>
<td>Use the <code>-schedule</code> option of the <code>snapmirror modify</code> command.</td>
</tr>
<tr>
<td>When you create the mirroring relationship</td>
<td>Use the <code>-schedule</code> option of the <code>snapmirror create</code> command.</td>
</tr>
</tbody>
</table>

Changing mirroring relationship schedules

You can change a schedule that updates mirroring relationships if the schedule impacts other backups or updates.

About this task

When you change a schedule to a load-sharing mirror relationship, Data ONTAP makes the change to the relationships of all the load-sharing mirrors in the group. Data ONTAP determines the load-sharing mirror group by the virtual server and source volume specified by the command.

Steps

1. Create the new schedule using the `job schedule cron create` command. Creating a schedule is described in the cron job creation section of the Data ONTAP Cluster-Mode System Administration Guide. The `job schedule cron create` command is described in the Data ONTAP Cluster-Mode Administration Reference.
2. Enter the following command to change a schedule for a mirroring relationship:
snapmirror modify -source-path source_endpoint -destination-path destination_endpoint -schedule sched

Example
The following example changes the update schedule used by a group of load-sharing mirrors for a source volume named dept_eng to a schedule named dept_eng_mirror_sched.

node::> snapmirror modify -source-path clus1://vs0/dept_eng -destination-path clus1://vs0/dept_eng_ls1 -schedule dept_eng_mirror_sched

Deleting a mirror
You can delete a mirror relationship.

Step
1. To delete a mirror relationship, enter the following command:

    snapmirror delete source_path destination_path

The command deletes the mirror relationship, but does not delete the destination volume.

Example
The following example deletes a mirror relationship between a destination volume named src_ui_ls_mir2 and a source volume named src_ui..

node::> snapmirror delete -source-path clust1://vs1/src_ui -destination-path clust1://vs1/src_ui_ls_mir2

The command deletes the mirror relationship, but does not delete the destination volume. In the case of a load-sharing mirror, the destination volume will be in the restricted state. If you want to use it as a destination volume of a data protection relationship, you must wait at least 10 minutes. This is the amount of time required to refresh internal caches and place the volume back online.

Note: When you delete a load-sharing mirror from a set of load-sharing mirrors, the destination volume of the deleted load-sharing mirror relationship cannot be used again as a destination volume of a load-sharing relationship if it contains any data or Snapshot copies.

 Recovering a lost source volume from a mirror
You might be able to use a load-sharing or data protection mirror to recover a source volume that is not accessible due to a failure that affects the cluster, assuming that the failure does not also affect
the mirror. This might be a good solution if you lose a source volume because a component failed, like a shelf or port failure.

**About this task**

This is not a procedure you use for recovering from a site disaster, such as a fire or flood, because both source volume and destination volume of the mirror are on the same cluster and same virtual server. A site disaster would affect both sides of the mirror because of this configuration restriction.

**Note:** If you created a junction path to a data protection destination volume, and you promote the destination using the `snapmirror promote` command, the junction path that you created is deleted.

**Step**

1. Enter the following command to make a mirror a read-write volume that replaces the original read-write volume:

   ```
   snapmirror promote -destination-path path -source-path path
   ```

   **Example**

   The following example recovers a lost source volume from the load-sharing mirror named `dept_eng_ls_mirror3` on a virtual server named `vs0` and a cluster named `cluster1`.

   ```
   node::> snapmirror promote -destination-path
   cluster1://vs0/dept_eng_ls_mirror3 -source-path
   cluster1://vs0/eng
   ```

   Data ONTAP makes the destination volume of the mirror a read-write volume, destroys the original read-write volume if it is accessible, and redirects mirrors and clients that accessed the original read-write volume to the new read-write volume.

   **Note:** The recovered source volume might not have all of the data that the original source volume had because the SnapMirror relationship for load-sharing and data protection mirrors is a scheduled, asynchronous update and the update might not have occurred recently.

**Deleting a mirror**

You can delete a mirror relationship.

**Step**

1. To delete a mirror relationship, enter the following command:

   ```
   snapmirror delete source_path destination_path
   ```

   The command deletes the mirror relationship, but does not delete the destination volume.
Example
The following example deletes a mirror relationship between a destination volume named src_ui_ls_mir2 and a source volume named src_ui..

```bash
node::> snapmirror delete -source-path clust1://vs1/src_ui
     -destination-path clust1://vs1/src_ui_ls_mir2
```

The command deletes the mirror relationship, but does not delete the destination volume. In the case of a load-sharing mirror, the destination volume will be in the restricted state. If you want to use it as a destination volume of a data protection relationship, you must wait at least 10 minutes. This is the amount of time required to refresh internal caches and place the volume back online.

**Note:** When you delete a load-sharing mirror from a set of load-sharing mirrors, the destination volume of the deleted load-sharing mirror relationship cannot be used again as a destination volume of a load-sharing relationship if it contains any data or Snapshot copies.
Data protection using tape

You use tape backup and recovery to create tape archives and to retrieve data from tape archives.

You back up data from disk to tape for the following reasons:

- You can store the backup tapes at an off-site archive to protect the data against natural disasters.
- You can restore data from tape if an application or a user inadvertently corrupts or deletes files that cannot be recovered using the Snapshot copy feature.
- You can restore data from tape after you reinstall the file system on the storage system (for example, when migrating to larger disks or converting a single-volume storage system to a multivolume storage system).

Next topics

- Data backup to tape in cluster-mode on page 197
- Tape alias support on page 198
- What the blocking factor is on page 202
- NDMP management on page 202
- Displaying NDMP configuration information for a node in a cluster on page 203
- Enabling and configuring NDMP for a node in a cluster on page 203
- Considerations when using NDMP for tape backups in Cluster-Mode on page 204
- Limitations of Cluster-Mode tape backup on page 204
- What environment variables do on page 204

Data backup to tape in cluster-mode

Data ONTAP 8.0 Cluster-Mode enables you to backup data to tape using NDMP services.

You can use the NDMP services on the storage system to enable network-based backup and recovery using a number of NDMP-enabled commercial backup applications. You can also monitor the NDMP services running on the storage system.

By default, Data ONTAP 8.0 cluster-mode supports NDMP version 3 and version 4.

Advantages and disadvantages of tape backup

Data backed up to tape requires fewer resources to maintain. However, restoring data from tape might take a long time.

Following are the advantages of tape backup over online storage:

- Tape backups require fewer resources to maintain.
- You can place the archives in a more secure place than you can place a storage system.
You can recover data from any release of Data ONTAP.

Following are the disadvantages of tape archives over online storage:

- Restoring data from tape takes a long time.
- Finding a particular file or directory on tape is time consuming.

Tape alias support

Starting from Data ONTAP 8.0, tape aliases are supported in the cluster-mode.

When Data ONTAP detects a new tape drive, it assigns an alias to it. Aliases help identify a tape device.

What assigning tape aliases is

Aliasing binds a tape or a medium changer device address, or a WWN, to a persistent, but modifiable alias name.

Aliasing simplifies the process of device identification. The following table describes how tape aliasing enables you to ensure that a tape drive (or tape library or medium changer) is always associated with a single alias name.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Reassigning of the alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>When the system reboots</td>
<td>The tape drive is automatically reassigned its previous alias.</td>
</tr>
<tr>
<td>When a tape device moves to another port</td>
<td>The alias can be adjusted to point to the new address.</td>
</tr>
<tr>
<td>When more than one system uses a particular tape device</td>
<td>The user can set the alias to be the same for all the systems.</td>
</tr>
</tbody>
</table>

Note: When you upgrade from Data ONTAP 10.x, the tape alias feature of Data ONTAP 8.0 modifies the existing tape alias names. In such a case, you might have to update the tape alias names in the third-party tape backup applications that you use for the backup.

Assigning tape aliases provides a correspondence between the logical names of backup devices (for example, st0 or mc1) and a name permanently assigned to a port, a tape drive, or a medium changer.

Note: st0 and st00 are different logical names.

Note: Logical names and WWNs are used only to access a device. After the device is accessed, it returns all error messages using the physical path name.

There are two types of names available for aliasing: PPNs and WWNs.
What physical path names are

Physical path names (PPNs) are the numerical address sequences that Data ONTAP assigns to tape drives and tape libraries based on the SCSI-2/3 adapter or switch (specific location) they are connected to, on the storage system. PPNs are also known as electrical names.

PPNs of direct-attached devices use the following format:

```
host_adapter.device_id_lun
```

For example, the PPN 8.6 indicates that the host adapter number is 8, the device ID is 6, and the logical unit number (LUN) is 0.

**Note:** The LUN value is displayed only for tape and medium changer devices whose LUN values are not zero; that is, if the LUN value is zero the \textit{lun} part of the PPN is not displayed.

PPNs of switch-attached devices use the following format:

```
switch:port_id.device_id_lun
```

For example, the PPN MY\_SWITCH:5.3L2 indicates that the tape drive connected to port 5 of a switch called MY\_SWITCH is set with SCSI ID 3 and has the LUN 2.

The LUN is determined by the drive itself. Fibre Channel, SCSI tape drives and libraries, and disks have PPNs.

PPNs of tape drives and libraries do not change unless the name of the switch changes, the tape drive or library moves, or the tape drive or library is reconfigured. PPNs remain unchanged after reboot.

For example, if a tape drive named MY\_SWITCH:5.3L2 is removed and a new tape drive with the same SCSI ID and LUN is connected to port 5 of the switch MY\_SWITCH, the new tape drive would be accessible using MY\_SWITCH:5.3L2.

What worldwide names are

Tape drives and libraries are assigned worldwide names (WWNs) at the time of manufacture. WWNs are similar to the media access control (MAC) addresses on Ethernet cards. All Fibre Channel devices have WWNs, but SCSI-attached devices do not have WWNs.

Accessing a tape drive or library using the WWN allows multiple storage systems to track the same device. Depending on whether a tape drive is connected to a Fibre Channel switch or hub, or is
directly attached to a Fibre Channel adapter, different storage systems can have different PPNs for
the same device. Using the WWN in these cases eliminates any confusion.

Also, if you rename a switch or move a tape drive in the storage system, the WWN of the tape drive
or library does not change. The scripts or backup programs do not need to change the name of the
tape drive or library to which they are backing up.

The WWN of a tape device uses the following format:

WWN[ #:###:#####:#######] L##

# is a hexadecimal character and L## is the LUN of the device. If the LUN is 0, the L## part of the
string is not displayed.

Each WWN consists of eight bytes, and the format for the WWN is not case-sensitive.

**Displaying existing aliases of tape drives**

You can determine the existing aliases of tape drives using the `storage alias` command.

**Step**

1. To determine the existing aliases of tape drives, enter the following command:
   
   ```
   storage alias
   ```
   
   **Note:** You can execute this command only from the nodeshell CLI.

   **Example**

   ```
   filer1>storage alias
   Alias  Mapping
   ------------------------
st0   MY_SWITCH:5.3L3
st2   MY_SWITCH:5.4L6
mc1   2:4e3:38fe3f:758eab
mc348 MY_SWITCH:5.3L0
   ```

   In this example, the display shows that there are two tape drives and two medium changers
attached to the storage system. Tape drives st0 and st2 and medium changer mc348 are attached
to port 5 of the switch MY_SWITCH. Medium changer mc1 has the WWN 2:4e3:38fe3f:758eab.

**Displaying information about tape drives or libraries**

Information about tape drives and tape libraries helps you to assign tape aliases.

**Step**

1. To display information about tape drives and tape libraries (medium changers), enter the
following command:
   
   ```
   tape {drive | library} show
   ```
drive specifies to display information about the tape drives.

library specifies to display information about the tape libraries.

Assigning tape aliases

You can assign aliases to tape drives or medium changers using the `storage alias` command.

Step

1. To assign an alias to a tape drive or medium changer, enter the following command:

   ```
   storage alias [alias {PPN | WWN}]
   ```

   **Note:** You can execute this command only from the nodeshell CLI.

   *alias* is the logical name of the tape drive or medium changer to which you want to add the alias.

   *PPN* is the physical path name to which you want to assign the tape drive or medium changer.

   *WWN* is the WWN to which you want to assign the tape drive or medium changer.

   **Examples**

   ```
   storage alias st0 MY_SWITCH:5.3L3
   ```

   The tape device st0 is assigned to the physical path name MY_SWITCH:5.3L3.

   ```
   storage alias mc80 WWN[2:4e3:38fe3f:758eab]
   ```

   The medium changer mc80 is assigned to the worldwide name WWN[2:4e3:38fe3f:758eab].

Removing tape aliases

You can remove aliases from tape drives or medium changers, or both, using the `storage unalias` command.

Step

1. To remove an alias from a tape drive or medium changer, enter the following command:

   ```
   storage unalias {alias | -a | -m | -t}
   ```

   **Note:** You can execute this command only from the nodeshell CLI.

   *alias* is the logical name of the tape drive or medium changer from which you want to remove the alias.

   *-a* removes all aliases.

   *-m* removes the aliases from all medium changers.
-t removes the aliases from all tape drives.

**Examples**

```plaintext
storage unalias st0
storage unalias mc80
```

**What the blocking factor is**

A tape block is 1,024 bytes of data. During a tape backup or restore, you can specify the number of tape blocks that are transferred in each read/write operation. This number is called the blocking factor.

On a remote host that is not a storage system, you can use a blocking factor from 4 through 256, provided that the host supports the blocking factor that you select.

If you plan to restore a backup to a system other than the system that did the backup, the restore system must support the blocking factor that you used for the backup. For example, if you use a blocking factor of 128, the system on which you restore that backup must support a blocking factor of 128.

During an NDMP backup, the MOVER_RECORD_SIZE determines the blocking factor. Data ONTAP allows a maximum value of 256 KB for MOVER_RECORD_SIZE.

**Note:** Data ONTAP 10.x supports a blocking factor in the range of 5 KB to 64 KB. Therefore, if you perform a backup of data in a storage system running Data ONTAP 8.0 with a blocking factor less than 5 KB or greater than 64 KB, you cannot perform a local restore of the data to a storage system running a version of Data ONTAP 10.x. However you can perform a 3-way restore of such data with the tape drive connected to a storage system running Data ONTAP 8.0.

**Related information**


**NDMP management**

The Network Data Management Protocol (NDMP) is a standardized protocol for controlling backup, recovery, and other transfers of data between primary and secondary storage devices, such as storage systems and tape libraries.

By enabling NDMP protocol support on a storage system, you enable that storage system to carry out communications with NDMP-enabled commercial network-attached backup applications (also called Data Management Applications or DMAs), data servers, and tape servers participating in backup or recovery operations. NDMP also provides low-level control of tape devices and medium changers.
Displaying NDMP configuration information for a node in a cluster

You can view the current NDMP configuration settings of your storage system by using the `ndmp show` at the clustershell prompt.

Step

1. To view the current NDMP configuration settings, enter the following command at the clustershell prompt:

   ```shell
   system services ndmp show
   ```

   The command displays the following details
   - The node name
   - Whether NDMP is enabled
   - Whether clear text passwords are allowed
   - The NDMP user ID

   The following is a sample output of the command.

   ```text
   node1::> system services ndmp show
   Node   Enabled Clear text  User Id
   ------ ------- ----------  -------
   node1  true    true        root
   ```

Enabling and configuring NDMP for a node in a cluster

You can enable NDMP for a node in a cluster and modify the clear text password setting, and user name by using the `ndmp modify` command. You can execute this command from the clustershell prompt of any of the nodes in the cluster.

Step

1. To enable and configure NDMP for a node in a cluster, enter the following command:

   ```shell
   system services ndmp modify -node storage_system [-enable true|false] [-clear-text true|false][-user-id user]
   ```

   - `node` specifies that the node for which the NDMP settings are to be configured is supplied in the command line.
   - `storage_system` is the node for which the NDMP settings are to be configured.

   `-enable` helps to enable or disable NDMP. It can be set to either true or false.
-clear-text helps you to enable or disable clear text passwords. It can be set to either true or false.

**Note:** md5 authentication is always enabled.

-user-id specifies that a new user ID for the node is supplied in the command line.

**Note:** If you specify the user-id option in the ndmp modify command, the storage system prompts you to enter a new password for the node. If you want to modify only the password of a node, you must use the ndmp password command.

The following example enables NDMP on the node testnode1 of a cluster and enables clear text password for the node:

testnode2>system services ndmp modify -node testnode1 -clear-text true

**Considerations when using NDMP for tape backups in Cluster-Mode**

You have to take into account certain considerations when using NDMP to perform tape backups in Cluster-Mode.

- To backup a FlexVol volume, you must initiate the backup from the node that has the volume.
- When a SnapMirror destination is backed up to tape, only data is backed up. The SnapMirror relationships and the associated metadata are not backed to tape. Therefore, during restore, only the data is restored and associated SnapMirror relationships are not restored.

**Limitations of Cluster-Mode tape backup**

Data backup to tape in cluster-mode has certain limitations.

- Tape backup can be invoked only through a DMA. You cannot initiate a backup or restore using CLI commands.
- Tape backups are possible only at a volume level and not at a qtree or subtree level.
- Data ONTAP Cluster-Mode does not support any NDMP extensions. Therefore, restartable backups are not supported.
- Concurrent backup sessions of the same volume are not possible.

**What environment variables do**

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system.

For example, if a user specifies that a backup application should back up /vol/vol0/etc, the backup application sets the FILESYSTEM environment variable to /vol/vol0/etc. Similarly, if a
user specifies that a backup should be a level 1 backup, the backup application sets the LEVEL environment variable to 1 (one).

**Note:** The setting and examining of environment variables are typically transparent to backup administrators; that is, the backup application sets them automatically.

A backup administrator rarely specifies environment variables; however, you might want to change the value of an environment variable from that set by the backup application to characterize or work around a functional or performance problem. For example, an administrator might want to temporarily disable file history generation to determine if the backup application's processing of file history information is contributing to performance issues or functional problems.

Many backup applications provide a means to override or modify environment variables or to specify additional environment variables. For information, see your backup application documentation.

### Environment variables supported by Data ONTAP

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system. Data ONTAP supports environment variables, which have an associated default value. However, you can manually modify these default values.

If you manually modify the values set by the backup application, the application might behave unpredictably. This is because the backup or restore operations might not be doing what the backup application expected them to do. But in some cases, judicious modification might help in identifying or working around problems.

The following table contains descriptions of what the environment variables supported by Data ONTAP do if they are used.

**Note:** In most cases, variables that have `Y` or `N` values also accept `T` or `F` values, respectively.

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>

Table continues...
<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASE_DATE</td>
<td>0, -1, or DUMP_DATE value</td>
<td>-1</td>
<td>Specifies the start date for incremental backups. There is no equivalent option for the dump command. When set to -1, the BASE_DATE incremental specifier is disabled. When set to 0 on a level 0 backup, incremental backups are enabled. Subsequent to the initial backup, the value of the DUMP_DATE variable from the previous incremental backup is assigned to the BASE_DATE variable. These variables are an alternative to the <code>/etc/dumpdates</code> file for controlling incremental backups.</td>
</tr>
</tbody>
</table>
| DEBUG                | Y or N       | N       | Specifies that debugging information is printed.  
**Note:** There is no command line equivalent for the DEBUG variable. |
<p>| DIRECT               | Y or N       | N       | Specifies that a restore should fast-forward directly to the location on the tape where the file data resides instead of scanning the entire tape. For direct access recovery to work, the backup application must provide positioning information. If this variable is set to Y, the backup application will specify the file or directory names and the positioning information. |</p>
<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DUMP_DATE</td>
<td>return value</td>
<td>none</td>
<td>You do not change this variable directly. It is created by the backup if the BASE_DATE variable is set to a value other than -1. The DUMP_DATE variable is derived by prepending the 32-bit level value to a 32-bit time value computed by the dump software. The level is incremented from the last level value passed into the BASE_DATE variable. The resulting value is used as the BASE_DATE value on a subsequent incremental backup.</td>
</tr>
</tbody>
</table>
| ENHANCED_DAR_ENABLED    | Y or N       | N       | Specifies if enhanced DAR functionality is instantiated. Enhanced DAR functionality supports directory DAR, and DAR of files with NT Streams. It provides performance improvements. Enhanced DAR during restore is possible only if the following conditions are met:  
  • Data ONTAP 8.0 or later supports enhanced DAR  
  • File history is enabled (HIST=Y) during the backup  
  • ENHANCED_DAR_ENABLED variable is set to "Y" during restore |
<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| EXCLUDE              | pattern string | none    | Specifies files or directories that are excluded when backing up data. The exclude list is a comma-separated list of file or directory names. If the name of a file or directory matches one of the names in the list, it is excluded from the backup. The following are rules for specifying names in the exclude list:  
  - The exact name of the file or directory must be used.  
  - An asterisk (*) is a wildcard character. The asterisk must be either the first or the last character of the string. Each string can have up to two asterisks.  
  - A comma in a file or directory name must be preceded with a backslash.  
  - The exclude list can contain up to 32 names. |
<p>| EXTRACT              | Y or N       | N       | Specifies that subtrees of a backed-up data set are to be restored. The backup application specifies the names of the subtrees to be extracted. If a file specified matches a directory whose contents were backed up, the directory is recursively extracted. |
| EXTRACT_ACL          | Y or N       | Y       | Specifies that ACLs from the backed up file are restored on a restore operation. The default is to restore ACLs when restoring data, except for DARs (DIRECT=Y). |
| FILESYSTEM           | string       | none    | Specifies the path name of the root of the data that is being backed up. |</p>
<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| HIST | Y or N | N | Specifies that file history information is sent to the backup application. Most commercial backup applications set the HIST variable to Y. If you want to increase the speed of a backup operation, or you want to troubleshoot a problem with the file history collection, you can set this variable to N.  
**Note:** You should not set the HIST variable to Y if the backup application does not support file history. |
<p>| LEVEL | 0-9 | 0 | Specifies the backup level. Level 0 copies the entire data set. Incremental backup levels, specified by values above 0, copy all files new or modified since the last incremental backup. For example, a level 1 backs up new or modified files since the level 0 backup, a level 2 backs up new or modified files since the level 1 backup, and so on. |
| NO_ACLS | Y or N | N | Specifies that ACLs not be copied when backing up data. |</p>
<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| RECURSIVE           | Y or N       | Y       | Specifies that directory entries during a DAR restore be expanded. The DIRECT and ENHANCED_DAR_ENABLED environment variables must be enabled (set to Y) as well. If the RECURSIVE variable is disabled (set to N), only the permissions and ACLs for all the directories in the original source path are restored from tape, not the contents of the directories. If the RECURSIVE variable is N or the RECOVER_FULL_PATHS variable is Y, the recovery path must end with the original path.  

**Note:** If the RECURSIVE variable is disabled and if there are more than one recovery path, all the recovery paths must be contained within the longest of the recovery paths. Otherwise, an error message is displayed.  

For example, the following are valid recovery paths as all the recovery paths are within foo/dir1/deepdir/myfile:

- /foo
- /foo/dir
- /foo/dir1/deepdir
- /foo/dir1/deepdir/myfile

The following are invalid recovery paths:

- /foo
- /foo/dir
- /foo/dir1/myfile
- /foo/dir2
- /foo/dir2/myfile |
<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RECOVER_FULL_PATHS</td>
<td>Y or N</td>
<td>N</td>
<td>Specifies that full recovery path will have their permissions and ACLs restored after the DAR. DIRECT and ENHANCED_DAR_ENABLED must be enabled (set to Y) as well. If RECOVER_FULL_PATHS is Y, recovery path must end with the original path. If directories already exist on the destination volume, their permissions and ACLs will not be restored from tape.</td>
</tr>
<tr>
<td>UPDATE</td>
<td>Y or N</td>
<td>Y</td>
<td>Updates the dumpdates file.</td>
</tr>
</tbody>
</table>
About using FlexCache clients with Data ONTAP Cluster-Mode

You can deploy FlexCache clients to cache FlexVol volumes stored in a Data ONTAP Cluster-Mode cluster.

You can use FlexCache volumes to speed up access to remote data or to offload traffic from heavily accessed volumes. Data ONTAP Cluster-Mode volumes are the origin and Data ONTAP 7-Mode volumes are the cache.

Next topics

Limitations when using a Data ONTAP Cluster-Mode volume as a FlexCache origin on page 213
Configuring origin volumes on page 213

Limitations when using a Data ONTAP Cluster-Mode volume as a FlexCache origin

Certain limitations apply when using a Data ONTAP Cluster-Mode volume as a FlexCache origin.

The following caveats apply to using FlexCache in Data ONTAP Cluster-Mode:

• All nodes in the cluster must be running Data ONTAP Cluster-Mode before you can deploy FlexCache clients.
• Junctions do not work across caches.

Configuring origin volumes

You can configure FlexVol volumes to be the origin of a FlexCache cache.

Before you begin

Before you can designate a volume as a FlexCache origin, the volume must exist.

Steps

1. Use the vserver export-policy rule create command with the -protocol parameter to control data interface access to a volume.
   • To restrict data interface access to volumes by any other protocol, specify the value flexcache for the -protocol parameter.
• To enable data interface access to volumes by any protocol, specify the value any for the –protocol parameter.

**Example**
The following example modifies an export-policy rule named user_expolicy with a rule index integer of 1 on a virtual server named vs0 to use the flexcache protocol.

```
node::> vserver export-policy rule modify -vserver vs0 -policyname user_expolicy -rule-index 1 -protocol flexcache
```

2. Use the statistics show command with the -category fcache parameter and value to display statistics about FlexCache operations. You can also view the node.node.fcache-ops object in the output of the statistics show command to obtain this information.

**After you finish**

See the *Data ONTAP 7-Mode Storage Management Guide* for more information about using FlexCache.
Storage limits

There are limits for aggregates, FlexVol volumes, traditional volumes, FlexCache volumes, FlexClone volumes, files, and LUNs, qtrees and RAID groups that you should consider when planning your storage architecture.

Limits are listed in the following sections:

- *Volume limits* on page 215
- *Aggregate limits* on page 216
- *RAID group limits* on page 217
- *RAID group sizes* on page 217
- *Minimum sizes for root FlexVol volumes* on page 218

### Volume limits

<table>
<thead>
<tr>
<th>Limit</th>
<th>Native storage</th>
<th>Back-end storage arrays</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Array LUNs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum size for root volume</td>
<td>N/A</td>
<td>Model-dependent</td>
<td>See the <em>V-Series Support Matrix</em>.</td>
</tr>
<tr>
<td><strong>Files</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum size in 32-bit FlexVol volume</td>
<td>16 TB</td>
<td>16 TB</td>
<td></td>
</tr>
<tr>
<td>Maximum size in 64-bit volume</td>
<td>16 TB</td>
<td>16 TB</td>
<td></td>
</tr>
<tr>
<td><strong>FlexCache volumes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum per node</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>FlexVol volumes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum per node</td>
<td>FAS2040: 200</td>
<td>FAS2040: 200</td>
<td>In an HA pair, these limits apply to each node individually, so the overall limit for the pair is doubled.</td>
</tr>
<tr>
<td></td>
<td>3210: 200</td>
<td>3210: 200</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All other models: 500</td>
<td>All other models: 500</td>
<td></td>
</tr>
<tr>
<td><strong>FlexVol volumes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum size</td>
<td>20 MB</td>
<td>20 MB</td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Native storage</td>
<td>Back-end storage arrays</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>FlexVol volumes (32-bit)</strong></td>
<td>16 TB</td>
<td>16 TB</td>
<td></td>
</tr>
<tr>
<td>Maximum size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FlexVol volumes (64-bit)</strong></td>
<td>Model-dependent</td>
<td>Model-dependent</td>
<td>Corresponds to the maximum size of the containing aggregate. See the System Configuration Guide.</td>
</tr>
<tr>
<td>Maximum size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FlexVol root volumes</strong></td>
<td>Model-dependent</td>
<td>Model-dependent</td>
<td>See table below.</td>
</tr>
<tr>
<td>Minimum size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Links (hard)</strong></td>
<td>99,998</td>
<td>99,998</td>
<td></td>
</tr>
<tr>
<td>Maximum per parent directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Qtrees</strong></td>
<td>4,995</td>
<td>4,995</td>
<td></td>
</tr>
<tr>
<td>Maximum number per volume</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Subdirectories</strong></td>
<td>99,998</td>
<td>99,998</td>
<td></td>
</tr>
<tr>
<td>Maximum per parent directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Snapshot copies</strong></td>
<td>128</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Maximum per FlexVol volume</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Aggregate limits**

<table>
<thead>
<tr>
<th>Limit</th>
<th>Native storage</th>
<th>Back-end storage arrays</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aggregates</strong></td>
<td>100</td>
<td>100</td>
<td>In an HA pair, this limit applies to each node individually, so the overall limit for the pair is doubled.</td>
</tr>
<tr>
<td>Maximum per system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Aggregates (32-bit)</strong></td>
<td>16 TB</td>
<td>16 TB</td>
<td></td>
</tr>
<tr>
<td>Maximum size</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Limit

<table>
<thead>
<tr>
<th>Limit</th>
<th>Native storage</th>
<th>Back-end storage arrays</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregates (64-bit)</td>
<td>Model-dependent</td>
<td>Model-dependent</td>
<td>See the <em>System Configuration Guide.</em></td>
</tr>
<tr>
<td>Maximum size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregates</td>
<td>N/A</td>
<td>10 GB</td>
<td></td>
</tr>
<tr>
<td>Minimum size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Array LUNs</td>
<td>N/A</td>
<td>Model-dependent</td>
<td>See the <em>V-Series Support Matrix.</em></td>
</tr>
<tr>
<td>Maximum per aggregate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAID groups</td>
<td>150</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Maximum per aggregate</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### RAID group limits

<table>
<thead>
<tr>
<th>Limit</th>
<th>Native storage</th>
<th>Back-end storage arrays</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID groups</td>
<td>400</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>Maximum per system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAID groups</td>
<td>150</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Maximum per aggregate</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### RAID group sizes

<table>
<thead>
<tr>
<th>RAID type</th>
<th>Default size</th>
<th>Maximum size</th>
<th>Minimum size</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID-DP</td>
<td>ATA/BSAS/SATA: 14</td>
<td>ATA/BSAS/SATA: 20</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>FC/SAS: 16</td>
<td>FC/SAS: 28</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSD: 23</td>
<td>SSD: 28</td>
<td></td>
</tr>
<tr>
<td>RAID4</td>
<td>ATA/BSAS/SATA: 7</td>
<td>ATA/BSAS/SATA: 7</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>FC/SAS/SSD: 8</td>
<td>FC/SAS/SSD: 14</td>
<td></td>
</tr>
<tr>
<td>RAID0</td>
<td>8</td>
<td>26</td>
<td>1</td>
</tr>
</tbody>
</table>
## Minimum sizes for root FlexVol volumes

<table>
<thead>
<tr>
<th>Storage system model</th>
<th>Minimum root volume size</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAS2040</td>
<td>160 GB</td>
</tr>
<tr>
<td>3040</td>
<td>160 GB</td>
</tr>
<tr>
<td>3070</td>
<td>230 GB</td>
</tr>
<tr>
<td>3140</td>
<td>160 GB</td>
</tr>
<tr>
<td>3160</td>
<td>240 GB</td>
</tr>
<tr>
<td>3170</td>
<td>250 GB</td>
</tr>
<tr>
<td>3210</td>
<td>151 GB</td>
</tr>
<tr>
<td>3240</td>
<td>205 GB</td>
</tr>
<tr>
<td>3270</td>
<td>300 GB</td>
</tr>
<tr>
<td>6030</td>
<td>250 GB</td>
</tr>
<tr>
<td>6040</td>
<td>250 GB</td>
</tr>
<tr>
<td>6070</td>
<td>250 GB</td>
</tr>
<tr>
<td>6080</td>
<td>250 GB</td>
</tr>
<tr>
<td>6210</td>
<td>300 GB</td>
</tr>
<tr>
<td>6240</td>
<td>300 GB</td>
</tr>
<tr>
<td>6280</td>
<td>300 GB</td>
</tr>
</tbody>
</table>
Storage commands that are available in the nodeshell

The `system node run` command enables you to run a subset of 7-Mode (the nodeshell) storage commands from Cluster-Mode (the clustershell).

The `system node run` command enables you to run certain storage commands from the nodeshell CLI on a specified node in the cluster. The nodeshell is the CLI that is available with Data ONTAP 7-Mode deployments. You can run a single nodeshell command from the clustershell that returns immediately. Or, you can switch within the clustershell to a nodeshell session from which you can run multiple nodeshell commands interactively.

For more information about using the `system node run` command to access the nodeshell, see its reference page in the *Data ONTAP Cluster-Mode Administration Reference*.

**Related concepts**

*Different shells that are available* on page 22

## Nodeshell storage and storage-related commands

A list of storage and storage-related commands that are available in the nodeshell follows. Storage-related commands include commands for data protection and HA configuration.

<table>
<thead>
<tr>
<th>Command name</th>
<th>Purpose</th>
<th>More information is available in these documents:</th>
<th>Parameter changes or limitations</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggr add</td>
<td>Adds disks or array LUNs to an aggregate</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em></td>
<td>Admin privilege level</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://www.netapp.com/documentation/na_aggr.1.0.1.html">na_aggr(1) man page</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aggr media_scrub</td>
<td>Reports the status of a media scrub on an aggregate</td>
<td>na_aggr(1) man page</td>
<td>Admin privilege level</td>
<td></td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| aggr offline | Takes an aggregate offline | *Data ONTAP 7-Mode Storage Management Guide*  
*na_aggr(1) man page* | Use is permitted only if the Volume Location Database (VLDB) is available and the aggregate is not listed in the database. Alternatively, use the clustershell storage aggregate modify command with the `-state` parameter. | Admin privilege level |
| aggr online  | Brings an aggregate online | *Data ONTAP 7-Mode Storage Management Guide*  
*na_aggr(1) man page* | Use is permitted only if the VLDB is available and the aggregate is not listed in the database. Alternatively, use the clustershell storage aggregate modify command with the `-state` parameter. | Admin privilege level |
<table>
<thead>
<tr>
<th>Command name</th>
<th>Purpose</th>
<th>More information is available in these documents:</th>
<th>Parameter changes or limitations</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aggr options</strong></td>
<td>Sets aggregate options</td>
<td>na_aggr(1) man page</td>
<td>Available options include the following:</td>
<td>Admin privilege level; You can set the raidsize option by using the clustershell storage aggregate modify command with the -maxraidsize parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• fs_size_fixed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• lost_write_protect</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• raidsize</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• raidtype</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• resyncsnapt ime</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• root</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• snapshot_autodelete</td>
<td></td>
</tr>
<tr>
<td><strong>aggr read_fsid</strong></td>
<td>Displays the FSID of an aggregate</td>
<td>na_aggr(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td><strong>aggr restrict</strong></td>
<td>Marks an aggregate as restricted</td>
<td>Data ONTAP 7-Mode Storage Management Guide</td>
<td>Use is permitted only if the volume location database is available and the aggregate is not listed in the database. Alternatively, use the clustershell storage aggregate modify command with the -state parameter.</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_aggr(1) man page</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>aggr rewrite_fsid</strong></td>
<td>Changes the FSID of an aggregate</td>
<td>na_aggr(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>----------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>aggr scrub</td>
<td>Controls aggregate scrubs</td>
<td>na_aggr(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>aggr show_space</td>
<td>Displays information about the used space in an aggregate</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em> na_aggr(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>aggr status</td>
<td>Displays the state and status of an aggregate</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em> na_aggr(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>aggr wafliron</td>
<td>Controls the wafliron process on an aggregate</td>
<td>na_aggr(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>array modify</td>
<td>Modifies attributes of array profile records</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>array purge-</td>
<td>Removes all records from the controller’s array profile database</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>database</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>array remove</td>
<td>Removes records for the specified array from the controller’s array profile database</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>array remove-port</td>
<td>Removes ports associated with an array profile</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>array show</td>
<td>Lists all array profile records known to the controller</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>array show-config</td>
<td>Summarizes the connectivity of SAN attached storage arrays to controller initiator ports</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>array show-luns</td>
<td>Lists all array LUNs exported from a named storage array</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>array show-ports</td>
<td>Lists all target ports known to the controller for a given storage array or for all storage arrays</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>cf</td>
<td>Controls takeover and giveback operations for the nodes in an HA configuration</td>
<td>Data ONTAP 8.0 7-Mode High Availability Configuration Guide</td>
<td>na_cf(1) man page</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>dd</td>
<td>Copies blocks of data</td>
<td>na_dd(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>df</td>
<td>Displays free space in a volume or aggregate</td>
<td>Data ONTAP 7-Mode Storage Management Guide</td>
<td>na_df(1) man page</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>disk assign</td>
<td>Assigns the ownership of a disk or array LUN to a node</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em></td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>disk fail</td>
<td>Forces a disk or array LUN in use in an aggregate to fail</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em></td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>disk maint</td>
<td>Runs maintenance tests on one or more disks</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em></td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>disk remove</td>
<td>Removes a spare disk from its RAID group and prepares it for physical removal; removes label information from array LUNs</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em></td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>disk remove_ownership</td>
<td>Removes disk ownership</td>
<td><em>na_disk(1a) man page</em></td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>disk replace</td>
<td>Replaces a disk or array LUN that is being used by an aggregate with a spare disk or stops the replacement process</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em></td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>disk sanitize</td>
<td>Removes the data from one or more disks</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em>&lt;br&gt;na_disk(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>disk scrub</td>
<td>Starts or stops disk scrubbing</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em>&lt;br&gt;na_disk(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>disk shm_stats</td>
<td>Displays Storage Health Monitor statistics for a disk</td>
<td>na_disk(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>disk show</td>
<td>Lists disks and their owners</td>
<td><em>Data ONTAP 7-Mode Storage Management Guide</em>&lt;br&gt;na_disk(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>disk unfail</td>
<td>Unfails a disk</td>
<td></td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>disk_stat</td>
<td>Prints a set of histograms for each disk installed in the system</td>
<td>na_disk_stat(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>fcadmin</td>
<td>Controls FC-AL driver administrative functions</td>
<td>na_fccadmin(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>fcstat</td>
<td>Controls FC-AL driver statistics</td>
<td>na_fccstat(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>ic</td>
<td>Administers the HA interconnect</td>
<td>na_ic(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>inodexpath</td>
<td>Displays the path name for an inode number</td>
<td>na_inodexpath(1a) man page</td>
<td>Standard FlexVol volumes only</td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>led_off</td>
<td>Turns off the specified disk-fault LED</td>
<td>na_led_off(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>led_off_all</td>
<td>Turns off the specified disk-fault LEDs</td>
<td>na_led_off_all(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>led_on</td>
<td>Turns on the specified disk-fault LED</td>
<td>na_led_on(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>led_on_all</td>
<td>Turns on the specified disk-fault LEDs</td>
<td>na_led_on_all(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>led_on_off</td>
<td>Toggles the specified disk-fault LED</td>
<td>na_led_on_off(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>led_test</td>
<td>Tests the disk-fault LEDs on all shelves</td>
<td>na_led_test(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>led_test_one</td>
<td>Tests the disk-fault LED on the specified disk</td>
<td>na_led_test_one(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>ls</td>
<td>Lists directory entries</td>
<td>na_ls(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>mailbox display</td>
<td>Displays information about HA mailbox disks</td>
<td>na_mailbox(1) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-----------------------------------------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| maxfiles     | Displays or increases the number of the files the file system can hold | *Data ONTAP 7-Mode Storage Management Guide*  
na_maxfiles(1) man page |  | Admin privilege level; Displays for all volumes. Modifies only FlexVol volumes. |
| mv           | Renames a file | na_mv(1h) man page |  | Advanced privilege level |
| options      | Sets system options | na_options(1) man page |  | Admin privilege level; To see the list of available options, enter the options command with no arguments. |
| partner      | Used to manage the HA partner in failover mode | *Data ONTAP 8.0 7-Mode High Availability Configuration Guide*  
na_partner(1) man page |  | Admin privilege level |
| qtree stats  | Displays a count of the number of NFS and CIFS operations caused by user accesses to files in qtrees | *Data ONTAP 7-Mode Storage Management Guide*  
na_qtree(1) man page |  | Admin privilege level |
| qtree status | Displays the attributes of all qtrees for the specified volume | *Data ONTAP 7-Mode Storage Management Guide*  
na_qtree(1) man page |  | Admin privilege level |
<table>
<thead>
<tr>
<th>Command name</th>
<th>Purpose</th>
<th>More information is available in these documents:</th>
<th>Parameter changes or limitations</th>
<th>Notes</th>
</tr>
</thead>
</table>
| quota report  | Displays the current file and space consumption for each user or group with a quota and for each qtree | *Data ONTAP 7-Mode Storage Management Guide*  
na_quota(1) man page |                                                                                                                   | Admin privilege level                                                                                                       |
| quota status  | Displays the quota status for the specified volume                      | *Data ONTAP 7-Mode Storage Management Guide*  
na_quota(1) man page |                                                                                                                   | Admin privilege level                                                                                                       |
| rdfile        | Reads a file to STDOUT                                                  | na_rdfile(1) man page                                                                                           |                                                                                                                                  | Admin privilege level                     |
| reallocate    | Manages reallocation                                                    | *Data ONTAP 7-Mode System Administration Guide*  
na_reallocate(1) man page | You cannot run a reallocation scan (the 'reallocate start' command) on a SnapMirror destination volume          | Admin privilege level                                                                                                       |
| rm            | Removes files                                                           | na_rm(1a) man page                                                                                              |                                                                                                                                  | Advanced privilege level                  |
| sasadmin      | Manages SAS adapters                                                    | *Data ONTAP 7-Mode Storage Management Guide*  
na_sasadmin(1) man page |                                                                                                                   | Admin privilege level                                                                                                       |
| sasstat       | Manages SAS adapters (alias for sasadmin command)                       | *Data ONTAP 7-Mode Storage Management Guide*  
na_sasstat(1) man page |                                                                                                                   | Admin privilege level                                                                                                       |
<table>
<thead>
<tr>
<th>Command name</th>
<th>Purpose</th>
<th>More information is available in these documents:</th>
<th>Parameter changes or limitations</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>sata</td>
<td>Issues SATA commands to devices</td>
<td></td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>scsi</td>
<td>Issues SCSI commands to devices</td>
<td>na_scsi(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>shelfchk</td>
<td>Verifies disk-shelf configuration</td>
<td>na_shelfchk(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>showfh</td>
<td>Displays the file handle for a file</td>
<td>na_showfh(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>snap create</td>
<td>Creates a Snapshot copy</td>
<td>Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide na_snap(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>snap delete</td>
<td>Deletes an existing Snapshot copy</td>
<td>Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide na_snap(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>snap rename</td>
<td>Renames an existing Snapshot copy</td>
<td>Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide na_snap(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>snap restore</td>
<td>Reverts a volume to a specified Snapshot copy</td>
<td>Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide na_snap(1) man page</td>
<td>root volume only</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>snap sched</td>
<td>Schedules automatic creation of Snapshot copies for a volume</td>
<td>Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide na_snap(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>snapmirror</td>
<td>Controls SnapMirror, an asynchronous method of mirroring volumes</td>
<td>Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide na_snapmirror(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>storage alias</td>
<td>Sets up aliases for tape libraries and tape drives to map to their electrical names or world wide names (WWNs)</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>storage disable</td>
<td>Disables an adapter</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_storage(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>storage download</td>
<td>Downloads new firmware to disk shelves attached to a specified adapter</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>storage enable</td>
<td>Enables an adapter</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_storage(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>storage release</td>
<td>Breaks existing exclusive access to a device and clears the existing device reservation</td>
<td></td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>storage rename</td>
<td>Sets the name of a switch</td>
<td></td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>storage show</td>
<td>Displays information about storage components</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_storage(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>storage stats</td>
<td>Displays tape-drive statistics</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>storage unalias</td>
<td>Removes alias settings</td>
<td>na_storage(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>tape_qual</td>
<td>Runs tape-qualification test</td>
<td>na_tape_qual(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>vol autosize</td>
<td>Allows a FlexVol volume to automatically grow in size if needed</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_vol(1) man page</td>
<td>Standard FlexVol volumes only</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>vol container</td>
<td>Displays a volume's containing aggregate</td>
<td>na_vol(1) man page</td>
<td>Standard FlexVol volumes only</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>vol destroy</td>
<td>Destroys a volume</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_vol(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>vol lang</td>
<td>Displays or changes the language of a volume</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_vol(1) man page</td>
<td>Read-only except for root volume</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>vol offline</td>
<td>Takes a volume offline</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_vol(1) man page</td>
<td>Standard FlexVol volumes only. Cannot be used on the root volume.</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>vol online</td>
<td>Brings a volume online</td>
<td>Data ONTAP 7-Mode Storage Management Guide na_vol(1) man page</td>
<td>Standard FlexVol volumes only</td>
<td>Admin privilege level</td>
</tr>
<tr>
<td>Command name</td>
<td>Purpose</td>
<td>More information is available in these documents:</td>
<td>Parameter changes or limitations</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| vol options | Displays or modifies volume options | *Data ONTAP 7-Mode Storage Management Guide*  
na_vol(1) man page | | See the list of supported volume options. |
| vol read_fsid | Displays the FSID of a volume | na_vol(1a) man page | | Advanced privilege level |
| vol restrict | Puts a volume into the restricted state | *Data ONTAP 7-Mode Storage Management Guide*  
na_vol(1) man page | Standard FlexVol volumes only | Admin privilege level |
| vol rewrite_fsid | Changes the FSID of a volume | na_vol(1a) man page | | Advanced privilege level |
| vol size | Displays or changes the size of a volume | *Data ONTAP 7-Mode Storage Management Guide*  
na_vol(1) man page | Maximum volume size determined by the type of the containing aggregate. | Admin privilege level |
| vol status | Displays state and status for the volume | *Data ONTAP 7-Mode Storage Management Guide*  
na_vol(1) man page | | Admin privilege level |
<p>| waffinity_stats | Displays waffinity statistics | | | Advanced privilege level |
| wafl | Controls the WAFL file system | na_wafl(1a) man page | | Advanced privilege level |</p>
<table>
<thead>
<tr>
<th>Command name</th>
<th>Purpose</th>
<th>More information is available in these documents:</th>
<th>Parameter changes or limitations</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>waf1_susp</td>
<td>Displays messages that WAFL has suspended</td>
<td>na_waf1_susp(1a) man page</td>
<td></td>
<td>Advanced privilege level</td>
</tr>
<tr>
<td>wrfile</td>
<td>Writes STDIN to a file</td>
<td>na_wrfile(1) man page</td>
<td></td>
<td>Admin privilege level</td>
</tr>
</tbody>
</table>

**Nodeshell volume options**

A list of volume options that are available through the nodeshell. For more information about these volume options, see the na_vol(1) man page.

**Note:** Be sure to consult the na_vol(1) options man page before using these volume options to change volume settings.

<table>
<thead>
<tr>
<th>Volume option name</th>
<th>Purpose</th>
<th>Available for root volume?</th>
<th>Available for Cluster-Mode volumes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>extent</td>
<td>Enables extents for the volume.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>fractional_reserve</td>
<td>Decreases the amount of space reserved for overwrites of reserved objects in the volume.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>fs_size_fixed</td>
<td>Causes the file system to remain the same size when a volume's SnapMirror relationship is broken or when a volume is added.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>guarantee</td>
<td>Controls whether the volume is guaranteed some amount of disk space. Settings &quot;none&quot; and &quot;volume&quot; are supported for cluster volumes.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Volume option name</td>
<td>Purpose</td>
<td>Available for root volume?</td>
<td>Available for Cluster-Mode volumes?</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>ignore_inconsistent</td>
<td>Determines whether aggregate-level inconsistencies, which would normally keep the associated volume offline, are ignored during booting.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>maxdirsize</td>
<td>Sets the maximum size (in KB) to which a directory can grow.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>maxfiles</td>
<td>Increases the number of files that a volume can hold. See the na_maxfiles(1) man page for more information.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>minra</td>
<td>Determines whether Data ONTAP uses speculative read-ahead or not.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>no_atime_update</td>
<td>Prevents the update of the access time when a file is read.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>no_delete_log</td>
<td>Enables the deletion of log files.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>no_i2p</td>
<td>Disables inode to pathname translations for the volume.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>nosnap</td>
<td>Disables automatic Snapshot copies on the volume.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>no_snapdir</td>
<td>Disables access to the .snapshot directories.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>nv_fail</td>
<td>Enables additional NVRAM checking at boot time.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Volume option name</td>
<td>Purpose</td>
<td>Available for root volume?</td>
<td>Available for Cluster-Mode volumes?</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>---------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>raidsize</td>
<td>Displays the size of raid groups for the volume's containing aggregate.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>raidtype</td>
<td>Displays the raid type for the volume's containing aggregate.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>read_realloc</td>
<td>Enables read reallocation for the volume.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>schedsnapname</td>
<td>Determines name format for scheduled Snapshot copies.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>snapmirrored</td>
<td>Control SnapMirror, an asynchronous method of mirroring volumes. See the na_snapmirror(1) man page for more information.</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>try_first</td>
<td>Determines how Data ONTAP attempts to provide more space for the volume.</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
Index

64-bit volumes
- 32-bit volumes and, moving data between 127
- 32-bit volumes, compared with 125
- interoperability with 32-bit volumes 126

A

ACP
- defined 48
- enabling 49
- subnet, about 50

adapters
- NVRAM5 107
- NVRAM6 107

aggregates
- 32-bit, 64-bit 95
- adding smaller disks to 100
- maximum per system 216
- maximum size of 216
- minimum size of 216
- mixing array LUNs in 98
- overview 95
- unmirrored, defined 96

Alternate Control Path (ACP)
- defined 48

array LUNs
- See LUNs (array)
- assigning array LUNs to a node 60
- assigning to a system 54

AT-FCX modules and Multipath Storage 121

autoassignment 56

B

BCS disks (block checksum disks) 40
block checksum type
- changing for array LUNs 63
- why change for array LUNs 63

C

changing system assignment 62
checksum type
- changing for array LUNs 63
- performance implications 63

storage capacity implications 63
- why change for array LUNs 63

checksum type rules 99

CLI
- command directories, navigating 25
- exiting 33
- keyboard shortcuts 27
- reissuing commands 27
- setting display preferences 29
- setting privilege levels 28
- specifying values 26
- using 25

commands
- availability 21
- storage alias (displays tape aliases) 200
- tape drive show (displays tape drive information) 200
- tape library show (displays tape library information) 200

D

data
- reconstruction, controlling performance impact 92

Data ONTAP, with array LUNs 85

data protection mirrors
- creating destination volume 190
- creating relationship 190
- initializing 190
- promoting a destination volume 193
- recovering source volume 193

definitions
- HA configuration 107
- degraded mode 87
- diagnostic account 22

disk
- block checksum 40
- connection types 37
- failures, reducing 46
- format 40
- ids 41
- offline temporarily 45
- ownership
  - automatically erasing 71
  - erasing manually 70
- performance monitors 44
sanitization 42
sanitization, selective 44
speed 39
types for RAID 41, 83
capacity by disk size 37
failed with available spare 88
failed with no spare 88
names 40
ownership
  about 53
  autoassignment 56
RPM 39
disk ownership
  application to array LUNs 53
  assigning an array LUN to a node 60
  ownership
    removing ownership information 66
    removing information written to an array LUN 66
disk remove -w
  removing ownership information on an array LUN 66
disks
  adding smaller to aggregate 100
direct-attached, names 40
switch-attached, names 40
display preferences
  setting in CLI 29
DS4243
  ACP protocol 48

E
environment variables
  ACL_START 205
  BASE_DATE 205
  DATA_BLOCK_SIZE 205
  DEBUG 205
  DIRECT 205
  DMP_NAME 205
  DUMP_DATE 205
  ENHANCED_DAR_ENABLED 205
  EXCLUDE 205
  EXTRACT 205
  EXTRACT_ACL 205
  FILESYSTEM 205
  FORCE 205
  HIST 205
  IGNORE_CTIME 205
  IGNORE_QTREES 205
  LEVEL 205
  LIST 205
  LIST_QTREES 205
  MULTI_SUBTREE_NAMES 205
  NDMP_UNICODE_FH 205
  NDMP_VERSION 205
  NO_ACLS 205
  NON_QUOTA_TREE 205
  NOWRITE 205
  RECOVER_FULL_PATH 205
  RECURSIVE 205
  uses 204

F
fan out limit 179
Fibre Channel Arbitrated Loop (FC-AL) 37
Fibre Channel Arbitrated Loop (FC-AL) disk connection
type 37
files
  maximum size 215
  maximum size of 215
FlexCache
  64-bit volumes and 126
FlexCache volumes
  maximum per system 215
FlexVol volumes
  maximum and minimum size 215
  maximum per system 215

H
HA configurations
  benefits of 107
  characteristics of 108
  definition of 107
hot spares
  defined 86
  appropriate 87
  best practices 86
  failed disk with available 88
  failed disk with no spare 88
  matching 87
  what disks can be used as 86

L
language setting
  between virtual servers 177
limitations
mirrors 177

links
maximum number of 215
load-sharing mirrors
aborting relationship 186
adding a mirror to the set 184
creating destination volume 182
creating relationships 183
determining if up-to-date 188
initializing relationship 184
modifying relationship 187, 192
modifying source volume 181
mounting volume for CIFS clients 181
mounting volume for NFS clients 181
promoting a destination volume 193
recovering source volume 193
showing relationship status 188
updating relationship 185

logical transfers 175
LUN (logical unit number) 199
LUNs (array)
assigning ownership 60
changing checksum type 63
checksum type of 63
Data ONTAP owning 53
Data ONTAP RAID groups with 85
managing through Data ONTAP 59
mixing in an aggregate 98
name format 59
prerequisites to changing composition 64, 65
prerequisites to changing size 64, 65
RAID groups
RAID0
RAID0 RAID group requirements 85
RAID0 RAID group requirements 85
relationship to RAID0 aggregates 85
requirements before removing a system running
Data ONTAP from service 67

M
mailbox disks 108
maintenance center
description 46
using manually 47
when disks go into 46
management interfaces
basics 25

exiting 33
explained 21
media scrub
  continuous 48
mirrors
aborting load-sharing relationship update 186
active transfer limit 178
adding to a load-sharing set 184
creating data protection destination 190
creating data protection relationship 190
creating load-sharing destination volume 182
creating load-sharing mirror relationships 183
data protection 175
deleting 193, 194
deleting Snapshot copies automatically 180
determining load-sharing up-to-date 188
fan out limit 179
initializing data protection 190
initializing load-sharing relationship 184
junction path 176
limitations 177
listing the state of a scheduled transfer 188, 191
load-sharing 175
logical transfers 175
modifying load-sharing relationship 187, 192
path name pattern matching 176
promoting a destination volume 193
recovering source volume 193
scheduling when transfers occur 186, 192
showing load-sharing relationship status 188
SnapMirror configuration limit 178
SnapMirror transfer limit 178
Snapshot copy limit 180
updating load-sharing relationship 185
where mounted 176
wildcards 176
mirrors, load-sharing
mounting volume for CIFS clients 181
mounting volume for NFS clients 181
Multipath Storage
  AT-FCX module versions supported 121

N
names
format of array LUNs 59
NDMP
  defined 202
ndmpcopy
  64-bit volumes and 126
P

path name
  abbreviating 176
  pattern matching 176
  wildcards 176
pattern matching 176
patterns
  using 31
performance
  effect of checksum type 63
persistent reservations
  releasing all 67
physical path names (PPNs)
  format 199
privilege levels
  admin 22
  advanced 22
  diagnostic 22
setting in CLI 28

Q

qtree SnapMirror
  64-bit volumes and 126
qtrees
  deletion, quotas and 152
  limits on how many you can have 140
  maximum per system 215
  renaming, quotas and 152
  volumes, compared with 140
  when to use 139
queries
  extended, using 32
  using 31
quotas
  activating, about 151
  default 150
  derived 150
  hard 151
  process 149
  qtree deletion, and 152
  qtree rename and 152
  reinitializing, about 151
  soft 151
  threshold 151
  tree 151
  why you use 149

R

RAID
  data reconstruction, controlling performance impact 92
  operations, controlling performance impact 91
  protection by third-party storage
    LUNs (array)
      RAID protection 82
  RAID0
    protection for array LUNs 82
    scrub, controlling performance impact 93
  RAID disk types 41, 83
  RAID groups
    definition 83
    naming convention 84
    size 84
    for array LUNs 82
    maximum number of 217
    sizes of 217
  RAID-DP 82
  RAID4 82
  Rapid RAID Recovery 46
  right-sizing 37
  root volume
    minimum size 218

S

scrub, controlling performance impact 93
Serial attached SCSI (SAS) 37
serial-attached SCSI (SAS) disk connection type 37
shells
  native 22
  node 22
  system 22
size
  changing array LUN size 64, 65
SnapMirror
  aborting relationship 186
  adding a mirror to the set 184
  configuration limit 178
  data protection relationship 190
  deleting a relationship 193, 194
  destination volume 190
  determining if mirrors are up-to-date 188
  fan out limit 179
  initializing data protection mirror 190
  initializing relationship 184
  listing the state of a scheduled transfer 188, 191
maximum number 178
modifying relationship 187, 192
promoting a destination volume 193
recovering source volume 193
scheduling when transfers occur 186, 192
showing relationship status 188
updating relationship 185
SnapMirror transfer limit 178
Snapshot copies
  limits on how many you can have 168
Snapshot copy
  limit on source volume 180
spare array LUNs
  changing array LUN assignment 62
  changing system assignment 62
  disk ownership 62
spare disks
  defined 86
  appropriate 87
  failed disk with available 88
  failed disk with no spare 88
  matching 87
  what disks can be used as 86
storage
  mixing array LUNs in an aggregate 98
storage (aliasing) commands
  storage alias (assigns tape alias) 201
  storage unalias (removes tape alias) 201
storage capacity
  effect of checksum type on 63
storage limits 215–218
synchronous SnapMirror
  64-bit volumes and 126
systemshell 22

T
tape aliases
definition 198
traditional volumes
  maximum per system 215
  maximum size of 215
tree quotas 151

V
virtual server
  mirror language setting 177
vol copy
  64-bit volumes and 126
volume
  type, determining 126
volume SnapMirror
  64-bit volumes and 126

W
Web interface
  accessing 29
  exiting 33
  navigating 30
when Data ONTAP can use 57
wildcards
  using 31
worldwide names (WWNs) 199

Z
zoned checksum type
  changing for array LUNs 63
  checksum type
    matching array LUN and aggregate checksum
type 63
  why change for array LUNs 63